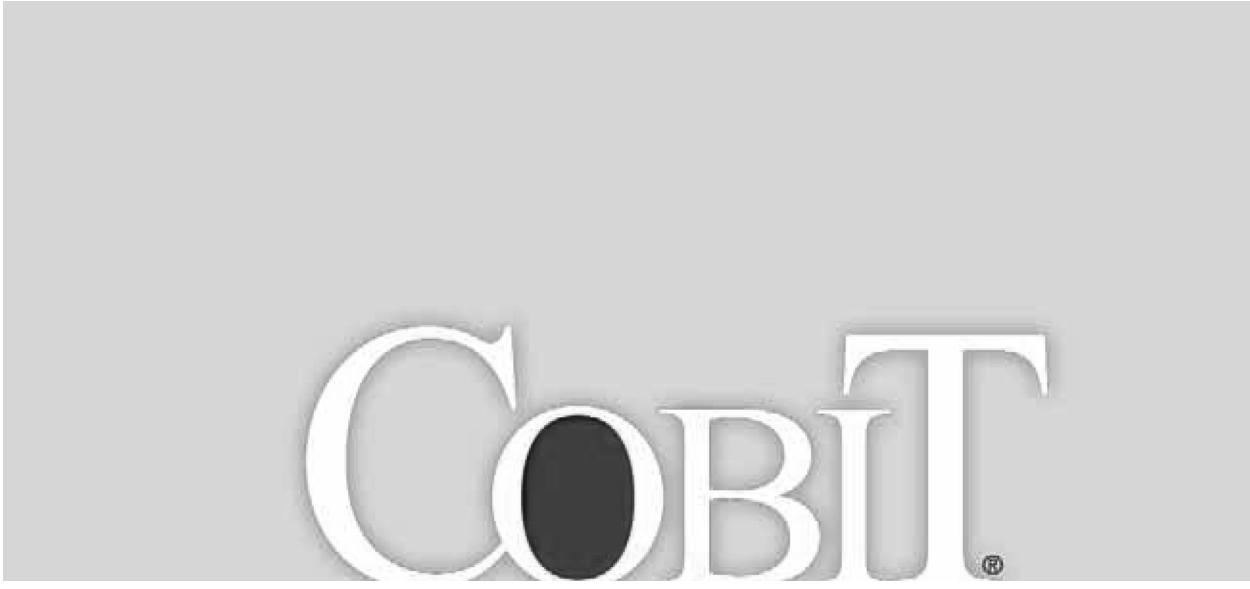
GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY



4.1

Методологія

Цілі контролю

Поради з управління

Моделі зрілості процесів

Інститут управління IT (The IT Governance Institute®)
Інститут управління інформаційними технологіями (IT Governance Institute, ITGI) (www.itgi.org) було засновано в 1998 році для обговорення на міжнародному рівні та вироблення стандартів в області управління та контролю інформаційними технологіями (IT). Ефективне управління IT сприяє досягненню цілей бізнесу, оптимізації інвестицій в IT та, відповідно, дозволяє керувати ризиками та можливостями, пов'язаними з IT. ITGI пропонує оригінальні дослідження, подані в електронному вигляді, та приклади з практики для допомоги керівництву організацій та Радам директорів у вирішенні питань області управління IT.

Заява про обмеження відповідальності
ITGI («Власник») підготував та опублікував дане видання під назвою CobiT® 4.1 («Витвір») в першу чергу як освітній посібник для директорів з інформаційних технологій, вищого керівництва, керівництва служби IT та спеціалістів в області контролів. Власник не стверджує, що використання Витвору може гарантувати отримання успішних результатів. Цей Витвір не можна розглядати як ексклюзивне джерело належної інформації, процедур, тестів; також не виключається те, що інша інформація, процедури та тести можуть зумовити отримання аналогічних результатів. У визначенні доцільності використання будь-якої інформації, процедури або тесту, директори з IT, вище керівництво, керівники служби IT та спеціалісти в області контролів повинні керуватись власним професійним міркуванням згідно з конкретними обставинами в умовах існуючих систем або середовища IT в цілому.

Disclaimer
ITGI® created CobiT® 4.1 ("Work") primarily as an educational resource for controls professionals. ITGI makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the controls professional should apply his or her own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Положення про якість
Даний документ перекладений на Українську мову Київським відділенням ISACA® з дозволу ITGI® та у відповідності з Англійським оригіналом CobiT® 4.1. За точність та достовірність перекладу відповідальність несе виключно Київське відділення ISACA®.

Quality Statement
This Work is translated into Ukrainian from the English language version of CobiT® 4.1 by the ISACA® Kyiv Chapter with the permission of the ITGI®. The ISACA® Kyiv Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

CobiT® 4.1

Подяки

IT Governance Institute висловлює подяку:

Експертам-розробникам та рецензентам

Марк Адлер (Mark Adler), CISA, CISM, CIA, CISSP, Allstate Ins. Co., США
Пітер Ендрюс (Peter Andrews),CISA, CITP, MCMI, PJA Consulting, Великобританіяя
Джорджес Атайя (Georges Ataya), CISA, CISM, CISSP, MSCS, PBA, Бізнес-Школа Solvay, Бельгія
Гарі Остін (Gary Austin), CISA, CIA, CISSP, CGFM, KPMG LLP, США
Гарі С. Бейкер (Gary S. Baker), CA, Deloitte & Touche, Канада
Девід Х. Барнетт (David H. Barnett), CISM, CISSP, Applera Corp., США
Крістін Белліно (Christine Bellino), CPA, CITP, Jefferson Wells, США
Джон В. Беверідж (John W. Beveridge), CISA, CISM, CFE, CGFM, CQA, Адміністрація державного аудитора в штаті Масачусетс, США
Алан Бордман (Alan Boardman), CISA, CISM, CA, CISSP, Fox IT, Великобританія
Девід Боневелл (David Bonewell), CISA, CISSP-ISSEP, Accomac Consulting LLC, США
Дірк Брюндонкс (Dirk Bruyndonckx), CISA, CISM, KPMG Advisory, Бельгія
Дон Канілгліа (Don Canilglia), CISA, CISM, США
ЛуісА. Капуа (Luis A. Capua), CISM, Sindicatura General de la Nacion, Аргентина
Бойд Картер (Boyd Carter), PMP, Elegantsolutions. ca, Канада
Ден Касціано (Dan Casciano), CISA, Ernst & Young LLP, США
Шон В. Кейсі (Sean V. Casey), CISA, CPA, США
Сушіл Чаттерій (Sushil Chatterji), Edutech, Сингапур
Ед Чаввенс (Ed Chavennes), Ernst & Young LLP, США
Крістіна Чен (Christina Cheng), CISA, CISSP, SSCP, Deloitte & Touche LLP, США
Дхармеш Чоксі (Dharmesh Choksey), CISA, CPA, CISSP, PMP, KPMG LLP, США
Джефрі Д. Кустер (Jeffrey D. Custer), CISA, CPA, CIA, Ernst & Young LLP, США
Беверлі Г. Девіс (Beverly G. Davis), CISA, Federal Home Loan Bank of San Francisco, США
Пітер Де Брюн (Peter De Bruyne), CISA, Banksys, Бельгія
Стівен Де Хейс (Steven De Haes), Школа менеджменту університету Антверпена, Бельгія
Пітер Де Конінк (Peter De Koninck), CISA, CFSA, CIA, SWIFT SC, Бельгія
Філіпп Де Пікер (Philip De Picker), CISA, MCA, Національний Банк Бельгії, Бельгія
Кімберлі де Вріс (Kimberly de Vries), CISA, PMP, Zurich Financial Services, США
Роджер С. Дебресені (Roger S. Debreceny), Ph. D., FCPA, Університет Гавайі, США
Зама Дламіні (Zama Dlamini), Deloitte & Touche LLP, ПАР
Руперт Доддс (Rupert Dodds), CISA, CISM, FCA, KPMG, Нова Зеландія
Трой ДюМолін (Troy DuMoulin), Pink Elephant, Канада
Білл А. Дюрран (Bill A. Durrand), CISA, CISM, CA, Ernst & Young LLP, Канада
Юстус Екейгв (Justus Ekeigwe), CISA, MBCS, Deloitte & Touche LLP, США
Рафаель Едуардо Фабіус (Rafael Eduardo Fabius), CISA, Republica AFAP S. A., Уругвай
Урс Фішер (Urs Fischer), CISA, CIA, CPA (Swiss), Swiss Life, Швейцарія Крістофер Фокс (Christopher Fox), ACA, PricewaterhouseCoopers, США Боб Фрелінгер (Bob Frelinger), CISA, Sun Microsystems Inc., США
Жівей Фу (Zhiwei Fu), Ph. D, Fannie Mae, США
Монік Гарсо (Monique Garsoux), Dexia Bank, Бельгія
Едсон Джин (Edson Gin), CISA, CFE, SSCP, США
Саувік Гхош (Sauvik Ghosh), CISA, CIA, CISSP, CPA, Ernst & Young LLP, США
Гай Гронтер (Guy Groner), CISA, CIA, CISSP, США
Ерік Гілдентопс (Erik Guldentops), CISA, CISM, Школа менеджменту університету Антверпена, Бельгія
Гарі Харді (Gary Hardy), IT Winners, ПАР
Джіммі Хешл (Jimmy Heschl), CISA, CISM, KPMG, Австрія
Бенджамін К. Хсайо (Benjamin K. Hsaio), CISA, Federal Deposit Insurance Corp., США
Том Хьюджхес (Tom Hughes), Acumen Alliance, Австралія
Моніка Джайн (Monica Jain), CSQA, Covansys Corp., US
Уейн Д. Джонс (Wayne D. Jones), CISA, Національна аудиторська служба Австралії, Австралія
Джон А. Кей (John A. Kay), CISA, США
Ліза Киньон (Lisa Kinyon), CISA, Countrywide, США
Родни Кокот (Rodney Kocot), Systems Control and Security Inc., США
Люк Кордел (Luc Kordel), CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Бельгія
Лінда Костік (Linda Kostic), CISA, CPA, США
Джон В. Лайнхарт IV (John W. Lainhart IV), CISA, CISM, IBM, США
Філіп Ле Гран (Philip Le Grand), Capita Education Services, Великобританія
Ельза К. Ли (Elsa K. Lee), CISA, CISM, CSQA, AdvanSoft International Inc., США
Кенні К. Ли (Kenny K. Lee), CISA, CISSP, Countrywide SMART Governance, США
Деббі Лью (Debbie Lew), CISA, Ernst & Young LLP, США
Дональд Лорете (Donald Lorete), CPA, Deloitte & Touche LLP, США

Едді С. П. Люі (Addie C. P. Lui), MCSA, MCSE, First Hawaiian Bank, США
Дебра Маллетте (Debra Mallette), CISA, CSSBB, Kaiser Permanente, США
Чарльз Мансур (Charles Mansour), CISA, Charles Mansour Audit & Risk Service, Великобританія
Маріо Мікалеф (Mario Micallef), CPAA, FIA, National Australia Bank Group, Австралія
Нільс Тор Миккелсен (Niels Thor Mikkelsen), CISA, CIA, Danske Bank, Данія
Джон Мітчелл (John Mitchell), CISA, CFE, CITP, FBCS, FIIA, MIIA, QiCA, LHS Business Control, Великобританія
Аніта Монтгомерии(Anita Montgomery), CISA, CIA, Countrywide, США
Карл Мюіз (Karl Muise), CISA, City National Bank, США
Джей С. Муннеллі (Jay S. Munnelly), CISA, CIA, CGFM, Federal Deposit Insurance Corp., США
Санг Нгуен (Sang Nguyen), CISA, CISSP, MCSE, Nova Southeastern University, США
Ед О'Доннелл (Ed O'Donnell), Ph. D., CPA, Університет Канзасу, США
Сью Оуен (Sue Owen), Department of Veterans Affairs, Австралія
Роберт Г. Паркер (Robert G. Parker), CISA, CA, CMC, FCA, Robert G. Parker Consulting, Канада
Роберт Пейн (Robert Payne), Trencor Services (Pty) Ltd., ПАР
Томас Фелпс IV (Thomas Phelps IV), CISA, PricewaterhouseCoopers LLP, США
Віктор Пріска (Vitor Prisca), CISM, Novabase, Португалія
Мартін Розенберг (Martin Rosenberg), Ph. D., IT Business Management, Великобританія
Клаус Розенквіст (Claus Rosenquist), CISA, TrygVesata, Данія
Джако Саді (Jaco Sadie), Sasol, ПАР
Макс Шанахан (Max Shanahan), CISA, FCPA, Max Shanahan & Associates, Австралія
Крейг В. Сільверторн (Craig W. Silverthorne), CISA, CISM, CPA, IBM Business Consulting Services, США
Чад Сміт (Chad Smith), Great-West Life, Канада
Роджер Саутгейт (Roger Southgate), CISA, CISM, FCCA, CubeIT Management Ltd., Великобританія
Паула Спіннер (Paula Spinner), CSC, США
Марк Стенлі (Mark Stanley), CISA, Toyota Financial Services, США
Дірк Е. Стюперер (Dirk E. Steuperaert), CISA, PricewaterhouseCoopers, Бельгія
Роберт Е. Страуд (Robert E. Stroud), CA Inc., США
Скотт Л. Саммерс (Scott L. Summers), Ph. D., Brigham Young University, США
Ленс М. Туркато (Lance M. Turcato), CISA, CISM, CPA, City of Phoenix IT Audit Division, США
Вім Ван Гремберген (Wim Van Grembergen), Ph. D., Школа менеджменту університету Антверпена, Бельгія
Джоан Ван Грікен (Johan Van Grieken), CISA, Deloitte, Бельгія
Грит Волдерс (Greet Volders), Voquals NV, Бельгія
Томас М. Вагнер (Thomas M. Wagner), Gartner Inc., США
Роберт М. Уолтерс (Robert M. Walters), CISA, CPA, CGA, Offce of the Comptroller General, Канада
Фредді Вітхегельс (Freddy Withagels), CISA, Capgemini, Бельгія
Том Вонг (Tom Wong), CISA, CIA, CMA, Ernst & Young LLP, Канада
Аманда Ксю (Amanda Xu), CISA, PMP, KPMG LLP, США

Опікунській раді ITGI
Еверетт С. Джонсон (Everett C. Johnson), CPA, Deloitte & Touche LLP (в отставке), США, Міжнародний президент
Джорджес Атайя (Georges Ataya), CISA, CISM, CISSP, Бізнес школа Solvay, Бельгія, Віце-президент
Вільям С. Боні (William C. Boni), CISM, Motorola, США, Віце-президент
Авінаш Кадам (Avinash Kadam), CISA, CISM, CISSP, CBCP, GSEC, GCIH, Miel e-Security Pvt. Ltd., Індія, Віце-президент
Жан-Луї Ленель (Jean-Louis Leignel), MAGE Conseil, Франція, Віце-президент
Лусіо Аугусто Моліна Фокаццио (Lucio Augusto Molina Focazzio), CISA, Колумбія, Віце-президент
Говард Ніколсон(Howard Nicholson), CISA, город Солсбери, Австралія, Віце-президент
Френк Ям (Frank Yam), CISA, FHKIoD, FHKCS, FFA, CIA, CFE, CCP, CFSA, Focus Strategic Group, Гонконг, Віце-президент
Маріос Дамініадес (Marios Damianides), CISA, CISM, CA, CPA, Ernst & Young LLP, США, Міжнародний президент (у відставці)
Роберт С. Руссі (Robert S. Roussey), CPA, University of Southern California, США, Міжнародний президент (у відставці)
Рональд Саулл (Ronald Saull), CSP, Great-West Life and IGM Financial, Канада, член правління

Комітету з управління IT
Тоні Хэйс (Tony Hayes), FCPA, Queensland Government, Австралія, Председатель
Макс Блічер (Max Blecher), Virtual Alliance,ПАР
Сушіл Чаттерий (Sushil Chatterji), Edutech, Сінгапур
Анід Йогані (Anil Jogani), CISA, FCA, Tally Solutions Limited, Великобританія
Джон В. Лайнхарт IV (John W. Lainhart IV), CISA, CISM, IBM, США
Румило Ломпарте (Rymulo Lomparte), CISA, Banco de Credito BCP, Перу
Майкл Шірмбранд (Michael Schirmbrand), Ph. D., CISA, CISM, CPA, KPMG LLP, Австрія
Рональд Саул (Ronald Saull), CSP, Great-West Life Assurance and IGM Financial, Канада

Керуючому комітету CobiT®
Роджер С. Дебресені (Roger Debreceny), Ph. D., FCPA, Університет Гавайі, США, Голова
Гарі С. Бейкер (Gary S. Baker), CA, Deloitte & Touche, Канада

Ден Касціано (Dan Casciano), CISA, Ernst & Young LLP, США
Стівен Де Хейс (Steven De Haes), Школа менеджменту університету Антверпена, Бельгія
Пітер Де Конінк (Peter De Koninck), CISA, CFSA, CIA, SWIFT SC, Бельгія
Рафаель Едуардо Фабіус (Rafael Eduardo Fabius), CISA, Republica AFAP S. A., Уругвай
Урс Фишер (Urs Fischer), CISA, CIA, CPA (Swiss), Swiss Life, Швейцарія
Ерік Гілдентопс (Erik Guldentops), CISA, CISM, Школа менеджменту університету Антверпена, Бельгія
Гарі Харді (Gary Hardy), IT Winners, ПАР
Джіммі Хешл (Jimmy Heschl), CISA, CISM, KPMG, Австрія
Деббі А. Льюі(Debbie A. Lew), CISA, Ernst & Young LLP, США
Максвелл Дж. Шанахан (Max Shanahan), CISA, FCPA, Max Shanahan & Associates, Австралія
Дірк Стюперер (Dirk E. Steuperaert), CISA, PricewaterhouseCoopers, Бельгія
Роберт Е. Страуд (Robert E. Stroud), CA Inc., США

Дорадчій групі ITGI
Рональд Саул (Ronald Saull), CSP, Great-West Life Assurance and IGM Financial, Канада, член правління
Роланд Бадер (Roland Bader), F. Hoffmann-La Roche AG, Швейцарія
Лінда Бетц (Linda Betz), IBM Corporation, США
Жан-Пьер Корнью (Jean-Pierre Corniou), Renault, Франція
Роб Клайд (Rob Clyde), CISM, Symantec, США
Річард Грангер (Richard Granger), NHS Connecting for Health, Великобританія
Говард Шмідт (Howard Schmidt), CISM, R&H Security Consulting LLC, США
Алекс Сіу Єн Хонг (Alex Siow Yuen Khong), StarHub Ltd., Сингапур
Аміт Йоран (Amit Yoran), Yoran Associates, США

Афіліатам та спонсорам ITGI
Відділенням ISACA
Американський інститут присяжних бухгалтерів (American Institute for Certified Public Accountants)
ASIS International
Центр безпеки Іентернет (The Center for Internet Security)
Асоціація Спільноти з корпоративного управління (Commonwealth Association of Corporate Governance)
FIDA Inform
Форум інформаційної безпеки (Information Security Forum)
Асоціація безпеки інформаційних систем (The Information Systems Security Association)
Інститут управління інформаційними системами (Institut de la Gouvernance des Systemes d'Information)
Інститут управлінських бухгалтерів (Institute of Management Accountants)
ISACA
ITGI Japan
Бізнес – школа Solvay
Школа менеджменту університету Антверпена
Aldion Consulting Pte. Lte.
CA
Hewlett-Packard
IBM
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

Підтримка вичитки українського перекладу
Олексій Янковський (PwC)
Ірина Івченко (SICenter)
Сергій Іванішин (Національний Банк України)
Андрій Третяк (PwC)
Гліб Пахаренко (East One)
Валентин Сисоєв (Агенство Активного Аудиту)
Андрій Рибальченко (East One)
Андрій Лисюк (Ernst & Young)
Генадій Чуприков (PwC)
Лілія Набоченко (PwC)

Спонсор підготовки українського перекладу до публікації
PwC Україна

Зміст

Просимо надавати ваші коментарі та пропозиції стосовно СовіТ® 4.1.
Відвідайте сайт *www.isaca.org/cobitfeedback*, де ви можете залишати свій коментар.

Огляд для керівництва

Огляд для керівництва

Для багатьох організацій інформація та технології, що їх підтримують, є найбільш цінними, хоча часто найменш зрозумілими активами. Успішні організації визнають переваги використання інформаційних технологій та застосовують їх для підвищення цінності для акціонерів. Ці організації також усвідомлюють ризики, пов'язані із використанням IT, включаючи необхідність дотримання регулятивних вимог та критичну залежність багатьох бізнес-процесів від інформаційних технологій (IT), та управляють ними цими ризиками.

Потреба у забезпечення впевненості щодо корисності, яку надають IT, управління ризиками пов'язаними з IT та зростаючі вимоги до контролю над інформацією на сьогоднішній день визнаються ключовими елементами корпоративного управління. Забезпечення цінності IT, управління ризиками та контролями, пов'язаними із застосуванням IT являють собою суть управління у сфері IT.

Управління IT – це відповідальність вищого керівництва та Ради директорів, яке складається з лідерства, організаційних структур та процесів, що забезпечують відповідність IT, що використовуються, поточним потребам та стратегічним цілям організації.

Крім того, управління IT запроваджує та застосовує найкращі практики, які гарантують адекватну підтримку бізнес-цілей організації з боку IT. Управління IT дозволяє організації в повній мірі використовувати переваги, пов'язані з інформацією, тим самим отримуючи максимум вигод, та підвищуючи власну конкурентоспроможність. Досягти подібних результатів можна за умови застосування такої методології контролю IT, яка відповідає вимогам документу Комітету спонсорських організацій Комісії Тредуея (COSO) *«Внутрішній контроль – інтегрована методологія»*, що отримав широке визнання як методологія контролю в області корпоративного управління та управління ризиками, або іншої визнаної методології.

Організації повинні відповідати вимогам якості, контрольованості та конфіденційності власної інформації, як в всіх інших активів. Керівництво повинно оптимізувати користування доступними IT ресурсами, які включають прикладні програмні продукти, інформацію, інфраструктуру та персонал. Щоб виконувати ці обов'язки, а також досягти поставлених цілей, вище керівництво повинно розуміти статус корпоративної IT архітектури та визначити, які методи управління та контролю слід використовувати.

У виданні *«Цілі контролю для інформаційних та суміжних технологій»* (СовіТ®) надано хороші практики управління та контролю IT, згруповані у домени (групи IT процесів) та окремі процеси. Ці хороші практики представляють собою сукупність дій, викладених у вигляді керованої та логічної структури. Передові практики, викладені в СовіТ®, являють собою узгоджене бачення багатьох експертів, які приймали участь у розробці цієї методології. Ці практики є в більшій мірі орієнтованими на забезпечення контролю, і в меншій мірі на деталі виконання IT-процесів. Ці практики допоможуть оптимізувати інвестиції, пов'язані з IT, забезпечити достатній рівень надання послуг, та виробити показники успішності виконання IT-процесів.

В сфері IT успішне надання сервісів відповідно до вимог бізнесу, потребує від керівництва налагодження системи внутрішнього контролю. СовіТ® відповідає цим потребам, оскільки:
- Пов'язує IT з вимогами бізнесу.
- Організує види IT діяльності у вигляді зрозумілої моделі процесів.
- Визначає основні ресурси IT, які потрібно ефективно використовувати.
- Визначає цілі контролю, які можна запроваджувати.

Бізнес-орієнтація СовіТ® передбачає встановлення відповідності між цілями бізнесу та цілями IT, надає метрики та моделі зрілості, та встановлює відповідальність власників бізнес- та IT-процесів.

Процесний підхід СовіТ® визначено за допомогою моделі, в якій IT поділено на чотири домени та 34 процеси згідно з сферами відповідальності в сфері планування, впровадження, підтримки, та контролю, при цьому забезпечується комплексне бачення IT в цілому. Концепція корпоративної архітектури допомагає визначити ресурси, необхідні для успішної реалізації процесів, тобто прикладні програми, інформацію, інфраструктуру та персонал.

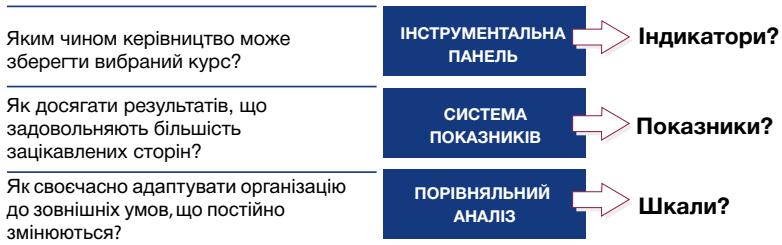
Підсумовуючи, для того, щоб забезпечити організацію інформацією, необхідною для досягнення певних бізнес-цілей, потрібно управляти ресурсами IT за допомогою сукупності процесів, об'єднаних у логічні групи.

Але яким чином організація може контролювати IT в такий спосіб, щоб отримувати інформацію, необхідну для досягнення своїх корпоративних цілей? Як управляти ризиками та забезпечувати безпеку тих IT ресурсів, від яких ця організація так сильно залежить? Як організація може бути певна в тому, що IT реалізує поставлені цілі та підтримує розвиток бізнесу?

В першу чергу керівництво повинно визначити цілі контролю, які, в свою чергу, визначають кінцеву мету впровадження політик, планів та процедур, а також організаційних структур, необхідних для забезпечення прийнятного рівня впевненості що:

- бізнес-цілі будуть досягнуті
- небажані події буде попереджено або виявлено, а їх наслідки ліквідовано

Малюнок 1. Питання керівництва



По-друге, в складних сучасних умовах керівництво постійно знаходиться в пошуку інформації для швидкого та успішного прийняття рішень стосовно цінності активів, ризиків та контролів. Що потрібно вимірювати та яким чином? Організації мають потребу в об'єктивних критеріях оцінки свого поточного стану та тих вдосконалень, яких вони потребують, а також в інструменті, за допомогою якого керівництво могло б оцінити ці вдосконалення. На **малюнку 1** показані деякі з традиційних запитань а також управлінський інструментарій, призначений для пошуку відповіді на ці запитання, однак, інструментальні панелі потребують індикаторів, системи показників – власне показників, а порівняльний аналіз – шкали порівняння.

Відповіддю на ці вимоги щодо визначення та моніторингу рівня контрольованості та ефективності в сфері IT є подані нижче визначення, які дає CobiT®:

- **Порівняльний аналіз (Benchmarking)** – Систематизований підхід до порівняння результатів діяльності організації з результатами діяльності схожих організацій та конкурентів, з метою вдосконалення діяльності організації (наприклад, порівняльний аналіз зрілості процесів розробки програмного забезпечення, у відповідності до моделі зрілості процесів, створеної Інститутом програмної інженерії (Software Engineering Institute (SEI)).
- **Цілі та метрики IT процесів** – необхідні для визначення та оцінки їх результатів та ефективності, що ґрунтуються на принципах системи збалансованих бізнес-показників, запропонованої Робертом Капланом та Девідом Нортоном.
- **Дії** – направлені на безпосереднє управління IT процесами, що ґрунтуються на цілях контролю CobiT®.

Оцінка потужності процесу на основі моделей зрілості CobiT® є ключовою складовою впровадження IT-управління. Після ідентифікації критичних IT-процесів і контролів, моделювання зрілості дозволяє ідентифікувати та представити керівництву організації виявлені розбіжності.

Малюнок 2. Області уваги IT-управління

- **Узгодженість зі стратегією** робить акцент на зв'язку між вимогами бізнесу та ленні планами IT, оцінюванні корисності IT; а також на встановленні відповідності між діяльністю IT та бізнесу.
- **Забезпечення цінності** являє собою реалізацію такий плану розвитку IT в такий спосіб, який гарантує те, що IT забезпечують обіцяні вигоди відповідно до бізнес-стратегії, при цьому акцент робиться на оптимізації витрат та доведенні внутрішньої цінності IT.
- **Управління ресурсами** присвячене питанням, пов'язаним з управлінням критичними IT ресурсами, а саме оптимізації інвестицій та належному управлінню прикладними системами, інформацією, інфраструктурою та персоналом. Ключові питання стосуються оптимізації знань та інфраструктури.
- **Управління ризиками** потребує обізнаності вищого керівництва в області ризиків, чіткого розуміння схильності організації до ризиків, розуміння необхідності дотримання існуючих вимог, прозорості по відношенню до суттєвих ризиків, до яких схильна організація, та впровадження системи управління ризиками.
- **Оцінка ефективності** представляє собою контроль реалізації стратегії, виконання проектів, використання ресурсів, ефективності процесів та надання послуг. Для цього застосовуються, зокрема, системи збалансованих показників, які перетворюють стратегію в послідовність дій, результати яких вимірюються методами, відмінними від традиційних методів бухгалтерського обліку.

На основі цього можуть бути розроблені плани дій спрямовані на забезпечення переведення даних процесів на необхідний рівень потужності. Таким чином CobiT® підтримує модель IT-управління (**малюнок 2**) спрямовану на такі задачі:

- Привести IT у відповідність до потреб бізнесу.
- IT допомагали бізнесу та максимізували переваги.
- IT ресурси використовувались відповідально.
- Здійснювалось належне управління IT ризиками.

Оцінка ефективності є ключовою складовою IT-управління. Оцінка ефективності розглядається в CobiT® та передбачає постановку та контроль цілей (досягнення яких підлягає оцінці), які визначають результативність IT процесів та шлях досягнення цих результатів (потенціал процесу та його ефективність). В ході багатьох досліджень було встановлено, що недостатня прозорість витрат на IT, недостатнє розуміння користі від цих витрат, та ризиків, пов'язаних з ними, є основними стимулами вдосконалення IT-управління.

Ці області управління IT характеризують коло питань, з якими доводиться мати справу вищому керівництву, щоб управляти інформаційними технологіями в своїх організаціях. Методологія CobiT® пропонує загальну модель процесів, яка представляє всі процеси, які зазвичай наявні в IT-організації, що робить цю базову модель зрозумілою для IT-персоналу та бізнес-керівництва. Модель процесів CobiT® співвіднесено з моделлю COSO та іншими стандартами (дивись Додаток II). Це забезпечує зв'язок між обов'язками операційного персоналу та тим, що бажає контролювати керівництво.

Для досягнення ефективного управління керівництво вимагає від операційного персоналу, щоб заходи контролю було вжито згідно з певною методологією для всіх IT процесів. Цілі контролю, які пропонує CobiT®, організовані за окремими IT процесами; тому методологія забезпечує зрозумілий зв'язок між вимогами, що пред'являються до управління IT, IT-процесами та засобами контролю IT.

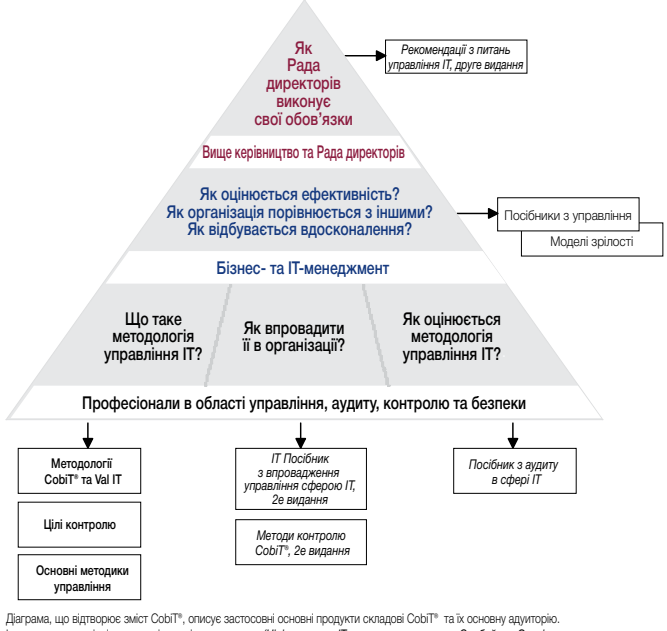
В CobiT® робиться акцент на тому, що потрібно для реалізації належного управління та контролю в сфері IT на високому рівні. CobiT® було співвіднесено та гармонізовано відносно інших, більш детальних стандартів в області IT та передових практик. Методологія CobiT® діє як інтегратор всіх цих різноманітних методологій та стандартів, підсумовуючи ключові цілі в межах єдиної методології, яка, в свою чергу пов'язана з вимогами корпоративного управління та бізнесу.

COSO (та подібні сумісні методології) звичайно використовуються як методології внутрішнього контролю в організаціях. CobiT®, як правило, є методологією внутрішнього контролю в сфері IT.

Продукти CobiT® мають трирівневу організацію (дивись **малюнок 3**) та призначені для підтримки:
- Вищого керівництва та Ради директорів.
- Бізнес- та IT- менеджмента.
- Професіоналів в області управління, аудита, контролю та безпеки.

Отже, до складу CobiT® входять:
- *Брифінг з питань управління IT для Ради Директорів, друге видання (Board Briefing on IT Governance, 2nd Edition)*. Цей документ допомагає вищому керівництву усвідомити, чому важливо управляти IT, що саме має стосунок до управління IT та в чому полягають обов'язки вищого керівництва щодо управління IT.
- Порадники з управління/моделі зрілості. Допомагають визначити обов'язки, оцінити ефективність виконати порівняльний аналіз та ідентифікувати втрачені можливості.
- Методологія. Організує цілі управління IT та передові методи згідно з доменами та процесами, а також пов'язує їх з вимогами бізнесу.
- Цілі контролю. Пропонують повний набір вимог високого рівня на розгляд менеджменту для ефективного контролю кожного IT процесу.
- *Посібник з впровадження управління сферою IT: Застосування CobiT® та Val IT™, друге видання (IT Governance Implementation Guide: Using CobiT® and Val IT™, 2nd Edition)*. Забезпечує загальну послідовність дій при впровадженні управління IT з використанням ресурсів CobiT® та Val IT™.
- *Методи контролю CobiT®: Посібник з питань досягнення цілей контролю для успішного управління сферою IT, друге видання (CobiT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition)*.Пояснює, чому слід реалізувати заходи контролю на практиці та як це зробити.
- *Посібник із забезпечення надійності в сфері IT: застосування CobiT® (IT Assurance Guide: Using CobiT®)*. Забезпечує інструкції стосовно того, як CobiT® можна

Малюнок 3. Діаграма змісту CobiT®

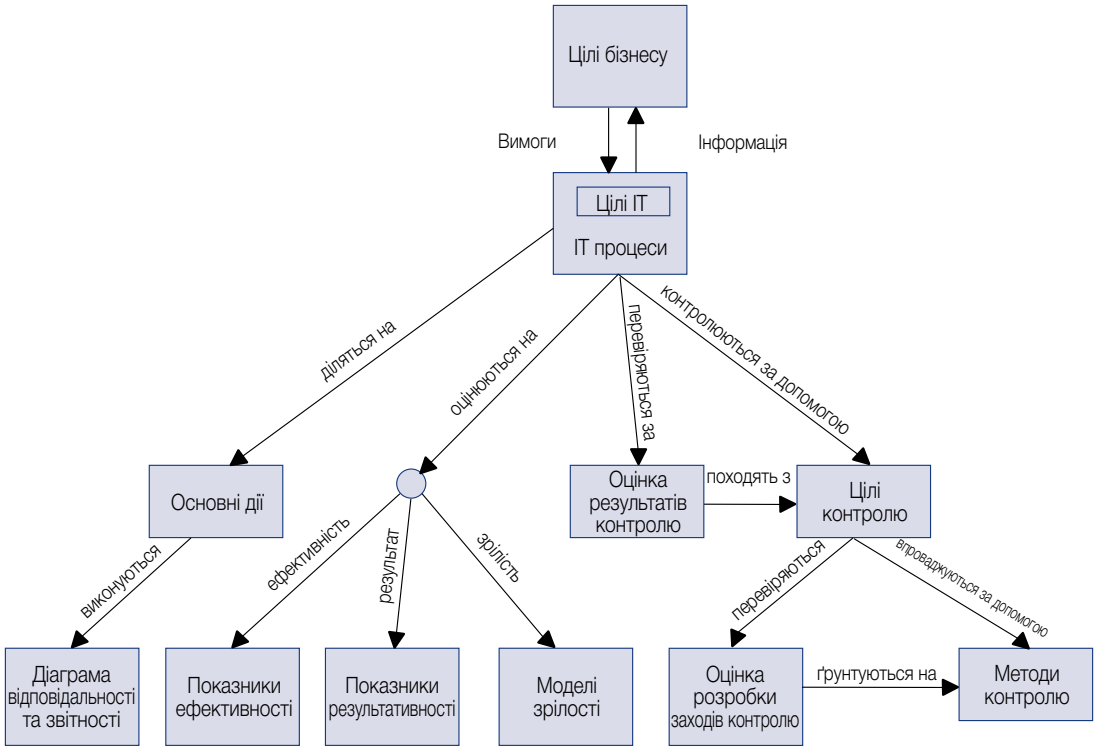


Діаграма, що відтворює зміст CobiT®, описує застосовні основні продукти складові CobiT® та їх основну адуиторію. Існують також похідні продукти із спеціальних питань *(Цілі контролю IT з врахуванням закону Сарбейнса-Оксли (IT Control Objectives for Sarbanes-Oxley, 2nd Edition)*, для таких розділів як безпека (CobiT® *Основні принципи безпеки. CobiT® Security Baseline* а також *Управління інформаційною безпекою: Посібник для Рад директорів та керуючих. Information Security Governance: Guidance for Boards of Directors and Executive Management*), або для специфічних організацій (Короткий посібник CobiT® для малих та середніх організацій, або для великих організацій, що бажають активізувати впровадження управління IT. CobiT® *Quickstart* for small and medium-sized enterprises or for large enterprises wishing to ramp up to a more extensive IT governance implementation).

використати для забезпечення надійності із застосуванням запропонованих процедур тестування для всіх IT процесів та цілей контролю.

Діаграма публікацій CobiT®, представлена на **малюнку 3**, відображає основні види аудиторії, їх проблеми в управлінні IT та продукти, які можуть дати відповідь на поставлені запитання. Також на малюнку представлено похідні роботи із специфічних питань, зокрема, з питань безпеки, або для особливих організацій.

Малюнок 4. Взаємозв'язок компонент CobiT®



Всі компоненти CobiT® взаємно пов'язані, надають підтримку в здійсненні управління, контролю та аудиту, як показано на **малюнку 4**.

CobiT® є методологією та інструментарієм, який дозволяє керівникам усунути недоліки з врахуванням вимог контролю, технічних питань та бізнес-ризиків, а також донести рівень контролю до відома зацікавлених сторін. CobiT® дає змогу розробляти чіткі політики та передові методи контролю IT в організаціях. CobiT® постійно вдосконалюється та гармонізується з іншими стандартами та інструкціями. В результаті стандарт CobiT® став інтегратором передових методів управління IT та являє собою основну методологію IT управління, яка сприяє розумінню та здійсненню управління ризиками та перевагами, пов'язаними із застосуванням IT.

Структура CobiT®, орієнтована на процеси, та викладений в ньому підхід високого рівня, орієнтований на досягнення бізнес-цілей, забезпечують комплексне бачення сфери IT та рішень, які необхідно приймати стосовно IT.

Перевагами впровадження стандарту CobiT® в якості методології управління IT є:
- Зрозуміле для керівництва бачення того, що саме являють собою IT.
- Чіткість в питаннях розподілу власності та відповідальності згідно з процесами.
- Загальна прийнятність з боку третіх сторін та регулятивних органів.
- Прийняття методології всіма зацікавленими сторонами завдяки тому, що вона викладена зрозумілою мовою.
- Виконання вимог COSO щодо контрольного середовища в сфері IT.

Решта цього документу є описом методології CobiT® та всіх основних складових частин CobiT®, які об'єднано в чотири групи (IT домени) та розділено на 34 IT процеси. Разом з кількома додатками цей документ являє собою зручний посібник з усіх основних рекомендацій CobiT®.

Найбільш повну та оновлену інформацію стосовно стандарту CobiT® та супутніх та споріднених матеріалів, в тому числі інтерактивні засоби, інструкції з впровадження, конкретні приклади з практики, інформаційні бюлетені та навчальні матеріали можна знайти на сайті *www.isaca.org/cobit*.

Методологія CobiT®

МЕТОДОЛОГІЯ СОВІТ®

CobiT®:
Дослідження, розробка та пропаганда сучасної, прийнятної в міжнародному масштабі методології управління IT з метою її впровадження організаціями та повсякденного використання керівниками організацій, спеціалістами з IT та аудиторами.

ПОТРЕБА У ВПРОВАДЖЕННІ СИСТЕМИ КОНТРОЛЮ ДЛЯ IT-УПРАВЛІННЯ

В системі контролю, призначеній для управління IT, визначено необхідність зрілого IT-управління, зацікавлених в цьому сторін та завдання, як необхідно виконувати.

Чому?

Вище керівництво усвідомлює зростаюче значення впливу інформації на досягнення успіху організацією. Керівництво бажає зрозуміти, як саме потрібно управляти IT та ефективно їх використовувати, щоб отримати переваги, які забезпечать організації конкурентоздатність. Зокрема, вищому керівництву необхідно знати, чи здійснює організація управління IT таким чином, що вона:

- зможе досягти своїх цілей
- має достатню гнучкість для того, щоб засвоювати уроки та адаптуватись у разі необхідності
- у розумний спосіб керує ризиками
- визнає перспективи та використовує їх

Успішні організації усвідомлюють ризики, які їм загрожують, використовують переваги IT та відшукують шляхи для того, щоб:

- узгодити IT стратегію із бізнес-стратегією
- переконати інвесторів та зацікавлені сторони в тому, що організація дотримується кращих практик в тому, що стосується управління IT ризиками
- донести стратегію та цілі у сфері IT всім співробітникам організації
- отримати бажаний результат від інвестицій в IT
- створити організаційні структури, які б сприяли реалізації стратегії та цілей
- побудувати конструктивні стосунки та ефективну систему комунікацій між бізнесом та IT, а також із зовнішніми партнерами
- забезпечити вимірювання ефективності IT

Організації не можуть ефективно забезпечити відповідність вимогам, що диктуються бізнесом та корпоративним управлінням, якщо вони не приймуть та не запровадять систему заходів управління та контролю інформаційних технологій з метою:

- забезпечення відповідності бізнес-вимогами
- забезпечення прозорості дотримання вказаних вимог
- організації власної діяльності згідно із загальноприйнятою моделлю процесів
- визначення основних ресурсів, які потрібно ефективно використати
- окреслення цілей контролю, які керівництво повинно взяти до уваги

Більш того, впровадження систем управління та контролю стає частиною належної практики для IT-організацій, завдяки чому забезпечується ефективне управління IT та дотримання постійно зростаючих вимог регулятивних органів.

Належні практики у сфері IT набули важливого значення завдяки представленим нижче чинникам:

- Вимоги бізнес-менеджерів та Рад директорів стосовно більшої віддачі від інвестицій в IT, тобто IT повинні відповідати потребам бізнесу, щоб забезпечити підвищення цінності активів
- Занепокоєність відносно загального зростання рівня витрат на IT
- Необхідність дотримання регулятивних вимог в області контролю IT в таких сферах, як конфіденційність та фінансова звітність (наприклад, закону Сарбейнса-Окслі (Sarbanes-Oxley Act), Basel II), та в таких специфічних галузях як фінанси, фармацевтична промисловість та охорона здоров'я
- Вибір сервіс-провайдерів та керування процедурою залучення сторонніх постачальників послуг та їх придбання
- Виникнення зростаючих комплексних ризиків, пов'язаних із застосуванням IT, таких як ризики мережевої безпеки
- Необхідність оптимізації витрат із застосуванням наскільки це можливо, стандартизованих, а не спеціально розроблених підходів
- Підвищення ступеню розвиненості та послідовне прийняття таких методологій, як стандарт СовіТ®, «Бібліотека інфраструктури IT» (IT Infrastructure Library (ITIL)), серії стандартів, що стосуються інформаційної безпеки ISO 27000, стандарту ISO 9001:2000 *«Системи управління якістю – Вимоги» (Quality Management Systems—Requirements)*, моделі

Capability Maturity Model® Integration (CMMI), документу «Проекти в контрольованих середовищах 2» (Projects in Controlled Environments 2 (PRINCE2)) та *«Посібник з питань управління проектами компаній на основі стандарту PMBOK» (A Guide to the Project Management Body of Knowledge (PMBOK))*.
- Необхідність здійснення організаціями оцінки результатів своєї діяльності на основі порівняння із загальноприйнятими стандартами та результатами діяльності аналогічних компаній (порівняльний аналіз).

Хто?

Система заходів управління та контролю повинна стати в нагоді різноманітним внутрішнім та зовнішні зацікавленим сторонам, кожна з яких має свої конкретні потреби:
- Зацікавлені сторони в межах організації, які бажають отримати переваги від інвестицій в IT:
  - Такі, що приймають рішення щодо інвестицій
  - Такі, що приймають рішення щодо відповідних вимог
  - Такі, що користуються IT
- Внутрішні та зовнішні зацікавлені сторони, які надають послуги із застосуванням IT:
  - Такі, що керують організацією IT та відповідними процесами
  - Такі, що створюють потенціал IT
  - Такі, що надають та використовують IT послуги
- Внутрішні та зовнішні зацікавлені сторони, які виконують функції контролю та управління ризиками:
  - Такі, що несуть відповідальність в частині забезпечення конфіденційності, та/або управління ризиками
  - Такі, що відповідають за дотримання існуючих вимог
  - Такі, що потребують або надають послуги страхування

Що?

Щоб задовольнити вимоги, викладені в попередньому розділі, методологія управління та контролю IT повинна:
- бути зосередженою на узгодженні бізнес-цілей з цілями IT
- забезпечити таку організацію процесів з метою визначення масштабу та ступеню охоплення, яка, за рахунок чіткої структури, давала б змогу вільно орієнтуватись у її змісті
- бути загальноприйнятною завдяки відповідності прийнятим в сфері IT передовим практикам та стандартам, а також незалежності від конкретних технологій
- використовувати універсальну мову на базі термінів та визначень, зрозумілих для всіх зацікавлених сторін
- сприяти дотриманню регулятивних вимог завдяки своїй відповідності загальноприйнятим стандартам корпоративного управління (наприклад, запровадженим Комісією COSO) та очікуванням регулятивних органів та зовнішніх аудиторів, які вони покладають на систему заходів контролю.

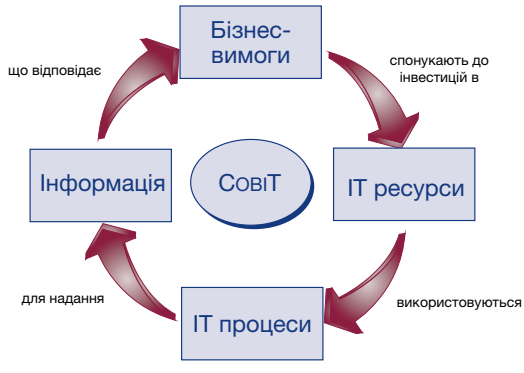
ЯКИМ ЧИНОМ СТАНДАРТ CobiT® ЗАДОВОЛЬНЯЄ ВКАЗАНІ ПОТРЕБИ

Щоб забезпечити задоволення вказаних вище потреб, методологію CobiT® було створено з врахуванням потреб бізнесу, на базі процесів, системи контролю та з можливістю оцінювання результатів діяльності.

Орієнтація на потреби бізнесу

Орієнтація на потреби бізнесу є головною метою стандарту CobiT®. Його розроблено не тільки заради використання сервіс-провайдерами IT послуг, їх користувачами та аудиторами, але й, що більш важливо, з метою надання універсального посібника для керівництва та власників бізнес-процесів.

Малюнок 5. Основні принципи CobiT®



В основі методології CobiT® лежить принцип, описаний нижче(**малюнок 5**, Основний принцип CobiT®):

Забезпечити інформацію, якої потребує організація для досягнення своїх цілей, у яку організація повинна робити інвестиції та надати можливість управління та контролю IT ресурсів з використанням структурованої сукупності процесів, що забезпечують необхідну організації інформацію.

Управління та контроль інформації є основою методології CobiT® та спрямовані на забезпечення відповідності вимогам бізнесу.

ІНФОРМАЦІЙНІ КРИТЕРІЇ СТАНДАРТУ CobiT®

Щоб задовольнити потреби бізнесу, інформація повинна відповідати певним критеріям контролю, які згадуються у стандарті CobiT®, як бізнес-вимоги до інформації. На основі більш широких вимог до якості, достовірності та безпеки було визначено сім окремих, інформаційних критеріїв, які можуть перетинатися:

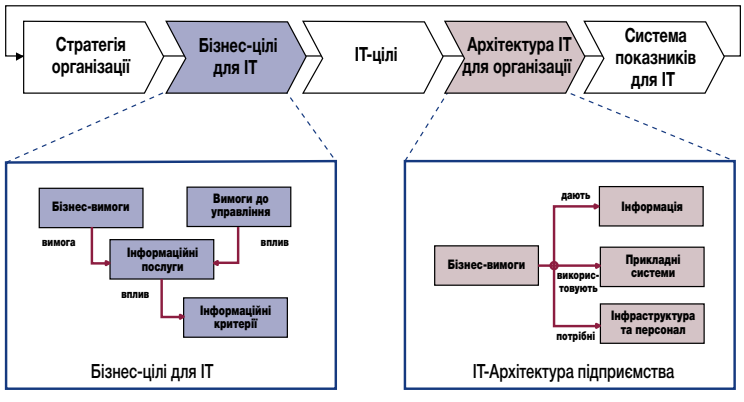
- **Ефективність** означає відповідність та релевантність інформації бізнес-процесам, а також її своєчасне надання у коректній, послідовній та придатній для використання формі.
- **Продуктивність** означає надання інформації з використанням ресурсів в оптимальний (максимально продуктивний та економічно вигідний) спосіб.
- **Конфіденційність** стосується забезпечення захисту секретної інформації від несанкціонованого розголошення.
- **Цілісність** стосується достовірності та повноти інформації, а також її корисності з точки зору цінності та очікувань бізнесу.
- **Доступність** передбачає наявність інформації в той момент, коли цього потребує бізнес-процес в поточний момент часу та в майбутньому. Це також передбачає захист необхідних ресурсів та пов'язаних з ними можливостей.
- **Відповідність** означає дотримання діючого законодавства, нормативно-правових актів та зобов'язань за контрактами, які мають стосунок до даного бізнес-процесу, тобто дотримання зовнішніх бізнес-критеріїв та внутрішніх політик.
- **Надійність** означає надання належної інформації керівництву, необхідної для керування організацією та виконання ним зобов'язань як довірених осіб та управлінців.

БІЗНЕС-ЦІЛІ ТА IT ЦІЛІ

Тоді як інформаційні критерії відображають загальний підхід до визначення бізнес-вимог, впровадження сукупності загальних бізнес-цілей та IT цілей являє собою більше пов'язаний з потребами бізнесу та більш чіткий базис для визначення бізнес-вимог та розробки системи показників, які дозволяють оцінювати відповідність результатів поставленим цілям. Кожна організація використовує IT для реалізації бізнес-проектів, що можна вважати постановкою бізнес-цілей для IT. В Додатку I представлено таблицю відповідності загальних бізнес-цілей та IT цілей та показано, як вони співвідносяться з інформаційними критеріями. Наведені приклади можна використовувати як орієнтир у визначенні конкретних бізнес-вимог, цілей та системи показників оцінювання результатів діяльності організації.

Для успішного функціонування IT на підтримку стратегії організації повинні існувати чітка приналежність та спрямування вимог підприємством (замовником) та глибоке розуміння того, які саме потреби повинні вдовольнити IT та в який спосіб (провайдер IT-послуг). На **малюнку 6** показано, як слід перетворити стратегію організації в цілі, пов'язані

Малюнок 6. Визначення IT цілей та архітектури IT в організації



з можливостями, які забезпечуються застосуванням IT (бізнес-цілі для IT). Вказані цілі повинні стати основою для визначення власних цілей IT (IT-цілі), згідно з якими, в свою чергу, визначають IT-ресурси та можливості (архітектура IT в організації), необхідні для успішної реалізації стратегії організації в сфері застосування IT.[1]

IT РЕСУРСИ

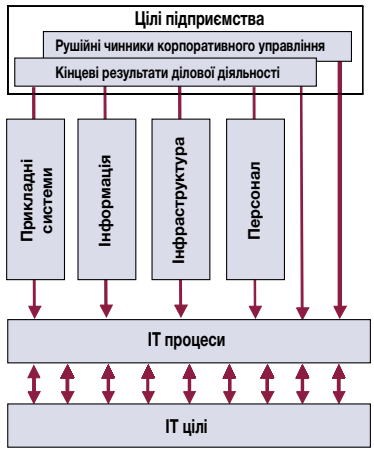
IT-організація ставить у відповідність цілям чітко визначену сукупність процесів, відповідно до яких силами професійного персоналу та технологічної інфраструктури виконуються автоматизовані прикладні бізнес-програми, які при цьому ефективно використовують бізнес-інформацію. Вказані ресурси, разом з процесами, складають архітектуру IT в організації, як показано на **малюнку 6**.

Щоб забезпечити відповідність IT бізнес-вимогам, організація повинна провести інвестиції в ресурси, щоб створити належну технічну можливість (впровадити, наприклад, систему планування ресурсів організації (ERP) на підтримку бізнес-вимог (наприклад, для автоматизації управління ланцюжком постачання), які дадуть бажаний результат (наприклад, підвищення обсягу продажу та фінансові вигоди).

[1] Слід відзначити, що побудова та впровадження архітектури IT для організації також зумовлюють появу внутрішніх IT-цілей, які сприятимуть появі бізнес-цілей, а не безпосередньо випливатимуть з них.

IT ресурси, визначені в CobiT® можна визначити наступним чином:
- **Прикладні системи** – автоматизовані системи для користувачів та ручні процедури для обробки інформації.
- **Інформація** – це дані у всіх можливих видах, які надходять, обробляються та виходять з будь-яких інформаційних систем, що використовуються організацією.
- **Інфраструктура** – це технологія та засоби (тобто, апаратне забезпечення, операційні системи, системи управління базами даних, комп'ютерні мережі, мультимедійні засоби та середовище, в якому вони розміщуються та функціонують), які створюють умови для роботи прикладних програм.
- **Персонал** – це персонал, необхідний для планування, придбання, впровадження, постачання, обслуговування, керування та оцінювання результатів роботи інформаційних систем та послуг. Персонал може бути власним, стороннім або таким, що працює за контрактом.

Малюнок 7. Експлуатувати та супроводжувати, Відстежувати та оцінювати



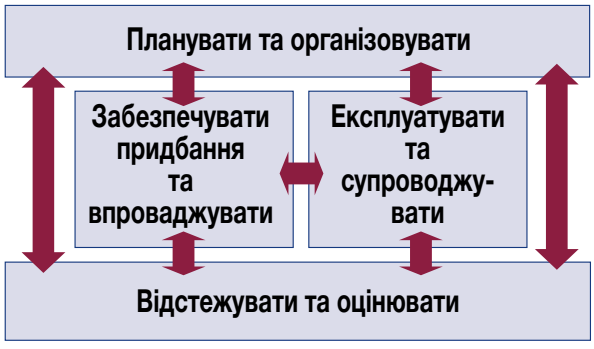
Малюнок 7 відображає вплив бізнес-цілей для IT на спосіб управління ресурсами IT, яке здійснюється IT процесами з метою досягнення IT-цілей.

Орієнтація на процеси

В CobiT® IT-операції описано за допомогою універсальної моделі процесів, які розподілено між чотирма доменами. Цими доменами є «Планувати та організовувати», «Забезпечувати придбання та впроваджувати», «Експлуатувати та супроводжувати»», «Відстежувати та оцінювати». Ці зони поставлено у відповідність до традиційних зон відповідальності у сфері IT, а саме плануванню, створенню, експлуатації та моніторингу.

Методологія CobiT® забезпечує еталонну модель процесів та загальноприйняту мову для всіх зацікавлених сторін з метою аналізу та управління IT-діяльністю. Впровадження операційної моделі та загальновживаної мови в усіх сферах бізнесу, пов'язаних із застосуванням IT, є одним з найважливіших перших кроків на шляху до належного управління IT. В цьому стандарті також представлено методологію оцінювання та моніторингу результатів діяльності IT, побудови схеми комунікацій з провайдерами послуг та запровадження передових практик належного управління. Модель процесів передбачає наявність власників процесів, що дає змогу здійснити розподіл відповідальності та визначити порядок підзвітності.

Малюнок 8. Чотири взаємопов'язані домени



Ефективне управління IT повинне будуватися приймаючи до уваги відповідні IT-процеси та оцінку ризиків притаманних IT. Ці IT-процеси згруповано в домени планування, побудови, експлуатації та моніторингу. В методології CobiT® ці домени, як показано на **малюнку 8**, називаються:
- **ПЛАНУВАТИ ТА ОРГАНІЗОВУВАТИ** (PO)—визначає напрямок для впровадження рішень (AI) та надання послуг (DS)
- **ЗАБЕЗПЕЧУВАТИ ПРИДБАННЯ ТА ВПРОВАДЖУВАТИ** (AI)—забезпечує рішення та послуги
- **ЕКСПЛУАТУВАТИ ТА СУПРОВОДЖУВАТИ** (DS)—отримує рішення та робить їх придатними для використання кінцевими користувачами
- **ВІДСТЕЖУВАТИ ТА ОЦІНЮВАТИ** (ME)—здійснює моніторинг всіх процесів, який підтверджує дотримання визначеного напрямку

ПЛАНУВАТИ ТА ОРГАНІЗОВУВАТИ (PO)

Для реалізації стратегічних цілей необхідно скласти плани, організувати схеми комунікацій та управління з різних точок зору. Слід побудувати належну організацію та діяльності та створити технологічну інфраструктуру. Ця сфера як правило стосується питань, пов'язаних з управлінням, поданих нижче:
- Чи узгоджена діяльність IT з бізнес стратегією?
- Чи використовує організація свої ресурси в оптимальний спосіб?
- Чи кожний працівник організації розуміє цілі застосування IT?
- Чи є розуміння ризиків, пов'язаних з використанням IT, та чи здійснюється управління ними?
- Чи відповідає рівень якості IT – систем потребам бізнесу?

ЗАБЕЗПЕЧУВАТИ ПРИДБАННЯ ТА ВПРОВАДЖУВАТИ (AI)

Щоб реалізувати IT – стратегію, необхідно визначити відповідні IT – системи, розробити чи придбати їх, в також

впровадити та інтегрувати їх в бізнес-процес. Крім того, до цієї сфери відносяться внесення змін до вже існуючих систем та їх обслуговування, що гарантує постійну відповідність рішень цілям бізнесу. В цій сфері вирішуються питання, подані нижче:
- Чи можуть нові проекти забезпечити впровадження систем, які відповідають потребам бізнесу?
- Чи можуть нові проекти бути реалізованими вчасно та в межах кошторису?
- Чи будуть нові системи функціонувати належним чином при їх впровадженні?
- Чи можна буде запровадити необхідні зміни, не порушуючи вже існуючих бізнес-операцій?

ЕКСПЛУАТУВАТИ ТА СУПРОВОДЖУВАТИ (DS)
В цій сфері відбувається фактичне надання послуг, управління безпекою та неперервністю, надання підтримки користувачам та управління даними. В цієї сфері вирішуються проблеми управління, подані нижче:
- Чи надаються IT – послуги відповідно до пріоритетів бізнесу?
- Чи оптимізовано витрати, пов'язані із IT?
- Чи здатний персонал ефективно та безпечно використовувати IT - системи?
- Чи гарантовано безпеку інформації завдяки дотриманню конфіденційності, цілісності та доступності?

ВІДСТЕЖУВАТИ ТА ОЦІНЮВАТИ (ME)
Всі IT – процеси необхідно регулярно оцінювати щодо рівня їх якості та відповідність вимогам, що висуваються системами контролю. В цій сфері приділяється увага проблемам управління результатами діяльності, здійснюється моніторинг системи внутрішнього контролю, оцінюється дотримання існуючих вимог, включаючи вимоги системи корпоративного управління. Як правило, тут шукають відповідь на запитання, подані нижче:
- Чи здійснюється оцінювання результатів експлуатації IT з метою виявлення проблем, поки вони не стали критичними?
- Чи забезпечує керівництво ефективну систему внутрішнього контролю?
- Чи можна встановить зв'язок між результатами застосування IT та бізнес-цілями?
- Чи впроваджено належну систему контролю конфіденційності, цілісності та доступності інформації, яка гарантує її безпеку?

Стандартом CobiT® в межах цих чотирьох доменів передбачено 34 процеси, які зазвичай використовуються (повний їх перелік подано на **малюнку 22**). Хоча більшість організацій вже розробили відповідний план, побудували, впровадили відповідальність у сфері IT та контролюють її, при цьому більшість з них мають аналогічні ключові процеси, лише декілька з них мають аналогічну структуру процесів або застосовують всі 34 процеси, передбачені CobiT®. Цей стандарт надає повний перелік процесів, які можна застосовувати для перевірки повноти системи операцій та розподілу відповідальності; однак в застосуванні всього переліку немає потреби, їх навіть можна комбінувати за потребою згідно із специфікою кожної організації.

Кожному з вказаних 34 процесів поставлено у відповідність бізнес-ціль та IT-ціль. Також надано інформацію щодо того, як можна співвіднести вказані цілі, яка діяльність та результати є ключовими, а також хто несе за них відповідальність.

Контроль
В CobiT® визначено цілі контролю для всіх 34 процесів, а також всебічна система контролю процесів та прикладних програм.

ПРОЦЕСИ НЕОБХІДНО КОНТРОЛЮВАТИ
Контроль, за визначенням, це система політик, процедур, практик та організаційних структур, передбачених для забезпечення розумних гарантій того, що бізнес-цілі будуть реалізовані, а небажані події буде попереджено, або виявлено та вжито коригувальних заходів щодо їх наслідків.

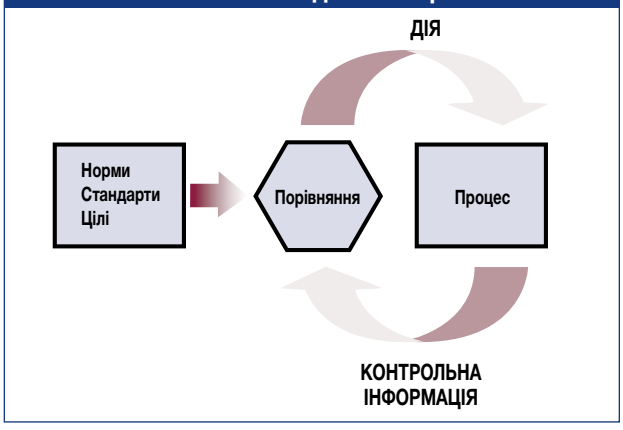
Цілі контролю у сфері IT являють собою завершену сукупність вимог високого рівня, які повинно взяти до уваги керівництво, щоб забезпечити ефективний контроль кожного IT - процесу. Вони:
- є підтвердженням дій керівництва, націлених на підвищення бажаних результатів або зниження ризиків
- складаються з політик, процедур, практик та організаційних структур
- розроблені з метою забезпечення розумних гарантій того, що бізнес-цілі буде реалізовано, а небажані події буде попереджено або виявлено та вжито коригувальних заходів щодо їх наслідків.

Керівництво організації має зробити вибір стосовно цілей контролю шляхом:
- вибору тих, які є прийнятними
- прийняття рішення щодо того, які з них буде запроваджено
- вибору способу їх втілення (частота, період, автоматизація тощо.)
- прийняття на себе ризику, обумовленого не впровадженням тих, які можуть виявитись необхідними

Основою управління може стати стандартна модель контролю, показана на **малюнку 9**. Її побудовано на принципах, що випливають з такої аналогії: Якщо системі обігріву (процесу) задано певну температуру в кімнаті (стандарт), ця система

буде постійно перевіряти (порівнювати) температуру оточуючого середовища (інформація, що контролюється) та буде спонукати (діяти на) систему обігріву щодо збільшення або зменшення подачі тепла.

Малюнок 9. Модель контролю



Оперативне керівництво користується процесами для організації та управління поточною діяльністю в сфері IT. В CobiT® описано універсальну модель процесу, яка представляє всі процеси, які зазвичай входять до складу функцій IT, роблячи загальну еталонну модель зрозумілою для оперативного IT персоналу та керівників організації. Щоб управління було ефективним, керівництво повинно запровадити заходи контролю у вигляді чіткої системи контролю всіх IT – процесів. Оскільки в стандарті CobiT® цілі контролю IT організовані IT процесами, в цій системі встановлено чіткі зв'язки між вимогами до управління IT, IT – процесами та заходами контролю IT.

Кожний з IT процесів стандарту CobiT® має свій опис та набір цілей контролю. Разом вони є характеристиками добре керованого процесу.

Цілі контролю позначаються посланням на відповідний домен, що складається з двох символів (PO, AI, DS та ME) та номером процесу і номером цілі контролю. В додаток до цілей контролю для кожного процесу у стандарті CobiT® є загальні вимоги контролю, які позначено як PC (номер контролю процесу). Їх слід розглядати у сукупності з цілями контролю процесу, щоб мати повне уявлення про вимоги контролю.

PC1 Цілі та завдання процесу
Визначити та повідомити конкретні, такі, що можуть бути виміряні, такі, що дають підстави для дій, реалістичні, орієнтовані на отримання результатів та своєчасні (SMART) цілі та завдання процесу з метою ефективного виконання кожного IT - процесу. Впевнитись, що вони пов'язані з бізнес-цілями та супроводжуються системою відповідних показників.

PC2 Призначення власників процесів
Призначити власника кожного IT процесу та чітко визначити ролі та обов'язки власника процесу. Включити, наприклад, відповідальність за розробку процесу, взаємодію з іншими процесами облік та звітність щодо кінцевих результатів, кількісне оцінювання результатів процесу та виявлення можливостей для вдосконалення.

PC3 Відтворюваність процесу
Розробити та впровадити кожний ключовий IT процес як такий, що може бути відтвореним та постійно давати очікувані результати. Створити логічну але гнучку та змінювану послідовність дій, виконання яких призведе до бажаних результатів, та достатньо мобільною, щоб реагувати на нестандартні та надзвичайні ситуації. Там, де це можливо, використовувати уніфіковані процеси, і адаптувати їх тільки в разі неминучості.

PC4 Ролі та обов'язки
Визначити ключові операції та кінцеві результати процесу. Чітко розподілити та повідомити ролі та обов'язки з метою ефективного та продуктивного виконання ключових операцій та їх документального оформлення а також обліку ті звітності стосовно процесу та його кінцевих результатів.

PC5 Політики, плани та процедури
Визначити та повідомити, в який спосіб всі політики, плани та процедури, які керують IT процесом, слід документувати, редагувати, підтримувати, затверджувати, зберігати, доводити до відома та використовувати для навчання. Здійснити розподіл обов'язків та відповідальності за виконання кожного з вказаних видів діяльності та в належний час перевіряти, чи правильно вини виконуються. Вжити необхідних заходів до того, щоб ці політики, плани та процедури були доступними, правильними, зрозумілими та актуальними.

PC6 Покращення показників процесу
Запровадити систему показників, яка дає уявлення про результати та показники процесу. Встановити планові показники, які відображають цілі процесу та визначити показники результативності, які сприяють досягненню цілей процесу. Визначити спосіб, у який слід отримувати дані. Порівняти фактичні результати з плановими та вжити заходів у випадку виникнення відхилень в разі необхідності. Узгодити ці показники, планові показники та методи із концепцією моніторингу загальних показників IT.
Ефективна система контролю знижує ризики, підвищує імовірність отримання бажаних результатів та продуктивність, оскільки зменшується кількість помилок та забезпечується більш послідовний підхід до управління.

На додаток до цього в CobiT® наведено приклади для кожного процесу, які мають ілюстративний, а не директивний або вичерпний характер, та стосуються:
- типових ресурсів, що використовуються процесом, та вихідних результатів
- дій та інструкцій стосовно ролей та обов'язків відповідно до діаграми RACI («Відповідальний», «Перед ким потрібно звітувати», «Особа, з ким необхідно консультуватись» та «Кого інформувати»)
- ключових цілей діяльності (найважливіших завдань, які слід виконати)
- метрик

Окрім визначення потреб контролю, власники процесів повинні зрозуміти, який внесок повинні зробити інші, та чого інші потребують від процесу, який їм належить. В стандарті CobiT® наведено типові приклади ключових вхідних ресурсів та вихідних результатів для кожного процесу, в тому числі зовнішні вимоги до IT. Деякі вихідні результати є вхідними для всіх інших процесів, позначених 'ALL' в таблицях вихідних результатів, але вони не є вхідними для всіх процесів, та як правило, передбачають наявність стандартів якості та вимог до системи показників, схеми IT процесів, документально оформленого розподілу ролей та обов'язків, системи заходів IT контролю в організації, політик у сфері IT та розподілу ролей та обов'язків персоналу.

Розуміння ролей та обов'язків для кожного процесу є ключовим моментом у забезпеченні ефективного управління. В стандарті CobiT® представлено діаграму RACI для кожного процесу. Особа, «перед ким потрібно звітувати» означає «Останню інстанцію» - це особа, яка вказує напрямок та санкціонує дію. Відповідальність покладається на особу, яка одержує завдання. Інші дві ролі («Особа, з ким необхідно консультуватись» та «особа, яку слід поінформувати») передбачені для того, щоб відповідні особи були залучені до процесу та надавали належну підтримку.

БІЗНЕС ТА IT-КОНТРОЛІ

Система внутрішнього контролю організації впливає на IT на трьох рівнях:
- На рівні вищого керівництва, на якому визначаються бізнес-цілі, впроваджуються політики та приймаються рішення щодо того, як розподіляти та управляти ресурсами організації з метою реалізації її стратегії. Загальний підхід до здійснення управління та контролю визначається Радою директорів та доводиться до відома усіх осіб в організації.. Керування контрольним середовищем в сфері IT здійснюється згідно з визначеною на цьому високому рівні сукупністю цілей та політик.
- На рівні бізнес-процесу, де контролі вживаються в межах конкретних бізнес-операцій. Більшість бізнес-процесів автоматизовано та інтегровано у прикладні IT системи, в результаті чого більшість контролів на цьому рівні також здійснюється автоматично. Подібні контролі мають назву автоматизованих контролів на рівні прикладних систем. Однак, контроль деяких бізнес-процесів реалізується з використанням процедур, що здійснюються вручну, наприклад, санкціонування операцій, розділення обов'язків та звіряння. Тому контролі на рівні бізнес процесів є комбінацією ручних контролів, застосування яких продиктоване вимогами бізнесу, та автоматизованих контролів бізнес процесів на рівні прикладних систем. Визначення та управління обома видами контролів здійснюється в бізнес-сфері, хоча для розробки та впровадження контролів на рівні прикладних систем необхідно залучати IT.
- IT сприяють здійсненню бізнес процесів, надаючи IT послуги , як правило, це послуги, що спільно використовуються багатьма бізнес процесами, оскільки ціла низка IT процесів з розробки та експлуатації виконуються в межах організації в цілому, а більша частина інфраструктури IT надається для загального користування (наприклад, мережі, бази даних, операційні системи та засоби збереження інформації). Контролі, що застосовуються для всіх IT послуг, що надаються, називаються загальними IT-контролями. Надійне функціонування цих загальних контролів є запорукою довіри до автоматизованих контролів на рівні прикладних систем. Наприклад, погане управління змінами може поставити під загрозу (випадково або умисно) надійність функціонування засобів автоматичної перевірки цілісності.

ЗАГАЛЬНІ КОНТРОЛІ IT ТА КОНТРОЛІ НА РІВНІ ПРИКЛАДНИХ СИСТЕМ

Загальними контролями є такі, що вбудовані в IT процеси та послуги. Наприклад, такі, що стосуються:
- Розробки систем
- Управління змінами
- Безпеки
- Підтримки

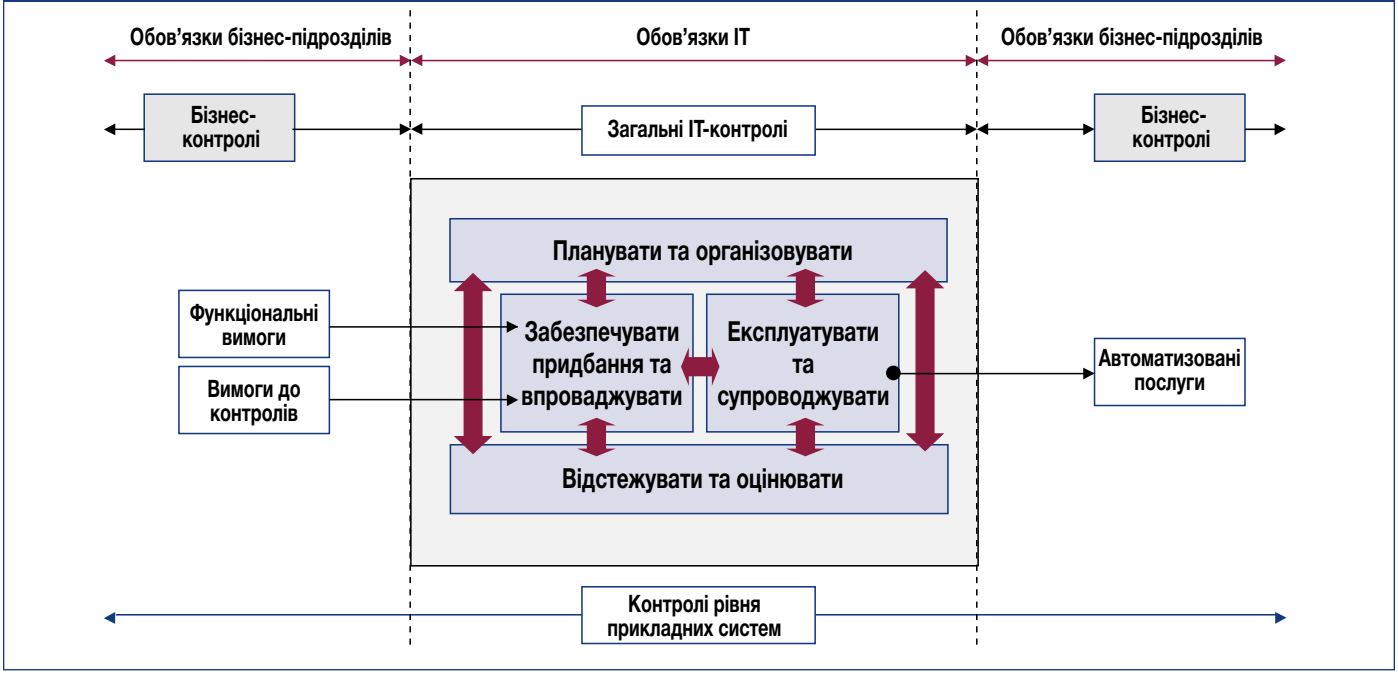
Контролі, вбудовані в прикладні системи, що обслуговують бізнес процеси, широко відомі, як контролі на рівні прикладних систем. Вони стосуються, наприклад:
- Повноти
- Точності
- Достовірності
- Авторизації (санкціонування)
- Розподілу обов'язків

Отже, за забезпечення контролю рівня прикладних систем несуть спільну відповідальність бізнес-підрозділи та IT-підрозділи, але за характером ця відповідальність розподіляється наступним чином:

- Бізнес-підрозділи зобов'язані належним чином:
  - Визначити функціональні вимоги та вимоги до контролів
  - користуватись автоматизованими послугами
- IT-підрозділи зобов'язані:
  - Здійснити автоматизацію та реалізацію функціональних вимог та вимог контролів, визначених бізнес-підрозділами
  - Запровадити систему контролю з метою збереження цілісності контролів рівня прикладних систем

Отже, IT процеси, згідно із стандартом CobiT® передбачають забезпечення контролю IT, але лише в частині розробки контролів рівня прикладних систем; відповідальність за їх визначення та використання лежить на бізнес-підрозділах. Нижче надано рекомендований перелік цілей контролю рівня прикладних систем. Їх позначають сполученням AC з номером контролю рівня прикладних програм.

Малюнок 10. Межі відповідальності бізнесу, загальні контролі та контролі рівня прикладних систем



AC1 Підготовка та дозвіл на використання вихідних даних
Впевнитись, що вихідні документи підготовлені уповноваженим та кваліфікованим персоналом згідно з встановленими процедурами з врахуванням розділення/виділення обов'язків в частині створення та схвалення подібних документів. Кількість помилок та пропусків можна звести до мінімуму, якщо подати вхідні дані у належній формі. Виявити помилки та невідповідності, щоб їх можна було внести до звіту та виправити.

AC2 Накопичення та введення вхідних даних
Встановити порядок, згідно з яким введення даних здійснюється своєчасно уповноваженими та кваліфікованим персоналом. Коригування та повторне введення даних, які було введено з помилками, слід здійснювати у спосіб, який не поставить під загрозу початкові рівні авторизації операцій. Якщо це доцільно для відновлення, зберігати оригінальні вихідні документи протягом належного проміжку часу.

AC3 Перевірки точності, повноти та автентичності даних
Переконатись, що операції є точними, повними та дійсними. Оціни дані, які було введено та відредагувати їх або відправити назад для коригування якомога ближче до місця їх походження (джерела).

AC4 Цілісність та достовірність даних при обробці
Зберігати цілісність та достовірність даних протягом всього циклу їх обробки. Виявлення помилкових операцій не порушує процесу виконання дійсних операцій.

AC5 Аналіз вихідних результатів, звіряння та обробка помилок
Визначити процедури та пов'язані з ними обов'язки, що гарантують належну обробку вихідних результатів, доставку їх належному адресату та захист протягом процесу передачі; забезпечують виконання перевірки, виявлення та коригування точності вихідних результатів та гарантують використання інформації, що міститься у вихідних результатах.

AC6 Аутентифікація операції та цілісність даних
Перш ніж здійснити передачу даних ланцюжком внутрішніх операцій та бізнес/операційних функцій (в межах або за межами підприємства), перевірити відповідність адресата, автентичність походження та цілісність змісту. Підтримувати автентичність та цілісність даних протягом процесу передачі або переносу даних.

Вимірювання результатів – основа для руху вперед

Головне, що має зробити кожне підприємство – це розібратись у стані справ в сфері IT та визначити, на якому рівні потрібно забезпечити управління та контроль IT. Щоб визначити належний рівень, керівництво має спитати себе: наскільки далеко ми повинні просунутись, та чи будуть виправдані витрати отриманою вигодою?

Формування об'єктивного погляду на власний рівень ефективності діяльності – це нелегке завдання. Що потрібно вимірювати та в який спосіб? Підприємства повинні оцінювати, на якому рівні вони знаходяться та які вдосконалення потрібно здійснити, а також запровадити систему заходів для контролю за цим вдосконаленням. В CobiT® ці питання вирішуються шляхом введення:
- Моделей зрілості, які дозволяють виконувати порівняльний аналіз на основі еталонних показників та визначати необхідність вдосконалення можливостей
- Цілей та показників діяльності IT процесів, які показують, як саме процеси мають відповідати цілям бізнесу та IT цілям та використовуються для оцінювання результатів внутрішніх процесів на основі системи збалансованих показників.
- Цілей діяльності, що мають за мету забезпечення ефективного функціонування процесів

МОДЕЛІ ЗРІЛОСТІ
Вище керівництво приватних та державних підприємств все частіше повинно давати відповідь на запитання, наскільки добре здійснюється управління в сфері IT. Щоб дати відповідь на це питання, потрібно розробити економічну модель, яка дозволить здійснити необхідні вдосконалення та досягти належного рівня управління та контролю інформаційної інфраструктури. Потрібно оцінити співвідношення між бізнес-вигодами та витратами та розглянути такі питання:
- Які аналогічні компанії працюють в нашій сфері економічної діяльності та як ми позиціонуємося по відношенню до них?
- Які практики вважаються прийнятними та передовими в цієї сфері економічної діяльності, та на якому рівні ми знаходимось з точки зору впровадження подібних практик?
- Чи можемо ми, на основі результатів подібних порівнянь, сказати, що ми достатньо добре працюємо?
- Як ми можемо визначити, що потрібно зробити, щоб досягти належного рівня управління IT процесами та контролю за ними?

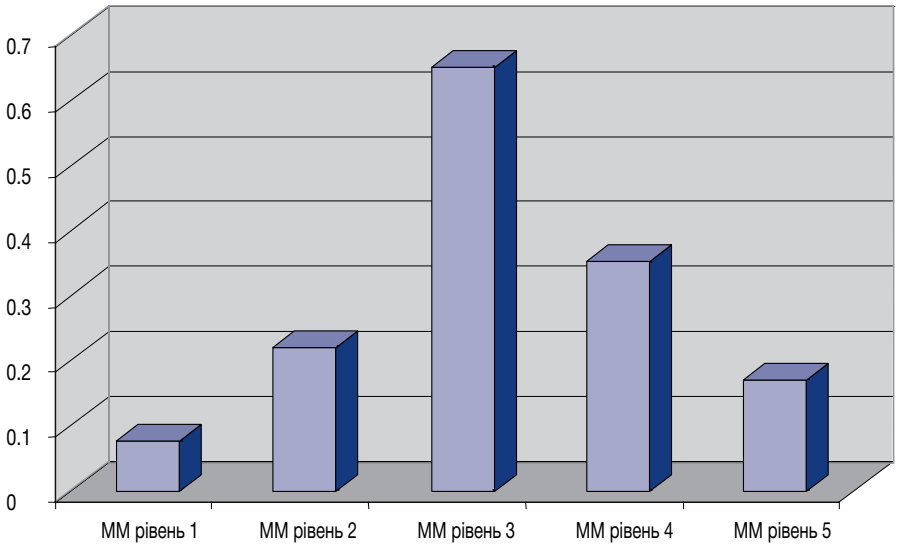
Може статись так, що відповісти на ці запитання буде нелегко. Керівництво IT підрозділів постійно слідкує за тим, щоб вчасно здійснити порівняльний аналіз з іншими організаціями та застосувати засоби само оцінювання, за результатами яких можна визначити, що необхідно зробити з максимумом ефективності. Виходячи з процесів, представлених в CobiT®, власник процесу матиме змогу здійснювати поступовий порівняльний аналіз на основі цілей контролю. Це дасть змогу визначити:
1. Відносний показник результатів та стану, які має підприємство
2. Спосіб ефективного прийняття рішень стосовно напрямку подальшого руху
3. Засіб оцінювання динаміки просування в напрямку поставленої цілі

В основі створення моделей зрілості в цілях управління та контролю IT процесів лежить метод визначення рівня розвитку організації від неіснуючого (0) до оптимізованого (5). Цей підхід було привнесено з моделей зрілості, розроблених Інститутом проектування та розробки програмного забезпечення (Software Engineering Institute (SEI)) створених для оцінки рівня зрілості розробки програмного забезпечення. Хоча концепцію, відображену в підході Інституту SEI і збережено в загальних рисах, варіант стандарту CobiT® суттєво відрізняється від початкових моделей зрілості, запропонованих SEI, які було орієнтовано на принципи розробки програмного забезпечення, організації, що бажають досягти досконалості в цієї сфері, та на здійснення формального оцінювання рівнів зрілості з метою «сертифікації» розробників програмного забезпечення. В стандарті CobiT® введено шкалу моделей зрілості, аналогічну шкалі моделей зрілості процесів створення програмного забезпечення CMM, але в інтерпретації з точки зору управління IT процесами, як передбачено стандартом CobiT®. Для кожного з 34 IT процесів CobiT® розроблено конкретну шкалу моделей зрілості. Якою б не була модель, шкала не повинна бути занадто дрібно розбитою, оскільки це може утруднити використання цієї системи та дати необґрунтовану точність результату, бо, взагалі, мета полягає в тому, щоб визначити, де саме концентруються проблеми та як розподілити пріоритети здійснення вдосконалень. Оцінка рівня відповідності цілям контролю в цьому випадку не є метою.

Рівні зрілості - це профілі IT процесів, які підприємство може визнати як опис можливих статусів організації – поточного та майбутнього. Вони не передбачені для використання в якості порогової моделі, в межах якої не можна пересуватись на наступний, більш високий рівень, не виконавши всіх умов, передбачених більш низьким рівнем. Ті, хто користується моделями зрілості CobiT®, на відміну від оригінального підходу з використанням моделі CMM, запропонованого

Інститутом SEI CMM, не мають наміру здійснити точне «вимірювання» рівнів, та не намагаються підтвердити, що існує абсолютна відповідність визначеному рівневі. Оцінка рівня зрілості за стандартом може в результаті дати профіль, згідно з яким задоволено умови, що відповідають кільком рівням зрілості, як показано на діаграмі, наведеній на **малюнку 11**. Це обумовлено тим, що при оцінюванні зрілості з використанням моделей CobiT® часто трапляється так, що певне впровадження діє на різних рівнях, навіть якщо воно не є завершеним або достатнім. На цьому може грунтуватись

Малюнок 11. Можливі рівні зрілості IT процесу



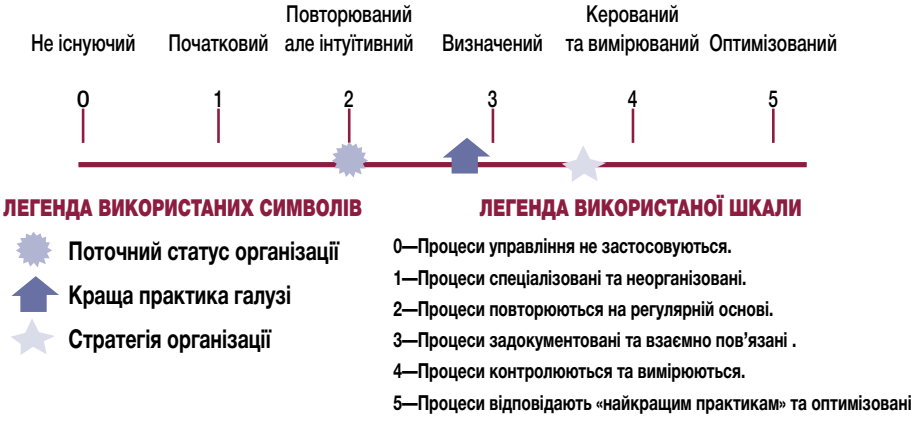
Можливий рівень зрілості IT процесу: подано приклад процесу, який в основному відповідає рівневі зрілості 3, але має деякі проблеми із задоволеннямвимогбільш низьких рівнів, в той самий час бере підтримує вимірювання результатів (рівень 4) та в оптимізацію (рівень 5)

майбутнє підвищення рівня зрілості. Наприклад, деякі складові процесу можуть бути добре визначені, та навіть якщо процес не є завершеним, не можна говорити, що він не є визначеним зовсім.

На основі шкали моделей зрілості, розробленої для кожного з 34 IT процесів CobiT®, керівництво може отримати відомості, надані нижче:
- Поточний рівень зрілості організації
- Поточний статус найкращої практики в цій галузі – порівняння своєї організації із найкращою в цій галузі
- Мета організації, яка має бути реалізована після вдосконалення — Де організація бажає опинитись
- Шлях росту, який треба подолати, рухаючись від статусу «як є» до статусу «як має бути»

Щоб полегшити використання цих результатів в ході нарад, подаючи їх на підтримку економічного обґрунтування майбутніх планів, керівництво може залучити метод графічного представлення (**малюнок 12**).

Малюнок 12. Графічне представлення моделей зрілості



В основу цього графічного представлення покладено основні визначення, що відповідають рівням шкали зрілості, наведені на **малюнку 13**.

CobiT® є методологією, яку розроблено з метою управління IT процесами, при цьому особливу увагу приділяють контролю IT. Ці шкали зрілості зручно застосовувати на практиці та відносно легко зрозуміти. Управління IT процесами має складний та суб'єктивний характер, тому найкращий спосіб його реалізувати – це виконати спрощені оцінки, які поглиблюють обізнаність, забезпечують широкий консенсус та стимулюють вдосконалення. Вказані оцінки можна виконувати або згідно з визначеннями рівнів зрілості в цілому, або більш предметно, виходячи з кожного окремого положення цих визначень. В будь-якому випадку необхідно добре розумітись на процесі, що розглядається.
Перевагою підходу з використанням моделей зрілості є те, що керівництво може достатньо легко позиціонувати себе на шкалі та визначити, що треба змінити, якщо потрібно покращити результати діяльності. Ця шкала починається з позначки 0, оскільки часто процеси управління не існують взагалі. Розподіл на категорії від 0 до 5 відображає просту шкалу зрілості, що показує, як процес розвивається від рівня «не існує» до рівня «оптимізований».
Однак, рівень зрілості процесу – це не результат процесу. Необхідний можливість рівень зрілості, визначений згідно з бізнес цілями та цілями IT, можливо, не потрібно застосовувати в один і той самий спосіб в межах всього середовища IT. Наприклад, деякі контролі потрібно застосовувати несистематично, або тільки до обмеженої кількості систем або модулів.

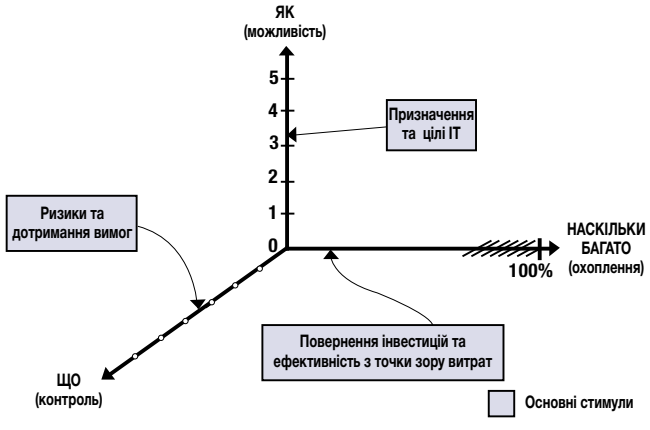
Малюнок 13. Загальна модель зрілості

0 Відсутній—повна відсутність будь-яких процесів управління IT. Організація не визнає існування проблем, пов'язаних з IT, які потрібно вирішувати.
1 Початковий—Організація визнає існування проблем управління IT та необхідність їх вирішення. При цьому не існує жодних стандартних рішень; натомість, існують випадкові одномоментні рішення, які приймаються кимось особисто або в кожному конкретному випадку. Підхід керівництва до вирішення IT проблем є хаотичним.
2 Повторюваний але інтуїтивний—Процеси розроблено до стану, коли аналогічні процедури виконуються різними людьми, що виконують аналогічні завдання. Не існує формалізованого навчання, набору взаємопов'язаних стандартних процедур управління, відповідальність покладено на співробітників. До великої міри має місце покладання на знання працівників, тому можливі помилки.
3 Визначений—Процедури стандартизовані та документовані, здійснюється навчання співробітників з виконання цих процедур. Більшість процесів управляється, як правило, окремими працівниками,тому керівництво не знає ні про які відхилення. Процедури не є складними, вони являються формалізацією існуючої практики.
4 Керований та вимірюваний—Керівництво контролює та оцінює дотримання процедур та вживає заходів в тих (але не у всіх) випадках, коли, на його думку, процеси не працюють ефективно. Процеси постійно вдосконалюються, їх результати відповідають «найкращим практикам». Обмежено застосовуються передові технології, що базуються на сучасній інфраструктурі та модифікованих стандартних інструментах.
5 Оптимізований—В результаті постійного вдосконалення процеси відповідають моделям зрілості, побудованим на основі «найкращих практик» та порівнянні з результатами інших організацій. Інформаційні технології інтегровано в бізнес-процеси, що забезпечує їх повну автоматизацію, це дає змогу підвищувати якість та ефективність роботи організації та її здатність до швидкої адаптації.

Хоча правильно застосована можливість вже забезпечує зниження ризиків, підприємство все ж таки повинно визначити, які заходи контролю потрібно вжити, щоб послабити ризик та отримати цінність від застосування IT з врахуванням схильності до ризику та бізнес-цілей. У виборі цих заходів контролю слід керуватись цілями контролю CobiT®. В додатку III представлено модель зрілості для аналізу системи внутрішнього контролю, яка ілюструє рівень зрілості організації у сфері впровадження та функціонування системи внутрішнього контролю. Часто виконання подібного аналізу є відповіддю на зовнішні стимули, але в ідеалі його потрібно запровадити як документовані процеси стандарту CobiT® PO6 *«Поінформованість щодо цілей керівництва та вказівок»* (Communicate management aims and directions) та ME2 *«Діяльність з моніторингу системи внутрішнього контролю та оцінки результатів»* (Monitor and evaluate internal control).
Можливість, охоплення та контроль є трьома вимірами зрілості процесу, як показано на **малюнку 14**.

Модель зрілості дозволяє здійснити оцінку рівня розвитку процесів управління, тобто, наскільки вони насправді є

Малюнок 14. Три виміри зрілості



дієздатними. Високий рівень розвиненості або дієздатності процесу насамперед визначається цілями ІТ та потребами бізнесу, підтримку яких забезпечують інформаційні технології. Ступінь фактичної зрілості процесу в основному визначається тим обсягом повернення інвестицій, які організація хоче отримати. Наприклад, можуть існувати критичні процеси та системи, які потребують більш ретельного управління безпекою, ніж інші, які мають менш критичний характер. З іншого боку, ступінь та складність контролю, що має бути вжитий до процесу, до більшої міри визначається схильністю організації до ризиків та застосовними вимогами, яких потрібно дотримуватись.

Модель зрілості допоможе спеціалістам пояснити керівництву організації, де саме в управлінні ІТ процесами існують недоліки, та визначити відповідні завдання, які потрібно виконати. Щоб правильно визначити рівень зрілості, потрібно врахувати бізнес-цілі організації, операційне середовище та найкращі практики, що існують в даній галузі. Зокрема, рівень зрілості управління визначатиметься залежністю організації від ІТ, складністю технологій та, що найбільш важливо, цінністю її інформації.

Стратегічний орієнтир для організації, яка хоче вдосконалити систему управління та контролю ІТ процесами, можна визначити на підставі міжнародних стандартів та «найкращих практик» галузі. Практики, що створюються в теперішній час, можуть забезпечити очікуваний рівень результатів в майбутньому, тому їх корисно враховувати при плануванні тих досягнень, які організація хоче отримати з часом.

Моделі зрілості будуються на основі загальної якісної моделі (дивись **малюнок 13**), до якої додаються основні ознаки зрілості, визначені згідно з принципами, поданими нижче, в порядку зростання рівнів зрілості:
- Усвідомлення проблем та рівень комунікацій
- Стан політик, планів та процедур
- Застосування стандартних інструментів та автоматизація процесів
- Професійні знання та досвід
- Відповідальність та підзвітність
- Визначення цілей та «вимірювання результатів»

Таблицю ознак зрілості наведено на **малюнку 15**. В ній показано, як здійснюється управління ІТ процесами, та описано, як саме процеси розвиваються від рівня «не існує» до рівня «оптимізація». Наведені ознаки можна використовувати при здійсненні поглибленої оцінки результатів, порівняльного аналізу та у плануванні вдосконалень.

Отже, використовуючи моделі зрілості, можна створити типовий профіль етапів, які організації проходять при запровадженні управління та контролю ІТ процесів. Це:
- Визначення низки вимог та можливостей їх дотримання на різних рівнях зрілості
- Введення шкали, за якою в простий спосіб можна кількісно вимірювати розходження
- Введення шкали, яка є придатною для проведення практичного порівняння
- Створення базису для визначення положень «як є» та «як має бути»
- Проведення порівняльного аналізу з метою визначення завдань, які треба виконати, щоб досягти вибраного рівня
- Формування бачення того, як здійснюється управління ІТ в організації

Моделі зрілості СовіТ® орієнтовані на визначення рівня зрілості організації, а не на обсяги та глибину необхідного контролю. Вони не є показниками, за які треба боротись, вони також не є формальним базисом сертифікації з дискретними рівнями, які обумовлюють границі, які важко здолати. Однак, вони є завжди застосовними та мають рівні визначень, які, на думку організації, можуть максимально підійти для відображення рівня розвитку процесів організації. Відповідний рівень можна визначити, виходячи з типу організації, середовища, в якому вона діє, та її стратегії..

Рішення щодо масштабів та глибини контролю, а також способу використання та розподілу можливостей приймаються, виходячи з аналізу витрат та вигоди. Наприклад, особливу увагу забезпеченню високого рівня управління безпекою, можливо, потрібно приділяти тільки для найкритичніших систем організації. Іншим прикладом може бути здійснення вибору між необхідністю здійснення щотижневої перевірки вручну та постійного автоматизованого контролю.

На довершення всього, хоча на більш високих рівнях зрілості здійснюється посилений контроль процесу, організація все ж таки повинна визначити, виходячи з результатів оцінки ризиків та рушійних сил створення цінності, які механізми контролю їй слід застосовувати. Типові бізнес цілі та цілі ІТ, окреслені в цій методології, сприятимуть проведенню подібного аналізу. Механізми контролю визначаються цілями контролю СовіТ® та орієнтовані на те, що відбувається в вході виконання процесу; моделі зрілості головним чином передбачені для встановлення того, наскільки добре здійснюється управління процесом. В Додатку ІІІ подано типову модель зрілості, яка відображає стан справ у середовищі внутрішнього контролю та рівень впровадження заходів внутрішнього контролю в організації.

Належне контрольне середовище забезпечується в тому випадку, коли враховано всі три напрямки оцінки зрілості (можливість (дієздатність), охоплення та контроль). Підвищення рівня зрілості сприяє зменшенню ризиків та

Малюнок 15. Таблиця ознак зрілості

Усвідомлення проблем та Комунікації	Рівень політик, планів та процедур	Застосування інструментів та автоматизація процесів	Професійні знання та досвід	Відповідальність та підзвітність	Визначення цілей та «вимірювання результатів»
1 Зароджується визнання необхідності управлінням процесами Комунікації стосовно проблем, що існують, мають епізодичний характер	Мають місце спеціалізовані процеси та практики. Процеси та політики не визначені.	Можуть застосовуватись деякі інструменти, а саме стандартизовані інструменти для настільних ПК. Не існує планування у підході до використання стандартизованих інструментів.	Не визначено рівень професійного досвіду, необхідний для виконання процесів. Не існує плану навчання, формальне навчання не проводиться.	Не існує визначення відповідальності та підзвітності. Люди приймають на себе відповідальність за проблеми, реагуючи на них та виходячи зі своєї власної ініціативи.	Цілі не є чітко визначеними вимірювання результатів не виконується.
2 Існує усвідомлення необхідності діяти. Здійснюється узгоджене управління лише проблемами в цілому.	Використовуються схожі та загальноприйняті процеси, але вони носять інтуїтивний характер внаслідок індивідуального підходу. Деякі аспекти процесів можуть бути відтворені завдяки індивідуальному підходу, можуть зустрічатись випадки документування та неформального розуміння політик та процедур.	Існують загальні підходи до використання інструментів управління, але вони базуються на рішеннях, розроблених окремими ключовими особами. Стандартні інструменти можуть бути придбані але, імовірно, не застосовуються в належний спосіб, та можуть навіть бути «покладені в стіл» .	Для критично важливих сфер визначено мінімальні вимоги стосовно професійного рівня Навчання здійснюється відповідно до потреб, а не на підставі узгодженого плану, не існує формалізованого навчання.	Окремі працівники усвідомлюють свої обов'язки та, як правило, є підзвітними, навіть якщо цю процедуру не узгоджено формально. У випадку виникнення проблем має місце безлад з точки зору відповідальності, існує тенденція до звинувачень.	До деякої міри визначено цілі; введено процедуру збору деяких фінансових метрик, але результати відомі лише керівництву. В окремих сферах ведеться нерегулярний моніторинг.
3 Існує чітке усвідомлення необхідності діяти. У сфері комунікацій управління є більш формалізованим та структурованим.	Є прояви використання «найкращих практик». Процеси, політики та процедури стандартизовані та документовані для всіх ключових дій.	Складено план використання та стандартизації інструментів управління та автоматизації процесу управління Інструменти управління використовуються за їх основним призначенням, але не у всьому можуть відповідати узгодженому плану та можуть не бути інтегровані один з одним.	У всіх сферах визначено та документовано вимоги до кваліфікації персоналу. Розроблено план формалізованого навчання, але формалізоване навчання все ще проводиться, виходячи з індивідуальних потреб.	Відповідальність та підзвітність за управління процесом визначено, встановлено власників процесів. Імовірно, власник процесу не має повного права на виконання цих обов'язків.	Визначено деякі цілі та метрики ефективності, але немає належної комунікації, існує чіткий зв'язок з бізнес цілями. Мають місце процеси вимірювання, але вони не застосовуються послідовно .В організації прийнято ідею збалансованих карт оцінки бізнесу, аналіз першопричин застосовується час від часу.
4 Існує повне розуміння проблем управління. Застосовуються ретельно обдумані методики комунікацій та стандартні інструменти комунікацій.	Процес є чітко визначеним та довершеним; застосовуються внутрішні найкращі практики Всі аспекти процесу документовані та можуть бути відтворені. Політики затверджені та підписані керівництвом. Стандарти розробки та здійснення процесів та процедур прийняті та дотримуються.	Інструменти управління впроваджено згідно із стандартизованим планом, деякі з них інтегровані з іншими пов'язаними інструментами управління. У більшості сфер використовуються Інструменти, призначені для автоматизації управління процесом та моніторингу найважливіших дій та заходів контролю.	Вимоги до кваліфікації персоналу постійно оновлюються у всіх сферах, професійність працівників, що працюють у всіх найважливіших сферах, гарантовано, наявність сертифікату (диплому) заохочується. Застосовуються ретельно розроблені методики навчання згідно з планом навчання, заохочується обмін знаннями. Всі внутрішні спеціалісти в предметних областях залучені до бізнес процесів, здійснюється оцінка ефективності навчального плану.	Відповідальність та підзвітність за виконання процесу розподілені та встановлені в такий спосіб, що власник процесу може виконувати свої обов'язки в повному обсязі і несе за них відповідальність. Існує система преміювання працівників, яка стимулює до здійснення дій з позитивним результатом.	Здійснюється вимірювання показників ефективності та продуктивності, встановлено їх взаємозв'язок з бізнес цілями та стратегічним планом в сфері IT. В деяких сферах запроваджено карти збалансованих показників, за виключеннями, відомими керівництву, порядок аналізу першопричин формалізовано. Має місце постійне вдосконалення процесів.
5 Має місце поглиблене розуміння управління, проблем та рішень IT, а також перспектив. Здійснюється проактивне узгоджене управління проблемами на основі аналізу тенденцій, застосовуються ретельно продумані методики комунікацій, використовуються інтегровані інструменти комунікацій.	Застосовуються найкращі практики інших організацій та зовнішні стандарти. Документування процесів забезпечує автоматизацію бізнес процесів. Процеси, політики та процедури стандартизовані та інтегровані, що дає змогу підвищувати якість управління та ефективність роботи організації, а також здійснювати постійне вдосконалення.	В масштабах всієї організації застосовуються стандартизовані пакети інструментів. Інструменти повністю інтегровані з іншими пов'язаними інструментами, що забезпечує комплексну підтримку процесів. Інструменти використовуються з метою вдосконалення процесів та забезпечують автоматизоване виявлення нестандартних ситуацій в системі контролю.	Організація офіційно заохочує прагнення до постійного підвищення кваліфікації, виходячи з чітко визначених особистих цілей та цілей організації. Навчання направлене на використання найкращих практик інших організацій та передових підходів та методик Обмін знаннями є частиною культури організації, розгортаються системи, засновані на використанні знань. Керівну участь беруть сторонні спеціалісти та організації, що займають провідне положення в галузі.	Власники процесів мають право приймати рішення та вживати заходів. Прийняття відповідальності на себе послідовно розповсюджене зверху донизу в масштабах всієї організації.	Існує інтегрована система вимірювання показників ефективності, яка пов'язує результати у сфері IT з бізнес цілями через збалансовані карти показників IT. Нестандартні ситуації цілком та повністю відомі керівництву, першопричини всіх проблем та відхилень ретельно аналізуються. Постійне вдосконалення процесів – це спосіб життя організації.

підвищенню ефективності роботи, що обумовлює меншу кількість помилок, більш високу прогнозованість процесів та ефективне використання ресурсів з точки зору витрат.

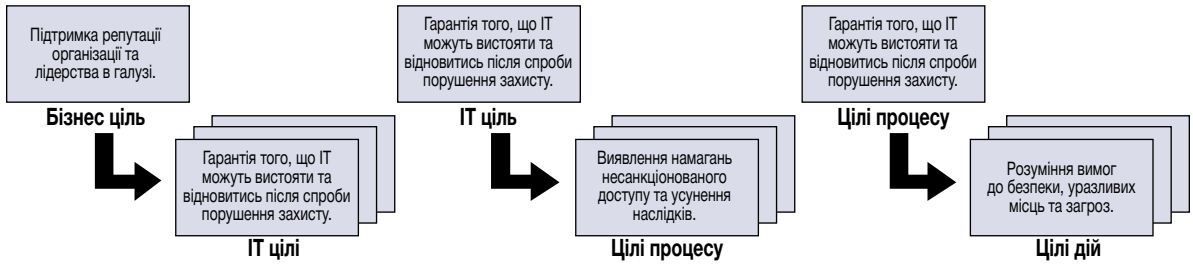
«ВИМІРЮВАННЯ» РЕЗУЛЬТАТІВ

Цілі та метрики (показники) визначено в CobiT® згідно з трьома рівнями:

- Цілі IT та показники, які дозволяють визначити, чого саме бізнес-підрозділи очікують від IT та як вимірювати ці результати
- Цілі процесу та відповідні показники, які дозволяють визначити, що саме IT процес повинен забезпечити на підтримку IT цілей, та як вимірювати відповідні результати
- Цілі діяльності та відповідні показники, які встановлюють, що повинно статись в межах процесу, щоб були досягнуті заплановані результати, та як їх вимірювати

Цілі визначено зверху донизу так, що бізнес-ціль визначає сукупність цілей IT, які її підтримують. Ціль IT реалізується одним процесом або в результаті взаємодії сукупності процесів. Тому цілі IT визначають різні цілі процесів. В свою чергу кожна ціль процесу потребує здійснення сукупності дій, таким чином визначаючи цілі дій. На **малюнку 16** надані приклади взаємозв'язку цілей бізнесу, IT та дій.

Малюнок 16. Приклад взаємозв'язку цілей

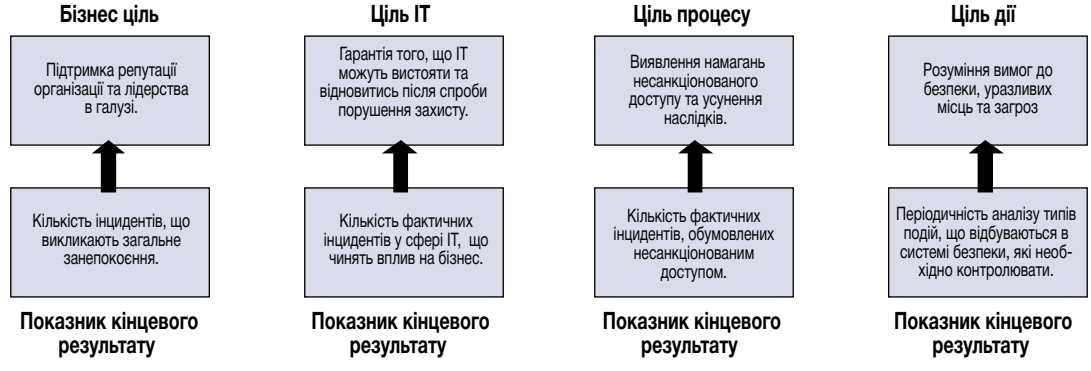


Терміни «Ключовий індикатор досягнення цілі» (KGI) та «Ключовий індикатор ефективності» (KPI), використані в попередніх версіях стандарту CobiT®, було замінено двома видами метрик:

- Показники кінцевих результатів (Outcome measures), раніше – ключові індикатори досягнення цілі (KGI), показують, чи були досягнуті цілі. Їх можна виміряти тільки після фактичного настання події, тому їх називають «показниками відставання» ('lag indicators').
- Показники ефективності (Performance indicators), раніше – ключові індикатори ефективності (KPI), показують, чи можуть бути досягнуті цілі. Їх можна виміряти ще до того, як будуть зрозумілі кінцеві результати, тому їх називають «показниками випередження» ('lead indicators').

На **малюнку 17** надано можливі цілі або показники кінцевих результатів, які стосуються наведеного прикладу.

Малюнок 17. Можливі показники кінцевих результатів для прикладу з малюнку 16



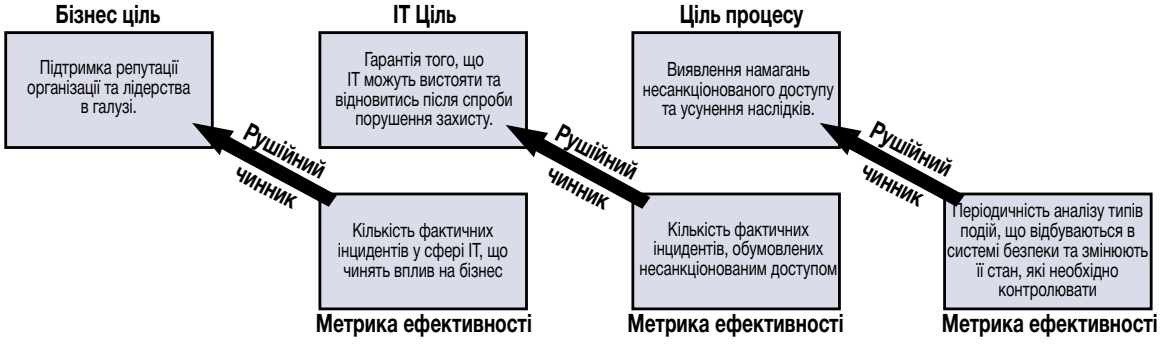
Показники кінцевих результатів нижчого рівня набувають значення показників результативності вищого рівня. В прикладі з **малюнку 16** показник кінцевих результатів, який підтверджує, що здійснюється виявлення спроб несанкціонованого доступу та реагування на них, в той самий час показує, що, імовірніше всього, IT-послуги можуть встояти проти подібних атак та мають здатність до відновлення. Тобто, показник кінцевих результатів став показником результативності високорівневої цілі. На **малюнку 18** показано, як Показники кінцевих результатів з даного прикладу перетворюються на метрики ефективності (performance metrics).

Показники кінцевих результатів визначають метрики, на підставі яких керівництво може зрозуміти – чи досягли функція IT, процес або дія своїх цілей. Показники кінцевих результатів IT часто виражають через інформаційні критерії (вимоги до інформації):

- Доступність інформації, необхідної для підтримки потреб бізнесу
- Відсутність ризиків, пов'язаних з порушенням цілісності та конфіденційності інформації
- Рентабельність процесів та операцій
- Підтвердження надійності, ефективності та узгодженості інформації

Показники результативності визначають метрики, які показують, наскільки ефективно бізнес процес, IT функція чи IT процес забезпечують досягнення поставлених цілей. Вони є показниками випередження, які демонструють, чи можуть бути досягнуті цілі, і, таким чином стають рушійними чинниками високорівневих цілей. Часто вони стають одиницею вимірювання доступності відповідних можливостей, практик та професійного рівня, а також кінцевих результатів базових дій. Наприклад, послуга, надана із застосуванням IT, є ціллю IT, і в той самий час показником ефективності та можливістю бізнесу. Ось чому іноді показники ефективності називають рушійними чинниками ефективності, зокрема в картах збалансованих показників.

Малюнок 18. Можливі рушійні чинники прикладу з малюнку 16



На **малюнку 19** показано взаємозв'язок між бізнес цілями, цілями IT, цілями процесу та різноманітними метриками. Вверху зліва направо наведено послідовність цілей. Під ціллю подано показник кінцевого результату для цієї цілі. Маленька стрілка вказує, що одна й та сама метрика є показником результативності для високорівневої цілі.

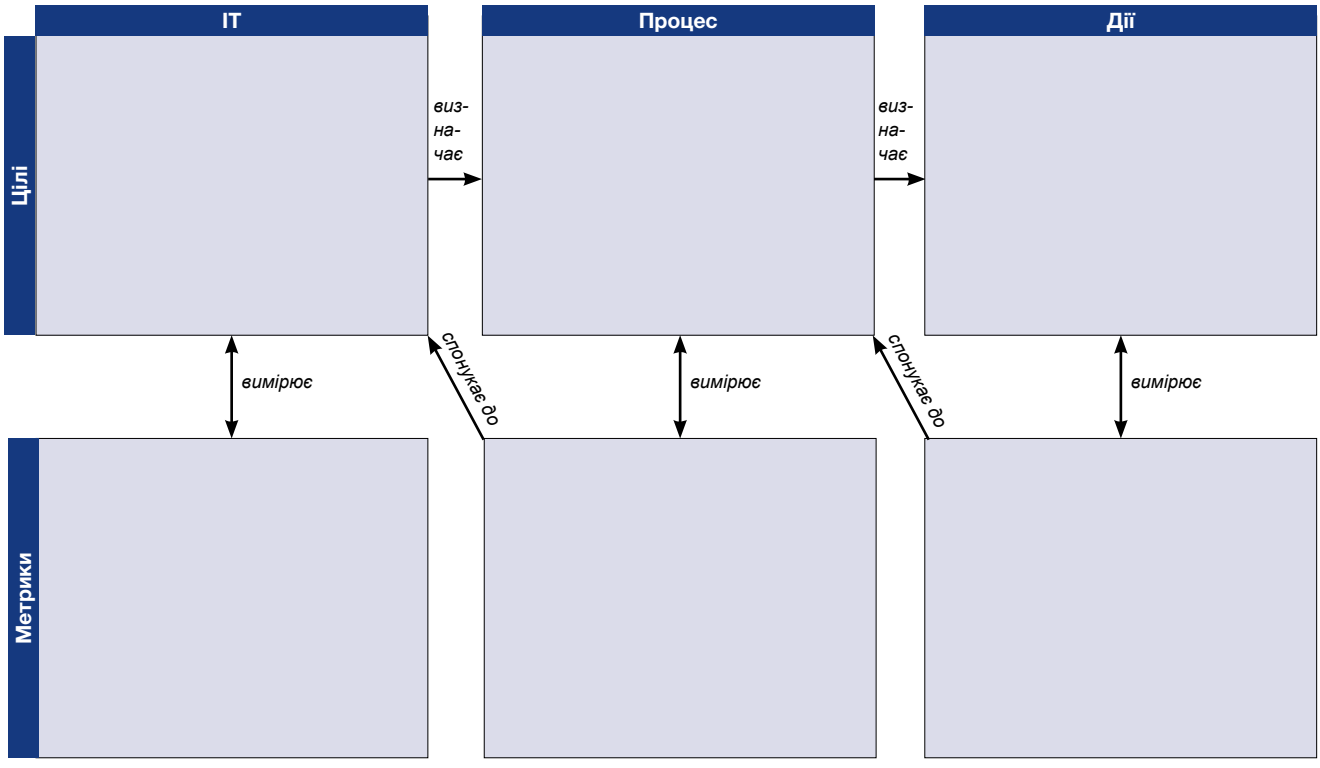
Малюнок 19. Взаємозв'язок між процесами, цілями та метриками (DS5)

Наведений приклад взято з процесу DS5 *«Гарантувати безпеку систем»* (Ensure systems security) домену «Функціонування та обслуговування». Стандартом СовіТ® передбачено метрики до самих кінцевих показників IT цілей, окреслених пунктирною лінією. Хоча вони є також показниками результативності бізнес цілей, які підтримують IT, стандартом СовіТ® не передбачені показники кінцевих результатів бізнес цілей.

Бізнес цілі та IT цілі, що згадуються в розділі «Цілі та метрики» стандарту СовіТ®, в тому числі їх взаємозв'язок, подані в Додатку I. Для кожного IT процесу в стандарті СовіТ® цілі та метрики представлено так, як показано на **малюнку 20**.

Метрики було розроблено з врахуванням міркувань, поданих нижче:
- Метрика повинна характеризуватись високим значенням співвідношення «розуміння – зусилля» (insight –to-effort ratio) (тобто розуміння результатів та досягнення цілей в порівнянні із зусиллями, витраченими на оволодіння ними)
- Метрики повинні бути порівнянними між собою (наприклад, виражатись у вигляді відсоткової частки в порівнянні з базовим показником або з показниками у динаміці за часом)
- Метрики повинні бути порівнянними з метриками інших організацій, незалежно від масштабів організації або галузі, в якій вона здійснює свою діяльність
- Краще мати невелику кількість надійних метрик (може навіть бути одна дуже надійна (хороша) метрика, на яку можна чинити вплив різними шляхами), аніж чисельну низку метрик низької якості
- Метрики повинні бути легко вимірюваними та такими, щоб їх не можна було сплутати з плановими або контрольними цифрами

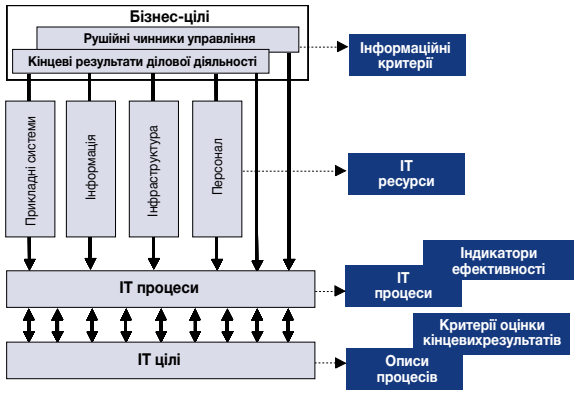
Малюнок 20. Представлення Цілей та метрик



Структура стандарту СовіТ®

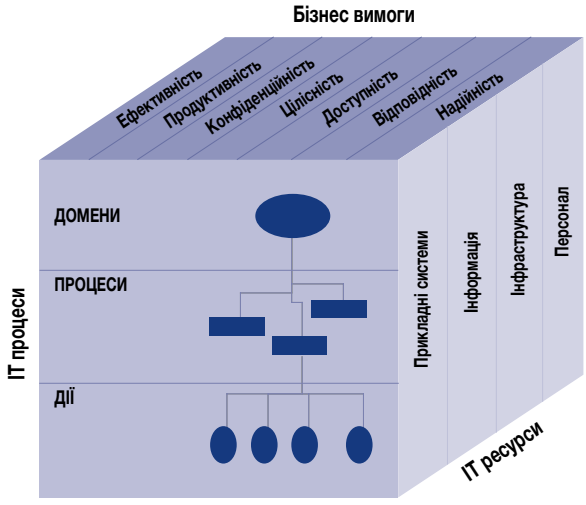
В структурі стандарту СовіТ® бізнес-вимоги до інформації та корпоративного управління прив'язані до цілей, що стоять перед IT-послугами. Процесна модель, що лежить в основі стандарту СовіТ®, дозволяє реалізувати належне управління та контроль діяльності IT та ресурсів, які її підтримують, виходячи з цілей контролю, визначених в стандарті СовіТ®, узгодження та моніторинг яких здійснюються з використанням цілей та метрик СовіТ®, як показано на **малюнку 21**.

Малюнок 21. Управління, контроль, узгодження та моніторинг в стандарті СовіТ®



Отже, IT ресурси керуються IT процесами з метою досягнення IT цілей, які відповідають вимогам, визначеним бізнесом. Це основний принцип побудови концептуального ядра стандарту СовіТ®, як показано за допомогою куба СовіТ® (**малюнок 22**).

Малюнок 22. Куб СовіТ



Більш детально всю структуру стандарту СовіТ® можна зобразити графічно, як це зроблено на малюнку 23, у вигляді процесної моделі СовіТ®, в основі якої лежать чотири домени, що охоплюють 34 основних процеси, які управляють IT ресурсами з метою надання інформації бізнес-підрозділам у відповідності до вимог, висунутих бізнес-підрозділами, та з врахуванням принципів корпоративного управління.

Загальна прийнятність стандарту СовіТ®
Стандарт СовіТ® створено на основі аналізу та гармонізації існуючих IT стандартів та найкращих практик, при цьому він відповідає загальноприйнятим принципам корпоративного управління. Рівень цього стандарту є високим, в його основі лежить відповідність бізнес-вимогам, він охоплює весь діапазон IT функцій та сконцентрований на тому, ЧОГО САМЕ потрібно досягти, а не ЯК реалізувати ефективне корпоративне управління, керування та контроль. Тому він є інтегратором практик в області IT управління та призначений для вищого керівництва, керівників середньої ланки (IT-директорів, начальників бізнес-підрозділів), спеціалістів з питань корпоративного управління, гарантії якості та безпеки, а також експертів в області IT аудиту та контролю IT. Він передбачений, як доповнення до інших стандартів та найкращих практик галузі, і має застосовуватись разом з ними.

Найкращі практики слід запроваджувати відповідно до принципів корпоративного управління та системи контролю організації, їх введення має бути доцільним, а вони самі повинні бути інтегровані з іншими методами та практиками, які вже використовуються в організації. Стандарти та найкращі практики не є панацеєю на всі життєві випадки. Їх ефективність залежить від того, як саме їх було запроваджено та яким чином їх дотримувались до цього часу. Найбільшу користь вони приносять, якщо застосовуються як сукупність принципів та як основа для формування конкретних процедур. Щоб практики не були «покладені в стіл» , керівництво та персонал повинні розуміти, що робити, як саме це робити та чому це важливо.

Щоб узгодити найкращі практики з бізнес-вимогами, рекомендовано застосовувати СовіТ® на найвищому рівні, запроваджуючи систему всебічного контролю на базі моделі, побудованої з IT процесів, які повинні в загальному випадку підходити кожній організації. Конкретні практики та стандарти, що стосуються окремих сфер, можна долучити відповідним чином до структури стандарту СовіТ®, в такий спосіб реалізується ієрархія методичних матеріалів.

Аудиторія стандарту СовіТ® складається з різних користувачів:
- **Вище керівництво**—стандарт допомагає отримати цінності у вигляді повернення від інвестицій в IT, а також збалансувати ризики та інвестиції у систему контролю в часто непередбачуваному IT середовищі
- **Керівники бізнес-підрозділів**—стандарт сприяє отриманню гарантії якості управління та контролю IT-послуг, що надаються власними силами організації, або третіми особами
- **Керівництво IT-підрозділів**—стандарт забезпечує можливість надання IT послуг, яких вимагають бізнес-підрозділи на підтримку бізнес-стратегії, у керований та контрольований спосіб
- **Аудитори**—стандарт допомагає в обґрунтуванні їх висновків та/або наданні рекомендацій керівництву або службі внутрішнього контролю.

Малюнок 23. Загальна структура стандарту CobiT®

Стандарт CobiT® розроблений та підтримується незалежним некомерційним дослідницьким інститутом на основі досвіду його афілійованих членів асоціації, експертів в даній галузі та спеціалістів з питань забезпечення контролю та безпеки. Він базується на результатах постійного аналізу найкращих практик в сфері IT, постійно підтримується на належному рівні, і тому є об'єктивним та практичним ресурсом для всіх видів користувачів.

Стандарт CobiT® орієнтований на цілі та обсяг IT управління, при цьому забезпечувана ним структура системи контролю

Малюнок 24. Структура CobiT® та основні зони управління IT

	Цілі	Метрики	Практики	Моделі зрілості
Узгодженість зі стратегією	P	P		
Забезпечення цінності		P	S	P
Управління ризиками		S	P	S
Управління ресурсами		S	P	P
Оцінка ефективності	P	P		S

P=основний інструмент реалізації S=другорядний інструмент реалізації

є універсальною, узгодженою з принципами корпоративного управління організації, і тому він є прийнятним для рад директорів, виконавчого керівництва, аудиторів та працівників регулятивних органів. В додатку II показано, як цілі контролю стандарту CobiT® поставлено у відповідність п'яти зонам особливої уваги корпоративного управління в сфері IT та заходам контролю, передбаченим моделлю, розробленою COSO.

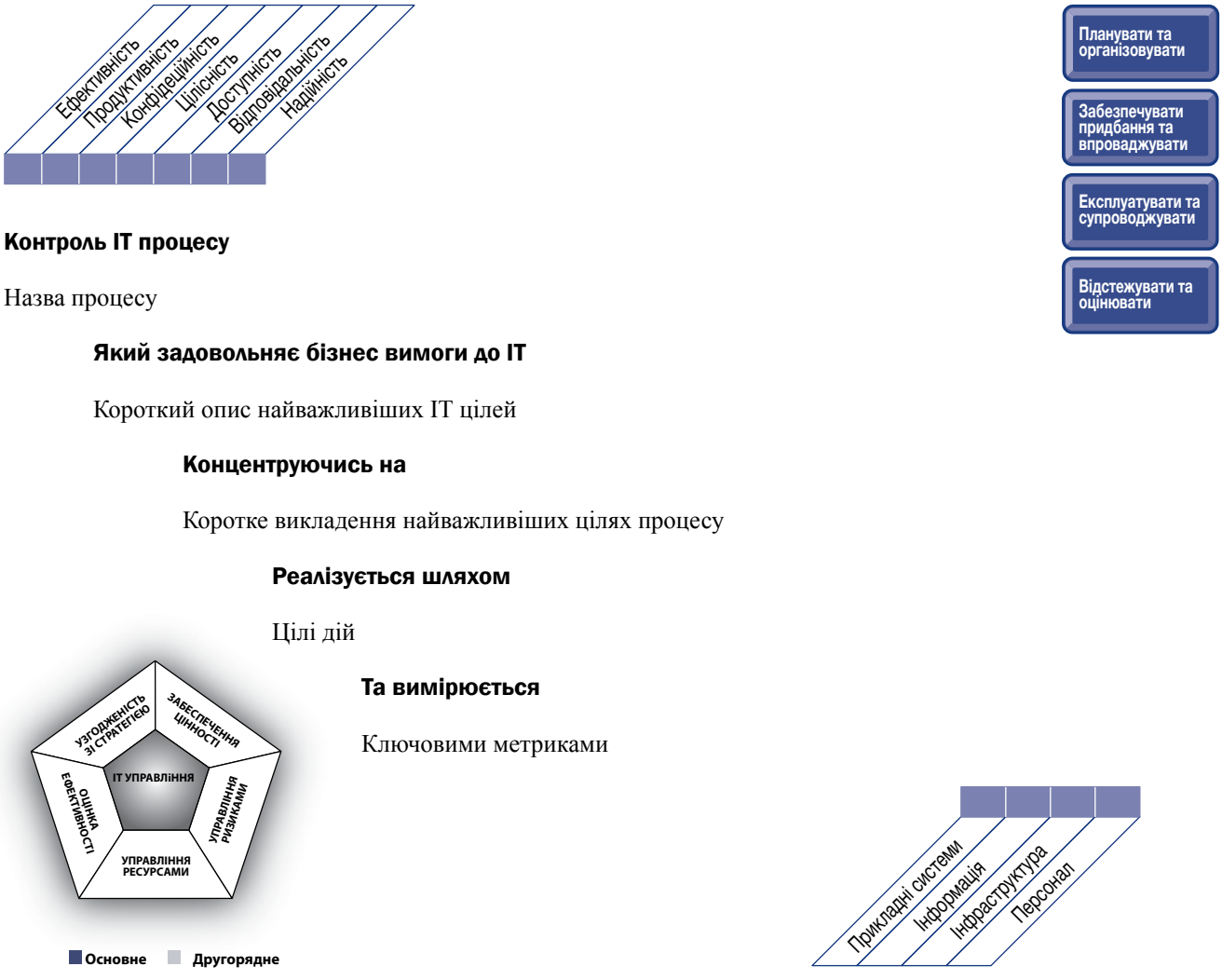
На **малюнку 24** показано, як різні елементи структури стандарту CobiT® поставлено у відповідність до основних зон уваги корпоративного управління в сфері IT.

ЯК КОРИСТУВАТИСЬ ЦІЄЮ КНИГОЮ

Навігація в структурі стандарту СовіТ®

Кожний ІТ процес стандарту СовіТ® має опис, ключові цілі та метрики, які подано в наступному вигляді (**малюнок 25**).

Малюнок 25. Навігатор СовіТ®



Огляд елементів концептуального ядра стандарту СовіТ®

До структури стандарту СовіТ® входять подані нижче основні елементи, описані далі в цій публікації, які поділені на 34 ІТ процеси, при цьому дається завершена схема того, як контролювати, управляти та вимірювати кожний з цих процесів. Кожний процес має чотири розділи, кожний розділ складається приблизно з однієї сторінки, а саме:

- Розділ 1 (**малюнок 25**) містить опис процесу, в якому коротко представлені цілі процесу, при цьому опис процесу представлений у вигляді каскаду. На цій сторінці також відображено відповідність процесу інформаційним критеріям, ІТ ресурсам та основним зонам управління ІТ літерою P, якщо це основний взаємозв'язок, та літерою S, якщо він є другорядним.
- Розділ 2 містить цілі контролю цього процесу.
- Розділ 3 містить вхідні ресурси процесу та результати, діаграму RACI, цілі та метрики.
- Розділ 4 містить модель зрілості процесу.

Іншим чином проаналізувати суть виконання процесу можна й так:

- Вхідні ресурси процесу – це те, чого власник процесу вимагає від інших.

- Цілі контролю в описі процесу відображають те, що власник процесу повинен зробити.
- Результати процесу – це те, що власник процесу повинен представити.
- Цілі та метрики показують, як слід вимірювати цей процес.
- RACI-діаграма відображає, що і кому треба доручити.
- Модель зрілості показує, що слід зробити, щоб поліпшити ситуацію.

Ролі в RACI-діаграмі для всіх процесів такі:
- Вища посадова особа в організації (CEO)
- Фінансовий директор (CFO)
- Керівники бізнес-підрозділів
- Директор з інформаційних технологій (CIO)
- Власник бізнес-процесу
- Виконавчий директор (Head operations)
- Головний архітектор (Chief architect)
- Керівник підрозділу з розробки ПЗ (Head of development)
- Керівники адміністративних функцій IT (для великих організацій керівники таких служб як відділ кадрів, служби фінансового планування та служби внутрішнього контролю)
- Відповідальний за управління проектам (PMO)
- Служби дотримання існуючих вимог, аудиту, управління ризиками та забезпечення безпеки (групи спеціалістів, наділені обов'язками в області контролю, а ніж IT-персонал, задіяний в операційних задачах)

Певні процеси мають додаткову спеціальну роль, властиву даному процесу,наприклад, менеджер служби підтримки/ реагування на інцидент в процесі DS8.

Слід зазначити, що хоча цей матеріал сформовано на основі досвіду сотень експертів за результатами ретельних досліджень та аналізу, вхідні ресурси, кінцеві результати, цілі та метрики є лише ілюстративними, вони не є директивними або вичерпними. Це базовий досвід , на основі якого кожна організація повинна вибрати, що саме їй підходить з точки зору ефективності та продуктивності, виходячи із стратегії організації, її цілей та політик.

Користувачі елементів стандарту CobiT®

Керівництво може використовувати стандарт CobiT® для оцінювання IT процесів, застосовуючи систему бізнес-цілей та IT цілей, представлених в Додатку I з метою визначення цілей IT процесів, а також модель зрілості процесів для оцінювання фактичних результатів діяльності організації.

Спеціалісти з впровадження та аудитори можуть визначити застосовні вимоги до системи контролю, виходячи з цілей контролю, а також розподілити обов'язки на основі дій та відповідних RACI-діаграм.

Всі потенційні користувачі можуть отримати користь від застосування CobiT®, користуючись цим стандартом разом із більш вузькими стандартами, а саме:
- ITIL стосовно надання послуг
- CMM стосовно рішень розробки ПЗ
- ISO 17799 у сфері інформаційної безпеки
- PMBOK or PRINCE2 в області управління проектами

Додатки

В кінці цієї книги надано такі додаткові матеріали:

I. Таблиці, що ілюструють зв'язок між цілями та процесами (три таблиці)
II. Встановлення відповідності між IT процесами та зонами особливої уваги управління IT, моделлю COSO, IT ресурсами стандарту CobiT® та інформаційними критеріями CobiT®
III. Модель зрілості системи внутрішнього контролю
IV. Основні довідкові матеріали стандарту CobiT® 4.1
V. Перехресні посилання видань CobiT® 3rd Edition© та CobiT® 4.1
VI. Стратегія наукових досліджень та розробки
VII. Глосарій
VIII. CobiT® та похідні роботи

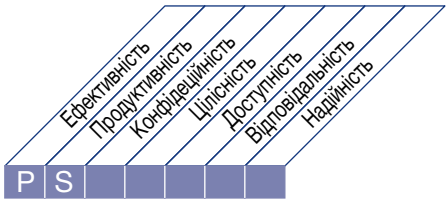
Планувати та організовувати

PO1 Розробляти стратегічний план розвитку IT
PO2 Формувати архітектуру інформації
PO3 Визначати технологічний напрямок
PO4 Формувати процеси, організацію та взаємозв'язки для IT
PO5 Управляти інвестиціями в IT
PO6 Інформувати про стратегічні цілі керівництва та напрямки розвитку
PO7 Управляти персоналом IT
PO8 Управляти якістю
PO9 Оцінювати та управляти IT – ризиками
PO10 Управляти проектами

Опис процесу

PO1 Розробляти стратегічний план розвитку IT

Необхідно здійснювати стратегічне планування IT з метою управління та спрямування всіх IT ресурсів згідно з бізнес-стратегією та встановленими пріоритетами. IT служби в рамках якого зацікавлені бізнес сторони несуть відповідальність за гарантоване отримання оптимального результату від реалізації портфеля проектів та послуг. Створення стратегічного плану сприяє розумінню ключовими зацікавленими сторонами можливостей та обмежень, пов'язаних із застосуванням IT, дозволяє оцінити поточну ефективність, визначити вимоги до потужностей й персоналу та обсяг необхідних інвестицій. Бізнес-стратегія та пріоритети мають бути відображені в портфелі та реалізовані згідно з тактичним(-и) планом (-ами) розвитку IT, в якому визначено конкретні цілі, плани дій та завдання, зрозумілі як для бізнес-підрозділів, так і для служб IT.



Контроль IT процесу

Розробляти стратегічний план розвитку IT

який задовольняє бізнес-вимоги до IT, а саме:

підтримка або сприяння розвитку бізнес-стратегії і вимог корпоративного управління, та в той самий час визначення вигоди, витрат та ризиків

зосереджений на

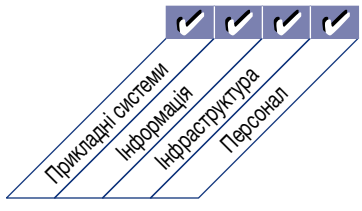
залученні керівництва IT та бізнес-підрозділів до процесу трансформації бізнес-вимог у ослуги та розробці концепції надання даних послуг у прозорий та ефективний спосіб

реалізується шляхом

- Залучення керівників бізнес-підрозділів і вищого керівництва організації до узгодження стратегічних планів розвитку IT з поточними та майбутніми потребами бізнесу
- Розуміння наявних потужностей IT
- Створення схеми визначення пріоритетів стосовно бізнес-цілей, у якій в кількісній формі надані бізнес-вимоги

та вимірюється

- Відсотком IT цілей, зазначених в стратегічному плані розвитку IT, які підтримують стратегічний бізнес-план
- Відсотком IT проектів, зазначених у портфелі IT проектів, які можна безпосередньо знайти у тактичних планах розвитку IT
- Відставанням між оновленням стратегічного плану розвитку IT та оновленням тактичного плану розвитку IT



Цілі контролю

PO1 Розробляти стратегічний план розвитку IT

PO1.1 Управління цінністю IT
Працювати з бізнес-підрозділами над забезпеченням того, щоб портфель інвестицій організації в IT містив програми, які мають переконливе економічне обґрунтування. Визнавати, що існують обов'язкові та підтримуючі інвестиції, які відрізняються між собою за комплексністю та ступенем свободи з точки зору розподілу коштів. IT процеси повинні забезпечувати ефективну та результативну експлуатацію IT компонент програм та заздалегідь попереджувати про будь-які відхилення від плану дотримання графіку або функціонування (в тому числі у відношенні витрат), які можуть вплинути на очікувані кінцеві результати програм. IT послуги повинні надаватись згідно із справедливими та здійсненними угодами про гарантований рівень послуг (SLA). Підзвітність щодо отримання вигод та контролювання витрат необхідно чітко визначати та контролювати. Запровадити чесну, прозору, відтворювану та порівнянну процедуру оцінювання економічних обґрунтувань, в тому числі фінансової вартості, ризику, пов'язаного з ненаданням потужностей та ризику, обумовленого неотриманням очікуваних вигод.

PO1.2 Узгодження питань у сфері бізнесу та IT
Запровадити процеси, що передбачають двостороннє навчання та взаємну участь у стратегічному плануванні з метою узгодження та інтеграції у сфері бізнесу та IT. Добиватись того, щоб пріоритети у сфері бізнесу та IT були взаємно узгоджені.

PO1.3 Оцінка поточних потужностей та результатів
Оцінювати поточні потужності та результати надання рішень та послуг з метою встановлення базису, з яким можна буде порівнювати подальші вимоги. Визначити результати, виходячи з внеску IT до реалізації бізнес цілей, функціонування, стабільності, комплексності, витрат, сильних та слабких сторін.

PO1.4 Стратегічний план розвитку IT
Створити стратегічний план, в якому визначити, разом із зацікавленими сторонами, як саме IT цілі будуть сприяти реалізації стратегічних цілей організації, а також відобразити пов'язані з цим витрати та ризики. В плані слід вказати, як IT будуть підтримувати інвестиційні програми IT, IT послуги та IT активи. IT підрозділи мають визначити, як будуть досягнуті вказані цілі, які вимірювання будуть проводитись та якими будуть процедури офіційного узгодження з боку зацікавлених сторін. В стратегічний план розвитку IT мають бути внесені питання, пов'язані з кошторисом інвестицій, кошторисом поточних витрат, джерелами фінансування, стратегією вибору постачальників, стратегією закупок, а також з дотриманням вимог діючого законодавства та регулятивних органів. Стратегічний план має бути достатньо детальним, щоб на його основі можна було скласти тактичні плани розвитку IT.

PO1.5 Тактичні плани розвитку IT
Сформувати портфель тактичних планів розвитку IT на основі стратегічного IT плану. Тактичні плани повинні стосуватись програм інвестицій в IT, IT послуг та IT активів. В тактичних планах слід описати необхідні IT ініціативи, вимоги до ресурсів, а також способи моніторингу та управління використанням цих ресурсів й досягненням вигод. Тактичні плани мають бути достатньо детальними для створення на їх основі планів проектів. Активно управляти сукупністю тактичних планів розвитку IT та ініціатив шляхом аналізу портфелів проектів та послуг.

PO1.6 Управління портфелем IT
Здійснювати активне управління з боку бізнес-підрозділів портфелем програм, що стосуються інвестицій в IT, передбаченим для досягнення конкретних стратегічних бізнес – цілей, шляхом ідентифікації, визначення, оцінювання, встановлення пріоритетів, вибору, ініціації, програм для управління та контролю. При цьому необхідно чітко визначити бажані кінцеві результати в сфері бізнесу, надати гарантії, що цілі програм підтримують досягнення бажаних результатів, розуміти повний обсяг зусиль, які потрібні для досягнення бажаних кінцевих результатів, встановити підзвітність із залученням відповідних засобів, окреслити проекти в межах програми, розподілити ресурси та кошти, делегувати повноваження та визначитись щодо здачі проекту, приступаючи до виконання програми.

Керівні принципи управління

PO1 Розробляти стратегічний план розвитку IT

Від	Вхідні дані
PO5	Звіти щодо витрат та результатів
PO9	Оцінка ризиків
PO10	Оновлений портфель IT проектів
DS1	Нові/оновлені вимоги до послуг; Оновлений портфель IT послуг
*	Бізнес-стратегія та пріоритети
*	Портфель програм
ME1	Вхідні дані щодо ефективності для IT планування
ME4	Звіт стосовно стану справ в управлінні IT; стратегічний напрямок організації в розвитку IT

Вихідні дані	Для					
Стратегічний план розвитку IT	PO2...PO6		PO8	PO9	AI1	DS1
Тактичні плани розвитку IT	PO2...PO6		PO9	AI1	DS1	
Портфель IT проектів	PO5	PO6	PO10	AI6		
Портфель IT послуг	PO5	PO6	PO9	DS1		
Стратегія вибору постачальників IT	DS2					
Стратегія закупок у сфері IT	AI5					

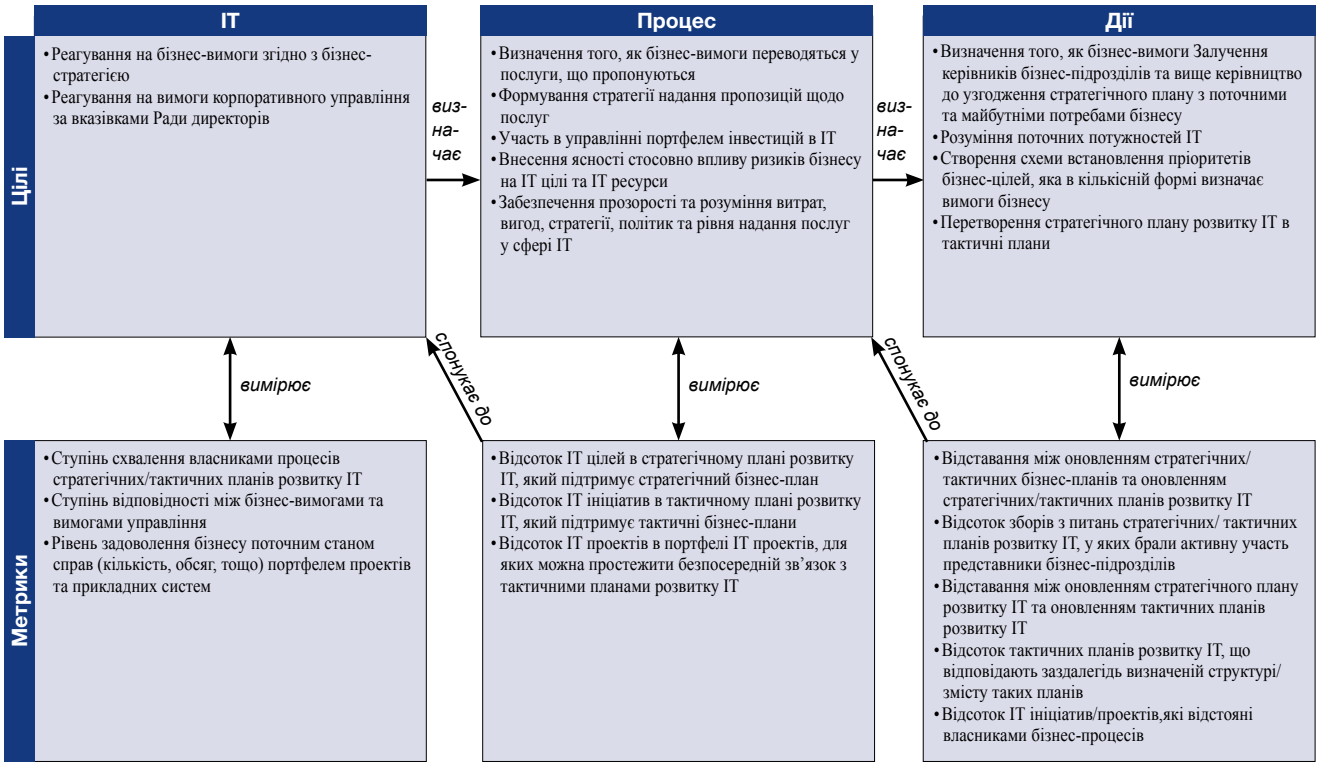
* Вхідні ресурси, що надходять з джерел поза межами стандарту CobiT®.

RACI-діаграма

Дії \ Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Встановлення зв'язку бізнес-цілей з цілями IT.	C	I	A/R	R	C						
Встановлення зв'язку бізнес-цілей з цілями IT.	C	C	R	A/R	C	C	C	C	C		C
Визначення критичних залежностей та поточну ефективність.	A	C	C	R	I	C	C	C	C	I	C
Складання тактичних планів розвитку IT.	C	I		A	C	C	C	C	C	R	I
Аналіз портфелів програм та управління портфелями проектів та послуг.	C	I	I	A	R	R	C	R	C	C	I

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).

Цілі та метрики



Модель зрілості

PO1 Розробляти стратегічний план розвитку IT

Рівні зрілості управління процесом *«Розробляти стратегічний план розвитку IT»*, які задовольняють бізнес-вимоги до IT стосовно *виконання або перевершення бізнес-стратегії та вимог управління та водночас є прозорими з точки зору вигод, витрат та ризиків*, знаходиться на рівні зрілості:

0 Не існуючий, якщо
Стратегічне планування у сфері розвитку IT не здійснюється. Керівництво не усвідомлює необхідності стратегічного планування розвитку IT з метою підтримки бізнес-цілей.

1 Початковий, якщо
Керівники IT-підрозділів розуміють необхідність стратегічного планування у сфері розвитку IT. IT планування здійснюється в залежності від потреби у відповідь на конкретні бізнес-вимоги. Стратегічні плани розвитку IT час від часу обговорюються під час зібрань керівників IT-підрозділів. Узгодження бізнес-вимог та прикладних систем і технологій відбувається у відповідь на конкретну потребу та не є стратегією, прийнятою в масштабах організації. Стратегічна позиція відносно ризиків визначається довільно для кожного конкретного проекту.

2 Повторюваний але інтуїтивний, якщо
Стратегічне планування в сфері розвитку IT здійснюється спільно з керівниками бізнес-підрозділів в залежності від потреби. Оновлення IT планів відбувається у відповідь на вимогу керівництва. Стратегічні рішення приймаються для кожного проекту окремо, відповідна стратегія в масштабах всієї організації відсутня. Ризики та вигоди користувачів у випадку важливих стратегічних рішень усвідомлюються на інтуїтивному рівні..

3 Визначений, якщо
Політика визначає, коли та як здійснювати стратегічне планування розвитку IT. У стратегічному плануванні розвитку IT задіяний підхід із заданою структурою , який є документованим та відомим всьому персоналу. Процес IT планування є достатньо чітким та гарантує можливість складання належного плану. Однак, окремим керівникам надано свободу дій стосовно впровадження цього процесу, при цьому відсутні процедури, призначені для вивчення процесу. Загальна стратегія розвитку IT передбачає послідовну оцінку ризиків, які організація приймає на себе як новатор або послідовник. Стратегічний підхід до вирішення фінансових, технічних та кадрових питань у сфері IT все більше спонукає до закупок нових продуктів та технологій. Питання стратегічного планування розвитку IT обговорюються на нарадах керівництва бізнес-підрозділів.

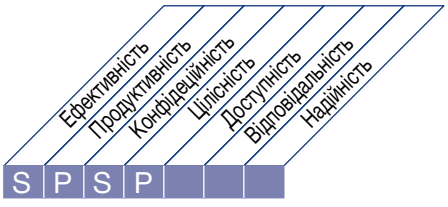
4 Керований та вимірюваний, якщо
Стратегічне планування у сфері розвитку IT є стандартною практикою, а нестандартні ситуації відстежуються керівництвом. Стратегічне планування розвитку IT є визначеною функцією керівництва на найвищому рівні Керівництво здатне контролювати процес стратегічного планування розвитку IT, приймати рішення, що ґрунтуються на наявній інформації та вимірювати його ефективність. Складаються короткострокові та довгострокові плани розвитку IT, які доводяться до відома працівників на всіх рівнях організації, у разі потреби ці плани оновлюються. Стратегія у сфері розвитку IT та загальна стратегія організації стають все більше узгодженими внаслідок приведення у відповідність бізнес-процесів та потужностей з додатковими можливостями, а також розширеного використання прикладних систем та технологій в результаті реінжинірингу бізнес-процесів. Існує чітко визначений процес використання внутрішніх та зовнішніх ресурсів, які потрібні для розробки та експлуатації систем.

5 Оптимізований, якщо
Стратегічне планування розвитку IT є документованим, активно діючим процесом; воно завжди береться до уваги в ході визначення бізнес-цілей; в результаті помітно підвищується цінність бізнесу внаслідок інвестицій в IT. В процесі стратегічного планування розвитку IT постійно вдосконалюються підходи до врахування ризиків та підвищення цінності. Розробляються реалістичні довгострокові плани розвитку IT, які постійно оновлюються з урахуванням змін у технологіях та вдосконалень, пов'язаних з бізнесом. Здійснюється порівняльний аналіз результатів діяльності (бенчмаркінг) з добре відомими та надійними стандартами, що діють в галузі. Його інтегровано у процес формування стратегії. Стратегічний план включає спосіб, у який нові технологічні розробки можуть стимулювати створення нових можливостей для бізнесу та підвищити конкурентоздатність організації.

Опис процесу

PO2 Формувати архітектуру інформації

Призначенням інформаційних систем є створення та регулярне оновлення моделі бізнес-інформації, а також визначення належних систем для оптимізації використання вказаної інформації. Це передбачає розробку корпоративного словника даних з відповідними правилами синтаксису даних організації, схеми класифікації інформації та рівнів її безпеки. Цей процес дозволяє підвищити якість процедури прийняття рішень за допомогою надання гарантій, що надається надійна та захищена інформація, і при цьому можна раціоналізувати ресурси інформаційних систем так, щоб вони належним чином узгоджувались з бізнес-стратегіями. Цей IT процес також необхідний для посилення індивідуальної відповідальності за цілісність та безпеку інформації, а також для підвищення ефективності та контролю спільного використання інформації прикладними системами та підрозділами організації.



Контроль IT процесу

Формувати архітектуру інформації

який задовольняє бізнес-вимоги до IT, а саме:

швидке реагування на вимоги для забезпечення надійності та узгодженості інформації, а також тісної інтеграції прикладних систем в бізнес-процеси

зосереджений на

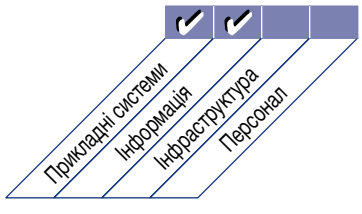
створенні моделі даних організації, яка включає схему класифікації інформації для гарантії цілісності та узгодженості усіх даних

реалізується шляхом

- Гарантування точності архітектури інформації та моделі даних
- Визначення власників даних
- Класифікації інформації з використанням узгодженої схеми класифікації

та вимірюється

- Відсотком надлишкових/продублюваних елементів даних
- Відсотком прикладних систем, що не відповідають методології побудови архітектури інформації, які використовуються в організації
- Частотою дій з перевірки правильності даних



PO2 Формувати архітектуру інформації

PO2.1 Модель архітектури інформації
Побудувати та підтримувати модель інформації організації для отримання можливості розробки прикладних систем та діяльності, що супроводжує прийняття рішень, яка відповідає IT планам, описаним в розділі PO1. Ця модель повинна полегшити процес створення, використання та обміну інформацією бізнес-підрозділами у спосіб, який забезпечує збереження цілісності та є гнучким, функціональним, рентабельним, сучасним , безпечним та стійким по відношенню до відмов.

PO2.2 Словник даних організації та правила синтаксису даних
Підтримувати в належному стані словник даних організації, до якого входять правила синтаксису даних організації. Цей словник повинен забезпечувати можливість обміну елементами даних між прикладними програмами та системами, сприяти загальному розумінню інформації його користувачами з IT служб та бізнес-підрозділів, а також перешкоджати створенню несумісних елементів даних.

PO2.3 Схема класифікації даних
Запровадити схему класифікації даних, яка застосовується в масштабах всієї організації, на основі критичності та чутливості даних організації (наприклад, загальнодоступна, конфіденційна інформація, дані з грифом «цілком таємно»). Ця схема повинна містити відомості щодо права власності на дані, визначення належних рівнів безпеки та заходів захисту інформації, а також короткий опис вимог до збереження даних та їх знищення, їх критичності та чутливості. Цю схему слід покласти в основу застосування таких заходів контролю як контроль доступу, архівація даних або їх шифрування.

PO2.4 Управління цілісністю інформації
Створити та запровадити процедури, що гарантують цілісність та узгодженість всіх даних, що зберігаються в електронній формі, наприклад, у вигляді баз даних, сховищ даних та архівів даних.

Керівні принципи управління

PO2 Формувати архітектуру інформації

Від	Вхідні дані
PO1	Стратегічний та тактичні плани розвитку IT
AI1	Аналіз можливості виконання бізнес вимог
AI7	Аналіз функціонування систем
DS3	Інформація стосовно ефективності і потужності
ME1	Вхідні дані щодо ефективності для IT планування

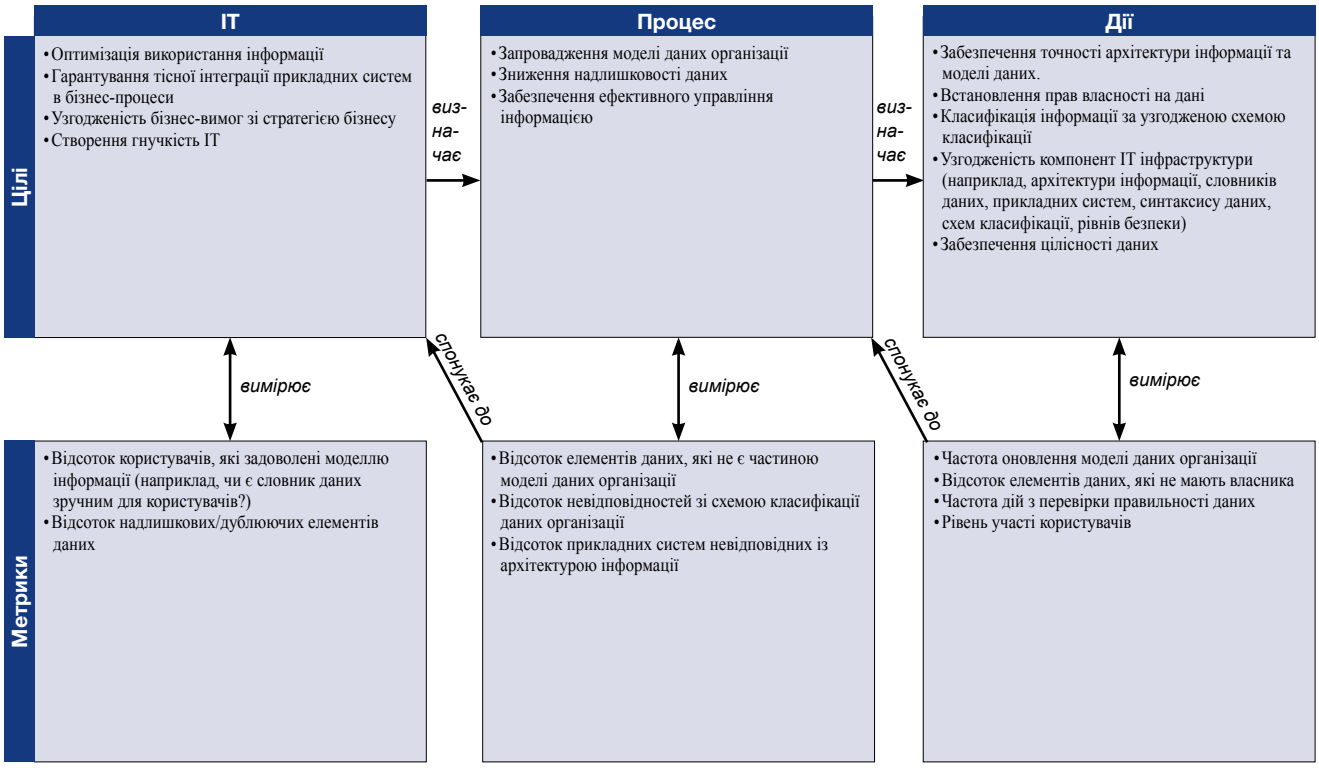
Вихідні дані	Для					
Схема класифікації даних	AI2					
Оптимізований план бізнес-систем	PO3	AI2				
Словник даних	AI2	DS11				
Архітектура інформації	PO3	DS5				
Визначення класифікації даних постачальників IT	DS1	DS4	DS5	DS12		
Класифікація процедур та інструментів	*					

* Вихідні дані знаходяться поза межами стандарту CobiT®.

RACI-діаграма

Дії \ Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Створення та підтримка моделі інформації корпорації/підприємства.		C	I	A	C		R	C	C		C
Створення та підтримка корпоративного словника (-ків) даних.					I	C		A/R	R		C
Розроблення та підтримка схеми класифікації даних.	I	C	A	C	C	I	C	C			
Забезпечення власників даних процедурами та інструментами для класифікованих інформаційних систем	I	C	A	C	C	I	C	C			
Аналіз портфелів програм та управління портфелями проектів та послуг.	C	C	I	A	C		R	C			

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

PO2 Формувати архітектуру інформації

Управління процесом *«Формувати архітектуру інформації»*, що задовольняє бізнес-вимогу до IT стосовно *здатності IT до гнучкого реагування на вимоги з метою забезпечення надійної та несуперечливої інформації, а також щільної інтеграції прикладних систем в бізнес-процеси*, знаходиться на рівні зрілості:

0 Не існуючий, якщо
Відсутнє розуміння важливості створення архітектури інформації в організації. Організація не має знань, досвіду та розподілу обов'язків, необхідних для розробки цієї архітектури.

1 Початковий, якщо
Керівництво визнає необхідність створення архітектури інформації. Розробка деяких елементів архітектури інформації відбувається несистематично. Ці рішення стосуються даних, а не інформації, та основуються на пропозиціях постачальників прикладного програмного забезпечення.. Комунікації щодо потреби в архітектурі інформації мають неузгоджений та несистематичний характер.

2 Повторюваний але інтуїтивний, якщо
Зароджується процес побудови архітектури інформації, і окремі особи в організації виконують відповідні, хоча і неформальні та інтуїтивні функції. Персонал отримує досвід з побудови архітектури інформації за допомогою практичної роботи та методик для повторного застосування прикладних систем. Тактичні вимоги стимулюють розробку елементів архітектури інформації окремими працівниками.

3 Визначений, якщо
Важливість побудови архітектури інформації розуміють та визнають в організації, обов'язки щодо її створення розподілені, існує чітка схема комунікацій з цього питання. Відповідні процедури, інструменти та методики, хоча й не є ретельно розробленими, але стандартизовані та задокументовані, і використовуються для неформального навчання. Розроблені базові політики в області архітектури інформації, в тому числі деякі стратегічні вимоги, але дотримання політик, стандартів та методів не є послідовним. Впроваджено формально визначена функція адміністрування даних, яка встановлює стандарти в масштабах всієї організації, та починається звітування стосовно забезпечення та використання архітектури інформації. Починають застосуватися автоматизовані інструменти, але процеси та правила, що використовуються, визначаються згідно з пропозиціями постачальника програмного забезпечення баз даних. Розроблено формальний план навчання, але формалізоване навчання все ще базується на ініціативі окремих осіб.

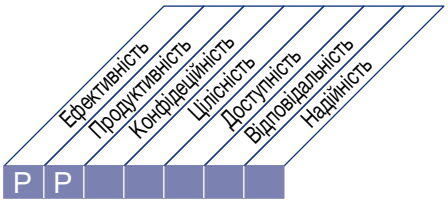
4 Керований та вимірюваний, якщо
Процес побудови структури інформації та її використання повністю підтримуються формалізованими методами та процедурами. Запроваджено підзвітність стосовно ефективності процесу розробки архітектури, вимірюються позитивні результати впровадження архітектури інформації. Широко застосовуються автоматизовані інструменти, але все ще немає їх інтеграції. Визначені базові метрики, впроваджену систему вимірювань. Процес формування архітектури інформації є проактивним та орієнтованим на майбутні потреби бізнесу. З метою забезпечення узгодженості служба адміністрування даних бере активну участь у всіх заходах з розробки прикладних систем. Повністю запроваджено автоматизований архів даних. З метою максимально вигідного використанні інформаційного вмісту баз даних впроваджуються більш складні моделі даних . У правлінські інформаційні системи та системи підтримки прийняття рішень максимально вигідно використовують доступну інформацію.

5 Оптимізований, якщо
Архітектура інформації послідовно запроваджується на всіх рівнях. Постійно наголошується цінність архітектури інформації для бізнесу. IT персонал має досвід та кваліфікацію, необхідні для розробки та підтримки у робочому стані стійкої по відношенню до збоїв та гнучкої архітектури інформації, яка відображає всі бізнес-вимоги. Інформація, яка забезпечується архітектурою інформації, послідовно та широко застосовується. В процесі розробки та підтримки архітектури інформації систематично та широко використовуються найкращі галузеві практики, в тому числі постійно триває процес внесення вдосконалень. Існує стратегія максимально вигідного використання інформації за допомогою сховищ даних та масивів даних. Архітектура інформації постійно вдосконалюється та враховує нестандартну інформацію стосовно процесів, організацій та систем.

Опис процесу

PO3 Визначати технологічний напрямок

Функція надання інформаційних послуг визначає технологічний напрямок підтримки бізнесу. Це потребує створення плану технологічної інфраструктури та ради з питань архітектури, яка визначає та керує чіткими та реалістичними очікуваннями того, що технології можуть запропонувати з точки зору програмних продуктів, послуг та механізмів їх забезпечення. Цей план регулярно оновлюється та охоплює такі аспекти, як архітектури систем, технологічний напрямок, плани закупок, стандарти, стратегії міграції та непередбачені обставини. Результатом є своєчасне реагування на зміни в конкурентному оточенні, економія за рахунок масштабів кадрового забезпечення та інвестицій в інформаційні системи, а також здатність до взаємодії платформ та прикладних систем.



Контроль IT процесу

Визначати технологічний напрямок

який задовольняє бізнес-вимоги до IT, а саме:

наявність стабільних, рентабельних, інтегрованих та стандартизованих прикладних систем, ресурсів та потужностей, які відповідають сьогоденним та майбутнім бізнес-вимогам

зосереджений на

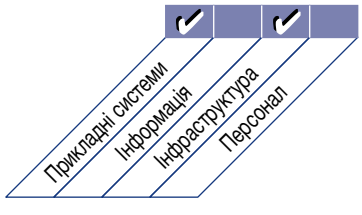
створенні та впровадженні плану побудови технологічної інфраструктури, архітектури та стандартів, які розпізнають та ефективно використовують технологічні потужності

реалізується шляхом

- Заснування органу для керування архітектурою та перевірки її відповідності
- Виконання плану технологічної інфраструктури, який є збалансованим з точки зору витрат, врахування ризиків та дотримання вимог
- Встановлення стандартів технологічної інфраструктури на основі вимог до архітектури інформації

та вимірюється

- Кількістю та характером відхилень від плану технологічної інфраструктури
- Частотою перегляду/оновлення плану технологічної інфраструктури
- Кількістю технологічних платформ, що функціонують в організації



Цілі контролю

PO3 Визначати технологічний напрямок

PO3.1 Планування технологічного напрямку
Проаналізувати наявні та перспективні технології і скласти план, в якому визначити який технологічний напрямок є прийнятним для реалізації стратегії розвитку IT та архітектури бізнес-систем. В цьому плані також вказати, які технології можуть забезпечити можливості для бізнес діяльності. В цьому плані слід приділити увагу витанням, пов'язаним з архітектурою систем, технологічним напрямком, стратегіями міграції а також із забезпеченням безперервної роботи та відновленням функціонування компонент інфраструктури..

PO3.2 План технологічної інфраструктури
Створити та підтримувати план технологічної інфраструктури, який відповідає стратегічним та тактичним планам розвитку IT. В основу плану слід покласти технологічний напрямок та включити заходи із забезпечення безперервної роботи та відновлення функціонування, а також вказівки щодо придбання технологічних ресурсів. Слід також врахувати зміни в конкурентному оточенні, економію за рахунок масштабів кадрового забезпечення та інвестицій в інформаційні системи, а також покращення інтероперабельності платформ та прикладних систем.

PO3.3 Моніторинг подальших перспектив та нормативних вимог
Запровадити процес, що дозволяє слідкувати за змінами у сфері бізнесу, галузі, технологій, інфраструктурі, законодавчої та нормативно-правовій базі. Враховувати наслідки цих змін при розробці плану технологічної інфраструктури IT.

PO3.4 Технологічні стандарти
З метою забезпечення узгоджених, ефективних та надійних технологічних рішень в масштабах всієї організації заснувати технологічний форум, який надаватиме напрямки щодо застосування технологій, рекомендації стосовно об'єктів інфраструктури та визначатиме основні принципи вибору технології, а також здійснюватиме оцінку відповідності вказаним стандартам та напрямкам. Цей форум повинен застосовувати технологічні стандарти та практики, виходячи з їх застосовності у бізнесі, ризиків та відповідності зовнішнім вимогам.

PO3.5 Рада з питань IT архітектури
Заснувати Раду з питань IT архітектури, яка повинна визначати напрямки побудови архітектури та надавати рекомендації щодо їх застосування, а також здійснювати перевірку їх дотримання. Цей орган повинен керувати розробкою IT архітектури, для забезпечення можливості реалізації бізнес-стратегії та гарантування дотримання вимог регулюючих органів та вимог до забезпечення неперервності. Цей процес пов'язаний з процесом PO2 *«Формування архітектури інформації»*.

Керівні принципи управління

PO3 Визначати технологічний напрямок

Від	Вхідні дані
PO1	Стратегічний та тактичні плани розвитку IT
PO2	Оптимізований план бізнес-систем, архітектури інформації
AI3	Оновлення технологічних стандартів
DS3	Інформація стосовно ефективності і потужностей

Вихідні дані	Для					
Технологічні можливості	AI3					
Технологічні стандарти	AI1	AI3	AI7	DS5		
Регулярні оновлення стану технологій	AI1	AI2	AI3			
План технологічної інфраструктури	AI3					
Вимоги до інфраструктури	PO5					

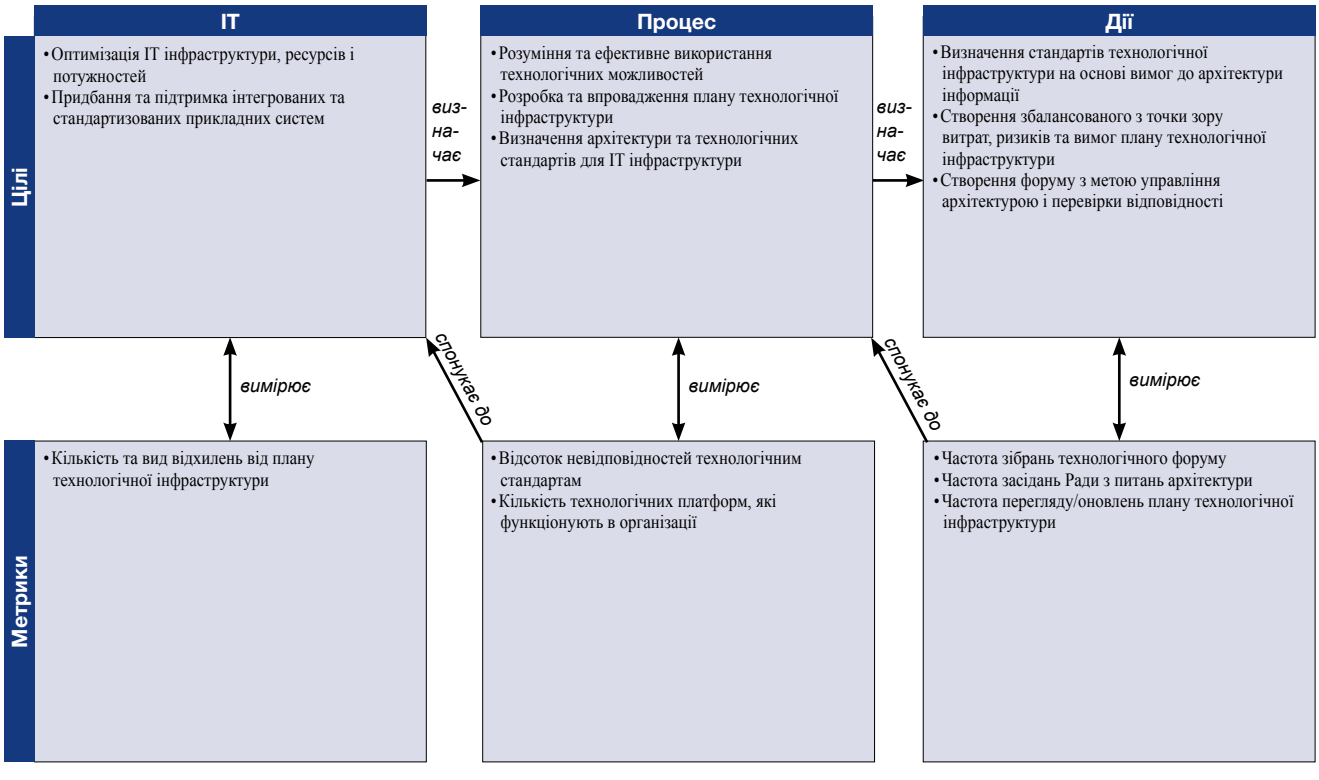
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Створення та підтримка технологічного плану інфраструктури		I	I	A		C	R	C	C		C
Створення та підтримка технологічних стандартів				A		C	R	C	I	I	I
Оприлюднення технологічних стандартів		I	I	A		I	R	I	I	I	I
Моніторинг технологічних змін		I	I	A		C	R	C		C	C
Визначення (майбутнього) (стратегічного) використання нових технологій		C	C	A		C	R	C		C	C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

PO3 Визначати технологічний напрямок

Управління процесом *«Визначати технологічний напрямок»*, що задовольняє бізнес-вимогу до IT, яка полягає в тому, щоб *«Мати стабільні, рентабельні, інтегровані та стандартизовані прикладні системи, ресурси та потужності, які відповідають сьогоденним та майбутнім бізнес-вимогам»* знаходиться на рівні зрілості:

0 Не існуючий, якщо
Відсутнє розуміння важливості планування технологічної інфраструктури в організації. Немає знань та досвіду, необхідних для розробки плану технологічної інфраструктури. Відсутнє розуміння того, що планування технологічних змін є дуже важливим для ефективного розподілу ресурсів.

1 Початковий, якщо
Керівництво визнає необхідність планування технологічної інфраструктури . Розробка компонентів технології та впровадження перспективних технологій здійснюються спеціально в кожному окремому випадку та не носить системний характер. Планування є реактивним та орієнтованим на інфраструктуру. Технологічні напрямки визначаються часто суперечливими планами розвитку апаратного забезпечення, а також системного та прикладного програмного забезпечення розробників. Комунікації щодо потенційного впливу технологічних змін є непослідовними та неузгодженими.

2 Повторюваний але інтуїтивний, якщо
Необхідність та важливість планування технологічної інфраструктури обговорюється. Планування носить тактичний характер та зосереджується на створенні рішень технічних проблем, а не на використанні технології, яка б задовольняла потреби бізнесу. Оцінку технологічних змін здійснюють різні окремі особи, які виконують інтуїтивні, але подібні процедури. Працівники набувають досвіду у сфері технологічного планування на практиці та в результаті багатократного застосування методик. Формуються загальні методики та стандарти, які застосовуються у розробці компонент інфраструктури.

3 Визначений, якщо
Керівництво усвідомлює важливість розробки плану технологічної інфраструктури. Процес розробки плану технологічної інфраструктури є достатньо добре організованим та узгодженим із стратегічним планом розвитку IT. Існує визначений, задокументований та узгоджений план технологічної інфраструктури, але застосовується непослідовно. Напрямки розвитку технологічної інфраструктури включають розуміння того, що саме організація прагне для випередження або відставання у використанні технологій, виходячи з оцінки ризиків та дотримання стратегії організації.. Вибір ключових постачальників здійснюється на підставі розуміння їх дострокових планів розробки технологій та продукції з врахуванням напрямку розвитку організації. Має місце формальне навчання та обговорення ролей та обов'язків.

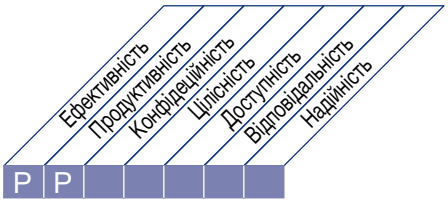
4 Керований та вимірюваний, якщо
Керівництво організації забезпечує розробку та виконання плану технологічної інфраструктури. Працівники IT підрозділів мають досвід та кваліфікацію, необхідні для розробки плану технологічної інфраструктури. Враховується можливий вплив змін у технологіях та появи нових технологій. Керівництво може виявити відхилення від плану та передбачити можливі проблеми.. зазначений розподіл обов'язків та відповідальності за розробку та дотримання плану технологічної інфраструктури. Процес розробки плану технологічної інфраструктури є ретельно продуманим, передбачено можливість внесення змін до нього. Застосовуються внутрішні найкращі практики. Стратегію у сфері кадрової політики узгоджено з напрямком розвитку технологій з тим, щоб працівники IT підрозділів могли керувати змінами у технологіях. Визначено плани міграції з метою впровадження нових технологій. Для отримання необхідного досвіду та експертизи ефективно використовуються послуги сторонніх організації та партнерські стосунки. Керівництво аналізує ризики, пов'язані із застосуванням технологій з випередженням або з запізненням в ході розроблення нових бізнес-можливостей або підвищення ефективності оперативної діяльності.

5 Оптимізований, якщо
Виконуються дослідження технологій, що виникають та розвиваються, а також здійснює порівняльний аналіз результатів діяльності організації з нормами, що існують в галузі. Напрямок створення плану технологічної інфраструктури визначається промисловими та міжнародними стандартами та розробками, а не вказівками постачальників технологій. Аналіз потенційного впливу змін у технологіях на бізнес здійснюється керівництвом на найвищому рівні. Існує процедура формального затвердження на рівні керівництва напрямків впровадження нових технологій та внесення змін до тих, що вже застосовуються. Організація має повноцінний план технологічної інфраструктури, який відображає вимоги, продиктовані бізнесом, здатний до пристосування до змін, що відбуваються в умовах ведення ділової діяльності, та до відповідної модифікації. Існує безперервний та виконуваний процес для покращення плану технологічної структури. Під час визначення технологічних напрямків використовуються кращі галузеві практики.

Опис процесу

PO4 Формувати процеси, організацію та взаємозв'язки для IT

Організація IT визначається шляхом врахування вимог до персоналу, рівня його кваліфікації, функцій, підзвітності, повноважень, ролей та обов'язків, контролю. Така організація вбудовується в структуру IT процесу, що гарантує прозорість та наявність контролю, а також залучення вищого керівництва та керівників бізнес-підрозділів. Комітет з питань стратегії забезпечує нагляд та контроль за IT з боку Ради директорів, а один або декілька координаційних комітетів , до складу яких входять працівники бізнес- та IT-підрозділів, визначають пріоритети IT ресурсів з урахуванням потреб бізнесу. Процеси, адміністративні політики та процедури запроваджено у відношенні всіх функцій, особливу увагу приділено функціям контролю, гарантії якості, управлінню ризиками, інформаційній безпеці, праву власності на дані та системи, а також розділенню обов'язків. Щоб забезпечити своєчасну підтримку потреб бізнесу, IT-спеціалісти повинні бути залучені до відповідних процесів прийняття рішень.



Контроль IT процесу

Формувати процеси, організацію та взаємозв'язки для IT

який задовольняє бізнес-вимоги до IT, а саме:

швидке реагування на бізнес-стратегію, в той самий час відповідність вимогам корпоративного управління та забезпечення можливості контакту з чітко визначеними та компетентними особами

зосереджений на

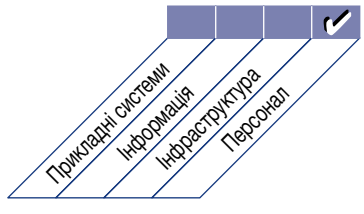
створенні прозорих, гнучких та швидко реагуючих організаційних IT структур та визначенні та впровадженні IT процесів з власниками, розподілом ролей та обов'язків, які інтегровані у бізнес-процеси та процеси прийняття рішень

реалізується шляхом

- Визначення структури IT процесу
- Формування відповідних організаційних органів та структури
- Розподілу ролей та обов'язків

та вимірюється

- Відсотком ролей з документованими посадами та описом повноважень
- Кількістю бізнес-підрозділів/процесів, які не мають підтримки у вигляді IT організації, але повинні її мати відповідно до стратегії організації
- Кількістю ключових видів IT діяльності за межами IT організації, які не затверджені або не регламентуються стандартами IT організації



Цілі контролю

PO4 Формувати процеси, організацію та взаємозв'язки для IT

PO4.1 Структура IT процесу
Визначити структуру IT процесу з метою виконання стратегічного плану розвитку IT. Ця структура повинна включати структуру IT процесу та зв'язки (наприклад, для того, щоб керувати проміжками між процесами та їх взаємним накладенням), право власності, передбачати оцінку зрілості, вимірювання результатів, можливість вдосконалень, відповідність існуючим вимогам, виконання завдань з якості та включати плани, які необхідно реалізувати. Вона повинна забезпечити взаємну інтеграцію процесів, характерних для IT, процесів, що стосуються управління портфелем організації, бізнес-процесів та процесів, що стосуються змін у операційній діяльності. Структуру IT процесів слід інтегрувати в систему управління якістю (QMS) та в систему внутрішнього контролю.

PO4.2 Комітет з питань IT стратегії
Заснувати комітет з питань стратегії розвитку IT на рівні Ради директорів. Цей комітет повинен забезпечити належне управління IT в межах корпоративного управління, обговорювати стратегічний напрямок розвитку організації та аналізувати здійснення основних інвестицій від імені Ради. Директорів.

PO4.3 Координаційний комітет з питань IT
Заснувати координаційний комітет з питань IT (або аналогічний орган), до складу якого входять представники вищого виконавчого керівництва, керівники бізнес- та IT підрозділів з метою:
- встановлення пріоритетів у виконання інвестиційних програм, пов'язаних з IT, у відповідності до бізнес-стратегії організації та пріоритетних напрямків діяльності
- контролю за ходом виконання проектів та врегулювання конфлікту ресурсів
- моніторингу рівня надання послуг та їх вдосконаленням

PO4.4 Місце IT служби в організаційній структурі
Ввести IT службу в загальну організаційну структуру, керуючись бізнес – моделлю в залежності від ступеню важливості IT для організації, зокрема, від важливості IT для реалізації стратегії організації та ступеню залежності функціонування організації від IT. Підпорядкування директора з інформаційних технологій (CIO) повинно відповідати ступеню важливості IT для організації.

PO4.5 Організаційна структура IT
Створити внутрішню та зовнішню організаційну структуру IT, яка відображає потреби бізнесу. Крім того, впровадити процедуру періодичного перегляду організаційної структури IT з метою коригування потреб у комплектуванні кадрів та стратегії пошуку постачальників та партнерів, які мають відповідати очікуваним бізнес-цілям та змінам умов та обставин.

PO4.6 Розподіл ролей та обов'язків
Здійснити розподіл ролей та обов'язків IT персоналу та кінцевих користувачів (та довести його до відома), який розмежовує повноваження, відповідальність та підзвітність IT персоналу та кінцевих користувачів відповідно до потреб організації .

PO4.7 Забезпечення гарантії якості IT
Визначити відповідальність за ефективність забезпечення гарантії якості (QA) та створити групу з питань гарантії якості, яка володіє належним досвідом у сфері роботи із системами гарантії якості, засобами контролю та комунікацій. Гарантувати, що організаційна структура, розподіл обов'язків в цій групі та її кількісний склад відповідає потребам організації.

PO4.8 Відповідальність за контроль ризиків, забезпечення безпеки та дотримання існуючих вимог
Визначити права власності та відповідальність за ризики бізнесу, пов'язані із застосуванням IT, на відповідному рівні керівництва. Визначити та розподілити ролі, які мають критичне значення для управління IT ризиками, в тому числі відповідальності за забезпечення інформаційної безпеки, фізичного захисту та дотримання існуючих вимог. На рівні організації в цілому запровадити відповідальність за управління ризиками та безпекою з метою врегулювання відповідних проблем в масштабах всієї організації. Може виникнути потреба у призначенні додаткових відповідальностей за управління безпекою на рівні конкретної системи з метою усунення відповідних проблемних питань безпеки. Отримувати настанови вищого керівництва щодо можливості виникнення ризиків, пов'язаних з IT, та позитивні рішення щодо будь-яких залишкових IT ризиків.

PO4.9 Встановлення власників систем та даних
Забезпечити бізнес-підрозділи процедурами та засобами, які дають їм змогу вирішувати питання обов'язкового

встановлення власників даних та інформаційних систем в організації. Власники повинні приймати рішення щодо класифікації інформації та систем та забезпечення їх захисту згідно з встановленою категорією.

PO4.10 Нагляд
Запровадити відповідні практики контролю та нагляду в службі IT, метою яких є гарантія належного виконання ролей та обов'язків, виявлення того, чи весь персонал має достатньо повноважень та ресурсів для виконання своїх ролей та обов'язків, а також загальний контроль ключових показників ефективності (KPI).

PO4.11 Розподіл обов'язків
Запровадити розподілення ролей та відповідальності персоналу з метою мінімізації можливостей компрометації критичних процесів з боку окремих осіб. Упевнитись, що персонал виконує тільки дозволені обов'язки, що відповідають їх робочим завданням та посадам.o, Organisation and Relationships

PO4.12 IT персонал
Здійснювати оцінку потреби у кадрах на регулярній основі або виходячи із суттєвих змін у підприємницькій діяльності, в умовах діяльності або в IT середовищі, щоб упевнитись, що IT служба має достатньо ресурсів для надання відповідної та належної підтримки у реалізації бізнес-цілей та завдань.

PO4.13 Ключовий IT персонал
Визначити та виділити ключовий IT персонал (наприклад, персонал для заміни, кадрових перестановок або додатковий персонал), та звести до мінімуму залежність від конкретної особи, яка виконує критичні операції.

PO4.14 Політики та процедури, що стосуються працівників, які працюють за контрактом
Вжити необхідних заходів для того, щоб персонал та консультанти, які працюють за контрактом та надають підтримку службі IT, знають та дотримуються політик організації стосовно захисту інформаційних активів організації у спосіб, що забезпечує виконання узгоджених умов контракту.

PO4.15 Взаємозв'язки
Забезпечити та підтримувати оптимальну схему координації, комунікації та взаємодії між IT службою та іншими зацікавленими особами всередині та зовні IT служби, такими як Рада директорів, вище керівництво, бізнес-підрозділи, окремі користувачі, постачальники, особи, відповідальні за безпеку, менеджери з ризиків, група корпоративного нагляду та контролю, сторонні постачальники послуг та керівництво прилеглими об'єктами.

Сторінку навмисне залишено вільною

Керівні принципи управління

PO4 Формувати процеси, організацію та взаємозв'язки

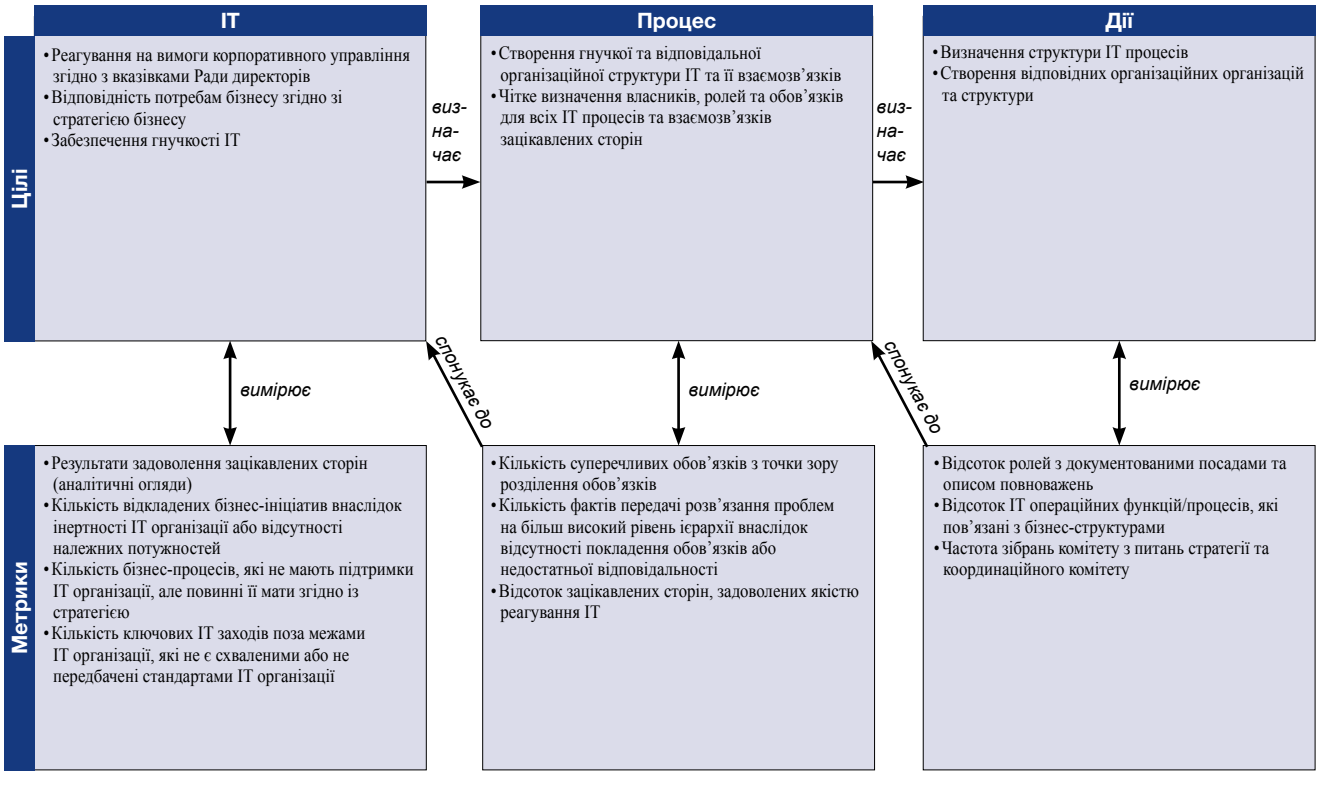
Від	Вхідні дані
PO1	Стратегічні та тактичні плани
PO7	Політики та процедури стосовно IT персоналу, матриця кваліфікації IT, посадові інструкції
PO8	Заходи з підвищення якості
PO9	Плани коригуючих заходів для IT ризиків
ME1	Плани коригуючих заходів
ME2	Звіт щодо ефективності IT контролю
ME3	Перелік законодавчих та нормативних вимог стосовно надання IT послуг
ME4	Вдосконалення структури процесів

Вихідні дані	Для					
Структура IT процесів	ME4					
Документовані власники систем	AI7	DS6				
IT організація та взаємозв'язки	PO7					
Структура IT процесів, документовані ролі та обов'язки	AI1					
Документований розподіл ролей та обов'язків	PO7					

RACI-діаграма

Дії \ Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Створення організаційної структури IT, в тому числі комітетів та взаємозв'язків із зацікавленими сторонами та постачальниками	C	C	C	A		C	C	C	R	C	I
Розроблення структури IT процесів	C	C	C	A		C	C	C	R	C	C
Визначення власників систем		C	C	A	C	R	I	I	I	I	I
Визначення власників даних		I	A	C	C	I	R	I	I	I	C
Розроблення та впровадження розподілу ролей та обов'язків, в тому числі забезпечення нагляду та розподілу обов'язків		I	I	A	I	C	C	C	R	C	C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

PO4 Формувати процеси, організацію та взаємозв'язки для IT

Управління процесом *«Формувати процеси, організацію та взаємозв'язки для IT»*, що задовольняє бізнес-вимогам до IT, полягає в тому, щоб *«IT швидко реагували на стратегію розвитку бізнесу, в той самий час відповідали вимогам до корпоративного управління та забезпечували наявність компетентних контактних осіб»* знаходиться на рівні зрілості:

0 Не існуючий, якщо
Не існує ефективної IT організації, націленої на досягнення бізнес-цілей.

1 Початковий, якщо
Дії та функції IT фахівців є реактивними та запроваджуються непослідовно. IT долучаються до бізнес-проектів лише на останньому етапі. IT фахівці виконують функцію підтримки, не маючи перспектив в масштабах всієї організації. Має місце нечітке розуміння необхідності IT організації, однак ролі та обов'язки не формалізовані та не виконуються.

2 Повторюваний але інтуїтивний, якщо
IT підрозділи організовані таким чином, що можуть реагувати швидко, але непослідовно, на потреби користувачів та взаємозв'язки постачальників. Необхідність структурованій організації та управлінню мережею постачальників послуг обговорюється, але рішення приймаються все ще в залежності від знань та досвіду окремих ключових працівників. Зароджуються універсальні методики управління IT організацією та взаємостосунками з постачальниками.

3 Визначений, якщо
Визначений розподіл ролей та обов'язків IT організації та третіх сторін. IT організацію сформовано, задокументовано, доведено до відома та узгоджено з IT стратегією. Визначено середовище внутрішнього контролю. Існує формалізація стосунків з іншими сторонами, в тому числі з координаційними комітетами , службою внутрішнього аудиту та керівництвом мережею постачальників послуг. IT організація є функціонально повною. Визначено функції, які повинен виконувати IT персонал та функції користувачів. Визначено та задоволено основну функціональної потребу в IT кадрах. Існує формальне визначення взаємостосунків з користувачами та третіми сторонами. Встановлено та впроваджено розподіл ролей та обов'язків.

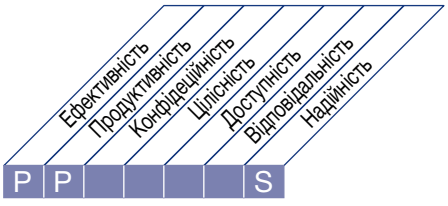
4 Керований та вимірюваний, якщо
IT організація проактивно реагує на зміни та передбачає всі ролі, необхідні для задоволення потреб бізнесу. IT управління, право власності на процеси, підзвітність та відповідальність визначені та збалансовані. В організації IT служб було застосовані найкращі власні практики. Керівництво IT служб має належний досвід та кваліфікацію, що дозволяють визначать, запроваджувати та контролювати організацію та взаємозв'язки, яким надано перевагу. Вимірювані метрики, що підтверджують реалізацію бізнес-цілей, та ключові факторі успіху (CSF), визначені та стандартизовані. Існує кваліфікаційний перелік співробітників, який використовується для комплектації проекту персоналом та з метою підвищення кваліфікації працівників. Визначено та реалізовано баланс між власними кваліфікованими спеціалістами і ресурсами та сторонніми кадрами і ресурсами, у яких є потреба. Організаційна структура IT належним чином відображає потреби бізнесу для забезпечення надання послуг відповідно до стратегічних бізнес-процесів, а не до ізольованих (відокремлений одна від одної) технологій.

5 Оптимізований, якщо
Організаційна структура IT є гнучкою та адаптивною. Застосовуються найкращі галузеві практики. Широко використовуються технології контролю ефективності IT організації та процесів. Технології ефективно використовуються на користь та відповідно до складності організаційної структури та її географічного розміщення. Постійно здійснюється процес вдосконалення та покращень.

Опис процесу

PO5 Управляти інвестиціями в IT

Створюється та підтримується схема для управління інвестиційними програмами в IT, яка вирішує питання витрат, вигод та встановлює пріоритети в межах бюджету, передбачає формальну процедуру формування бюджету та управління відповідно до бюджету. Зацікавлені сторони отримують консультації з питань визначення та контролю загальних витрат та вигод в контексті стратегічних та тактичних планів розвитку IT, а також ініціюють застосування коригувальних заходів у разі потреби. Цей процес сприяє розвитку партнерських стосунків між зацікавленими сторонами, якими є IT- та бізнес-підрозділи, забезпечує ефективне використання IT ресурсів та прозорість і відповідальність за забезпечення загальної вартості володіння (TCO), сприяє отриманню вигод від бізнесу та прибутку на інвестицію (ROI) в IT.



Контроль IT процесу

Управляти інвестиціями в IT

який задовольняє бізнес-вимоги до IT, а саме:

постійне та наочне підвищення ефективності витрат на IT та вкладу IT у підвищенні рентабельності бізнесу шляхом надання інтегрованих та стандартизованих послуг, які задовольняють очікування кінцевих користувачів

зосереджений на

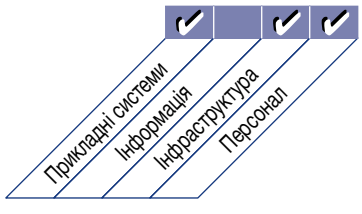
Ефективному та продуктивному інвестуванні в IT та прийнятті рішень щодо портфелю, а також шляхом формування та контролю IT-бюджетів згідно із IT стратегією та рішеннями, прийнятими стосовно інвестицій

реалізується шляхом

- Прогнозування та розподілу бюджету
- Визначення формальних критеріїв оцінки інвестицій (ROI, період окупності інвестицій, чистої теперішньої вартості (NPV))
- Вимірювання та оцінка цінності бізнесу у порівнянні з прогнозом

та вимірюється

- Відсотком зниження собівартості наданих IT послуг
- Відсотком відхилень від бюджету в порівнянні із загальним бюджетом
- Відсотком витрат на IT, виражених у чинниках, що керують цінністю бізнесу (наприклад, підвищення продажу/надання послуг внаслідок покращення зв'язків)



Цілі контролю

PO5 Управляти інвестиціями в IT

PO5.1 Схема управління фінансами
Запровадити та дотримуватись схеми управління фінансами з метою управління інвестиціями та вартістю IT активів та послуг шляхом формування портфелів інвестицій в IT, бізнес-кейсів та IT бюджетів.

PO5.2 Встановлення пріоритетів в межах бюджету IT
Впровадити процес прийняття рішень з метою визначення пріоритетів у розподілі IT ресурсів між операціями, проектами та технічним забезпеченням з метою максимального сприяння IT оптимізації, поверненню інвестицій в IT та інших IT послуг.

PO5.3 Формування IT бюджету
Визначити та запровадити практики для підготовки бюджету, який відображає пріоритети, визначені портфелем інвестиційних програм IT та передбачає поточні витрати на експлуатацію та технічне обслуговування існуючої інфраструктури. Ці практики повинні підтримувати розробку загального IT бюджету, а також формування бюджетів для окремих програм з приділенням особливої уваги IT компонентам вказаних програм.. Ці практики повинні передбачати можливість здійснення поточного перегляду, вдосконалення та затвердження загального бюджету та бюджетів окремих програм

PO5.4 Управління витратами
Запровадити процес управління витратами, що дозволяє порівнювати фактичні витрати із закладеними в бюджет. Якщо виникають відхилення від бюджету, їх слід вчасно виявляти та оцінювати вплив таких відхилень на виконання програми. Разом з особою, відповідальною за фінансування вказаної програми в організації, у разі необхідності слід вжити коригувальних заходів, а також внести поправки та уточнення до економічного обґрунтування програми.

PO5.5 Управління прибутком
Запровадити процес, що дозволяє контролювати прибутки від використання та підтримки IT потужностей. Внесок IT, що сприяє розвитку бізнесу та реалізується або як складова інвестиційних програм, передбачених в сфері IT, або в межах звичайної оперативної підтримки, слід оцінювати, задокументувати у вигляді економічного обґрунтування, узгоджувати, контролювати та звітувати. Зазначені звіти необхідно аналізувати та, у випадку існування можливості підвищення цінності внеску IT, слід визначати обсяг та перелік необхідних заходів та вживати їх. Якщо зміни, що стосуються внеску IT у розвиток бізнесу, впливають на реалізацію програми, або якщо зміни, що відбуваються в інших пов’язаних з цією програмою проектів, впливають на її виконання, необхідно внести відповідні доповнення та зміни до економічного обґрунтування.

Керівні принципи управління

PO5 Управляти інвестиціями в IT

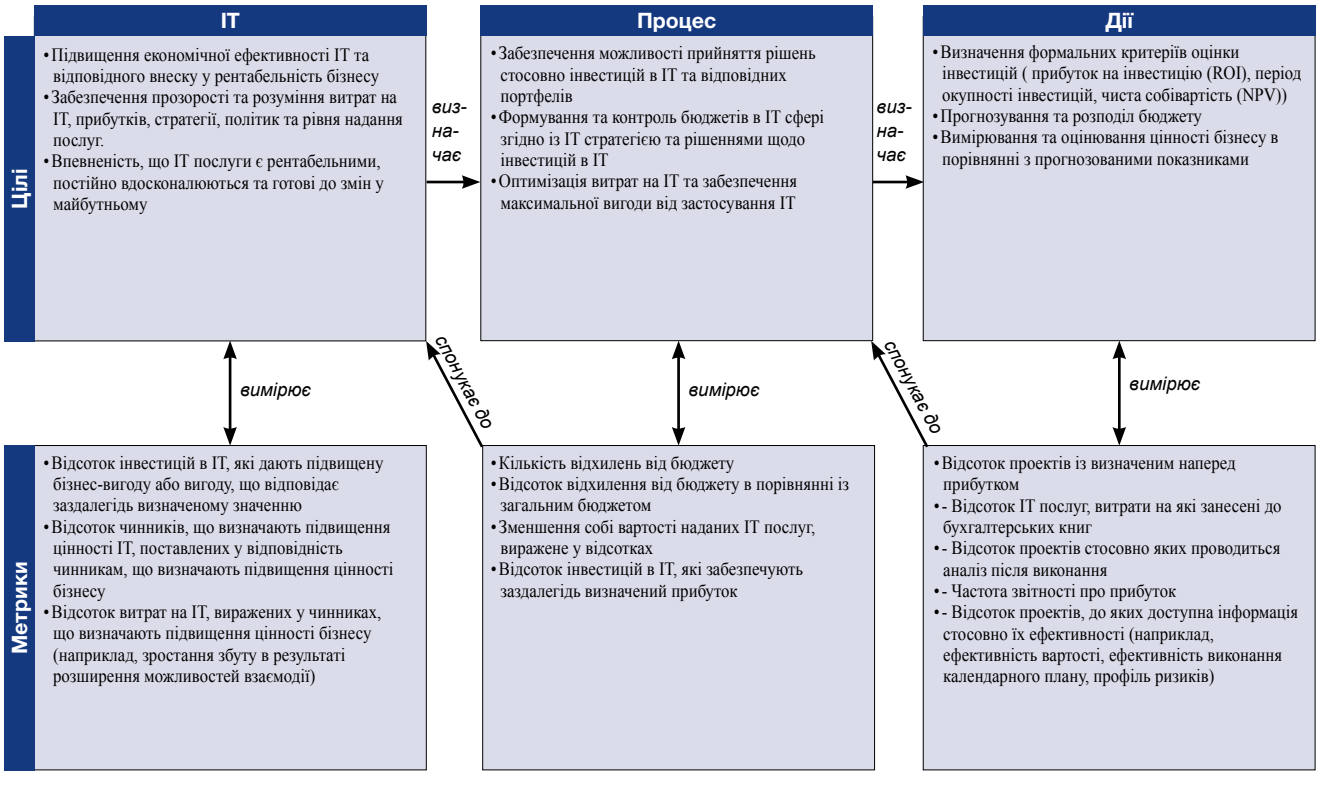
Від	Вхідні дані
PO1	Стратегічний план та тактичні плани розвитку IT, портфелі проектів та послуг
PO3	Вимоги до інфраструктури
PO10	Портфель IT проектів із змінами та доповненнями
AI1	Аналіз можливості виконання бізнес-вимог
AI7	Аналіз функціонування системи
DS3	Планування ефективності та потужностей (вимоги)
DS6	Фінансові показники IT
ME4	Очікувані результати інвестицій бізнесу в IT

Вихідні дані	Для					
Звіти про витрати та прибутки	PO1	AI2	DS6	ME1	ME4	
Бюджети IT	DS6					
Оновлений портфель IT послуг	DS1					
Оновлений портфель IT проектів	AI1					
Звіти про витрати та прибутки	PO10					

RACI-діаграма

Дії \ Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Підтримка портфелю програм	A	R	R	R	C					I	I
Підтримка портфелю проектів	I	C	A/R	A/R	C		C	C		C	I
Підтримка портфелю послуг	I	C	A/R	A/R	C	C				C	I
Запровадження та підтримка процесу формування IT бюджету	I	C	C	A		C	C	C	R	C	
Визначення, інформування та контроль IT інвестиції, витрат та цінності, яку вони забезпечують для бізнесу	I	C	C	A/R		C	C	C	R	C	C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

PO5 Управляти інвестиціями в IT

Управління процесом *«Управляти інвестиціями в IT»*, що задовольняє бізнес-вимогу до IT, яка полягає в тому, щоб забезпечити *«Постійне та наочне підвищення ефективності витрат на IT та посилення їх ролі у підвищенні рентабельності бізнесу шляхом надання інтегрованих та стандартизованих послуг, які задовольняють очікування кінцевих користувачів»* знаходиться на рівні зрілості:

0 Не існуючий, якщо
Відсутнє усвідомлення важливості вибору інвестицій в IT та формування відповідних бюджетів. Інвестиції в IT та пов'язані з ними витрати не контролюються та не відстежуються.

1 Початковий, якщо
Організація визнає необхідність управління інвестиціями в IT, але комунікації стосовно цього не є послідовними. Розподіл обов'язків та відповідальності щодо вибору інвестицій в IT та формування бюджету здійснюється не регулярно в кожному конкретному випадку. Мають місце ізольовані випадки впровадження процесу вибору інвестицій в IT і формування бюджету, та супроводжуються неофіційною (неформальною) документацією. Рішення щодо формування бюджету мають реактивний характер та орієнтовані на конкретні операції.

2 Повторюваний але інтуїтивний, якщо
Існує інтуїтивне розуміння потреби у виборі інвестицій в IT та формування бюджету. Потреба у процесі вибору інвестицій та формування бюджету обговорюється. Виконання процесу залежить від ініціативи окремих осіб в організації. Зароджуються стандартні методи розробки складових IT бюджету. Рішення щодо формування бюджету мають реактивний та тактичний характер.

3 Визначений, якщо
Політики та процедури вибору інвестицій та формування бюджету визначені, задокументовані та обговорюються, при цьому вони охоплюють ключові аспекти бізнесу та застосування технологій. IT бюджет узгоджений із стратегічними планами розвитку IT та бізнес-планами. Процеси формування бюджету та вибору інвестицій в IT формалізовані, задокументовані та обговорюються. Розпочато формальне навчання, але воно все ще ґрунтується головним чином на ініціативі окремих осіб. Має місце процедура офіційного (формального) затвердження результатів вибору інвестицій та складених бюджетів. IT персонал має досвід та кваліфікацію, необхідні для розробки IT бюджету та надання рекомендацій щодо здійснення відповідних інвестицій в IT.

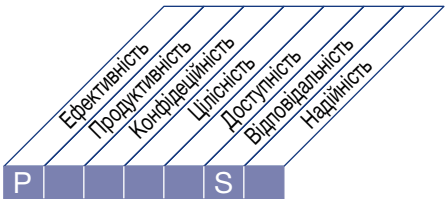
4 Керований та вимірюваний, якщо
Відповідальність за вибір інвестицій та формування бюджету, а також обов'язок представлення відповідної звітності покладено на конкретну особу. Відхилення від бюджету виявляються та врегульовуються. Проводиться формальний аналіз розподілу витрат, що охоплює прямі та непрямі витрати на поточну операційну діяльність, а також запропоновані інвестиції, з врахуванням всіх витрат, понесених протягом повного життєвого циклу. Процес формування бюджету є стандартизованим та передбачає прогнозування ситуації. В інвестиційних планах відображається переведення витрат на розробку та операційних витрат з програмно-апаратного комплексу на інтеграцію систем та забезпечення IT робочою силою. Вигоди від реалізації програм та прибутковість інвестицій розраховуються з фінансової та не фінансової точки зору.

5 Оптимізований, якщо
Порівняльний аналіз витрат та визначення способів підвищення рентабельності інвестицій здійснюються із застосуванням найкращих практик, що існують в галузі. Вибір інвестицій та формування бюджету здійснюються на основі результатів аналізу технологічних розробок. Процес управління інвестиціями постійно вдосконалюється з урахуванням досвіду, отриманого на підставі аналізу фактичних результатів інвестування. Рішення щодо інвестицій передбачають тенденцію до підвищення співвідношення витрати/ефективність. Формально вивчаються та оцінюються альтернативні варіанти фінансування в контексті існуючої структури капіталу організації з використанням методів формального оцінювання. Заздалегідь здійснюється виявлення відхилень від бюджету. Рішення щодо інвестицій передбачають виконання аналізу довгострокових витрат та вигод, понесених та отриманих протягом їх загального життєвого циклу.

Опис процесу

PO6 Інформувати про стратегічні цілі керівництва та напрямки розвитку

Керівництво розробляє систему контролю IT, а також розробляє та інформує про відповідні політики. Впроваджена та діє, на постійній основі, затверджена керівництвом програма комунікацій, в якій чітко сформульована місія та цілі надання послуг, політики та процедури тощо. Програма комунікацій сприяє досягненню цілей IT, а також забезпечує усвідомлення і розуміння бізнес-ризиків та ризиків, пов'язаних із застосуванням IT, та відповідних цілей й напрямку розвитку. Цей процес забезпечує дотримання відповідних законодавчих та нормативних вимог.



Контроль IT процесу

Інформувати про стратегічні цілі керівництва та напрямки розвитку

який задовольняє бізнес-вимоги до IT, а саме:

надання точної та своєчасної інформації стосовно IT послуг, що надаються та будуть надаватись в майбутньому, а також щодо ризиків, пов'язаних з їх наданням, та відповідальності сторін, залучених в процес надання IT послуг

зосереджений на

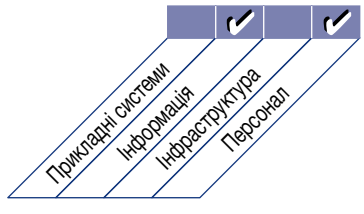
наданні точних, зрозумілих і затверджених політик, процедур, інструкцій та іншої регламентної документації сторонам, задіяним у роботі системи контролю IT

реалізується шляхом

- створення системи контролю IT
- розробки та впровадження політик у сфері IT
- забезпечення виконання політик у сфері IT

та вимірюється

- кількістю порушень неперервності бізнесу в результаті перебоїв у наданні IT послуг
- відсотком зацікавлених сторін, які розуміють принципи функціонування системи контролю IT
- відсотком сторін-учасниць, які не дотримуються політик



Цілі контролю

PO6 Інформувати про стратегічні цілі керівництва та напрямки розвитку

PO6.1 Політика та контрольне середовище IT
Визначити елементи контрольного середовища IT згідно з філософією управління організацією та стилем її роботи. Ці елементи повинні відображати очікування / вимоги щодо цінності інвестицій в IT, величину ризик-апетиту, цілісність, етичні цінності, компетенції персоналу та відповідальність сторін-учасників. Контрольне середовище повинне ґрунтуватись на культурі, яка гарантує забезпечення цінності та, водночас, сприяє управлінню суттєвими ризиками, налагодженню співпраці між підрозділами організації, дотриманню існуючих вимог, постійному вдосконаленню процесу та ефективному управлінню відхиленнями від заданого процесу.

PO6.2 IT ризики та структура контролю
Розробити та підтримувати у належному стані модель, яка відображає загальний підхід організації до управління IT ризиками та забезпечення контролю на рівні IT, узгоджену з політикою в сфері IT та відповідним контрольним середовищем, а також з моделлю управління ризиками організації та її контрольним середовищем.

PO6.3 Управління політиками в сфері IT
Розробити та підтримувати в належному стані набір політик, направлених на підтримку IT стратегії. Ці політики повинні описувати їх призначення, розподіл ролей та обов'язків, процедуру реагування на виключення, механізми забезпечення дотримання існуючих вимог, а також містити посилання на процедури, стандарти та інструкції. Їх актуальність необхідно аналізувати та підтверджувати на регулярній основі.

PO6.4 Введення в дію політик, стандартів та процедур
Ввести в дію та забезпечити виконання політик в сфері IT всіма працівниками, на яких вони розповсюджуються, таким чином, щоб вони стали невід'ємною частиною діяльності організації.

PO6.5 Інформування про IT цілі та напрямок розвитку
Забезпечити усвідомлення і розуміння бізнес-цілей, а також цілей і напрямку розвитку IT відповідними сторонами-учасниками та користувачами в масштабі всієї організації.

Керівні принципи управління

PO6 Інформувати про стратегічні цілі керівництва та напрямки розвитку

Від	Вхідні дані
PO1	Стратегічні і тактичні плани IT, портфелі IT проектів та послуг
PO9	Основні принципи управління IT ризикам
ME2	Звіт щодо ефективності у сфері IT контролю

Вихідні дані	Для						
Система контролю IT в організації	Всіх						
Політики в сфері IT	Всіх						

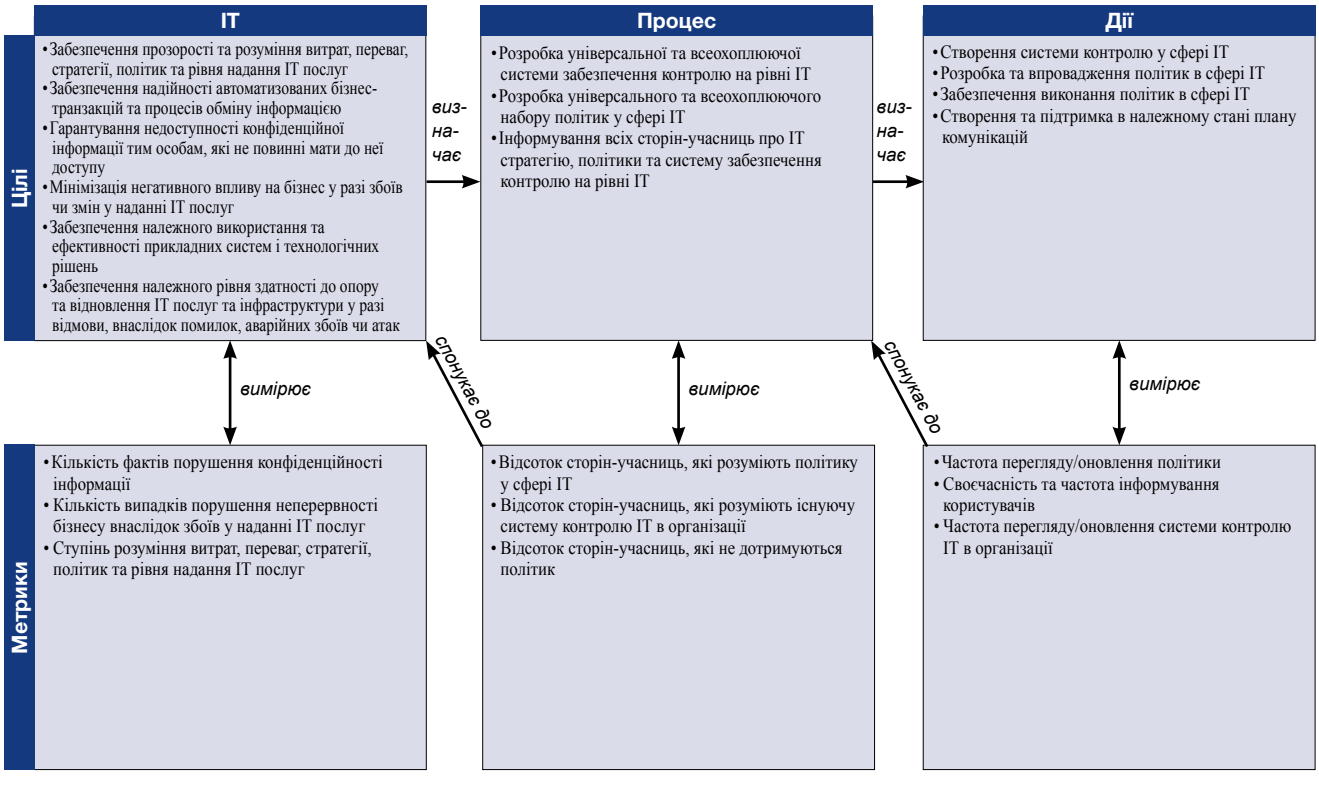
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Створити та підтримувати в належному стані контрольне середовище та система IT	I	C	I	A/R	I	C		C	C		C
Розробити та підтримувати в належному стані політики IT	I	I	I	A/R		C	C	C	R		C
Інформувати про система контролю, цілі та напрямок розвитку IT	I	I	I	A/R					R		C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

PO6 Інформувати про стратегічні цілі керівництва та напрямки розвитку

Управління процесом *«Інформувати про стратегічні цілі керівництва та напрямки розвитку»*, що задовольняє бізнес-вимогу до IT, а саме *«надання точної та своєчасної інформації стосовно IT послуг, що надаються та будуть надаватись в майбутньому, а також щодо ризиків, пов'язаних з їх наданням, та відповідальності сторін, залучених в процес надання IT послуг»*, знаходиться на рівні зрілості:

0 Не існуючий, якщо
Керівництво не створило контрольного середовища в IT. Відсутнє усвідомлення потреби у запровадженні набору політик, планів та процедур, а також механізмів для забезпечення їх дотримання.

1 Початковий, якщо
Керівництво розуміє необхідність створення інформаційного контрольного середовища. Політики, процедури та стандарти розробляються та доводяться до відома працівників кожного разу по мірі виникнення необхідності. Процеси розробки, комунікацій та дотримання існуючих вимог не є формальними та цілісними.

2 Повторюваний але інтуїтивний, якщо
Керівництво повністю усвідомлює необхідність формування вимог та створення ефективного інформаційного контрольного середовища, але практичні підходи щодо його реалізації залишаються, переважно, неформальними. Керівництво інформує про необхідність запровадження системи політик, планів та процедур контролю, але прийняття кінцевого рішення щодо їх розробки залишено на розсуд керівників підрозділів. Якість трактується як бажана ідеологія ведення бізнесу, якої слід дотримуватись, але вибір конкретних підходів щодо її інтеграції в існуючу філософію ведення бізнесу залишено на розсуд керівників підрозділів. Навчання проводиться індивідуально у разі виникнення необхідності.

3 Визначений, якщо
Керівництво розробило, задокументувало та поінформувало сторони-учасники про контрольне середовище та механізми управління якістю інформації, яке передбачає наявність набору відповідних політик, планів та процедур. Процес розробки політик є системним, відбувається на постійній основі та доведений до відома персоналу, а існуючі політики, плани і процедури є достатньо повноцінними та охоплюють всі ключові аспекти. Керівництво усвідомлює важливість забезпечення IT безпеки та проводить заходи, направлені на підвищення рівня інформованості персоналу у цьому питанні. Час від часу також проводиться навчання з метою розширення рівня поінформованості персоналу про існуюче інформаційне контрольне середовище. Одночасно з цим, запроваджена система комплексної розробки політик та процедур, частково проводиться моніторинг дотримання даних політик та процедур. Методики сприяння усвідомленню та розумінню важливості IT безпеки стандартизовані та формалізовані.

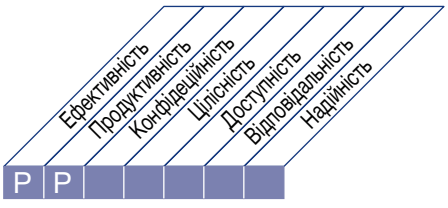
4 Керований та вимірюваний, якщо
Керівництво бере на себе відповідальність за забезпечення поінформованості персоналу щодо існуючих політик внутрішнього контролю, а також делегує відповідальність та виділяє необхідні ресурси для підтримки контрольного середовища у належному стані у випадку суттєвих змін. Створено проактивне інформаційне контрольне середовище, направлене на забезпечення якості та розуміння важливості безпеки в сфері IT. Розроблено та доведено до відома персоналу повний набір політик, планів та процедур, який є невід'ємною частиною сукупності всіх внутрішніх політик і процедур. Розроблено систему впровадження цих політик і процедур, а також регламент проведення перевірок на предмет їх дотримання.

5 Оптимізований, якщо
Інформаційне контрольне середовище узгоджене з існуючою системою стратегічного управління, відповідним баченням керівництва, піддається регулярному перегляду, оновленню та постійно вдосконалюється. Залучено внутрішніх та зовнішніх експертів для адаптації та впровадження найкращих галузевих практик в частині забезпечення внутрішнього контролю та здійснення комунікацій. В масштабах всієї організації проводиться моніторинг, розповсюджена практика само-оцінювання та перевірки дотримання існуючих вимог. Для підтримки баз знань про існуючі політики та підвищення рівня поінформованості про них, а також для оптимізації комунікацій використовуються спеціалізовані інформаційні технології, включаючи засоби комп'ютеризованого навчання.

Опис процесу

PO7 Управляти персоналом IT

Для створення та надання IT послуг бізнес-підрозділам підібраний та найнятий компетентний персонал. Це реалізовано шляхом дотримання затверджених практик, що стосуються набору, навчання, оцінювання результатів роботи, просування по службі та звільнення працівників. Цей процес є вкрай важливим, оскільки персонал є найбільш цінним активом організації, а корпоративне управління і середовище внутрішнього контролю великою мірою залежить від мотивації та компетентності персоналу.



Контроль IT процесу

Управляти персоналом IT

який задовольняє бізнес-вимоги до IT, а саме:

залучення компетентного та мотивованого персоналу для створення і надання IT послуг

зосереджений на

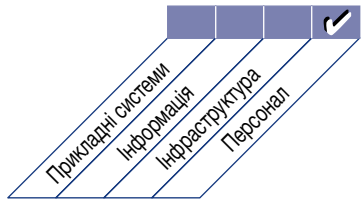
наборі, навчанні та мотивації персоналу на всіх етапах кар'єри, визначенні переліку ролей в залежності від навичків, запровадженні прозорого процесу оцінки персоналу, підготовці посадових інструкцій і забезпеченні усвідомлення цінності ключових

реалізується шляхом

- аналізу ефективності роботи персоналу
- набору та навчання IT персоналу для реалізації тактичних планів розвитку IT
- мінімізація ризиків, пов'язаних із залежністю від ключових спеціалістів

та вимірюється

- рівнем вдоволеності сторін-учасників досвідом та професійним навичками IT персоналу
- рівнем відтоку кадрів, задіяних у сфері IT
- відсотком IT спеціалістів, сертифікованих відповідно до вимог їхніх посадових інструкцій



Цілі контролю

PO7 Управляти персоналом IT

PO7.1 Набір та утримування персоналу
Проводити набір та утримання IT персоналу відповідно до існуючих політик та процедур організації (наприклад, прийом на роботу, створення сприятливих умов праці, проведення орієнтаційного курсу). Розробити та запровадити процеси, спрямовані на залучення кваліфікованого IT персоналу, необхідного для досягнення цілей організації.

PO7.2 Компетенції персоналу
Регулярно пересвідчуватись у тому, що персонал має достатній рівень компетенції для виконання своїх ролей на основі навчання, тренінгів та/або досвіду. Визначати ключові вимоги щодо компетенції IT персоналу та перевіряти їх дотримання шляхом впровадження кваліфікаційних та сертифікаційних програм для працівників там, де це є доцільним.

PO7.3 Розподіл ролей серед персоналу
Визначати перелік ролей, обов'язків, а також систему компенсації персоналу, здійснювати моніторинг та контроль за виконанням ролей, обов'язків та дотриманням політик і процедур управління, кодексу етики та професійних практик. Рівень нагляду повинен відповідати важливості посади та об'єму наданих повноважень.

PO7.4 Навчання персоналу
Організовувати та проводити для працівників IT сфери належні орієнтаційні курси при прийомі на роботу та підтримувати рівень їх знань, навичок, кваліфікації, а також поінформованості про існуючі внутрішні контролі та принципи безпеки на рівні, необхідному для досягнення цілей організації.

PO7.5 Залежність від ключових спеціалістів
Мінімізувати залежність від ключових спеціалістів шляхом накопичення та обміну знаннями, планування наступності в частині обіймання тих чи інших посад, підготовки кадрового резерву.

PO7.6 Процедури перевірки надійності персоналу
Включити процедуру перевірки анкетних даних в процес набору IT персоналу. Глибина та частота оцінки ефективності подібних перевірок повинна залежати від ступеня важливості та/або критичності посади, і повинна застосовуватись як до штатних працівників, так і до партнерів, і постачальників.

PO7.7 Оцінка ефективності роботи працівників
На регулярній основі проводити оцінку ефективності роботи працівників на основі їх індивідуальних цілей, сформований у відповідності до цілей організації, затверджених стандартів та конкретних посадових обов'язків. Працівники повинні проходити інструктаж з питань ефективності своєї роботи та професійної поведінки по мірі доцільності.

PO7.8 Зміна на посаді та звільнення з посади
Вживати належних заходів у відношенні управління процесом зміни на посаді, зокрема звільнення з посади. Запровадити процедури передачі знань, перерозподілу та передачі обов'язків, а також позбавлення прав доступу, які б дозволили звести до мінімуму ризики та забезпечити безперервність виконання тих чи інших функцій.

Керівні принципи управління

PO7 Управляти персоналом IT

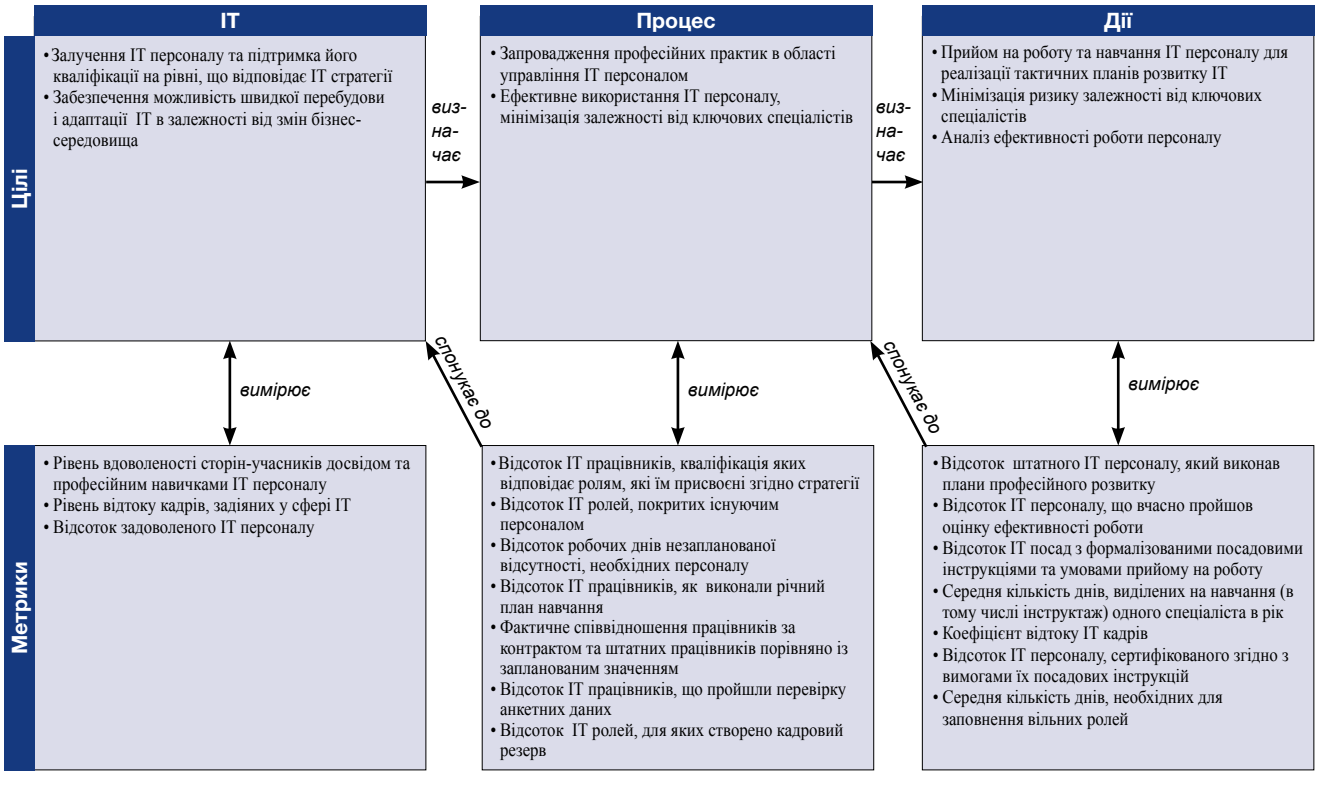
Від	Вхідні дані
PO4	IT організація та взаємозв'язки, задокументовані ролі та обов'язки
AI1	Аналіз виконання бізнес-вимог

Вихідні дані	Для						
Політики та процедури у відношенні IT персоналу	PO4						
Матриця компетенції IT персоналу	PO4	PO10					
Посадові інструкції	PO4						
Кваліфікація та компетенція користувачів, включаючи індивідуальне навчання	DS7						
Конкретні вимоги до навчання	DS7						
Ролі та обов'язки	Всіх						

RACI-діаграма

Дії \ Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Визначити рівень кваліфікації IT персоналу, створити посадові інструкції, встановити діапазон рівня заробітної плати та показники ефективності роботи персоналу		C		A		C	C	C	R	C	
Виконувати політики та процедури у сфері управління кадрами в IT (набір, прийняття на роботу, перевірка при прийомі на роботу, визначення рівня заробітної плати, навчання, оцінка ефективності роботи, просування по службі та звільнення з роботи)				A		R	R	R	R	R	C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

Управління процесом *«Управляти персоналом IT»*, що задовольняє бізнес-вимогу до IT, а саме *«залучення компетентного та мотивованого персоналу для створення і надання IT послуг»* знаходиться на рівні:

0 Не існуючий, якщо
Керівництво організації не усвідомлює необхідності та важливості узгодження процесу управління кадрами, що задіяні в сфері IT, з процесом технологічного планування розвитку організації. Відсутня особа або група осіб, що несуть відповідальність за управління кадрами у сфері IT.

1 Початковий, якщо
Керівництво організації визнає необхідність управління кадрами, що задіяні в сфері IT. Процес управління IT персоналом неформалізований та носить реактивний характер. Процес управління IT кадрами зосереджений виключно на процедурі прийому на роботу та управлінні IT персоналом. Поступово починає формуватись усвідомлення того, що швидкі зміни в розвитку бізнесу, а також підвищення складності технологічних рішень, що їх використовує організація, потребують більш високого рівня компетенції та кваліфікації персоналу.

2 Повторюваний але інтуїтивний, якщо
Запроваджений тактичний підхід до прийому на роботу та управління IT персоналом, в залежності від потреб конкретних проектів, а не від збалансованості штатних співробітників та стороннього кваліфікованого персоналу. Новий персонал проходить неформальне навчання (орієнтаційні курси). В подальшому, навчання спеціалістів відбувається лише у разі потреби.

3 Визначений, якщо
Формалізовано процес управління кадрами, що задіяні в сфері IT. Існує план управління IT персоналом. Застосовується стратегічний підхід до прийому на роботу та управління IT персоналом. Формалізовано план навчання, що відповідає потребам IT персоналу. Впроваджено програму ротації кадрів з метою розповсюдження та обміну досвідом з технічних питань та управління бізнесом.

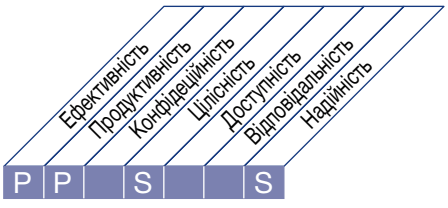
4 Керований та вимірюваний, якщо
Відповідальність за розробку та підтримку в належному стані плану управління кадрами, що задіяні у сфері IT, покладено на конкретну особу або групу осіб, що володіють необхідним досвідом та кваліфікацією. Процес розвитку та управління кадрами, що задіяні у сфері IT, адаптивний до змін. В організації існують стандартизовані метрики, які дозволяють виявляти відхилення від положень плану управління кадрами, що задіяні у сфері IT. При цьому, особливу увагу приділено питанням управління зростанням кількості IT персоналу та його відтоком. Запроваджено процедури перегляду заробітної плати та оцінки ефективності роботи, а також здійснюється їх порівняльний аналіз з іншими організаціями та найкращими галузевими практиками. Управління кадрами, що задіяні у сфері IT, несе проактивний характер з урахуванням кар'єрного росту.

5 Оптимізований, якщо
План управління кадрами, що задіяні у сфері IT, постійно оновлюється для забезпечення його відповідності потребам та вимогам бізнесу. Процес управління кадрами, що задіяні у сфері IT, інтегровано в процес технологічного планування, з метою забезпечення оптимального розвитку та використання IT знань та навичок. Процес управління IT персоналом адаптивний та інтегрований зі стратегічним напрямком розвитку організації. Складові процесу управління IT персоналом приведені у відповідність із найкращими галузевими практиками, що існують в галузі, включаючи: визначення рівня заробітної плати, оцінку ефективності роботи, участь у спеціалізованих форумах, передача знань, навчання та наставництво. Для всіх нових технологічних стандартів та продуктів, що їх планує впроваджувати організація, заздалегідь створюються спеціалізовані навчальні програми.

Опис процесу

PO8 Управляти якістю

Розробляється та впроваджується система управління якістю (QMS), до складу якої входять апробовані процеси та стандарти в сфері розробки та придбання. Це відбувається завдяки плануванню, впровадженню та експлуатації системи управління якістю (QMS) шляхом визначення чітких вимог щодо якості, а також щодо процедур та політик. Вимоги щодо якості визначаються та доводяться до відома сторін-учасниць у вигляді кількісних та досяжних показників. Постійне вдосконалення здійснюється завдяки моніторингу, аналізу, реакції на відхилення та інформування сторін-учасниць про досягнуті результати. Управління якістю є важливою складовою для отримання впевненості у тому, що IT послуги мають цінність для бізнесу, постійно вдосконалюються та є прозорими для сторін-учасниць.



Контроль IT процесу

Управляти якістю

який задовольняє бізнес-вимоги до IT, а саме:

забезпечення постійного підвищення якості надання IT послуг та можливості моніторингу якості на основі кількісних показників

зосереджений на

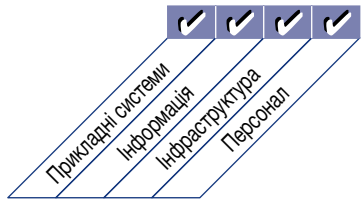
створенні системи управління якістю, здійсненні постійного моніторингу результатів у порівнянні із заздалегідь визначеними цілями та впровадженні програми постійного підвищення якості IT послуг

реалізується шляхом

- визначення стандартів якості та відповідних галузевих практик
- моніторингу та аналізу результатів внутрішньої та зовнішньої діяльності на предмет відповідності стандартам якості та відповідним галузевим практикам
- постійного вдосконалення системи управління якістю

та вимірюється

- відсотком сторін-учасників, задоволених якістю IT послуг (в залежності від важливості IT послуг)
- відсотком IT процесів, для яких формалізована процедура регулярного перегляду, що здійснюється службою гарантування якості (QA), та які відповідають поставленим цілям і цільовим показникам якості
- відсотком процесів, що проходять перевірку службою гарантування якості (QA)



Цілі контролю

PO8.1 Система управління якістю
Створити та підтримувати в належному стані систему управління якістю (QMS), яка дозволяє стандартизувати, формалізувати та на постійній основі здійснювати управління якістю відповідно до вимог та потреб бізнесу. Система управління якістю (QMS) повинна визначати вимоги та критерії якості; ключові IT процеси, а також їх послідовність та взаємодію, політики, критерії та методи визначення, виявлення, коригування та попередження випадків недотримання існуючих вимог щодо якості. Система управління якістю (QMS) повинна визначати організаційну структуру, необхідну для забезпечення управління якістю, включаючи опис ролей, завдань та обов'язків. Для всіх ключових сфер діяльності повинні бути розроблені плани по управлінню якістю, узгоджені з існуючими критеріями, політиками та стандартами якості даних. Також, необхідно здійснювати моніторинг і оцінку ефективності системи управління якістю (QMS) та вдосконалювати її в разі потреби.

PO8.2 IT стандарти та галузеві практики в області управління якістю
Впровадити та підтримувати на належному рівні виконання вимог стандартів, процедур та кращих галузевих практик в рамках ключових IT процесів з метою забезпечення реалізації завдань, покладених на систему управління якістю (QMS). Використовувати найкращі галузеві практики як еталон для системи управління якістю в організації.

PO8.3 Стандарти в області розробки та придбання
Адаптувати та підтримувати в належному стані стандарти для здійснення всіх розробок та закупівель, які охоплюють весь життєвий цикл розробки чи придбання, включаючи контроль якості та відповідності вимогам на різних етапах. Розглянути можливість впровадження єдиних стандартів програмування, системи найменувань, форматів файлів, схем та стандартів розробки словників даних, стандартів інтерфейсу користувачів, інтероперабельності, продуктивності та масштабованості систем, розробки та тестування, процедур перевірки відповідності вимогам, планів тестування (включаючи тестування елементів системи, регресивне тестування та тестування системи в цілому).

PO8.4 Орієнтація на замовника
Зосередити процес управління якістю на замовниках шляхом визначення їхніх вимог та узгодження їх з IT стандартами та практиками. Визначити ролі та обов'язки, що стосуються врегулювання конфліктів між користувачем / замовником та IT організацією.

PO8.5 Постійне вдосконалення
Підтримувати у належному стані та на регулярній основі інформувати сторони-учасниці про існуючий план забезпечення якості, який передбачає постійне вдосконалення.

PO8.6 Вимірювання, моніторинг та аналіз якості
Розробити та запровадити механізми постійного моніторингу відповідності вимогам системи управління якістю (QMS) та оцінки її цінності. Власник цього процесу повинен проводити моніторинг та вживати необхідні коригувальні та превентивні заходи на основі отриманих результатів.

Керівні принципи управління

PO8 Управляти якістю

Від	Вхідні дані
PO1	Стратегічний IT план
PO10	Детальні плани проектів
ME1	Плани коригувальних заходів

Вихідні дані	Для						
Стандарти придбання	AI1	AI2	AI3	AI5	DS2		
Стандарти розробки	PO10	AI1	AI2	AI3	AI7		
Стандарти якості та вимоги до метрик	Всіх						
Заходи з підвищення якості	PO4	AI6					

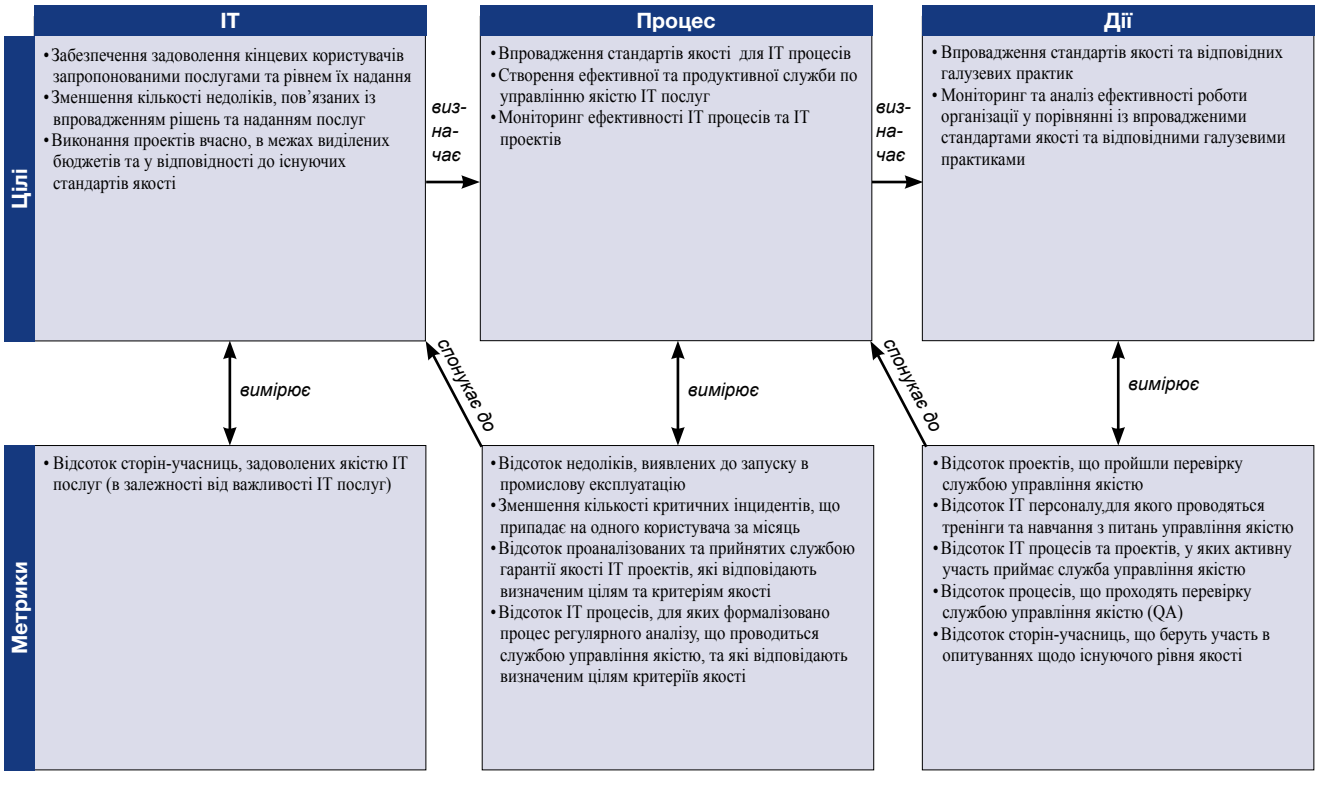
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Визначити систему управління якістю (QMS)	C		C	A/R	I	I	I	I	I	I	C
Запровадити та підтримувати в належному стані систему управління якістю QMS	I	I	I	A/R	I	C	C	C	C	C	C
Запровадити та довести до відома сторін-учасниць стандарти якості в масштабах всієї організації		I		A/R	I	C	C	C	C	C	C
Розробити на управляти планом забезпечення якості з метою постійного вдосконалення				A/R	I	C	C	C	C	C	C
Проводити моніторинг та вимірювати ступінь відповідності існуючим цілям та критеріям якості				A/R	I	C	C	C	C	C	C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

Управління процесом *«Управляти якістю»*, задовольняє бізнес-вимогу до IT, а саме *«забезпечення постійного підвищення якості надання IT послуг та можливості моніторингу якості на основі кількісних показників»*, знаходиться на рівні:

0 Не існуючий, якщо
В організації відсутні процес планування системи управління якістю (QMS) та методологія управління життєвим циклом розробки систем (SDLC). Вище керівництво та IT персонал не усвідомлюють необхідності розробки та впровадження програми управління якістю. Проекти та операційна діяльність організації не проходять перевірку якості.

1 Початковий, якщо
Керівництво усвідомлює потребу у впровадженні системи управління якістю (QMS). По мірі необхідності різні штатні працівники організації використовують систему управління якістю. Керівництво здійснює процедуру неформальної оцінки існуючого рівня якості.

2 Повторюваний але інтуїтивний, якщо
Розроблено та впроваджено програму для визначення переліку та моніторингу заходів в рамках системи управління якістю (QMS) в IT. Заходи, що здійснюються в рамках системи управління якістю (QMS), орієнтовані на IT проекти та IT процеси, але не охоплюють процеси в масштабах всієї організації.

3 Визначений, якщо
Система управління якістю (QMS) формалізований і доведений керівництвом організації до відома всіх співробітників, включаючи IT та керівників бізнес-підрозділів. Починає розроблятись програма навчання, спрямована на висвітлення питань якості на всіх рівнях організації. Визначено основні очікування щодо рівня якості, критерії якості закладені в IT проекти та на рівні IT організації. Починають застосовуватись універсальні інструменти та галузеві практики у сфері управління якістю. Час від часу проводяться опитування щодо існуючого рівня якості.

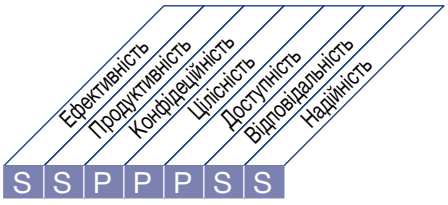
4 Керований та вимірюваний, якщо
Система управління якістю (QMS) охоплює всі процеси, в тому числі й процеси, що залежать від третіх сторін. Для зберігання метрик якості створено окрему базу знань. Оцінка ініціатив в рамках системи управління якістю (QMS) здійснюється з використанням методів аналізу витрат та вигод. Починає застосовуватись практика проведення порівняльного аналізу з найкращими галузевими практиками та конкурентами. Впроваджена програма навчання, спрямована на висвітлення питань якості на всіх рівнях організації. Проводиться стандартизація переліку використовуваних засобів та практичних підходів, періодично проводиться аналіз першопричин. На постійній основі проводяться опитування щодо існуючого рівня якості. Впроваджено ефективну програму оцінки рівня якості.

5 Оптимізований, якщо
Система управління якістю (QMS) інтегрована та діє у всіх сферах, де використовуються інформаційні технології. Процеси в рамках системи управління якістю (QMS) є гнучкими та можуть бути легко адаптовані до змін в IT середовищі. База знань для метрик якості доповнена зовнішніми найкращими галузевими практиками. Регулярно здійснюється порівняльний аналіз з вимогами зовнішніх стандартів. Опитування щодо існуючого рівня якості проводяться на постійній основі, направлені на виявлення першопричин та вживання ефективних заходів з метою підвищення якості. Формально підтверджується існуючий рівень ефективності процесу управління якістю.

Опис процесу

PO9 Оцінювати та управляти IT-ризиками

Створена та підтримується у належному стані модель управління ризиками IT. В рамках моделі описаний загальноприйнятий та узгоджений рівень IT ризиків, стратегія зниження ризиків та залишкові ризики. Будь-який потенційний вплив на цілі організації, спричинений тією чи іншою незапланованою подією,ідентифікується, аналізується та оцінюється. З метою мінімізації залишкових ризиків та зниження їх до прийнятного рівня, існують затверджені стратегії зниження ризиків. Результат оцінки ризиків є зрозумілим для сторін-учасниць та виражається в фінансовому еквіваленті, що дозволяє сторонам-учасникам звести ризик до прийнятного рівня толерантності.



Контроль IT процесу

Оцінювати та управляти IT-ризиками

який задовольняє бізнес-вимоги до IT, а саме:

аналіз та інформування сторін-учасниць про існуючі ризики IT та їх вплив на бізнес-процеси та бізнес-цілі

зосереджений на

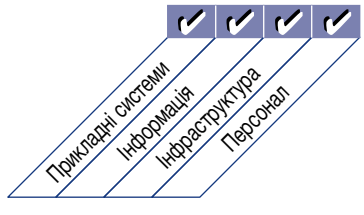
розробці моделі управління ризиками, інтегрованої в моделі управління операційними та бізнес-ризиками, оцінці ризиків, зниженні ризиків та інформуванні сторін-учасниць про залишкові ризики

реалізується шляхом

- забезпечення повної інтеграції та постійного застосування моделі управління ризиками в рамках процесів управління (внутрішніх і зовнішніх)
- проведення оцінки ризиків
- підготовки рекомендацій та інформуванні сторін-учасниць про плани зниження ризиків

та вимірюється

- відсотком ключових IT цілей, які охоплює процедура оцінки ризиків
- відсотком ідентифікований критичних IT ризиків, для яких розроблені плани реагування
- відсотком затверджених планів реагування на ризики



Цілі контролю

PO9 Оцінювати та управляти IT-ризиками

PO9.1 Модель управління ризиками IT
Впровадити модель управління ризиками IT, узгоджену з моделлю управління ризиками організації.

PO9.2 Визначення середовища ризиків
Визначити середовище застосування моделі управління ризиками з метою її ефективного застосування. При цьому необхідно визначити як внутрішнє так і зовнішнє середовища в контексті кожного випадку проведення оцінки ризиків, а також мету та критерії оцінки ризиків.

PO9.3 Ідентифікація подій
Ідентифікація подій (суттєвих загроз,направлених на компрометацію відповідних вразливостей), що можуть спричинити негативний вплив на цілі або операційну діяльність організації, включаючи бізнес-діяльність, нормативно-правові аспекти діяльності, функціонування інформаційних технологій, взаємостосунки з партнерами, кадрову політику і т.д. Визначити характер подібного впливу та забезпечити збереження даної інформації. Документувати релевантні ризики в реєстрі ризиків.

PO9.4 Оцінка ризиків
Періодична оцінка імовірності виникнення та наслідків всіх ідентифікованих ризиків із застосуванням якісних та кількісних методів. Імовірність виникнення та наслідки властивих та залишкових ризиків повинні визначатись окремо нарівні категорії та портфелю.

PO9.5 Реагування на ризики
Розробити та впровадити процес реагування на ризики з метою забезпечення використання фінансово-економічно обґрунтованих заходів для постійного зменшення схильності до ризиків. Процес реагування на ризики повинен включати такі стратегії управління ризиками, як: уникнення ризиків, зменшення ризиків, розподіл ризиків або прийняття ризиків, а також містити визначення обов'язків сторін-учасниць та враховувати ступінь толерантності до ризику.

PO9.6 Моніторинг та підтримка в належному стані плану реагування на ризики
Підготувати і визначити перелік та пріоритетний порядок здійснення заходів для реагування на ризики на всіх рівнях, включаючи ідентифікацію витрат, переваг, а також відповідальності за здійснення самих заходів. Отримати схвалення рекомендованих заходів та підтвердження прийняття всіх залишкових ризиків,а також впевнитись в тому, що заходи по реагуванню на ризики здійснюються власниками відповідних процесів. Здійснювати моніторинг виконання плану реагування на ризики та інформувати вище керівництво організації про будь-які відхилення.

Керівні принципи управління

PO9 Оцінювати та управляти IT-ризиками

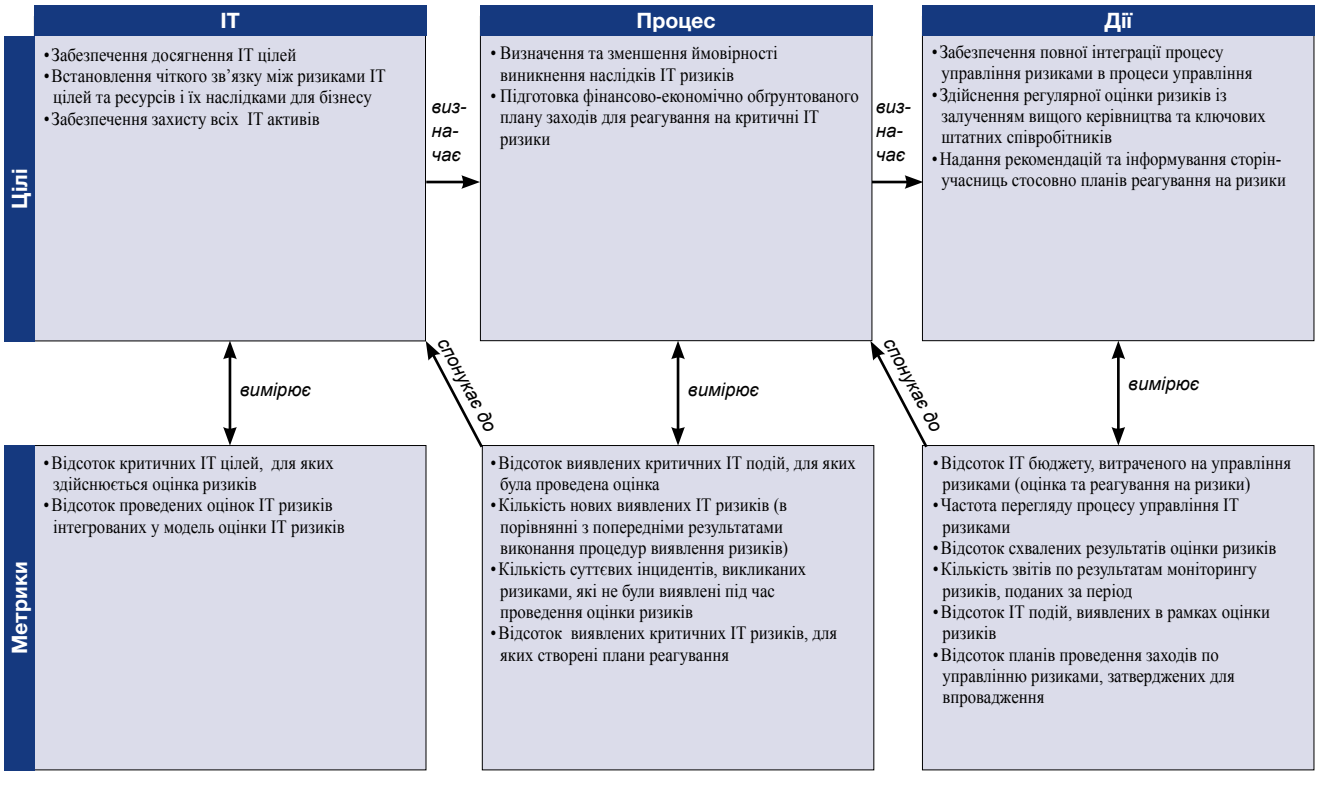
Від	Вхідні дані
PO1	Стратегічні і тактичні IT плани, портфель IT послуг
PO10	План управління ризиками проекту
DS2	Ризики у роботі з постачальниками
DS4	Результати оцінки непередбачуваних обставин
DS5	Загрози та вразливості з т.з. безпеки
ME1	Хронологія тенденцій та подій пов'язаних із ризиками
ME4	Апетит організації щодо ризиків IT

Вихідні дані	Для						
Оцінка ризиків	PO1	DS4	DS5	DS12	ME4		
Звітність в контексті ризиків	ME4						
Принципи управління ризиками IT	PO6						
Плани реагування на ризики IT	PO4	DS6					

RACI-діаграма

Дії \ Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Визначити підхід до управління ризиками	A	R/A	C	C	R/A	I					I
Зрозуміти відповідні стратегічні бізнес-цілі		C	C	R/A	C	C					I
Зрозуміти цілі відповідних бізнес-процесів				C	C	R/A					I
Визначити внутрішні IT цілі та середовище ризику					R/A		C	C	C		I
Ідентифікувати події, пов'язані з цілями (деякі події орієнтовані на бізнес (бізнес- це A), деякі орієнтовані на IT (IT – це A, бізнес – це C))	I			A/C	A	R	R	R	R		C
Оцінити ризики, пов'язані з подіями				A/C	A	R	R	R	R		C
Оцінити та обрати заходи для реагування на ризики	I	I	A	A/C	A	R	R	R	R		C
Підготувати і визначити перелік та пріоритетний порядок здійснення заходів для реагування на ризики	C	C	A	A	R	R	C	C	C		C
Затвердити та забезпечити фінансування реалізації планів реагування на ризики		A	A		R	I	I	I	I		I
Проводити моніторинг виконання та підтримувати в належному стані план реагування на ризики	A	C	I	R	R	C	C	C	C	C	R

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

Управління процесом *«Оцінювати та управляти IT- ризиками»*, що задовольняє бізнес-вимогу до IT, а саме: *«Аналізувати IT ризики та їх потенційний вплив на бізнес-процеси та цілі, а також надавати відповідну інформацію»*, знаходиться на рівні:

0 Не існуючий, якщо
Не проводиться оцінка ризиків у відношенні процесів та бізнес-рішень, що приймаються в організації. Організація не приймає до уваги бізнес-наслідки, до яких можуть привести вразливості безпеки та невизначеності в рамках проектів. Управління ризиками не здійснюється у відношенні придбання IT рішень та надання IT послуг.

1 Початковий, якщо
IT ризики враховуються несистематично. Неформальна оцінка ризиків здійснюється окремо для кожного проекту. Оцінка ризиків є частиною проектних планів, однак процедури оцінки ризиків в переважній більшості випадків не закріплені за конкретними менеджерами. Конкретні IT ризики, наприклад: ризики безпеки, доступності та цілісності час від часу приймаються до уваги в рамках проектів. На засіданнях керівництва рідко обговорюються IT ризики, що впливають на операційну діяльність організації. Навіть у випадках, коли ризики і приймаються до уваги, заходи по реагуванню на них не є систематичними. Зароджується усвідомлення того, що IT ризики мають важливе значення і їх слід брати до уваги.

2 Повторюваний але інтуїтивний, якщо
Практика проведення оцінки ризиків розвивається в організації, але запроваджується на розсуд керівників проектів. Управління ризиками, як правило, носить високорівневий характер застосовується тільки у відношенні ключових проектів, або в рамках реакції на проблеми, що виникають. По мірі виявлення ризиків починають запроваджуватись процеси реагування на них.

3 Визначений, якщо
Політика по управлінню ризиками визначає, коли та як здійснювати оцінку ризиків на рівні всієї організації. Управління ризиками здійснюється в рамках формалізованого процесу. Всі штатні працівники мають можливість пройти навчання (тренінг) в області управління ризиками. Рішення щодо використання процесу управління ризиками та участь у тренінгу співробітники приймають на власний розсуд. Методологія оцінки ризиків є ефективною та забезпечує можливість виявлення ключових ризиків для бізнесу. Процес реагування на ризики зазвичай ініціюється відразу після виявлення ризиків. Посадові інструкції персоналу охоплюють обов'язки, пов'язані із управлінням ризиками.

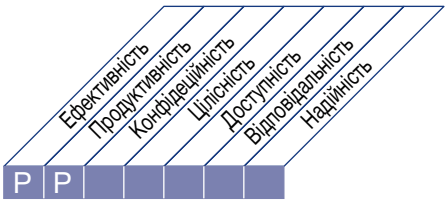
4 Керований та вимірюваний, якщо
Оцінка та управління ризиками є стандартними процедурами в організації. Керівництво IT інформується про виключення, що мають місце в рамках процесу управління ризиками. Відповідальність за управління IT ризиками покладено на вище керівництво. Оцінка та реагування на ризики здійснюється в рамках кожного проекту а також регулярно на рівні всієї операційної діяльності IT. Керівництву організації надаються консультації щодо необхідних змін у бізнесі та IT середовищі, які могли б суттєво вплинути на існуючі сценарії IT ризиків. Керівництво може контролювати своє ставлення до ризиків та приймати обґрунтовані рішення щодо прийнятного рівня ризиків. Для всіх виявлених ризиків призначаються їх власники, при цьому вище керівництво та керівництво IT визначають рівень толерантності організації до ризиків. Керівництво IT розробляє перелік стандартних метрик для оцінки ризиків та визначає співвідношення між величиною ризику та віддачею від заходів по реагуванню на нього. Керівництво закладає в бюджет організації видатки на управління операційними ризиками, а також на проведення регулярної переоцінки ризиків. Створено базу даних по управлінню ризиками, починається поступова автоматизація складових процесу управління ризиками. Керівництво IT розглядає різні стратегії реагування на ризики.

5 Оптимізований, якщо
Управління ризиками носить структурований систематичний характер в масштабах всієї організації. На всіх рівнях організації використовуються найкращі галузеві практики. Автоматизований процес збору, аналізу даних та підготовки звітів по результатам здійснення управління ризиками. Провідні спеціалісти надають консультації з питань управління ризиками, а представники IT беруть участь у роботі експертних груп з метою обміну досвідом. Управління ризиками тісно інтегроване в операційну діяльність Бізнесу і IT, та охоплює всіх користувачів IT послуг. Керівництво виявляє випадки прийняття рішень, щодо здійснення операційної діяльності та інвестицій в IT, без врахування аспектів управління ризиками і вживає відповідних заходів. Керівництво постійно здійснює оцінку ефективності існуючих стратегій реагування на ризики.

Опис процесу

PO10 Управляти проектами

Впроваджена програма та модель управління всіма IT проектами. Ця модель надає можливість правильно визначати пріоритети та здійснювати координацію всіх проектів. Модель включає загальний план, опис підходу до розподілу ресурсів та визначення кінцевих результатів, процес схвалення користувачами, поетапність виконання, забезпечення якості, план тестування та аналізу якості виконання з метою забезпечення належного рівня управління ризиками і цінності для бізнесу. Подібний підхід дозволяє знизити ризик непередбачуваних витрат та відміни проекту, покращує комунікації і підвищує ступінь участі в проектах бізнес-підрозділів та кінцевих користувачів, гарантує цінність та якість результатів проекту, а також сприяє виконанню інвестиційних програм IT.



Контроль IT процесу

Управляти проектами

який задовольняє бізнес-вимоги до IT, а саме:

виконання проектів в межах узгоджених строків, бюджетів та рівня якості

зосереджений на

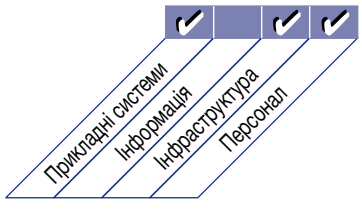
визначеній програмі та підході до управління IT проектами, яка дає можливість сторонам-учасницям приймати участь та здійснювати моніторинг ризиків проекту та прогресу його виконання

реалізується шляхом

- створення та впровадження програми та моделі управління проектами
- створення інструкцій щодо управління проектами
- детального планування кожного проекту, що входить до складу портфеля проектів

та вимірюється

- відсотком проектів, що відповідають очікуванням сторін-учасниць (в частині строків виконання, бюджету та відповідності вимогам – в залежності від важливості)
- відсотком проектів, які успішно пройшли аналіз якості виконання
- відсоток проектів, що відповідають стандартам та кращим галузевим практикам в області управління проектами



Цілі контролю

PO10 Управляти проектами

PO10.1 Модель управління програмою
Підтримувати в належному стані програму проектів, пов'язану з портфелем інвестицій в IT, шляхом виявлення, оцінки, визначення пріоритетів, вибору, ініціації, управління та контролю проектів. Гарантувати те, що проекти підтримують цілі програми. Координувати виконання та взаємозалежність проектів, забезпечувати отримання очікуваних кінцевих результатів, наявність та узгодженість необхідних ресурсів.

PO10.2 Модель управління проектами
Впровадити та підтримувати в належному стані модель управління проектами, яка визначає об'єм робіт та межі управління проектами, а також метод управління кожним проектом. Ця модель та метод повинні бути інтегровані в процеси управління програмами.

PO10.3 Підхід до управління проектами
Впровадити підхід до управління проектами в залежності від обсягу проектних робіт, складності та регуляторних вимог до кожного проекту. Структура управління проектом може включати опис ролей та відповідальності спонсора програми, спонсорів проекту, координаційного комітету, проектного офісу та менеджера, а також механізми, що дозволяють їм виконувати свої обов'язки (такі, як підготовка звітності та аналіз якості виконання проекту на кожному етапі). Впевнитись у тому, що всі IT проекти мають спонсорів з достатніми повноваженнями для того, щоб здійснювати виконання проекту в рамках загальної стратегічної програми організації.

PO10.4 Ступінь залучення сторін-учасниць
Забезпечить готовність всіх сторін-учасниць приймати участь в реалізації проекту в рамках існуючої програми інвестицій в IT.

PO10.5 Формування обсягу проектних робіт
Визначити та задокументувати характер та обсяг проектних робіт з метою формування у всіх сторін-учасниць єдиного розуміння обсягу проектних робіт, а також його взаємозв'язків з іншими проектами в межах загальної програми інвестицій в IT. Об'єм проектних робіт має бути офіційно затверджений спонсорами програми та проекту до початку реалізації проекту.

PO10.6 Ініціювання етапу проекту
Затвердити початок виконання кожного важливого етапу проекту та інформувати про це всі сторони-учасниці. В основу затвердження початкового етапу покласти рішення щодо управління програмою. На основі результатів аналізу та прийняття кінцевих результатів попереднього етапу проекту відбувається затвердження до виконання наступних етапів, а також затвердження оновленого та доповненого фінансово-економічного обґрунтування проекту. У випадку накладання етапів проекту спонсори програми визначають етапність з метою забезпечення ефективного виконання проекту.

PO10.7 План проекту
Розробити, затвердити та впровадити формальний план проекту (що охоплює як бізнес-ресурси, так і ресурси інформаційних систем), для забезпечення управління та контролю виконання проекту. Проектні роботи та взаємозалежності проектів в межах програми повинні бути визначені та задокументовані. План проекту повинен підтримуватись в належному стані протягом усього проекту. План проекту та зміни, що вносяться до нього, повинні бути узгоджені з існуючою програмою та моделлю управління проектами.

PO10.8 Проектні ресурси
Визначити обов'язки, взаємозв'язки, повноваження та критерії ефективності роботи учасників проекту, а також охарактеризувати підстави для залучення компетентних штатних спеціалістів та/або спеціалістів за контрактом для виконання проектних робіт. Необхідно здійснювати планування та управління закупівлями товарів та послуг, для виконання кожного проекту, згідно з існуючими підходами до здійснення закупівель, затвердженими в організації.

PO10.9 Управління ризиками проекту
Усунути або звести до мінімуму конкретні ризики, пов'язані з тим чи іншим проектом, шляхом систематичного планування, виявлення, аналізу, реагування, моніторингу та контролю подій, які можуть призвести до небажаних змін. Усі ризики, які загрожують процесу управління проектом та кінцевим результатам проекту, повинні виявлятись та документуватись.

PO10.10 Планування якості проекту
Підготувати план управління якістю, в якому описано систему забезпечення якості проекту та підхід до її впровадження.

Цей план повинен бути детально вивчений, офіційно узгоджений всіма сторонами-учасницями та внесений до плану проекту.

PO10.11 Контроль за змінами в рамках проекту
Впровадити систему контролю за змінами в рамках кожного проекту, з метою забезпечення їх належного аналізу, затвердження (наприклад: витрати, графік виконання, обсяг робіт, рівень якості) та внесення до плану проекту згідно з існуючою моделлю управління програмою та проектом.

PO10.12 Методи планування та забезпечення якості проекту
Визначити завдання, що стосуються забезпечення гарантії якості, які необхідно виконати в рамках планування проекту, та включити їх в існуючий план проекту. Успішне виконання цих завдань повинно гарантувати відповідність внутрішніх контролів та засобів безпеки заданим вимогам.

PO10.13 Моніторинг та оцінка ефективності реалізації проекту, підготовка звітів
Вимірювати показники ефективності реалізації проекту та порівнювати їх з ключовими критеріями в контексті обсягу проектних робіт, графіку їх виконання, якості, витрат та ризиків. Виявити будь-які відхилення від плану. Оцінити вплив виявлених відхилень на виконання проекту і програми в цілому, а також інформувати по це ключові сторони-учасниці. У разі необхідності підготувати рекомендації, а також вжити необхідних заходів, узгоджених з програмою та схемою управління проектом.

PO10.14 Завершення проекту
Вимагати, щоб в кінці кожного проекту його сторони-учасниці надали інформацію про те, чи були ними досягнуті заплановані результати та отримані переваги від реалізації проекту. Виявити та надати інформацію щодо будь-яких додаткових завдань, які необхідно виконати для досягнення запланованих результатів проекту і отримання вигод від реалізації програми, а також задокументувати отриманий досвід для його подальшого використання у майбутніх проектах і програмах.

Сторінку навмисне залишено вільною

Керівні принципи управління

PO10 Управляти проектами

Від	Вхідні дані
PO1	Портфель IT проектів
PO5	Оновлений портфель IT проектів
PO7	Матриця кваліфікації IT спеціалістів
PO8	Стандарти розробки
AI7	Аналіз функціонування системи після впровадження

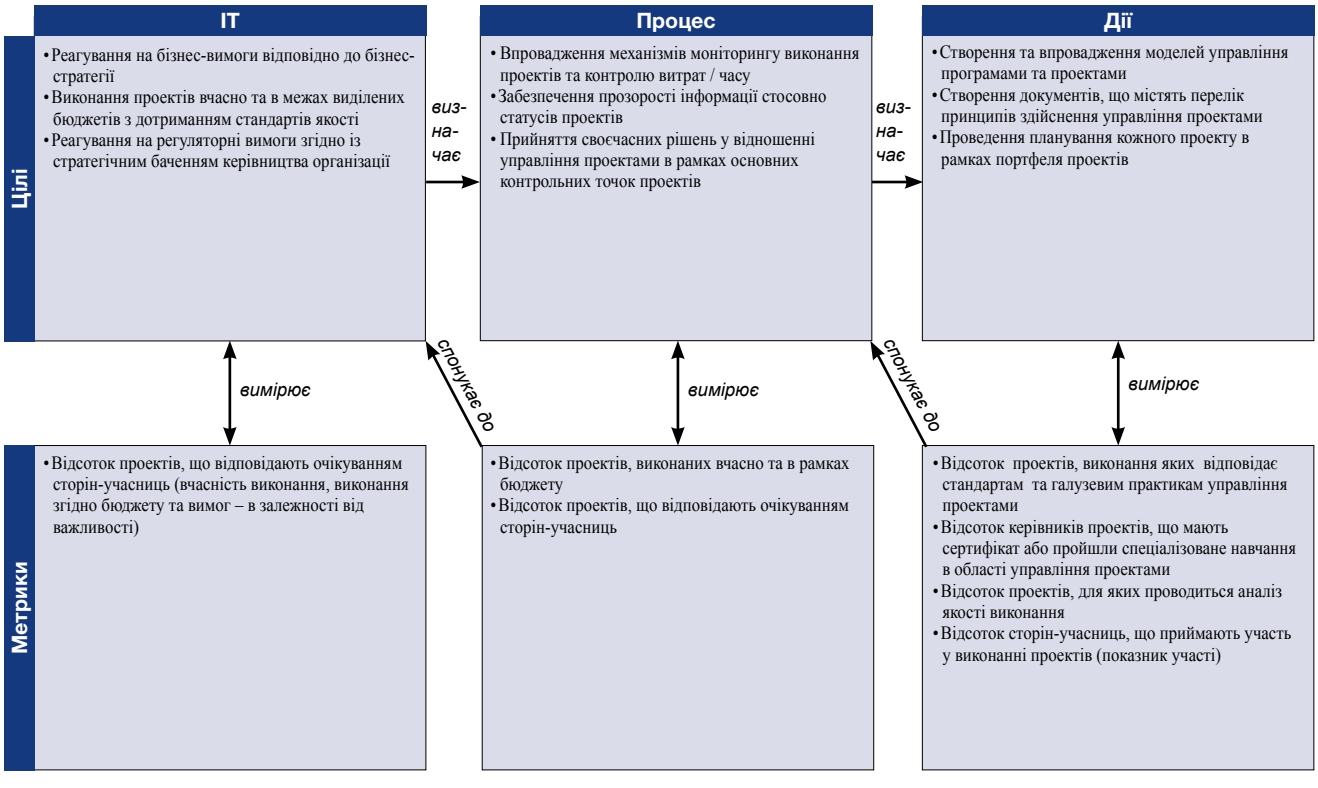
Вихідні дані	Для						
Стандарти придбання	AI1	AI2	AI3	AI5	DS2		
Стандарти розробки	PO10	AI1	AI2	AI3	AI7		
Стандарти якості та вимоги до метрик	Всіх						
Заходи з підвищення якості	PO4	AI6					

RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
ВстанСтворити модель управління програмою/портфелем інвестицій в IT	C	C	A	R						C	C
Впровадити та підтримувати в належному стані модель управління IT проектами	I	I	I	A/R	I	C	C	C	C	R	C
Впровадити та підтримувати в належному стані систему моніторингу, оцінки та управління IT проектами	I	I	I	R		C	C	C	C	A/R	C
Сформувати статути проектів, графіки виконання, плани забезпечення якості, бюджети, плани комунікацій та управління ризиками			C	C	C	C	C	C	C	A/R	I
Забезпечити залучення сторін-учасниць до співпраці в рамках реалізації проекту	I		A	R	C						C
Забезпечити ефективний контроль виконання проектів та внесення змін до проектів			C	C		C	C	C		A/R	C
Створити та запровадити методики оцінки якості реалізації проекту			I	C				I		A/R	C



Модель зрілості

PO10 Управляти проектами

Управління процесом *«Управляти проектами»*, що задовольняє бізнес-вимогу до IT, а саме: *«виконання проектів в межах узгоджених строків, бюджетів та рівня якості»* знаходиться на рівні:

0 Не існуючий, якщо
В організації не використовуються методики управління проектами, не проводиться оцінка бізнес-наслідків, пов'язаних із неналежним управлінням проектами та невдалими розробками.

1 Початковий, якщо
Використання методів та підходів до управління проектами в IT здійснюється вибірково. Керівництво організації недостатньою мірою залучено в якості власників проектів в процес управління проектами. Найбільш важливі рішення щодо управління проектами приймаються без участі кінцевих користувачів та керівників підрозділів. Участь замовників та користувачів у формуванні переліку IT проектів незначна або взагалі відсутня. На рівні функції IT відсутня організаційна структура для здійснення управління проектами. Ролі та обов'язки у відношенні управління проектами не визначені. Проекти, графік їх виконання та основні етапи майже або зовсім не визначені. Кількість часу, витраченого персоналом, залученим у проекти, а також фінансові витрати, пов'язані із виконанням проектів, не контролюються та не порівнюються з бюджетом.

2 Повторюваний але інтуїтивний, якщо
Вище керівництво усвідомлює та доводить до відома сторін-учасниць необхідність в управлінні IT проектами. Організація починає розробляти та використовувати деякі методики управління проектами. Бізнес-цілі та технічні цілі IT проектів визначені, але не формалізовані. Спостерігається низький рівень залучення сторін-учасниць в процес управління IT проектами. Для багатьох аспектів управління проектами починають розроблятись формалізовані принципи управління. Застосування принципів управління проектами залишене на розсуд менеджерів проектів.

3 Визначений, якщо
Процес та методологія управління IT проектами формалізовані, затверджені та доведені до відома всіх сторін-учасниць. IT проекти відповідають узгодженим бізнес-цілям та технічним цілям. Вище керівництво IT та бізнес-підрозділів починає активно долучатись до управління IT проектами. В рамках IT створено підрозділ по управлінню проектами, проведено початковий розподіл ролей та обов'язків. Здійснюється моніторинг виконання IT проектів, при цьому узгоджуються та переглядаються основні етапи проекту, графік їх виконання, проводиться аналіз відповідності бюджету та оцінка ефективності реалізації проекту. З ініціативи окремих співробітників розроблено тренінг для навчання в області управління проектами . Створено процедури для забезпечення належного рівня якості реалізації проектів, а також визначено перелік заходів, спрямованих на оцінку результатів реалізації проектів, однак вони не набули широкого застосування менеджерами IT проектів. Починає впроваджуватись концепція управління портфелями проектів в IT.

4 Керований та вимірюваний, якщо
Керівництво організації вимагає проведення аналізу якості виконання проектів на основі оцінки стандартизованих узгоджених метрик та досвіду, отриманого процесі реалізації проектів . Ефективність управління проектами вимірюються та оцінюються в межах всієї організації, а не тільки в рамках IT служби. Рекомендації щодо вдосконалення процесу управління проектами формалізуються та доводяться до відома всіх сторін-учасниць членами проектної команди, які пройшли навчання з питань вдосконалення проектного управління. Керівництво IT служби створює офіс з управління проектами, а також готує формалізований опис ролей, обов'язків та критеріїв оцінки ефективності учасників проекту. Запроваджено критерії для проведення оцінки результатів, досягнутих на кожному етапі проекту. Цінність та ризики вимірюються та контролюються до початку проекту, в процесі його виконання та після завершення. Проекти все більше орієнтовані на досягнення цілей організації в цілому, а не тільки конкретних цілей IT. Надається активна підтримка проектам з боку спонсорів з боку вищого керівництва та інших сторін-учасниць. Ні рівні офісу з управління проектами та в рамках IT планується проведення тренінгу з питань управління проектами.

5 Оптимізований, якщо
В організації запроваджена та використовується широко-визнана методологія управління життєвим циклом проектів і програм. На постійній основі проводиться виявлення, адаптація та запровадження найкращих галузевих практик в області управління проектами. Впроваджена IT стратегія, направлена на підтримку реалізації проектів. Офіс з управління проектами несе відповідальність за виконання проектів та програм на всіх етапах їх життєвого циклу. Планування програм та проектів в масштабах всієї організації забезпечує ефективне використання ресурсів для підтримки реалізації стратегічних ініціатив.

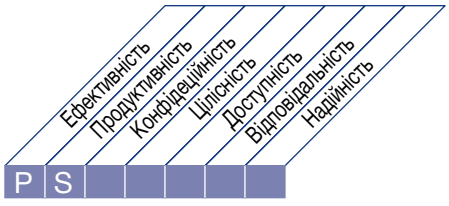
ЗАБЕЗПЕЧУВАТИ ПРИДБАННЯ ТА ВПРОВАДЖУВАТИ

AI1 Визначати рішення з автоматизації
AI2 Забезпечувати придбання та підтримку прикладного програмного забезпечення
AI3 Забезпечувати придбання та підтримку технологічної інфраструктури
AI4 Забезпечувати експлуатацію та використання
AI5 Закуповувати IT-ресурси
AI6 Управляти змінами
AI7 Впроваджувати в експлуатацію та проводити акредитацію IT-рішень та змін

Опис процесу

AI1 Визначати рішення з автоматизації

Потрібність у новому прикладному програмному продукті або функції потребує до його придбання або створення проведення аналізу, який дозволяє впевнитись в тому, що вимоги бізнесу задовольняються в ефективний та продуктивний спосіб. В межах цього процесу визначаються потреби, розглядаються можливості використання альтернативних джерел, здійснюється аналіз техніко-економічного обґрунтування, аналіз ризиків та аналіз рентабельності, а також робляться висновки щодо прийняття остаточного рішення – « створювати» чи «купувати». Всі вказані кроки дозволяють організаціям звести до мінімуму витрати на придбання та впровадження рішень, в той же час гарантуючи те, що вказані рішення дозволять бізнесу досягти поставлених цілей.



Контроль IT процесу

визначати рішення з автоматизації

який задовольняє бізнес-вимоги до IT, а саме:

втілення вимог бізнесу до функціональних можливостей та засобів контролю в ефективний та продуктивний дизайн автоматизованих рішень

зосереджений на

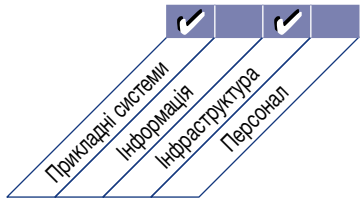
визначенні рентабельних рішень, доцільних та придатних з технічної точки зору

реалізується шляхом

- Визначення бізнес-вимог та технічних вимог
- Виконання техніко-економічного вивчення відповідно до стандартів розробки
- Прийняття (або неприйняття) вимог та результатів вивчення

та вимірюється

- Кількістю проектів, в яких зазначені вигоди не були отримані внаслідок невірних припущень стосовно здійсненності
- Відсотком техніко-економічних вивчень, узгоджених (затверджених) власником бізнес-процесу
- Відсотком користувачів, задоволених наданою функціональністю



Цілі контролю

AI1 Визначати рішення з автоматизації

AI1.1 Визначення та підтримання функціональних та технічних вимог з боку бізнесу
Визначити, встановити пріоритети, окреслити та узгодити функціональні та технічні вимоги, продиктовані бізнесом, які охоплюють весь спектр ініціатив, необхідних для досягнення очікуваних кінцевих результатів від реалізації програми інвестицій в IT.

AI1.2 Звіт щодо результатів аналізу ризиків
Виявити, задокументувати та проаналізувати ризики, пов'язані з виконанням бізнес вимог та дизайном рішення, в межах передбаченого в організації процесу розробки вимог.

AI1.3 Техніко-економічне вивчення та формулювання альтернативних планів дій
Розробити техніко-економічне вивчення яке досліджує можливість реалізації вимог. Керівництво бізнес-підрозділів, за підтримки IT служби, повинно оцінити можливість виконання вимог та альтернативні плани дій, та надати рекомендації бізнес замовнику.

AI1.4 Прийняття рішення та схвалення вимог і техніко-економічного вивчення
Пересвідчитись в тому, що процес вимагає від бізнес замовника узгодження та затвердження функціональних та технічних вимог та звітів стосовно техніко-економічного вивчення на заздалегідь визначених ключових етапах проекту. Бізнес замовник повинен прийняти остаточне рішення відносно вибору IT рішення та способу його набуття.

Керівні принципи управління

AI1 Визначати рішення з автоматизації

Від	Вхідні дані
PO1	Стратегічні та тактичні IT плани
PO3	Регулярно поновлювана інформація про «стан технології"; технологічні стандарти
PO8	Стандарти придбання та розробки
PO10	Керівні принципи управління проектами та детальні плани проектів
AI6	Опис процесу змін
DS1	Угоди про рівень обслуговування
DS3	План забезпечення продуктивності та потужностей (вимоги)

Вихідні дані	Для						
Аналіз можливості реалізації бізнес-вимог	PO2	PO5	PO7	AI2	AI3	AI4	AI5

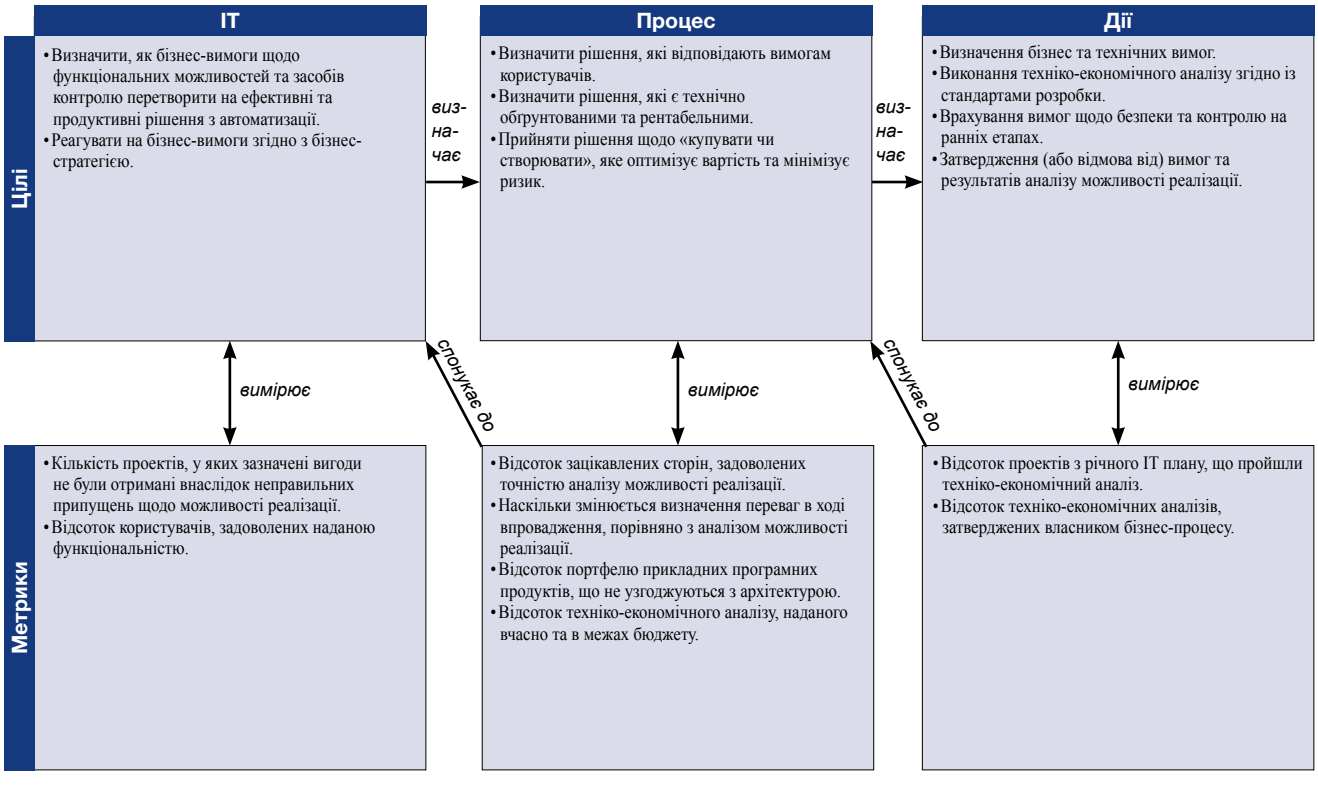
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Визначити функціональні та технічні вимоги з боку бізнесу			C	C	R	C	R	R		A/R	I
Запровадити процеси, що забезпечують цілісність/актуальність вимог				C		C		C		A/R	C
Визначити, задокументувати та проаналізувати ризики бізнес-процесів			A/R	R	R	R	C	R		R	C
Виконати аналіз можливості реалізації/оцінку наслідків щодо впровадження запропонованих бізнес-вимог			A/R	R	R	C	C	C		R	C
Оцінити операційні вигоди для IT від запропонованих рішень		I	R	A/R	R	I	I	I		R	
Оцінити бізнес вигоди від запропонованих рішень			A/R	R		C	C	C	I	R	
Розробити процес затвердження вимог			C	A		C	C	C		R	C
Узгодити та затвердити запропоновані рішення		C	A/R	R	R	C	C	C	I	R	C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



МОДЕЛЬ ЗРІЛОСТІ

AI1 Визначати рішення з автоматизації

Управління процесом *«Визначати рішення з автоматизації»*, який задовольняє бізнес-вимогу до IT *«втілення вимог бізнесу до функціональних можливостей та засобів контролю в ефективний та продуктивний дизайн автоматизованих рішень»*, знаходиться на рівні:

0 Не існуючий, якщо
Організація не вимагає визначення функціональних та експлуатаційних вимог щодо розробки, впровадження або модифікації рішень, які стосуються систем, послуг інфраструктури, програмного забезпечення та даних. Організація не стежить за наявними технологічними рішеннями, потенціальне корисними до її діяльності.

1 Початковий, якщо
Має місце усвідомлення потреби у визначенні вимог та відповідних технологічних рішень. Окремі групи спеціалістів збираються для неформального обговорення існуючих потреб, інколи вимоги документуються. Рішення визначають окремі особи на основі обмеженої інформованості про стан ринку або у відповідь на пропозиції постачальників. Структурований аналіз або вивчення доступних технологій знаходиться на мінімальному рівні.

2 Повторюваний але інтуїтивний, якщо
Для визначення IT рішень існує декілька інтуїтивних підходів, які відрізняються серед бізнес-підрозділів. Рішення визначаються неформально на підставі власного досвіду та знань спеціалістів IT служби. Успіх кожного проекту залежить від досвіду кількох ключових спеціалістів. Рівень якості документування та процесу прийняття рішень суттєво коливається. До визначення вимог та оцінки технологічних рішень застосовуються безсистемні підходи.

3 Визначений, якщо
Мають місце чіткі та системні підходи до визначення IT рішень. Визначення IT рішень вимагає розгляду альтернативних варіантів, враховуючі вимоги бізнесу та користувачів, технологічні можливості, економічну обґрунтованість, оцінку ризиків та інші чинники. Процес визначення IT рішень застосовується у деяких проектах, в залежності від таких чинників як рішення, прийняті окремими учасниками проекту, кількість часу, витраченого на управління, а також обсяг та першочерговість початкових бізнес-вимог. До визначення вимог та оцінки IT рішень застосовуються системні підходи.

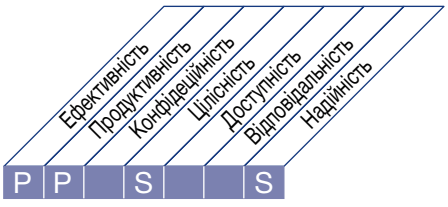
4 Керований та вимірюваний, якщо
Запроваджено затверджену методологію визначення та оцінки IT рішень, яка застосовується для більшості проектів. Проектна документація має високий рівень якості, кожний етап проекту належним чином затверджується. Вимоги чітко сформульовані та відповідають заздалегідь визначеним схемам. Розглядаються альтернативні варіанти рішень,в тому числі з точки зору витрат та вигод. Методологія є чіткою, визначеною, зрозумілою для всіх та вимірюваною. Існує чітко визначений механізм взаємодії між керівництвом IT та бізнесом у питаннях визначення та оцінки IT рішень.

5 Оптимізований, якщо
Методологія визначення та оцінки IT рішень постійно вдосконалюється. Методологія придбання та впровадження гнучко застосовується до проектів великого та малого масштабу. Ця методологія підтримується внутрішньою та зовнішньою базами знань, що містять довідкові матеріали стосовно технологічних рішень. Сама методологія формує документацію заздалегідь визначеної структури, яка забезпечує ефективне створення та супровід продукту. Часто визначаються нові можливості використання технологій з метою отримання конкурентної переваги, впливу на оптимізацію бізнес-процесів та підвищення загальної ефективності. Керівництво виявляє факти затвердження IT рішень без розгляду альтернативних технологій або без врахування функціональних бізнес-вимог, та вживає відповідних заходів.

Опис процесу

AI2 Забезпечувати придбання та підтримку прикладного програмного забезпечення

Прикладні програмні продукти впроваджуються враховуючи бізнес-вимоги. Цей процес складається з проектування прикладних програмних продуктів, належного врахування вимог до засобів контролю над прикладними програмними продуктами та вимог із безпеки, а також розробки та конфігурування згідно із стандартами. Це дозволяє організаціям належним чином підтримувати бізнес-операції відповідними автоматизованими прикладними програмними продуктами.



Контроль IT процесу

Забезпечувати придбання та підтримку прикладного програмного забезпечення

який задовольняє бізнес-вимоги до IT, а саме:

приведення наявних прикладних програмних продуктів у відповідність до бізнес вимог, роблячи це своєчасно та за розумною вартістю

зосереджений на

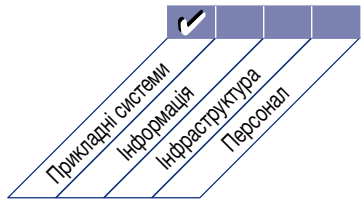
забезпеченні своєчасного та рентабельного процесу розробки

реалізується шляхом

- Врахування бізнес-вимог у технічних специфікаціях
- Дотримання стандартів розробки для усіх змін
- Розмежування діяльності з розробки, тестування та експлуатації

та вимірюється

- Кількістю проблем у ході розробки, з розрахунку на один прикладний програмний продукт, що спричинили очевидну втрату часу
- Відсотком користувачів, задоволених наданою функціональністю



Цілі контролю

AI2 Забезпечувати придбання та підтримку прикладного програмного забезпечення

AI2.1 Дизайн високого рівня
Перетворити бізнес-вимоги у специфікації дизайну високого рівня з метою придбання програмного забезпечення, беручи до уваги напрямок технологічного розвитку та інформаційну архітектуру в організації. Затвердити специфікації дизайну у керівництва, щоб бути впевненим у відповідності дизайну високого рівня існуючим вимогам. Переоцінювати у випадках виникнення значних технічних або логічних невідповідностей в ході розробки або підтримки програмного забезпечення.

AI2.2 Детальний дизайн
Підготувати детальний дизайн та технічні вимоги до прикладного програмного забезпечення. Визначити критерії прийняття вимог. Затвердити вимоги, щоб упевнитись у їх відповідності дизайну високого рівня. Робити перегляд у випадках виникнення значних технічних або логічних невідповідностей в ході розробки або підтримки програмного забезпечення.

AI2.3 Контрольованість прикладних програм
Втілити бізнес-контролі, де це потрібно, в автоматизовані механізми контролю прикладних програм таким чином, щоб процес обробки даних був точним, повним, своєчасним, санкціонованим та з можливостями перевірки.

AI2.4 Безпека та доступність прикладних програм
Звернути увагу на вимоги до безпеки та доступності прикладних програм відповідно до виявлених ризиків та згідно із класифікацією даних у організації, інформаційною архітектурою, архітектурою інформаційної безпеки та відношенням до допустимих ризиків.

AI2.5 Конфігурація та впровадження придбаного прикладного програмного забезпечення
Провести конфігурацію та впровадити придбане прикладне програмне забезпечення відповідно до бізнес-цілей.

AI2.6 Суттєві зміни в існуючих системах
У випадку внесення суттєвих змін в існуючі системи, що призводить до значних змін у дизайні та/або функціональних можливостях, дотримуватись процесу розробки, аналогічного тому, що використовується для розробки нових систем.

AI2.7 Розробка прикладного програмного забезпечення
Забезпечити розробку автоматизованого функціоналу у відповідності до специфікацій дизайну, стандартів розробки та створення документації, вимог до гарантування якості та стандартів схвалення рішень. Забезпечити визначення та врахування всіх законодавчих та договірних аспектів щодо прикладного програмного забезпечення, розробленого третіми сторонами.

AI2.8 Забезпечення гарантування якості прикладного програмного забезпечення
Розробити, забезпечити ресурсами та виконати план гарантування якості програмного забезпечення, щоб отримати рівень якості, передбачений визначеними вимогами та політиками і процедурами щодо якості, що діють в організації.

AI2.9 Управління вимогами до прикладного програмного забезпечення
Відстежувати стан окремих вимог (в тому числі всіх відхилених вимог) в процесі проектування, розробки та впровадження, та затверджувати зміни до вимог згідно встановленого процесу управління змінами.

AI2.10 Підтримка прикладного програмного забезпечення
Розробити стратегію та план підтримки прикладного програмного забезпечення.

Керівні принципи управління

AI2 Забезпечувати придбання та підтримку прикладного програмного забезпечення

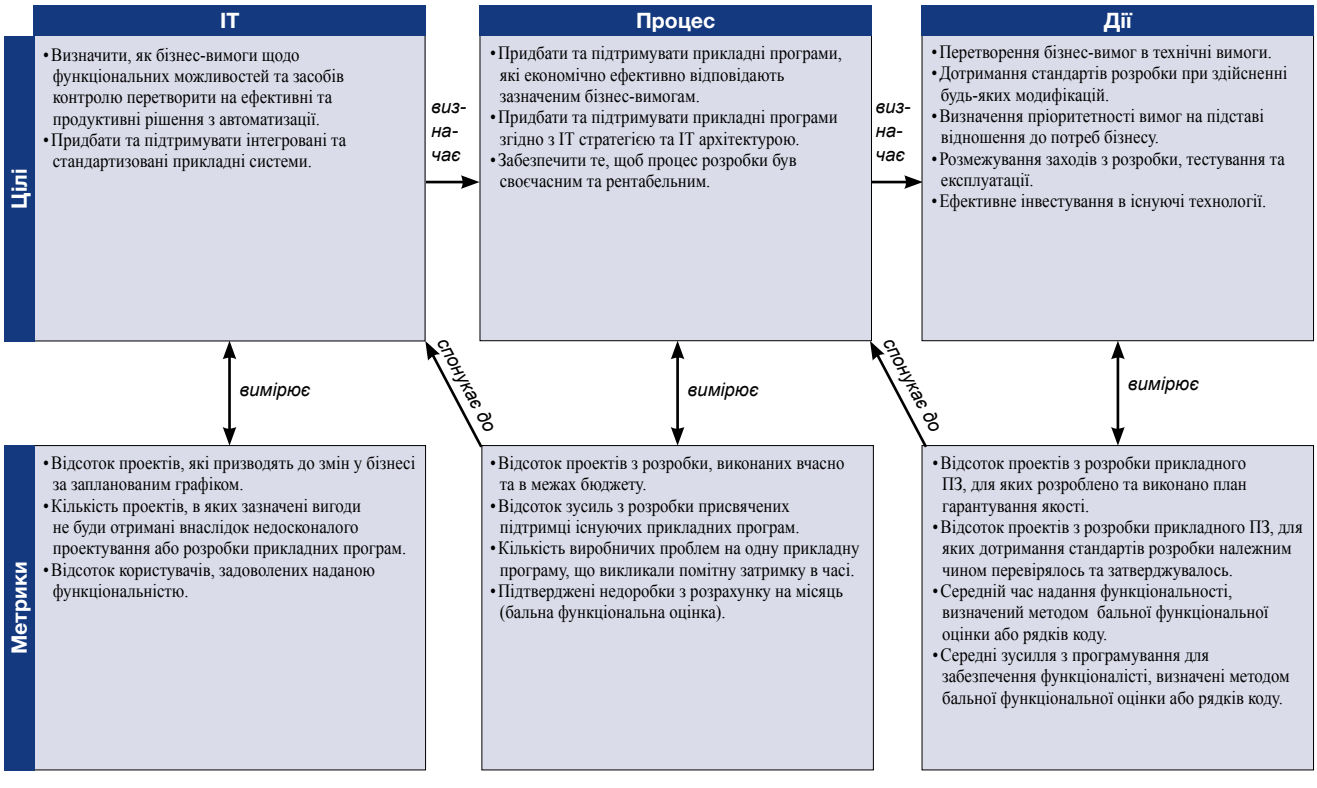
Від	Вхідні дані
PO2	Словник даних, схема класифікації даних, оптимізований план бізнес-систем
PO3	Регулярні оновлення даних щодо «стану технології»
PO5	Звіти щодо витрат та вигод
PO8	Принципи управління проектами, плани робочих проектів
PO10	Опис процесу змін
AI1	Техніко-економічне вивчення бізнес вимог
AI6	Опис процесу внесення змін

Вихідні дані	Для						
Вимоги до засобів безпеки прикладного ПЗ	DS5						
Знання прикладного ПЗ та пакетів	AI4						
Рішення щодо придбання	AI5						
Початкові заплановані угоди щодо рівня послуг	DS1						
Вимоги до доступності, безперебійності та відновлення	DS3	DS4					

RACI-діаграма

Дії	Функції										
	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Перетворити бізнес-вимоги у специфікації дизайну високого рівня.					C		C	A/R		R	C
Підготувати детальний дизайн та технічні вимоги до прикладного програмного забезпечення.				I	C	C	C	A/R		R	C
В рамках дизайну визначити контролі прикладного програмного забезпечення.					R	C		A/R		R	R
Налагодити та впровадити придбаний автоматичний функціонал.					C	C		A/R		R	C
Розробити формалізовані методології та процеси управління процесом розробки прикладного ПЗ.				C		C	C	A	C	R	C
Скласти план гарантування якості програмного забезпечення для проекту.					I		C	R		A/R	C
Відстежувати та управляти вимогами до прикладних програм.								R		A/R	
Розробити план підтримки прикладного програмного забезпечення.				C		C		A/R		C	

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

AI2 Забезпечувати придбання та підтримку прикладного програмного забезпечення

Управління процесом «Забезпечувати придбання та підтримку прикладного програмного забезпечення», який задовольняє бізнес-вимогу до IT «приведення наявних прикладних програмних продуктів у відповідність до бізнес вимог, роблячи це своєчасно та за розумною вартістю», знаходиться на рівні:

0 Не існуючий, якщо
Не існує процесу розробки та визначення прикладного програмного забезпечення. Як правило, прикладні програми придбаються базуючись на пропозиціях постачальників, відомістю торгової марки або на ознайомленості спеціалістів IT служби з конкретними програмними продуктами, при цьому фактичні вимоги майже або зовсім не враховуються.

1 Початковий, якщо
Має місце усвідомлення того, що потрібен процес придбання та підтримки прикладних програм. Підходи до придбання та підтримки прикладного програмного забезпечення для різних проектів різні. Деякі окремі рішення конкретних бізнес-вимог, скоріш за все, були придбані незалежно, що призвело до неефективності їх експлуатації та підтримки.

2 Повторюваний але інтуїтивний, якщо
Існують різні, але подібні процеси для придбання та підтримки прикладних програм, які базуються на досвіді та кваліфікаціях спеціалістів IT служби. Успішність впровадження прикладних програм в значній мірі залежить від власної кваліфікації та досвіду спеціалістів IT. Підтримка зазвичай проблематична та погіршується, коли кваліфіковані спеціалісти залишають організацію. При розробці або придбанні прикладного програмного забезпечення недостатньо враховуються питання безпеки та доступності прикладних програм.

3 Визначений, якщо
Існує чіткий, визначений та в цілому зрозумілий процес придбання та підтримки прикладного програмного забезпечення. Цей процес узгоджений з IT стратегією та бізнес-стратегією. Зроблено спробу послідовно застосовувати документовані процеси до різних прикладних програм та проектів. Методології, як правило, не є гнучкими та їх складно застосувати в усіх випадках, тому деякі етапи можуть бути проігноровані. Заходи з підтримки плануються, виконуються за графіком та координуються.

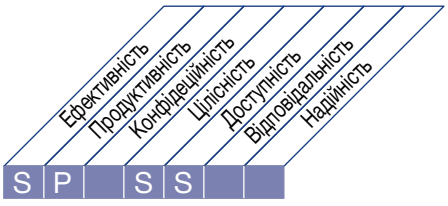
4 Керований та вимірюваний, якщо
Існує формальна та добре зрозуміла методологія, до якої належать процес дизайну та розробки технічних специфікацій, критерії придбання, процес тестування та вимоги до документації. Впроваджено документовані та узгоджені механізми затвердження, задля впевненості у дотриманні всіх етапів процесу та санкціонування відхилень. Практики та процедури розвиваються та добре підходять для організації, використовуються всіма штатними працівниками та є застосовними до більшості вимог до прикладних програм.

5 Оптимізований, якщо
Практики придбання та підтримки прикладного програмного забезпечення відповідають встановленому процесу. Цей підхід є компонентно-орієнтованим, з заздалегідь визначеними, стандартизованими прикладними програмами відповідно до потреб бізнесу. Підхід застосовується в масштабах всього підприємства. Методологія придбання та підтримки є «просунутою» та дозволяє швидке розгортання програмного продукту, що забезпечує високий рівень гнучкості та швидкості реагування на зміни у бізнес-вимогах. Методологія придбання та впровадження прикладного програмного забезпечення постійно вдосконалюється та підтримується власними та сторонніми базами знань, що містять довідкові матеріали та найкращі практики. За методологією документація створюється за заздалегідь визначеною структурою, що забезпечує ефективність процесу виробництва та підтримки.

Опис процесу

AI3 Забезпечувати придбання та підтримку технологічної інфраструктури

Організації мають процеси, що передбачають придбання, впровадження та оновлення технологічної інфраструктури. Це потребує планового підходу до придбання, підтримки та захисту інфраструктури відповідно до узгодженим стратегіям впровадження технологій та забезпечення середовищ розробки та тестування. Таким чином гарантується постійна технологічна підтримка прикладних програмних продуктів для бізнесу.



Контроль IT процесу

Забезпечувати придбання та підтримку технологічної інфраструктури

який задовольняє бізнес-вимоги до IT, а саме:

забезпечення придбання та підтримки інтегрованої та стандартної IT інфраструктуру

зосереджений на

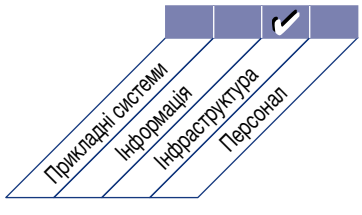
забезпеченні відповідних платформ для прикладних програмних продуктів для ділової сфери згідно з визначеною IT архітектурою та технологічними стандартами

реалізується шляхом

- Створення плану придбання технології, який узгоджується з планом технологічної інфраструктури
- Плануванням підтримки інфраструктури
- Запровадження заходів внутрішнього контролю, забезпечення безпеки та можливості перевірки

та вимірюється

- Відсотком платформ, які не відповідають визначеній IT інфраструктурі та технологічним стандартам
- Кількістю критичних бізнес-процесів, підтриманих застарілою (або яка найближчим часом застаріє) інфраструктурою



Цілі контролю

AI3 Забезпечувати придбання та підтримку технологічної інфраструктури

AI3.1 План придбання технологічної інфраструктури
Скласти план придбання, впровадження та підтримки технологічної структури, що відповідає визначеним функціональним та технічним вимогам та узгоджується з напрямком розвитку технологій в організації.

AI3.2 Захист та доступність ресурсів інфраструктури
Впровадити засоби внутрішнього контролю, безпеки та можливості перевірки в ході створення конфігурації, інтеграції та супроводу апаратного та програмного забезпечення інфраструктури з метою захисту ресурсів та гарантії доступності та цілісності. Відповідальність за використання важливих компонентів інфраструктури має бути чітко визначеною та усвідомленою тими особами, які розробляють компоненти інфраструктури та здійснюють їх інтеграцію. Їх використання слід контролювати та оцінювати.

AI3.3 Підтримка інфраструктури
Розробити стратегію та план підтримки інфраструктури, а також забезпечити контроль змін згідно з процедурою управління змінами, прийнятою в організації. Передбачити періодичні перевірки на відповідність потребам бізнесу, управління патчами, стратегії оновлення, врахувати ризики, здійснювати оцінку вразливостей та ввести вимоги до системи захисту.

AI3.4 Умови (середовище) для перевірки технічної можливості
Створити середовища розробки та тестування для проведення ефективного та продуктивного тестування технічних можливостей та комплексних випробувань системи в цілому.

Керівні принципи управління

AI3 Забезпечувати придбання та підтримку технологічної інфраструктури

Від	Вхідні дані
PO3	План технологічної інфраструктури, стандарти та можливості, оновлені дані щодо «стану технології»
PO8	Стандарти придбання та розробки
PO10	Принципи управління проектами, плани робочих проектів
AI1	Техніко-економічне обгрунтування
AI6	Опис процесу змін
DS3	План продуктивності та потужностей

Вихідні дані	Для						
Рішення щодо придбання	AI5						
Скомпонована система для тестування/інсталяції	AI7						
Вимоги до фізичного оточення	DS12						
Поправки до технологічних стандартів	PO3						
Вимоги до моніторингу систем	DS3						
Знання інфраструктури	AI4						
Початкові заплановані угоди OLA	DS1						

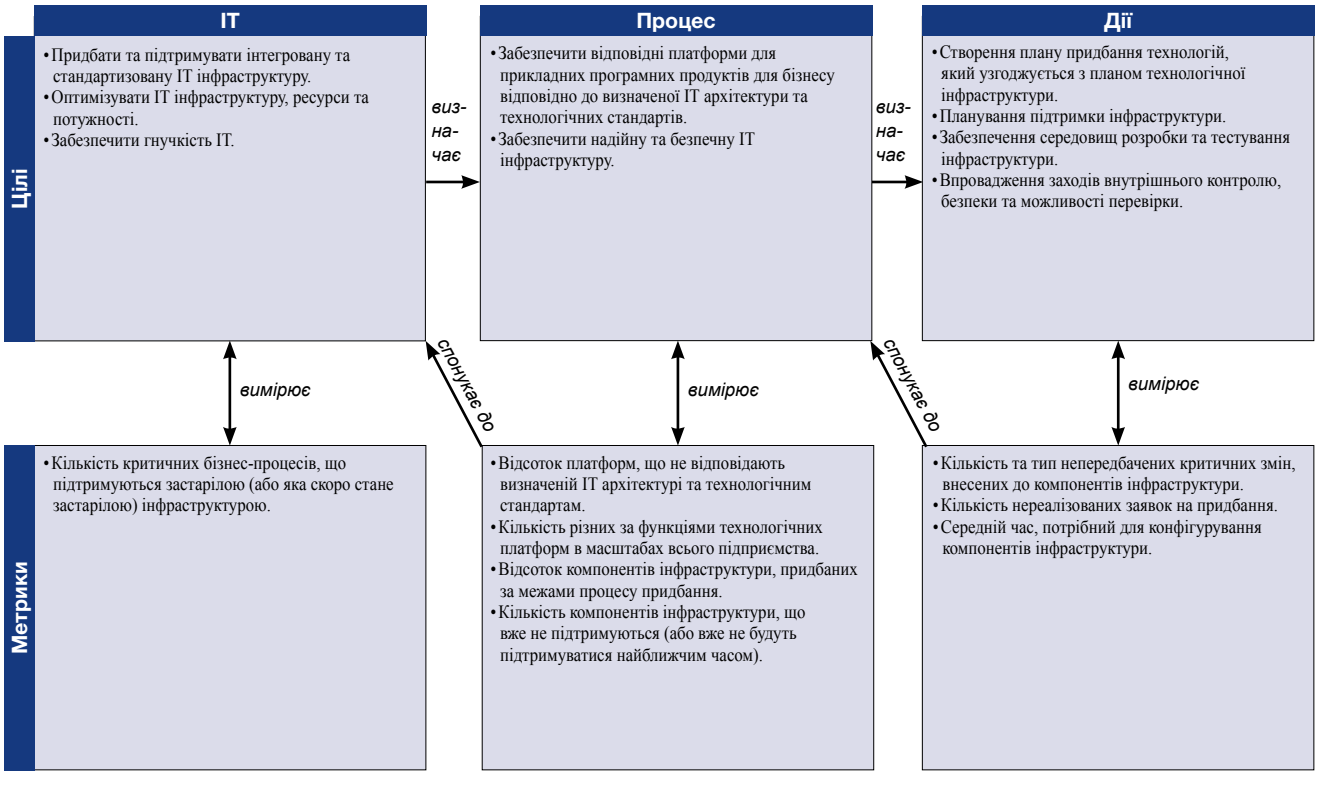
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог аудиту, ризиків та безпеки
Визначити процедуру/процес придбання.		C		A		C	C	C	R		I
Обговорити вимоги до інфраструктури з (затвердженими) постачальниками.		C/I		A	I	R	C	C	R		I
Визначити стратегію та план підтримки інфраструктури.				A		R	R	R	C		
Здійснити конфігурацію компонентів інфраструктури.				A		R	C				I

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

AI3 Забезпечувати придбання та підтримку технологічної інфраструктури

Управління процесом *«Забезпечувати придбання та підтримку технологічної інфраструктури»*, який задовольняє бізнес-вимогу до IT *«придбати та підтримувати інтегровану та стандартну IT інфраструктуру»*, знаходиться на рівні:

0 Не існуючий, якщо
Управління технологічною інфраструктурою не визнається вкрай важливою проблемою, яку потрібно вирішувати.

1 Початковий, якщо
До інфраструктури для кожного нового прикладного програмного продукту вносяться зміни, але жодного загального плану не існує. Хоча і є усвідомлення важливості інфраструктури, немає послідовного загального підходу. Заходи з підтримки здійснюються у відповідь на короткострокові потреби. Робоче середовище є середовищем тестування.

2 Повторюваний але інтуїтивний, якщо
Існує узгодженість між тактичними підходами до придбання та підтримки IT інфраструктури. Придбання та підтримка IT інфраструктури не базуються на жодній визначеній стратегії та при цьому не враховуються потреби прикладних програмних продуктів для сфери бізнесу, які необхідно підтримувати. Має місце розуміння важливого значення IT інфраструктури, яке підтримане кількома формальними практиками. Підтримка в деякій мірі здійснюється за планом, але повноцінного плану та відповідної координації не існує. У випадку деяких середовищ існує окреме середовище тестування.

3 Визначений, якщо
Існує чіткий, визначений та в основному зрозумілий процес придбання та підтримки IT інфраструктури. Цей процес підтримує потреби критично важливих прикладних програмних продуктів та узгоджується з IT стратегією та бізнес-стратегією, але застосовується непослідовно. Підтримка інфраструктури планується, здійснюється за графіком та є координованою. Існують індивідуальні середовища для тестування та промислової експлуатації.

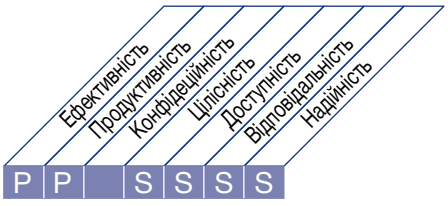
4 Керований та вимірюваний, якщо
Процес придбання та підтримки технологічної інфраструктури розвинений до такої стадії, на якій він добре працює у більшості ситуацій, виконується послідовно та орієнтований на можливість багатократного застосування. IT інфраструктура належним чином підтримує прикладні програмні продукти для ділової сфери. Процес є добре організованим та прогнозованим. Витрати та період часу, необхідні для досягнення очікуваного рівня масштабованості, гнучкості та інтеграції частково оптимізовані.

5 Оптимізований, якщо
Процес придбання та підтримки технологічної інфраструктури є прогнозованим та максимально узгодженим з критичними прикладними програмними продуктами та технологічною архітектурою. Використовуються найкращі практики, що стосуються сфери технологічних рішень, організація поінформована про найновіші розробки в області платформ та засобів управління. Витрати зменшено завдяки раціоналізації та стандартизації компонентів інфраструктури та застосуванню автоматизації. Високий рівень технічної обізнаності дозволяє визначити оптимальні способи підвищення продуктивності, в тому числі розглянути варіанти залучення сторонніх ресурсів. IT інфраструктура розглядається як ключовий чинник, який дозволяє отримати максимальну користь від застосування IT.

Опис процесу

AI4 Забезпечувати експлуатацію та використання

Знання про нові системи стають доступними. Цей процес передбачає створення документації та посібників для користувачів та IT спеціалістів, а також забезпечує проведення навчання, щоб гарантувати належне використання та експлуатацію прикладних програмних продуктів та інфраструктури.



Контроль IT процесу

Забезпечувати експлуатацію та використання

який задовольняє бізнес-вимоги до IT, а саме:

гарантування задоволення кінцевих користувачів переліком послуг, що пропонуються, та рівнем надання послуг, а також забезпечення органічної інтеграції прикладних програмних продуктів та технологічних рішень в бізнес-процеси

зосереджений на

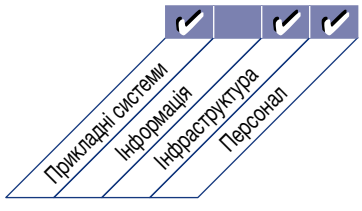
наданні ефективних інструкцій для користувачів та інструкцій з експлуатації, а також навчальних матеріалів з метою передачі знань, необхідних для успішної експлуатації та використання прикладних програмних продуктів та інфраструктури

реалізується шляхом

- Розробки та доступності документації, що забезпечує передачу знань
- Інформування та навчання користувачів, керівництва бізнес-підрозділів, персоналу служби підтримки та операційної служби
- Створення навчальних матеріалів

та вимірюється

- Кількістю прикладних програмних продуктів, у яких IT процедури є органічно інтегрованими в бізнес-процеси
- Відсотком власників процесів, задоволених рівнем навчальних та допоміжних матеріалів, що стосуються прикладних програмних продуктів
- Кількістю прикладних програмних продуктів, для яких забезпечене належне навчання з питань використання та експлуатації



Цілі контролю

AI4 Забезпечувати експлуатацію та використання

AI4.1 Планування діяльності з операційних рішень
Розробити план, який передбачає визначення та документування всіх технічних, експлуатаційних аспектів, а також аспектів використання, щоб всі особи, які будуть експлуатувати, використовувати та здійснювати підтримку автоматизованих рішень, могли виконувати свої обов'язки.

AI4.2 Передача знань керівництву бізнес-підрозділів
Передати знання та інформацію керівництву бізнес-підрозділів для того, щоб вказані особи могли узяти на себе володіння системами та даними та виконувати свої обов'язки з надання послуг та забезпечення якості, внутрішнього контролю та адміністрування прикладних продуктів та систем.

AI4.3 Передача знань кінцевим користувачам
Передавати знання та професійний досвід, щоб кінцеві користувачі могли ефективно та продуктивно використовувати систему на підтримку бізнес-процесів.

AI4.4 Передача знань персоналу служби підтримки та операційної служби
Передавати знання та професійний досвід персоналу служби підтримки та операційної служби, щоб вказані спеціалісти могли ефективно та продуктивно здійснювати надання послуг, підтримку та обслуговування систем та відповідної інфраструктури.

Керівні принципи управління

AI4 Забезпечувати експлуатацію та використання

Від	Вхідні дані
P010	Принципи управління проектами, плани робочих проектів
AI1	Техніко-економічне вивчення бізнес-вимог
AI2	Знання щодо прикладного програмного забезпечення
AI3	Знання щодо інфраструктури
AI7	Відомі та прийнятні помилки
DS7	Необхідні оновлення документації

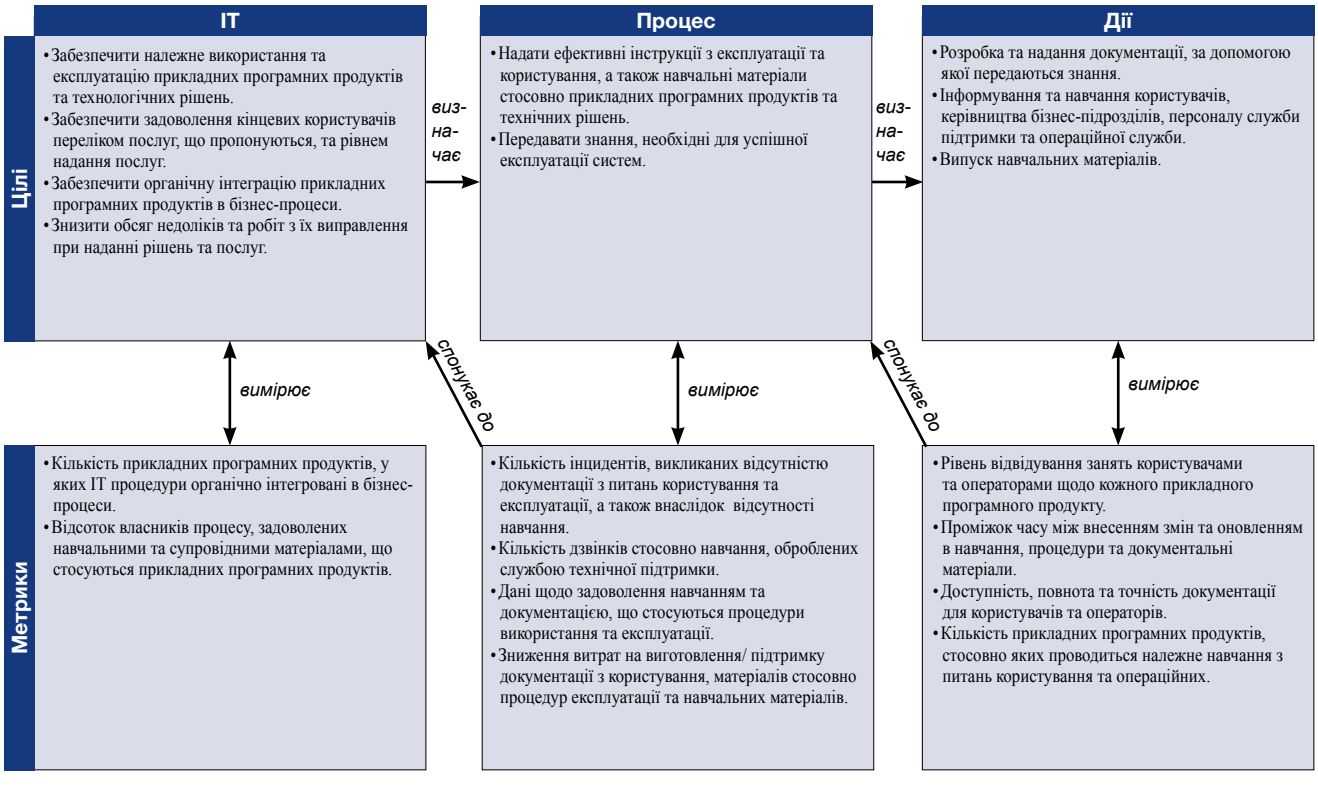
Вихідні дані	Для						
Інструкції користувача, операціоніста, підтримки, технічного обслуговування та адміністрування	AI7	DS4	DS8	DS9	DS11	DS13	
Вимоги до передачі знань у випадку впровадження рішень	DS7						
Навчальні матеріали	DS7						

RACI-діаграма

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки	Команда розгортання	Департамент тренувань
Розробити стратегію введення рішення в експлуатацію.				A	A	R		R			I	R	C
Розробити методологію передачі знань.				C	A							C	R
Розробити процедурні інструкції для кінцевих користувачів.					A/R			R			C	C	
Розробити документацію з технічної підтримки для персоналу служби підтримки та операційної служби.						A/R		C			C		
Розробити навчальні курси та проводити навчання.					A	A		R					R
Оцінити результати навчання та в разі необхідності оновити документацію.					A	A						R	R

Функції

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

AI4 Забезпечувати експлуатацію та використання

Управління процесом *«Забезпечувати експлуатацію та використання»*, який задовольняє бізнес-вимогу до IT *«гарантувати задоволення кінцевих користувачів переліком послуг, що пропонуються, та рівнем надання послуг, а також забезпечити органічну інтеграцію прикладних програмних продуктів та технологічних рішень в бізнес-процеси»*, знаходиться на рівні:

0 Не існуючий, якщо
В організації не впроваджено процес, передбачений для створення документації для користувачів, операційних інструкцій та навчальних матеріалів. У наявності є тільки ті матеріали, що надійшли разом з придбаною продукцією.

1 Початковий, якщо
Є усвідомлення потреби у процесі створення документації. Час від часу документація створюється та безсистемно розповсюджується серед деяких груп. Більшість документації та велика кількість процедур застаріли. Навчальні матеріали зазвичай передбачені для окремих випадків та різної якості. Немає фактично ніякої інтеграції процедур між різними системами та бізнес-підрозділами. Бізнес-підрозділи не беруть участі в розробці навчальних програм.

2 Повторюваний але інтуїтивний, якщо
Для створення процедур та документації використовуються подібні процеси, але в їх основі не лежить системний підхід або якась схема. Немає однакового підходу до розробки процедур використання та операційних. Навчальні матеріали випускаються окремими особами або проектними групами, їх якість залежить від рівня залучених до цього процесу осіб. Рівень процедур та якість підтримки користувачів змінюються від низького до дуже високого, ступінь сумісності та інтеграції їх в масштабах організації є дуже слабким. Навчальні програми для спеціалістів ділової сфери та користувачів існують або надаються, але немає загального плану проведення навчальних заходів.

3 Визначений, якщо
Існує чітко визначений, визнаний та зрозумілий механізм створення документації для користувачів, операційних інструкцій та навчальних матеріалів. Процедури зберігаються та підтримуються у формальній бібліотеці, до них може отримати доступ будь-хто, кому потрібно ознайомитись з ними. Коригування документації та процедур відбувається у відповідь на конкретну проблему. Процедури доступні в режимі офлайн, у випадку аварійної ситуації можна здійснювати їх підтримку. Існує процес, який передбачає, що оновлення процедур та навчальні матеріали повинні робляться винятково у результаті проекту внесення змін. Незважаючи на існування визначених підходів, конкретна сутність різниться, оскільки не здійснюється контроль за дотриманням стандартів. Користувачі неформально залучені до процесу. Все частіше для генерації та розповсюдження процедур використовуються автоматизовані засоби. Навчання спеціалістів зі сфери бізнесу та користувачів здійснюється за планом та відповідним графіком.

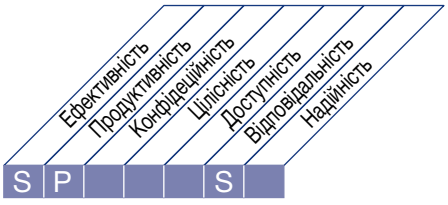
4 Керований та вимірюваний, якщо
Існує визначений механізм підтримки процедур та навчальних матеріалів, який підтримує керівництво IT. Підхід, що застосовується для підтримки процедур та навчальних матеріалів, охоплює всі системи та бізнес-підрозділи, з метою погляду на процеси з точки зору бізнесу. Процедури та навчальні матеріали інтегровані з урахуванням взаємозалежностей та інтерфейсу. Існує контроль щодо дотримання стандартів, процедури розробляються та підтримуються для всіх процесів. Накопичуються відгуки бізнесу та користувачів стосовно документації та навчання, які аналізуються як частина постійного процесу вдосконалення. Документація та навчальні матеріали, як правило, мають прогнозований та високий рівень надійності та доступності. Впроваджується процес документування та керування автоматизованими процедурами. Розробка автоматизованих процедур все більш інтегрується з розробкою прикладних систем, що забезпечує їх узгодженість та доступ користувачів. Навчання представників бізнесу та користувачів відповідає потребам бізнесу. Керівництво IT розробляє показники для оцінки створення та надання документації, навчальних матеріалів та програм.

5 Оптимізований, якщо
Процес створення документації для користувачів та операціоністів постійно вдосконалюється шляхом введення в дію нових інструментів або методів. Навчальні матеріали та все, що стосуються процедур, існує у вигляді прогресуючої бази знань, яка підтримується у електронному виді з використанням сучасних технологій управління знаннями, діловодства та документообігу, та їх розповсюдження, що забезпечує можливості доступу та легкість підтримки. Документація та навчальні матеріали оновлюються з врахуванням змін в організації, операціях та програмному забезпеченні. Розробка документації та навчальних матеріалів, а також їх надання, повністю інтегровані з бізнесом та з визначеннями бізнес-процесів, що забезпечує відповідність вимогам, які висуваються в організації в цілому, а не тільки у сфері IT.

Опис процесу

AI5 Закуповувати IT-ресурси

IT ресурси, в томі числі персонал, апаратне забезпечення, програмне забезпечення та послуги необхідно забезпечувати. Для цього потрібно визначити та забезпечити виконання процедур здійснення закупівель, вибору постачальників, порядку укладення контрактних угод та безпосередньо процесу придбання. Виконання вищевикладеного гарантує, що організація отримає всі необхідні IT ресурси своєчасно та з максимальною економічною ефективністю.



Контроль IT процесу

Закуповувати IT-ресурси

який задовольняє бізнес-вимоги до IT, а саме:

підвищення економічної ефективності IT та внесок IT у рентабельність бізнесу

зосереджений на

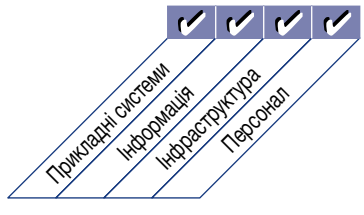
здобутті та підтримці IT кваліфікацій, що відповідають виконанню стратегії, інтегрованої та стандартизованої IT інфраструктури, та зниженню ризиків IT забезпечення

реалізується шляхом

- Отримання консультацій спеціалістів з юридичних та договірних питань
- Визначенням процедур, порядку та стандартів закупівель
- Забезпечення необхідного апаратного та програмного забезпечення та послуг згідно з визначеними процедурами

та вимірюється

- Кількістю спорів, що виникли у зв'язку з контрактами на закупівлі (постачання)
- Сумою знижок вартості придбання
- Відсотком ключових зацікавлених сторін, задоволених діяльністю постачальників



Цілі контролю

AI5 Закуповувати IT-ресурси

AI5.1 Контроль закупівель
Розробити та дотримуватись сукупності процедур та стандартів, які узгоджуються із загальноприйнятим в організації процесом здійснення поставок та стратегією закупівель щодо придбання інфраструктури, засобів, апаратного та програмного забезпечення та послуг, пов'язаних із сферою IT та необхідних бізнесу.

AI5.2 Управління контрактами з постачальниками
Впровадити порядок укладення, внесення змін та розірвання контрактів з усіма постачальниками. Вказаний порядок повинен передбачати, як мінімум, відповідальність з правових, фінансових, організаційних питань, а також з питань, пов'язаних з документацією, експлуатацією, безпекою, інтелектуальною власністю та припиненням дії контракту (в тому числі включення пунктів щодо штрафів). Всі контракти та зміни до них мають бути перевірені юристами.

AI5.3 Вибір постачальників
Вибирати постачальників згідно з справедливою та формальною практикою з метою забезпечення максимальної відповідності встановленим вимогам. Вимоги необхідно оптимізувати на підставі інформації від потенційних постачальників.

AI5.4 Придбання IT ресурсів
Захищати та забезпечувати реалізацію інтересів організації при виконанні всіх контрактних угод, в тому числі реалізацію прав та обов'язків всіх сторін згідно з умовами контракту щодо придбання програмного забезпечення, ресурсів для здійснення розробки, інфраструктури та послуг.

Керівні принципи управління

AI5 Закуповувати IT-ресурси

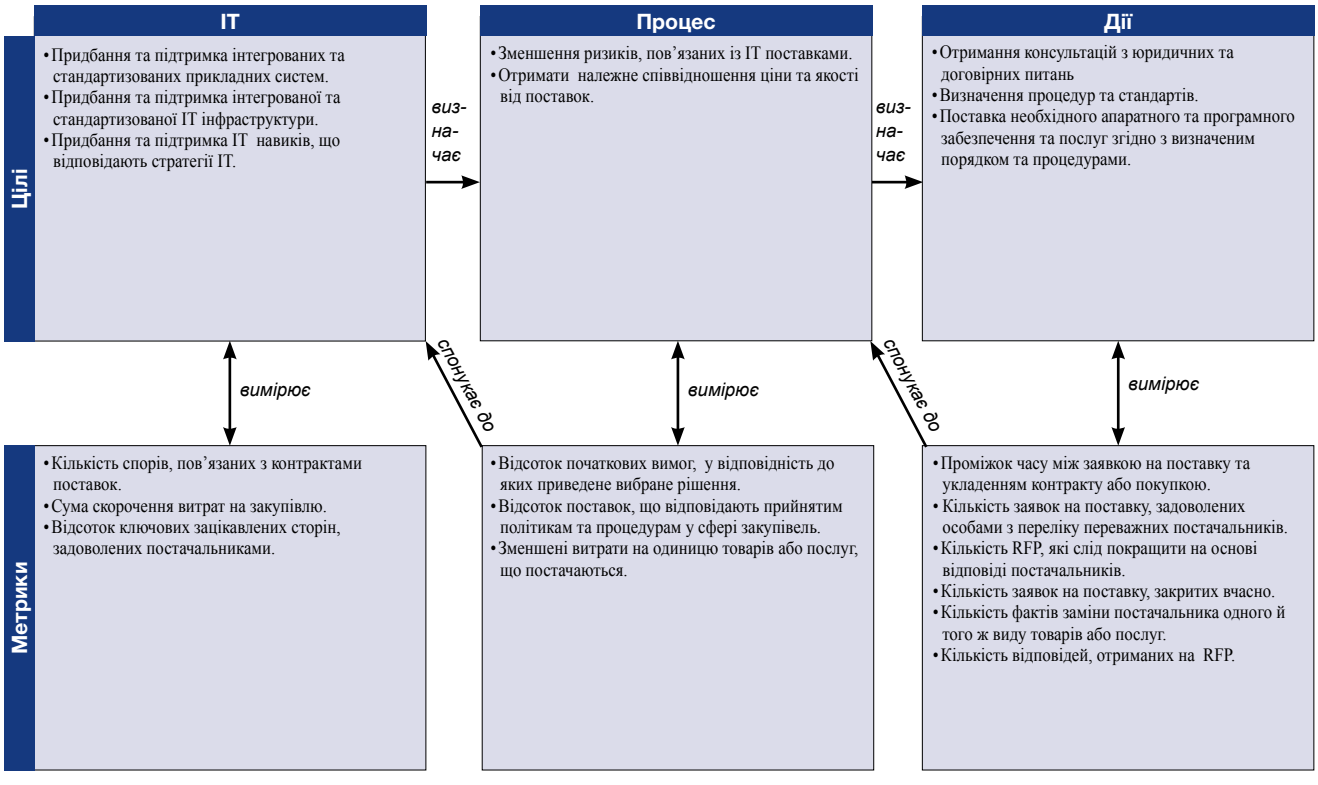
Від	Вхідні дані
PO1	Стратегія IT закупівель
PO8	Стандарти закупівель
PO10	Принципи управління проектами, плани робочих проектів
AI1	Техніко-економічне вивчення бізнес-вимог
AI2-3	Рішення по закупівлі
DS2	Каталог постачальників

Вихідні дані	Для						
Вимоги до управління стосунками з третіми сторонами	DS2						
Позиції до закупівлі	AI7						
Контрактні угоди	DS2						

RACI-діаграма

Дії / Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту ризиків та безпеки
Розробити політики та процедури здійснення закупівель та поставок у сфері IT, узгоджені з політиками закупівель, прийнятими на корпоративному рівні.	I	C		A		I	I	I	R		C
Визначити/оновлювати перелік акредитованих постачальників.									A/R		
Оцінити та вибрати постачальників за допомогою процесу заявок на пропозицію (RFP).	C	C		A		R		R	R	R	C
Розробити контракти, які захищають інтереси організації.	R	C		A		R		R	R		C
Здійснити закупівлі відповідно до встановлених процедур.				A		R		R	R		C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

AI5 Закуповувати IT-ресурси

Управління процесом *«Закуповувати IT-ресурси»*, який задовольняє бізнес-вимогу до IT *«підвищення економічної ефективності IT та внесок IT у рентабельність бізнесу»*, знаходиться на рівні:

0 Не існуючий, якщо
Не введений визначений процес поставок IT ресурсів. Організація не усвідомлює потреби у запровадженні чітко визначених політик та процедур, які забезпечують вчасне та економічно ефективне забезпечення всіх IT ресурсів.. . . . . .

1 Початковий, якщо
Організація визнає необхідність впровадження документованих політик та процедур, які пов'язують процес придбання IT з процесом здійснення закупівель в масштабах всієї організації. Розробка та управління контрактами на придбання IT ресурсів здійснюються керівниками проектів та іншими окремими особами, які керуються своїм рішенням, а не формальними процедурами та політиками. Має місце лише епізодичний зв'язок між корпоративними закупівлями та процесами управління контрактами в сфері IT. Адміністрування контрактів на закупівлю здійснюється лише при виконання проектів, а не на постійній основі.

2 Повторюваний але інтуїтивний, якщо
Організація усвідомлює потребу у впровадженні основних політик та процедур придбання IT. Політики та процедури частково інтегровані у процес здійснення закупівель в масштабах всієї організації. Процеси, пов'язані із закупівлями, головним чином використовуються у випадку великих та показових проектів. Обов'язки та конкретна відповідальність за закупівлю IT та управління контрактами визначаються згідно з індивідуальним досвідом керівників, які відповідають за контракти. Визнається важливе значення управління постачальниками та взаємостосунками з ними; однак, вказане управління реалізується з індивідуальної ініціативи. Договірні процеси здебільшого використовуються у випадку великих та показових проектів.

3 Визначений, якщо
Керівництво реалізує систему політик та процедур у сфері закупівель IT. Вказані політики та процедури інтегровані у загальний процес здійснення закупівель в масштабах всієї організації. Існують IT стандарти, що стосуються закупівлі та поставки IT ресурсів. Управління контрактами з постачальниками IT ресурсів інтегровано в схеми управління проектами організації в цілому. Керівництво IT служби поширює інформацію щодо необхідності здійснення належних закупівель та управління контрактами серед працівників IT служби.

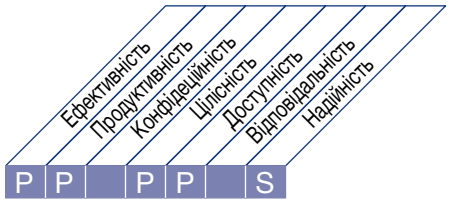
4 Керований та вимірюваний, якщо
Процес закупівлі IT повністю інтегровано у процес закупівель масштабах всієї організації. IT стандарти відносно закупівель IT ресурсів застосовуються до всіх закупівель та поставок. Здійснюються оцінки результатів управління контрактами та закупівлями згідно з економічним обґрунтуванням закупівель IT. Наявна звітність щодо діяльності з придбання IT, яка підтримує бізнес-цілі. Розвивається стратегічне управління взаємовідносинами з партнерами. Керівництво IT забезпечує виконання процесу закупівель та управління контрактами у випадку всіх закупівель, відстежуючи показники ефективності.

5 Оптимізований, якщо
Керівництво реалізує поставку ресурсів шляхом виконання процесів придбання IT. Керівництво забезпечує дотримання політик та процедур у сфері придбання IT. Здійснюються оцінки результатів управління контрактами та закупівлями згідно з економічним обґрунтуванням закупівель IT. З перебігом часу встановлюються надійні взаємостосунки з більшістю постачальників та партнерів, при цьому якість вказаних стосунків вимірюється та контролюється. Здійснюється стратегічне управління вказаними стосунками. Використовується стратегічний підхід до управління IT стандартами, політиками та процедурами в сфері закупівлі IT, який базується на результатах оцінки цього процесу. Керівництво IT служби роз'яснює стратегічно важливе значення належного процесу придбання IT та управління контрактами працівникам IT служби.

Опис процесу

AI6 Управляти змінами

Управління всіма змінами, які пов'язані з інфраструктурою та прикладним програмним забезпеченням, в тому числі непередбаченим обслуговуванням та установкою патчів, є формальним та контролюється. Зміни (в тому числі зміни до процедур, процесів, параметрів систем та обслуговування) протоколюються, оцінюються та санкціонуються перед їх внесенням, а після впровадження здійснюється їх оцінка у порівнянні із запланованими кінцевими результатами. Таким чином забезпечується зменшення ризиків негативного впливу на стабільність та цілісність робочого середовища.



Контроль IT процесу

Управляти змінами

який задовольняє бізнес-вимоги до IT, а саме:

відповідність бізнес-вимог бізнес-стратегії, водночас з цим зменшуючи обсяг недоліків та виправлень при наданні рішень та послуг

зосереджений на

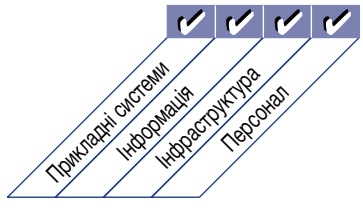
контролі оцінки наслідків, санкціонуванні та впровадженні всіх змін до IT інфраструктури, прикладного програмного забезпечення та технічних рішень; мінімізації помилок, обумовлених неповними специфікаціями запитів, а також на зупиненні впровадження несанкціонованих змін

реалізується шляхом

- Визначення та доведення до відома процедур внесення змін, в тому числі аварійних змін
- Оцінювання, визначення пріоритетів внесення та санкціонування змін
- Контролю стану справ та звітності щодо внесення змін

та вимірюється

- Кількістю збоїв або помилок в даних, обумовлених неточністю специфікацій або недостатньою оцінкою наслідків внесення змін
- Обсягом робіт з переробки прикладного програмного забезпечення або інфраструктури, обумовлених неналежними специфікаціями до змін
- Відсотком змін, які відповідають формальним процесам управління змінами



Цілі контролю

AI6 Управляти змінами

AI6.1 Вносити зміни до стандартів та процедур
Запровадити формальні процедури управління змінами з метою обробки всіх заявок (запитів) (включаючи технічне обслуговування та введення підпрограм з виправленнями програмного забезпечення) на внесення змін до прикладного програмного забезпечення, процедур, процесів, системних та сервісних параметрів та у стандартний спосіб.

AI6.2 Оцінка наслідків внесення змін, встановлення пріоритетів та санкціонування змін
Оцінювати всі запити на внесення змін, застосовуючи системний підхід, з метою визначення наслідків внесення змін для операційної системи та її функціональних можливостей. Забезпечити розподіл змін за категоріями, пріоритетами та гарантувати їх санкціонування.

AI6.3 Аварійні зміни
Впровадити процес, що передбачає визначення, ініціювання, тестування, документування, оцінку та санкціонування аварійних змін, які не відповідають встановленому процесу внесення змін.

AI6.4 Контроль статусу змін та звітність
Ввести в дію систему відстеження та звітності з метою документування відкинутих змін, повідомлення статусу санкціонованих змін та змін, що знаходяться в процесі виконання, а також завершених змін. Упевнитись в тому, що санкціоновані зміни впроваджено відповідно до плану.

AI6.5 Завершення процесу внесення змін та документація
В кожному випадку внесення змін належним чином відкоригувати документацію, що стосується системи та призначену для користувачів, а також відповідні процедури.

Керівні принципи управління

AI6 Управляти змінами

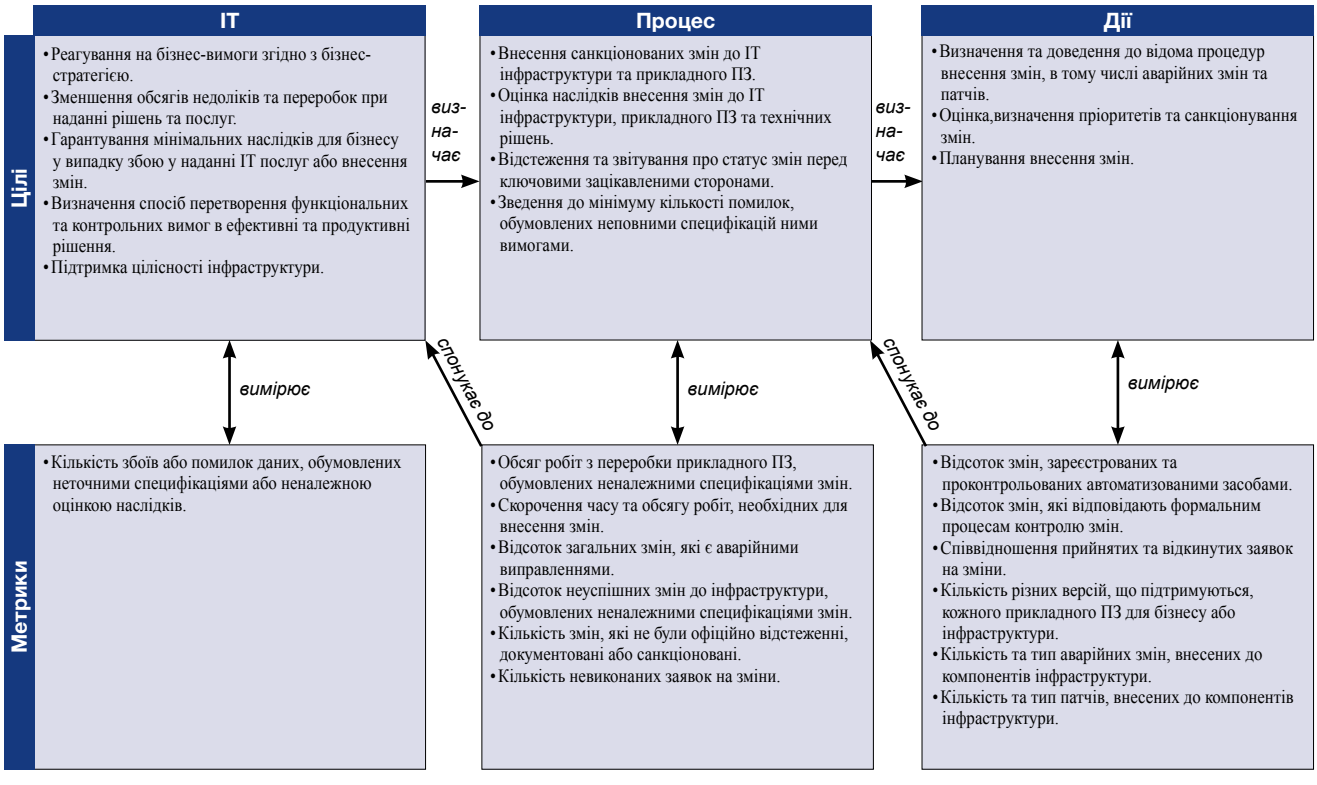
Від	Вхідні дані
PO1	Портфель IT проектів
PO8	Заходи з підвищення якості
PO9	Плани заходів по усуненню IT ризиків
PO10	Принципи управління проектами та план робочого проекту
DS3	Необхідні зміни
DS5	Необхідні зміни у сфері безпеки
DS8	Заявки на послуги/заявки на зміни
DS9-10	Заявки на зміни (де та як вносити виправлення)
DS10	Облік проблем

Вихідні дані	Для						
Опис процесу внесення змін	AI1…AI3						
Звіти щодо статусу змін	ME1						
Санкціонування змін	AI7	DS8	DS10				

RACI-діаграма

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Розробити та впровадити процес постійної реєстрації, оцінки та визначення пріоритетів заявок на внесення змін.				A	I	R	C	R	C	C	C
Оцінювати наслідки та визначати пріоритети внесення змін виходячи з потреб бізнесу.				I	R	A/R	C	R	C	R	C
Забезпечити виконання всіх аварійних та критичних змін згідно із затвердженим процесом.				I	I	A/R	I	R			C
Затверджувати внесення змін.				I	C	A/R		R			
Керувати розповсюдженням відповідної інформації стосовно змін.				A	I	R	C	R	I	R	C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

AI6 Управляти змінами

Управління процесом *«Управляти змінами»*, який задовольняє бізнес-вимогу до IT *«відповідати на бізнес-вимоги згідно з бізнес-стратегією, водночас з цим зменшуючи обсяг недоліків та виправлень при наданні рішень та послуг»*, знаходиться на рівні:

0 Не існуючий, якщо
Не існує визначеного процесу управління змінами, а зміни можуть бути здійснені фактично без жодного контролю. Немає усвідомлення того, що зміни можуть виявитись руйнівними для IT та бізнес-операцій, немає розуміння вигод, які забезпечує якісне управління змінами.

1 Початковий, якщо
В організації визнають, що змінами необхідно управляти та контролювати їх. Практики є різними, існує імовірність того, що можуть бути здійснені несанкціоновані зміни. Документація стосовно змін або погано підготовлена, або зовсім відсутня, документація щодо конфігурації є неповною та не заслуговує довіри. Можуть виникати помилки, а також затримки у робочому середовищі, обумовлені поганим управлінням змінами.

2 Повторюваний але інтуїтивний, якщо
Існує неформальний процес управління змінами, більшість змін вноситься згідно з цим підходом. Проте, він є несистемним, примітивним та уразливим до помилок. Точність документації стосовно конфігурації не витримана, внесенню змін передують дуже обмежене планування та оцінка наслідків внесення змін.

3 Визначений, якщо
Впроваджено визначений формальний процес управління змінами, що передбачає розподіл змін за категоріями, пріоритетами, аварійні процедури, санкціонування змін та управління випусками, зароджується тенденція дотримання вимог. Застосовуються обхідні прийоми (тимчасові рішення), процеси часто ігноруються. Можуть виникати помилки, час від часу мають місце несанкціоновані зміни. Аналіз наслідків змін, що вносяться в IT, для бізнес-операцій набуває формалізованого характеру, що сприяє успішному запланованому розгортанню нових прикладних програмних продуктів та технологій.

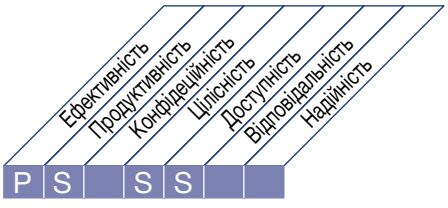
4 Керований та вимірюваний, якщо
Процес управління змінами добре розроблений та послідовно виконується у випадку внесення всіх змін, управління є стабільним, тому появу нестандартних ситуацій зведено до мінімуму. Процес є ефективним та продуктивним, але при перевірці того, чи досягнуто необхідного рівня якості, використовується багато процедур та засобів контролю, що виконуються вручну. Всі зміни здійснюються згідно з ретельно розробленим планом, їх наслідки оцінюються з метою мінімізації імовірності виникнення проблем після їх внесення у робоче середовище. Запроваджено процес затвердження змін. Документація з питань управління змінами є дійсною та точною, має місце формальне відстеження статусу змін. Документація, що стосується конфігурації, загалом є точною. Підвищується ступінь інтеграції планування та впровадження процесів управління змінами в IT із внесенням змін в бізнес-процеси, що забезпечує належне вирішення питань, пов'язаних із навчанням, організаційними змінами та безперервністю бізнесу. Підвищується рівень координованості між процесом управління змінами в IT та реорганізацією бізнес-процесів. Існує послідовний процес, що передбачає здійснення моніторингу рівня якості та продуктивності процесу управління змінами.

5 Оптимізований, якщо
Здійснюється регулярний перегляд процесу управління змінами та його оновлення, націлені на відповідність найкращим практиками. Вказаний процес перевірки відображає кінцевий результат моніторингу. Інформація стосовно конфігурації є комп'ютеризованою, що дозволяє здійснювати управління версіями. Модернізовано процедуру відстеження статусу змін, при цьому задіяні засоби, що дозволяють виявляти несанкціоноване та неліцензійне програмне забезпечення. Управління змінами в IT інтегроване з управлінням бізнес-процесами, в результаті чого IT є чинником, що сприяє підвищенню ефективності та створенню нових можливостей у сфері ділової діяльності організації.

Опис процесу

AI7 Впроваджувати в експлуатацію та проводити акредитацію IT-рішень та змін

Нові системи необхідно здати в експлуатацію після завершення розробки. Для цього потрібно провести належне тестування у відповідному середовищі із залученням відповідних тестових даних, сформулювати інструкції щодо розгортання та міграції систем, здійснити планування версій та фактичне впровадження в експлуатацію, а також виконати аналіз функціонування системи після інсталяції. Цим забезпечується відповідність діючих систем узгодженим очікуванням та кінцевим результатам.



Контроль IT процесу

Впроваджувати в експлуатацію та проводити акредитацію IT-рішень та змін

який задовольняє бізнес-вимоги до IT, а саме:

впровадження нових або модифікованих систем, що працюють без суттєвих проблем після інсталяції

зосереджений на

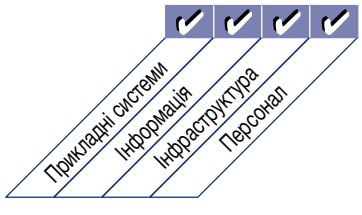
перевірці того, що прикладні програмні продукти та інфраструктура відповідають запланованої меті та не мають дефектів, а також на плануванні впровадження нових версій

реалізується шляхом

- Встановлення методології тестування
- Запровадження планування версій
- Оцінка та затвердження результатів тестів керівництвом бізнесу
- Виконання аналізу після інсталяції

та вимірюється

- Часом простою прикладного програмного забезпечення або кількістю виправлень даних, викликаних неналежним тестуванням
- Відсотком систем, які забезпечують очікувані вигоди, що вимірюються процесом аналізу функціонування системи після інсталяції
- Відсотком проектів, які мають документований та затверджений план тестування



Цілі контролю

AI7 Впроваджувати в експлуатацію та проводити акредитацію IT-рішень та змін

AI7.1 Навчання
Проводити навчання штатних працівників зацікавлених підрозділів-користувачів та оперативних груп працівників IT служби згідно з встановленим планом навчання та впровадження та супровідними матеріалами в межах кожного проекту з розробки, впровадження або модифікації інформаційних систем..

AI7.2 План тестування
Скласти план тестування на основі стандартів, що діють в масштабах всієї організації , в якому визначено ролі, обов'язки, а також вхідні та вихідні критерії. Забезпечити затвердження вказаного плану відповідними сторонами.

AI7.3 План введення в дію
Скласти план введення в дію та план відміни змін/повернення у вихідну точку. Отримати погодження вказаних планів відповідними сторонами.

AI7.4 Середовище тестування
Визначити та сформувати безпечне середовище тестування, що відповідає середовищу, в якому заплановані зміни, відносно безпеки, внутрішніх контролів, експлуатації, якості даних та вимог конфіденційності, а також завантаженості.

AI7.5 Конверсія систем та даних
Запланувати процедури перетворення даних та міграції інфраструктури, як частину у складі методів розробки, прийнятих в організації, в тому числі передбачити контрольні журнали, варіанти відміни змін і повернення в попередній стан.

AI7.6 Тестування змін
Виконувати незалежне тестування змін відповідно до встановленого плану тестування до початку міграції в середовище промислової експлуатації. Гарантувати врахування вказаним планом забезпечення безпеки та продуктивності.

AI7.7 Остаточні випробування з прийомки
Впевнитись, що власники бізнес-процесів та зацікавлені сторони, що використовують IT, здійснюють оцінку кінцевого результату процесу тестування у спосіб, визначений планом тестування. Усунути суттєві недоліки, виявлені в ході процесу тестування, завершити комплекс випробувань, визначених планом тестування, а також провести, у разі необхідності, регресійне тестування. Після проведення оцінювання затвердити рішення про введення в експлуатацію.

AI7.8 Введення в експлуатацію
Після проведення тестування проконтролювати передачу модифікованої системи в експлуатацію з дотриманням плану впровадження. Отримати схвалення всіх зацікавлених сторін, таких як користувачі, власник системи та особи, що здійснюють оперативне управління в ході експлуатації. Коли це доцільно, запустити нову систему паралельно зі старою на деякий час та порівняти їх поведінку та результати цього запуску.

AI7.9 Аналіз функціонування системи після інсталяції
Запровадити процедури, що узгоджуються зі стандартами управління змінами, які діють в організації, чим передбачити проведення аналізу функціонування системи після інсталяції та впровадження, як це визначено планом введення в дію.

Керівні принципи управління

AI7 Впроваджувати в експлуатацію та проводити акредитацію IT-рішень та змін

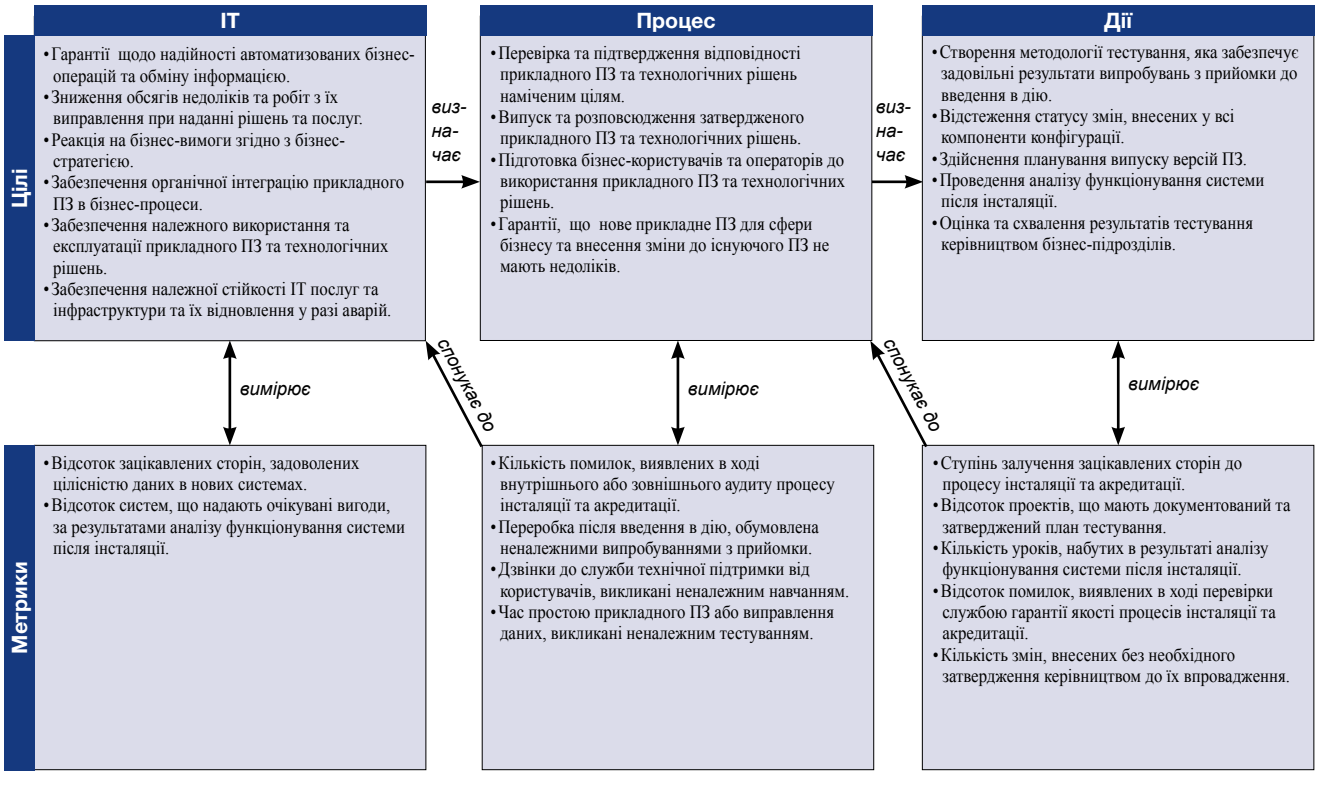
Від	Вхідні дані
PO3	Технологічні стандарти
PO4	Документовані власники систем
PO8	Стандарти розробки
PO10	Принципи управління проектами та план робочого проекту
AI3	Система, що сконфігурована для тестування/ інсталяції
AI4	Інструкції користувача, з експлуатації, підтримки, технічних та питань управління
AI5	Перелік закупівель
AI6	Санкціонування змін

Вихідні дані	Для						
Прийняті елементи конфігурації	DS8	DS9					
Визнані та прийняті помилки	AI4						
Введення в експлуатацію	DS13						
План випуску та розповсюдження ПЗ	DS13						
Аналіз після інсталяції	PO2	PO5	PO10				
Моніторинг здійснення внутрішнього контролю	ME2						

RACI-діаграма

Дії	Функції											
	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Розробляти та переглядати плани впровадження.			C	A	I	C	C	R		C	C
Визначити та переглядати стратегію тестування (вхідні та вихідні критерії) та											
методологію планування операційних тестів.			C	A	C	C	C	R		C	C
Створити та підтримувати репозиторій бізнес вимог та технічних вимог, а також сценаріїв тестування акредитованих систем.				A				R			
Здійснювати тести з конверсії та інтеграції систем в середовищі тестування.			I	I	R	C	C	A/R		I	C
Розгортати середовища тестування та виконувати випробування з остаточної прийомки.			I	I	R	A	C	A/R		I	C
Рекомендувати введення в експлуатацію на підставі узгоджених критеріїв акредитації.			I	R	A	R	C	R		I	C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

AI7 Впроваджувати в експлуатацію та проводити акредитацію IT-рішень та змін

Управління процесом *«Впроваджувати в експлуатацію та проводити акредитацію IT-рішень та змін»*, який задовольняє бізнес-вимогу до IT *«впроваджувати нові або модифіковані системи, що працюють без суттєвих проблем після інсталяції»*, знаходиться на рівні:

0 Не існуючий, якщо
Повністю відсутні формальні процеси інсталяції та акредитації, ні вище керівництво, ні працівники IT служби не усвідомлюють потреби у перевірці того, чи відповідають технологічні рішення наміченому використанню та цілям.

1 Початковий, якщо
Існує усвідомлення потреби у перевірці та підтвердженні того, що впроваджені рішення відповідають наміченим цілям. У випадку деяких проектів проводиться тестування, але ініціативу з його проведення залишено на розсуд окремих проектних груп, при цьому підходи, що застосовуються, дуже відрізняються між собою. Формальна процедура акредитації та здавання-приймання або здійснюється рідко, або не здійснюється зовсім.

2 Повторюваний але інтуїтивний, якщо
Існує деяка узгодженість між процесами тестування та акредитації, але, як правило, в їх основі не лежить жодна методологія. Як правило, окремі групи розробників приймають рішення щодо способу проведення тестування, при цьому зазвичай не проводиться тестування системи в цілому.

3 Визначений, якщо
Впроваджено формальну методологію інсталяції, міграції, конверсії та прийомки систем. Процеси інсталяції та акредитації IT рішень інтегровані у життєвий цикл системи та до деякої міри автоматизовані. Процедури навчання, тестування та переведення у статус експлуатації та акредитації можуть різнитись для визначеного процесу, в залежності від окремих прийнятих щодо них рішень. Якість систем, що вводяться в експлуатацію, не завжди стабільна, нові системи часто демонструють суттєвий обсяг проблем, що виникають після введення в дію.

4 Керований та вимірюваний, якщо
Процедури формалізовані та розроблені так, щоб продемонструвати високу організацію та корисність у визначеному середовищі тестування та акредитації. На практиці всі основні зміни, що вносяться до системи, здійснюються згідно з цим формалізованим методом. Процедура оцінювання відповідності вимогам користувачів стандартизована та вимірювана, та дає показники, які керівництво може ефективно переглянути та проаналізувати. Якість систем, що вводяться в експлуатацію, задовольняє керівництво навіть за умови існування допустимого обсягу проблем, що виникають після введення в дію. Автоматизація процесів має епізодичний характер та залежить від конкретного проекту. Керівництво може бути задоволеним наявним рівнем продуктивності, незважаючи на відсутність результатів оцінювання роботи системи після введення в дію. Тестова система адекватно відтворює робоче середовище. Стрес-тестування нових систем та регресійне тестування існуючих систем здійснюються у випадку більшості проектів.

5 Оптимізований, якщо
Процеси інсталяції та акредитації доведені до рівня найкращих практик в результаті постійного вдосконалення та підвищення якості. Процеси інсталяції та акредитації IT повністю інтегровані в життєвий цикл системи та, коли це доцільно, автоматизовані, що забезпечує максимальну ефективність при проведення навчання, тестування та переведення нової системи у промислову експлуатацію. Добре розроблені середовища тестування, процеси реєстрації проблем та процеси усунення відмов забезпечують ефективний та продуктивний перехід у середовище промислової експлуатації. Акредитація, як правило, проходить без переробок, а проблеми, що виникають після введення в дію, як правило, обмежуються необхідністю незначних коригувань. Систематично проводиться стрес-тестування нових систем та регресивне тестування діючих систем.

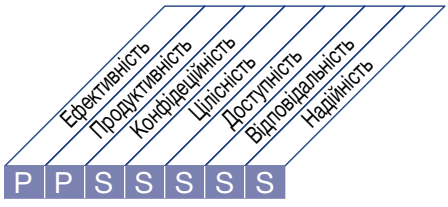
Експлуатувати та супроводжувати

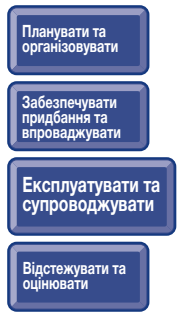
DS1 Визначати та управляти рівнями надання послуг
DS2 Управляти послугами третіх сторін
DS3 Управляти ефективністю та потужностями
DS4 Забезпечувати безперервність надання послуг
DS5 Забезпечувати безпеку систем
DS6 Визначати та розподіляти витрати
DS7 Навчати користувачів
DS8 Управляти службою підтримки та інцидентами
DS9 Управляти конфігураціями
DS10 Управляти проблемами
DS11 Управляти даними
DS12 Управляти фізичним середовищем
DS13 Управляти операційною діяльністю

Опис процесу

DS1 Визначати та управляти рівнями надання послуг

Ефективні комунікації між керівництвом IT служби та бізнес-користувачами стосовно необхідних послуг забезпечуються шляхом документального визначення та угоди щодо переліку IT послуг та рівня їх надання. Цей процес також передбачає здійснення моніторингу та вчасне надання звітності зацікавленим сторонам стосовно дотримання належного рівня надання послуг. Даний процес забезпечує узгодженість між IT послугами та відповідними бізнес-вимогами.





Контроль IT процесу

Визначати та управляти рівнями надання послуг

який задовольняє бізнес-вимоги до IT, а саме:

забезпечення узгодженості ключових IT послуг з бізнес-стратегією

зосереджений на

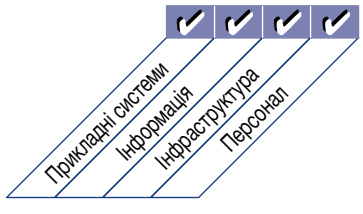
визначенні вимог до рівня надання послуг, узгодженні рівня надання послуг та здійсненні моніторингу досягнення належного рівня надання послуг

реалізується шляхом

- формалізації внутрішніх та зовнішніх угод відповідно до вимог та здатності
- звітування щодо досягнення належного рівня надання послуг (звіти та збори)
- визначення та доведення до відома нових та модифікованих вимог до послуг з метою здійснення

та вимірюється

- Відсотком зацікавлених сторін зі сторони бізнесу, задоволених тим, що надання послуг здійснюється на узгодженому рівні
- Кількістю наданих послуг, яких немає в каталозі
- Кількістю офіційних зборів з перегляду угод про рівень надання послуг (SLA) за участі замовників зі сфери бізнесу на рік



Цілі контролю

DS1 Визначати та управляти рівнями надання послуг

DS1.1 Система управління рівнем надання послуг
Визначити систему, яка забезпечує здійснення формалізованого процесу управління рівнем надання послуг між замовником та постачальником послуг. Ця система повинна передбачати постійне дотримання узгодженості з бізнес-вимогами і пріоритетами, а також сприяти загальному порозумінню між замовником та постачальником(ами) послуг. Ця система повинна передбачати наявність процесів для створення вимог до послуг, визначення послуг, угод про рівень надання послуг (SLA), угод про надання послуг на операційному рівні(OLA) та джерел фінансування. Вказані атрибути (елементи) потрібно організувати у каталог послуг. Ця система повинна визначати організаційну структуру управління рівнем надання послуг, яка охоплює розподіл ролей, завдань та обов'язків внутрішніх та зовнішніх постачальників послуг а також їх замовників.

.

DS1.2 Визначення послуг
Побудувати визначення IT послуг на характеристиках послуг та бізнес-вимогах. Гарантувати те, що вони організовані та зберігаються централізовано в результаті впровадження портфельного підходу до формування каталогу послуг.

DS1.3 Угоди про рівень надання послуг (SLA)
Окреслити та укласти угоди про рівень надання послуг (SLA)для всіх критичних IT послуг, виходячи з вимог замовника та здатності IT. Вони повинні передбачати зобов'язання замовника; вимоги до підтримки послуг, якісні та кількісні метрики для вимірювання послуг, затверджені зацікавленими сторонами; домовленості щодо фінансування та комерційних питань, якщо це можливо; а також розподіл ролей та обов'язків, в тому числі нагляд за виконанням угод SLA. Врахувати такі аспекти як доступність, надійність, результативність, здатність до росту, рівні підтримки, план забезпечення безперебійної діяльності, а також обмеження стосовно безпеки та потреб.

DS1.4 Угоди про надання послуг на операційному рівні (OLA)
Скласти угоди про надання послуг на операційному рівні, в яких пояснюється, як саме послуги будуть надаватись з технічної точки зору, щоб забезпечити виконання угод SLA в оптимальний спосіб. Угоди про надання послуг на операційному рівні повинні визначити технічні процеси в термінах, що мають зміст для постачальника послуг і можуть підтримувати декілька угод про рівень надання послуг.

DS1.5 Моніторинг та звітність щодо досягнень рівнів надання послуг
Постійно здійснювати моніторинг дотримання визначених критеріїв рівня надання послуг. Звіти щодо досягнення рівнів надання послуг слід подавати у форматі, зрозумілому для зацікавлених сторін. Статистичні дані, отримані в результаті моніторингу, необхідно аналізувати та діяти на їх підставі для визначення негативних та позитивних тенденцій надання окремих послуг, а також всіх послуг в цілому.

DS1.6 Перегляд угод про рівень надання послуг та контрактів
Регулярно переглядати угоди SLA та фундаментальні контракти (UC) з внутрішніми ти зовнішніми постачальниками послуг, щоб впевнитись с тому, що вони є ефективними та знаходяться на рівні сучасних вимог, а також в тому, що зміни, внесені у вимоги, враховано.

Керівні принципи управління

DS1 Визначати та управляти рівнями надання послуг

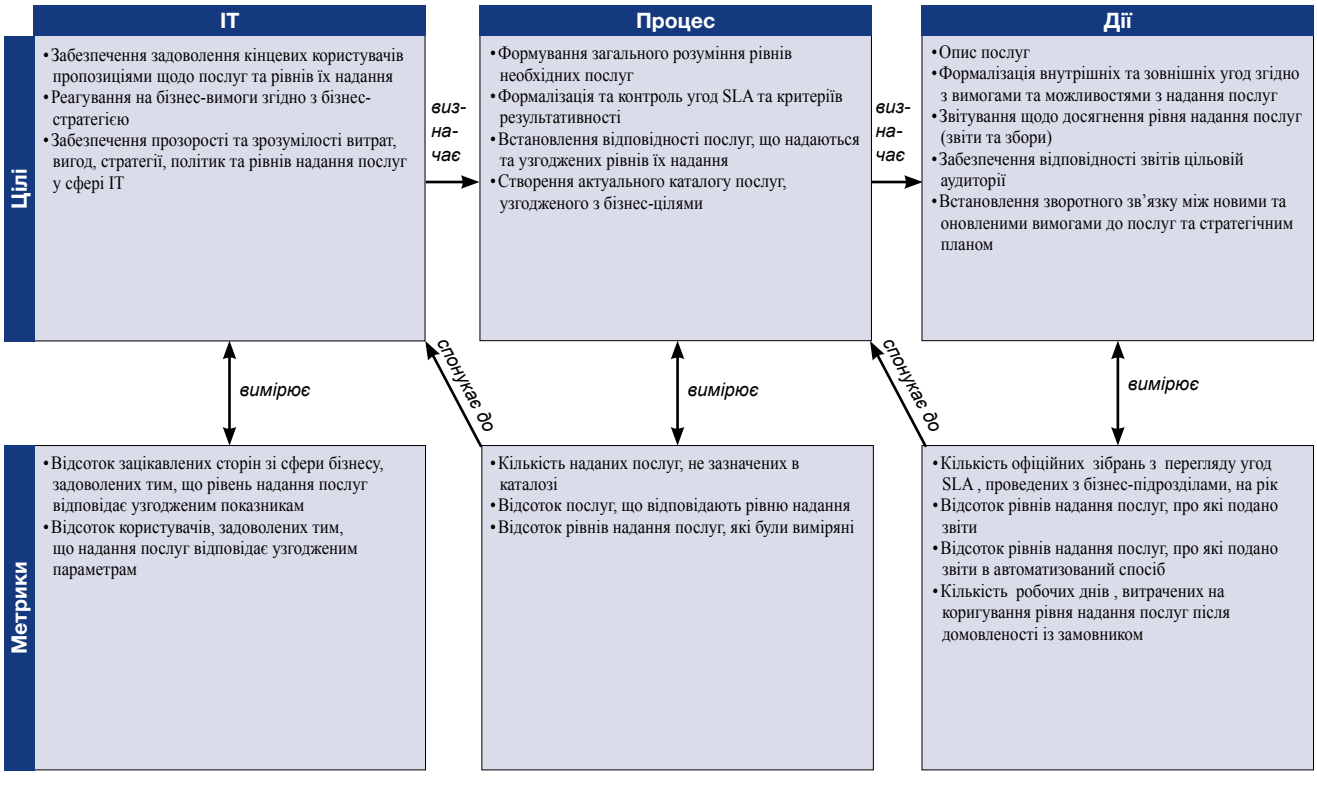
Від	Вхідні дані
PO1	Стратегічні та тактичні IT плани, портфель IT послуг
PO2	Визначена класифікація даних
PO5	Оновлений портфель IT послуг
AI2	Початкові заплановані угоди про рівень надання послуг
AI3	Початкові заплановані угоди про надання послуг на операційному рівні
DS4	Вимоги до послуг при аварії, включаючи ролі та обов'язки
ME1	Вхідні дані щодо результативності для IT планування

Вихідні дані	Для						
Звіт щодо перегляду контрактів	DS2						
Звіт щодо результативності процесів	ME1						
Нові/оновлені вимоги до процесів	PO1						
Угоди про рівень надання послуг	AI1	DS2	DS3	DS4	DS6	DS8	DS13
Угоди про надання послуг на операційному рівні	DS4	DS5	DS6	DS7	DS8	DS11	DS13
Оновлений портфель IT послуг	PO1						

RACI-діаграма

Дії	Функції											
	СЕО	СГО	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	РМО	Служба контролю дотримання вимог, аудиту, ризиків та безпеки	Керівник, відповідальний за надання послуг
Створення схеми визначення IT послуг			C	A	C	C	I	C	C	I	C	R
Формування каталог IT послуг			I	A	C	C	I	C	C	I	I	R
Укладення угод SLA для критичних IT послуг		I	I	C	C	R	I	R	R	C	C	A/R
Укладення угод OLA, які відповідають угодам SLA				I	C	R	I	R	R	C	C	A/R
Здійснення моніторингу та надання звітів щодо результативності рівня надання послуг				I	I	R		I	I		I	A/R
Здійснення перегляду угод SLA та фундаментальних контрактів		I		I	C	R		R	R		C	A/R
Переглядання та оновлення каталогу IT послуг			I	A	C	C	I	C	C	I	I	R
Складання плану вдосконалення послуг			I	A	I	R	I	C	R	C	I	R

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS1 Визначати та управляти рівнями надання послуг

Рівні зрілості управління процесом *«Визначати та управляти рівнями надання послуг»*, які задовольняють бізнес-вимоги до IT *«забезпечити узгодженість ключових IT послуг з бізнес-стратегією»*, є такими:

0 Не існуючий, якщо
Керівництво не усвідомило потреби у процесі визначення рівнів надання послуг. Відповідальність та підзвітність щодо контролю цих показників не розподілені.

1 Початковий, якщо
Існує усвідомлення потреби в управлінні рівнями надання послуг, але цей процес є неформальним та реактивним. Відповідальність та підзвітність за визначення та управління послугами не визначені. Якщо і існує процедура вимірювання результативності, вона є якісною та здійснюється у порівнянні з неточно визначеними цілями. Процедура звітності є неформальною, виконується нечасто та непослідовно.

2 Повторюваний але інтуїтивний, якщо
Введені узгоджені рівні надання послуг, але ці показники є неформальними та не переглядаються. Звітність щодо рівня надання послуг є неповноцінною та може бути неактуальною або дезорієнтувати замовника. Якість звітності щодо рівня надання послуг залежить від кваліфікації та ініціативи окремих керівників. Призначено координатора з питань рівня надання послуг, який має визначені обов'язки, але обмежені повноваження. Якщо процес дотримання угод SLA і існує, він є добровільним та не виконується в обов'язковому порядку.

3 Визначений, якщо
Обов'язки чітко визначені, але з добровільною відповідальністю. Впроваджено процес розробки угод SLA, який передбачає контрольні точки для перегляду рівня надання послуг та ступеню задоволення замовника. Послуги та рівні надання послуг визначені, документовані та узгоджені згідно стандартного процесу. Виявляються недоліки у рівні надання послуг, але процедури коригування вказаних недоліків є неформальними. Має місце чіткий зв'язок між очікуваним рівнем послуг та наданим фінансуванням. Рівні надання послуг узгоджені, але вони можуть не відповідати потребам бізнесу.

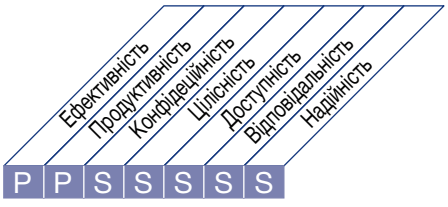
4 Керований та вимірюваний, якщо
Рівні надання послуг все частіше визначаються на етапі встановлення вимог до системи та фігурують у середовищах розробки прикладних програмних продуктів та експлуатації. Ступінь задоволення замовників регулярно вимірюється та оцінюється. Оцінка результативності відображає потреби замовника, а не IT цілі. Метрики оцінювання рівнів надання послуг набувають стандартизованого характеру та відповідають нормативам, що існують в даній галузі. Критерії визначення рівня послуг основані на критичності для бізнесу, і включають доступність, надійність, результативність, здатність до росту, підтримку користувачів, планування безперебійності діяльності та аспекти безпеки. Регулярно проводиться аналіз першопричин у випадку невідповідності рівня надання послуг існуючим вимогам. Підвищується ступінь автоматизації процесу надання звітності щодо результатів моніторингу рівня надання послуг. Виявляються та чітко усвідомлюються фінансові та операційні ризики, пов'язані з недотриманням вимог щодо рівня надання послу. Впроваджено формальну систему вимірювань та оцінки, яка має належну підтримку.

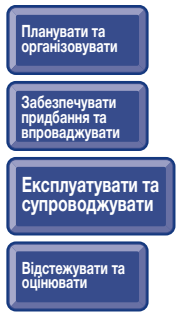
5 Оптимізований, якщо
Рівні надання послуг постійно переглядаються з метою забезпечення відповідності IT цілям та бізнес-цілям, в той самий час використовуються переваги технології, в тому числі співвідношення «витрати-вигоди». Всі процеси управління рівнем обслуговування постійно вдосконалюються. Ступінь задоволення замовників постійно контролюється та регулюється. Очікувані рівні надання послуг відображають стратегічні цілі бізнес-підрозділів та проходять оцінку згідно нормативів, що існують в даній галузі. Керівництво IT служби має ресурси та повноваження, необхідні для виконання завдань із забезпечення рівня надання послуг, існує система виплати заробітної плати, яка стимулює ініціативу щодо виконання поставлених завдань. Вище керівництво контролює метрики результативності в межах постійного процесу вдосконалення.

Опис процесу

DS2 Управляти послугами третіх сторін

Для забезпечення відповідності послуг, що надаються третіми сторонами(постачальниками, продавцями та партнерами), бізнес-вимогам необхідно ввести ефективний процес управління послугами третіх сторін. Цей процес реалізується завдяки чіткому визначенню ролей, обов'язків та очікувань в угодах з третіми сторонами, а також завдяки перегляду та контролю вказаних угод на предмет результативності та дотримання існуючих вимог. Ефективне управління послугами третіх сторін зводить до мінімуму бізнес-ризик, пов'язаний з невиконанням постачальниками своїх зобов'язань.





Контроль IT процесу

Управляти послугами третіх сторін

який задовольняє бізнес-вимоги до IT, а саме:

забезпечення рівня надання послуг третіми сторонами, що відповідає вимогам, та надання прозорої інформації щодо вигод, вартості та ризиків

зосереджений на

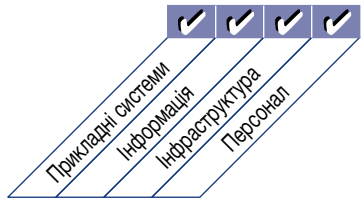
встановленні взаємовідносин та визначенні взаємних обов'язків з сторонніми постачальниками послуг, які відповідають певним вимогам, та контролювати процес надання послуг з метою перевірки та гарантії виконання умов відповідних контрактів

реалізується шляхом

- визначення та класифікації послуг, що надаються постачальниками
- виявлення та пом'якшення наслідків ризиків, пов'язаних з послугами постачальників
- моніторингу та вимірювання результативності діяльності постачальників послуг

та вимірюється

- кількістю скарг користувачів, пов'язаних з послугами, наданими згідно з контрактами
- відсотком основних постачальників послуг, які відповідають чітко визначеним вимогам та надають послуги на належному рівні
- відсотком ключових постачальників послуг, діяльність яких контролюється



Цілі контролю

DS2 Управляти послугами третіх сторін

DS2.1 Встановлення взаємовідносин з усіма постачальниками
Визначити всі послуги, що надаються постачальниками, розподілити їх за категоріями відповідно до типу постачальника, значущості та критичності. Вести офіційну документацію стосовно взаємовідносин в технічній та організаційній сфері, у якій зафіксовано розподіл ролей та обов'язків, відображено цілі, очікувані кінцеві результати та повноваження представників вказаних постачальників послуг.

DS2.2 Управління взаємовідносинами з постачальниками
Закріпити документально процес управління взаємовідносинами з постачальниками у випадку кожного постачальника послуг. Власники взаємовідносин повинні працювати над вирішенням проблем у взаємостосунках замовників та постачальників послуг та гарантувати якість взаємовідносин, в основу яких покладено довіру та прозорість (наприклад, шляхом укладення угод SLA).

DS2.3 Управління ризиками, пов'язаними з постачальниками
Виявляти та зменшувати ризики, пов'язані із здатністю постачальників до безперервного ефективного надання послуг в безпечний та результативний спосіб на постійній основі. Забезпечити відповідність контрактів універсальним стандартам ведення бізнесу згідно з вимогами законодавчих та регулятивних органів. Управління ризиками в подальшому повинно передбачати укладення угод про нерозголошення (NDA), контрактів про передачу інтелектуальної власності, довготривалу життєздатність постачальника, дотримання вимог до захисту, наявність альтернативних постачальників, систему покарань та заохочень тощо.

DS2.4 Моніторинг якості роботи постачальників послуг
Впровадити процес, що передбачає здійснення моніторингу надання послуг з метою гарантії того, що постачальник відповідає діючим бізнес-вимогам та постійно дотримується контрактних угод та угод щодо рівня надання послуг (SLA), а показники його діяльності є конкурентоздатними у порівнянні з показниками альтернативних постачальників та з врахуванням кон'юнктури ринку.

Керівні принципи управління

DS2 Управляти послугами третіх сторін

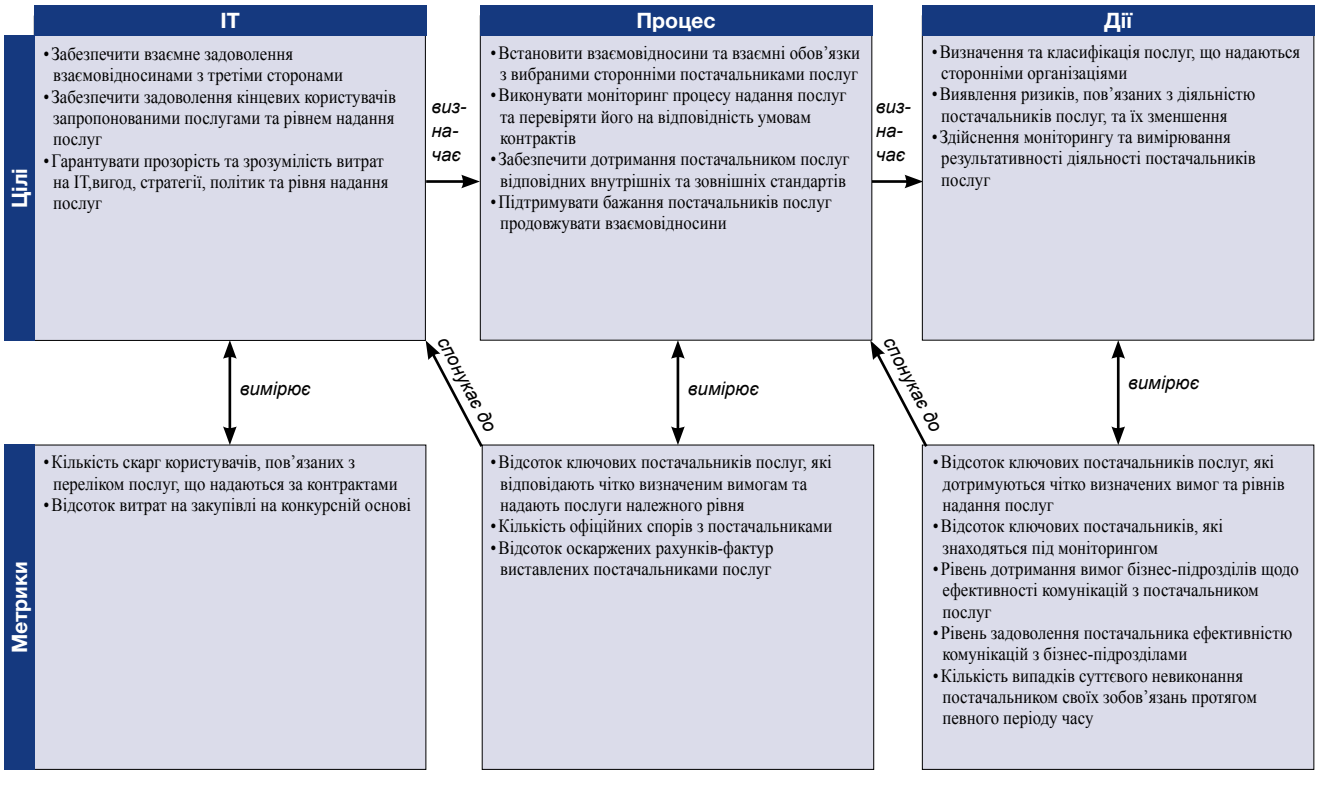
Від	Вхідні дані
PO1	Стратегія вибору постачальників в IT
PO8	Стандарти закупівель
AI5	Контрактні угоди, вимоги до управління взаємовідносинами зі сторонніми організаціями
DS1	Угоди SLA, звіт про оцінку контрактів
DS4	Вимоги до обслуговування в умовах аварії, ролі та обов'язки

Вихідні дані	Для
Звіти щодо результативності процесу	ME1
Каталог постачальників	AI5
Ризики, пов'язані з постачальниками	PO9

RACI-діаграма

Дії \ Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Визначення та класифікація взаємовідносин з третіми сторонами, що надають послуги				I	C	R	C	R	A/R	C	C
Встановлення та закріплення документально процесів управління відносинами з постачальниками послуг		C		A	I	R	I	R	R	C	C
Впровадження політики та процедури оцінювання постачальників послуг та їх відбору		C		A	C	C		C	R	C	C
Виявлення, оцінка та зменшення ризиків, пов'язаних з діяльністю постачальників послуг		I		A		R		R	R	C	C
Моніторинг процесу надання послуг сторонніми організаціями				R	A	R		R	R	C	C
Оцінка реалізації довгострокових цілей, що визначені для стосунків між всіма зацікавленими сторонами у процесі надання послуг	C	C	C	A/R	C	C	C	C	R	C	C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS2 Управляти послугами третіх сторін

Рівні зрілості управління процесом *«Управляти послугами третіх сторін»*, які задовольняють бізнес-вимоги до IT *«забезпечити рівень надання послуг сторонніми організаціями, що відповідає вимогам, та надавати прозору інформацію щодо вигод, вартості та ризиків»*, є такими:

0 Не існуючий, якщо
Обов'язки та підзвітність не визначені. Не введені формальні політики та процедури, що стосуються контрактних відносин з третіми сторонами. Послуги, що надаються третіми сторонами не проходять процедури затвердження та перегляду керівництвом організації. Заходи з вимірювання показників не здійснюються, треті сторони не надають відповідної звітності. Оскільки в контрактах не закріплено зобов'язання щодо надання звітності, вище керівництво не усвідомлює якості наданих послуг.

1 Початковий, якщо
Керівництво усвідомлює потребу введення документованих політик та процедур, що стосуються управління стосунками з третіми сторонами, в тому числі необхідність укладенні відповідних контрактів. Стандартні умови укладення угод з постачальниками послуг відсутні. Оцінювання та вимірювання показників наданих послуг має неформальний та реактивний характер. Виконання процедур залежить від знання (наприклад, за вимогою) окремих співробітників і постачальників.

2 Повторюваний але інтуїтивний, якщо
Процес контролю діяльності сторонніх постачальників послуг, ризиків, пов'язаних з їх діяльністю, та процедури надання послуг має неофіційний характер. Здійснюється підписання типового контракту зі стандартними положеннями та умовами поставки (наприклад, з описом послуг, які будуть надаватись). Звіти щодо наданих послуг надаються, але не відповідають бізнес-цілям.

3 Визначений, якщо
Введено документально підтверджені процедури управління стосунками зі сторонніми організаціями, що надають послуги, з чітко визначеними процесами інспектування постачальників послуг та ведення переговорів з ними. Якщо досягається згода про надання послуг, тоді взаємовідносини зі сторонніми організаціями ґрунтуються виключно на контракті. Характер послуг, що будуть надаватись, детально описується в контракті, при цьому враховуються законодавчі, експлуатаційні вимоги та вимоги до засобів контролю. Здійснено розподіл обов'язків щодо нагляду та контролю за наданням послуг сторонніми організаціями. В основі контрактів лежать типові умови та положення. Здійснюється оцінка підприємницького ризику, яка доводиться до відома зацікавлених сторін.

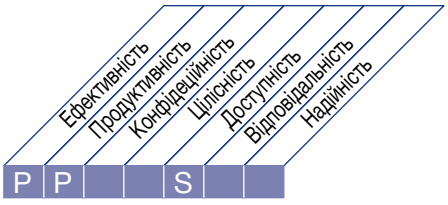
4 Керований та вимірюваний, якщо
Введено формальні та стандартні критерії визначення умов контрактів, включаючи обсяг робіт;опис послуг/кінцевих результатів та документів, які мають бути надані; умовні допущення; графік контрактних робіт;вартість; домовленості щодо виставлення рахунків та зобов'язання за контрактом. На відповідних осіб покладено обов'язки з управління контрактами та мережею постачальників послуг. Ступінь відповідності постачальників послуг певним вимогам, наявність ризиків та здатності постачальника постійно контролюються. Вимоги до послуг визначені та знаходяться у зв'язку з бізнес-цілями. Здійснюється процес аналізу надання послуг з точки зору виконання умов контракту, що дає змогу оцінити поточний та майбутній рівень надання послуг третіми сторонами. В процесі закупки використовується трансферне ціноутворення. Всі залучені сторони усвідомлюють послугу, вартість і проміжні очікування. Визначено узгоджені цілі та метрики, що дають змогу контролювати діяльність постачальників послуг.

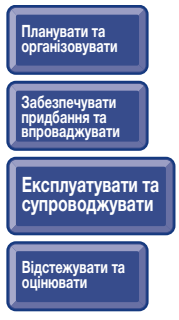
5 Оптимізований, якщо
Контракти, укладені з третіми сторонами, проходять періодичний перегляд через певні, заздалегідь визначені проміжки часу. Визначено відповідальність за управління постачальниками послуг та якістю наданих послуг. Документальне підтвердження відповідності контракту вимогам щодо експлуатації, дотримання правових норм та контролю підлягає моніторингу, та забезпечується вжиття коригувальних заходів. Послуги третіх сторін підлягають незалежному періодичному перегляду, надається відгук щодо результативності послуг і він використовується для покращення надання послуг. Процедури оцінювання та вимірювання змінюються в залежності від зміни умов бізнесу. Введені метрики дозволяють на ранньому етапі виявити потенційні проблеми, що можуть виникнути в ході надання послуг третіми сторонами. Встановлено зв'язок між всебічною та чіткою звітністю щодо досягнення належного рівня послуг та винагородою, призначеною для третіх осіб. Керівництво регулює процес придбання та контролю послуг третіх осіб, виходячи з відповідних метрик.

Опис процесу

DS3 Управляти ефективністю та потужностями

Для управління продуктивністю та потужностями IT ресурсів потрібно впровадити процес періодичного аналізу та перевірки поточної продуктивності та потужностей IT ресурсів. Цей процес передбачає прогнозування майбутніх потреб з врахуванням поточної завантаженості, вимог до збереження даних та стійкості до відмов. Вказаний процес дозволяє забезпечити постійну наявність та придатність інформаційних ресурсів, необхідних для задоволення потреб бізнесу.





Контроль IT процесу

Управляти ефективністю та потужностями

який задовольняє бізнес-вимоги до IT, а саме:

оптимізація продуктивності IT інфраструктури, ресурсів та потужностей у відповідь на потреби бізнесу

зосереджений на

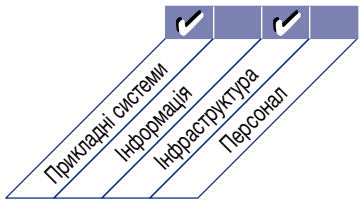
виконанні вимог щодо часу реагування, визначених угодами SLA, мінімізації непродуктивних втрат часу та забезпеченні постійного підвищення продуктивності та потужностей IT шляхом здійснення моніторингу та вимірювань

реалізується шляхом

- планування та забезпечення потужності та доступності систем
- здійснення моніторингу та звітування щодо продуктивності систем
- моделювання та прогнозування продуктивності систем

та вимірюється

- кількістю втрачених годин, з розрахунку на одного користувача на рік внаслідок незадовільного планування потужностей
- відсотком пікового навантаження, коли планове використання було перевищено
- відсотком недотриманих вимог щодо часу реагування, визначених в угодах SLA



Цілі контролю

DS3 Управляти ефективністю та потужностями

DS3.1 Планування ефективності та потужностей
Впровадити процес планування з метою аналізу ефективності та потужностей IT ресурсів, щоб гарантувати наявність економічно обґрунтованих потужностей та ефективності для обробки узгоджених навантажень, визначених угодами про рівень надання послуг. В планах щодо потужностей та продуктивності необхідно ефективно використовувати відповідні методи моделювання з метою створення моделі поточної та прогнозованої ефективності, потужностей та пропускної здатності IT ресурсів.

DS3.2 Поточні показники ефективності та потужностей
Оцінювати поточну ефективність та потужності IT ресурсів, щоб визначити, чи присутні достатні потужності та ефективність, здатні забезпечити узгоджений рівень надання послуг.

DS3.3 Перспективні показники ефективності та потужностей
Здійснювати прогноз показників ефективності та потужностей IT ресурсів через певний інтервал, щоб звести до мінімуму ризик переривання надання послуг внаслідок недостатніх потужностей або зниження ефективності, та виявити надлишкові потужності, щоб здійснити їх можливий перерозподіл. Визначити тенденції завантаженості та скласти відповідні прогнози для подальшого включення в плани продуктивності та потужностей.

DS3.4 Придатність IT ресурсів
Забезпечити необхідні потужності та ефективність, беручи до уваги такі аспекти як нормальна завантаженість, резерви на непередбачені ситуації, потребу в засобах збереження та життєві цикли IT ресурсів. Слід передбачити такі моменти, як визначення пріоритетів завдань, механізми забезпечення стійкості до відмови та практики розподілу ресурсів. Керівництво повинно гарантувати, що в планах виділення ресурсів на непередбачені ситуації належним чином враховані такі аспекти як доступність, потужність та ефективність окремих IT ресурсів.

DS3.5 Моніторинг та звітність
Здійснювати постійний моніторинг продуктивності та потужностей IT ресурсів. Накопичені дані повинні слугувати двом цілям:
- Підтримувати та регулювати поточну продуктивність IT та вирішувати такі проблеми, як стійкість систем до відмов, забезпечення відновлення функціонування, забезпечення поточної та прогнозованої завантаженості, виконання планів щодо зберігання інформації та придбання ресурсів
- Звітувати перед бізнес-підрозділами про доступність послуг, як вказано в угодах про рівень надання послуг

Супроводжувати всі звіти про виключні ситуації рекомендаціями щодо вжиття відповідних коригувальних заходів.

Керівні принципи управління

DS3 Управляти ефективністю та потужностями

Від	Вхідні дані
AI2	Технічні вимоги стосовно доступності, цілісності та відновлення
AI3	Вимоги щодо моніторингу систем
DS1	Угоди SLA

Вихідні дані	Для						
Дані щодо ефективності та потужностей	PO2	PO3					
План (вимоги) щодо ефективності та потужностей	PO5	AI1	AI3	ME1			
Необхідні зміни	AI6						
Звіти щодо продуктивності процесів	ME1						

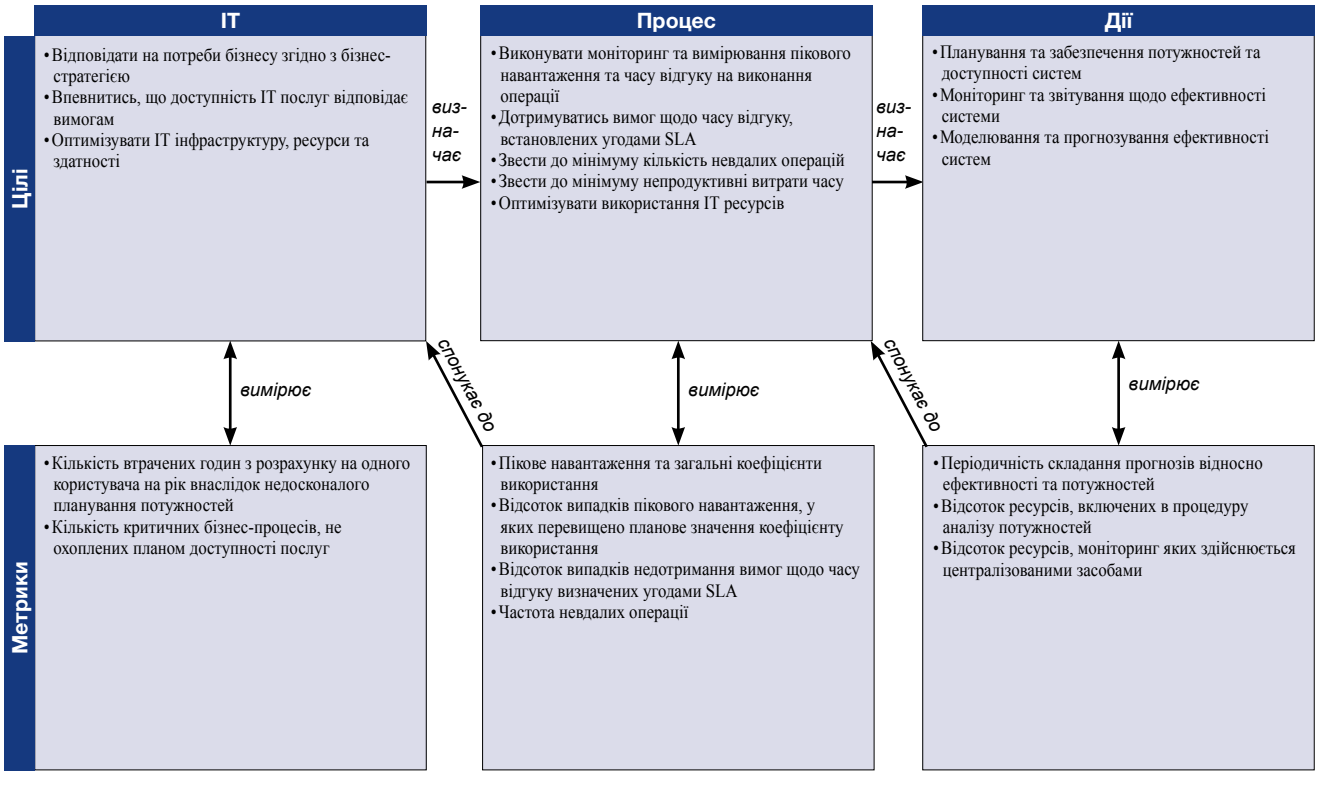
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Впровадження процесу планування для аналізу ефективності та потужностей IT ресурсів				A		R	C	C	C	C	
Аналіз поточних показників ефективності та потужностей IT ресурсів				C	I	A/R		C	C	C	
Прогнозування ефективності та потужностей IT ресурсів				C	C	A/R	C	C	C	C	
Аналіз розривів (недоліків) з метою визначення дисбалансу IT ресурсів				C	I	A/R		R	C	C	I
Планування дій при аварії на випадок можливої недоступності IT ресурсів				C	I	A/R		C	C	I	C
Здійснення постійного моніторингу доступності, ефективності та потужностей IT ресурсів та надання відповідних звітів				I	I	A/R		I	I	I	I

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS3 Управляти ефективністю та потужностями

Управління процесом *«Управляти ефективністю та потужностями»*, що задовольняє бізнес-вимогу до IT, а саме: *«оптимізувати продуктивність IT інфраструктури, ресурсів та потужностей у відповідь на потреби бізнесу»* знаходиться на рівні:

0 Не існуючий, якщо
Керівництво не усвідомлює того, що для здійснення ключових бізнес-процесів можуть знадобитись більш високі рівні ефективності IT або того, що загальна потреба бізнес-підрозділів у підтримці з боку IT може перевищувати їх потужності. Не введений процес планування потужностей.

1 Початковий, якщо
Користувачі винаходять обхідні шляхи у разі виникнення обмежень ефективності або потужностей. Має місце дуже незначне усвідомлення потреби у плануванні потужностей та ефективності власниками бізнес-процесів. Заходи з управління ефективністю та потужностями, як правило, мають реактивний характер. Процес планування потужностей та ефективності є неформальним. Осмислення суті поточних та перспективних показників продуктивності та потужностей IT ресурсів є обмеженим .

2 Повторюваний але інтуїтивний, якщо
Керівництво бізнес-підрозділів та IT служби усвідомлює наслідки відсутності процесу управління ефективністю та потужностями. Потреби у ефективності загалом задовольняються, виходячи з оцінки окремих систем та на основі знань спеціалістів з груп підтримки та проектних груп. Можуть використовуватись деякі окремі засоби діагностики проблем, пов'язаних з продуктивністю та потужностями, але стабільність результатів залежить від досвіду окремих ключових осіб. Загальна оцінка продуктивності та потужностей IT, або аналіз ситуацій пікового або найгіршого варіанту навантаження не здійснюються. Несподівано та хаотично можуть виникати проблеми з доступністю, які потребують значних витрат часу для їх виявлення та усунення. Всі вимірювання ефективності головним чином здійснюються з врахуванням потреб IT, а не потреб замовника.

3 Визначений, якщо
Потреби у продуктивності та потужностях визначено протягом повного життєвого циклу системи. Введені визначені вимоги до рівня надання послуг та відповідні метрики, які можна використовувати для вимірювання експлуатаційної ефективності. Здійснюється моделювання потреб у ефективності та потужностях на перспективу згідно з визначеним процесом. Надаються звіти, у яких представлені статистичні дані щодо ефективності. Все ще можуть мати місце проблеми, пов'язані з ефективністю та потужностями, які потребують значного часу для їх усунення. Незважаючи на опубліковані показники щодо рівнів надання послуг, користувачі та замовники можуть проявляти скептицизм стосовно забезпечення відповідної працездатності послуг.

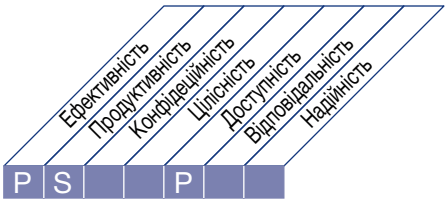
4 Керований та вимірюваний, якщо
У розпорядженні організації є процеси та засоби, які дозволяють вимірювати використання системи, її ефективність та потужність, та порівнювати результати з визначеними цілями. Є доступ до актуальної інформації, яка представлена у вигляді стандартизованих статистичних даних щодо ефективності та дозволяє сповіщати про інциденти, викликані недостатнім рівнем ефективності та потужностей. Проблеми, пов'язані з недостатнім рівнем ефективності та потужностей, вирішуються з використанням визначених та стандартних процедур. Моніторинг конкретних ресурсів, таких як дискова пам'ять, комп'ютерна мережа, сервер та мережевий шлюз, здійснюється із застосуванням автоматизованих засобів. Статистичні дані щодо ефективності та потужностей представлені у термінах бізнес-процесів, тому користувачі та замовники можуть зрозуміти, на якому рівні надаються IT послуги. Користувачі загалом задоволені поточними потужностями послуг та можуть вимагати нових та підвищених рівнів доступності послуг. Метрики для вимірювання продуктивності та потужності IT узгоджені, але можуть застосовуватись лише час від часу та несистематично.

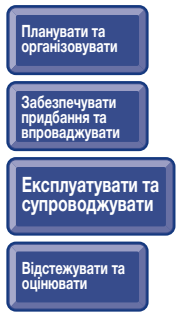
5 Оптимізований, якщо
Плани щодо продуктивності та потужностей повністю узгоджені з прогнозами щодо потреб бізнесу. Інфраструктура IT та потреби бізнесу регулярно переглядаються на предмет досягнення оптимальної потужності за рахунок максимально низьких витрат. Засоби моніторингу критичних IT ресурсів є стандартними та використовуються на для всіх платформ у прив'язці до системи управління інцидентами, розгорнутої в масштабах всієї організації. Засоби моніторингу дозволяють виявляти та в автоматизований спосіб коригувати проблеми, пов'язані з ефективністю та потужністю. Здійснюється аналіз тенденцій, який дозволяє виявити неминучі проблеми, викликані зростанням обсягу бізнес операцій, що дає змогу складати відповідні плани та уникати неочікуваних проблем. Метрики, передбачені для вимірювання ефективності та потужностей IT, були адаптовані до чітких метрики кінцевих результатів та показники ефективності для всіх критичних бізнес-процесів та систематично вимірюються. Керівництво адаптує процес планування ефективності та потужностей за результатами аналізу вказаних метрик.

Опис процесу

DS4 Забезпечувати безперервність надання послуг

Щоб забезпечити безперервність надання IT послуг, необхідно розробити, підтримувати та тестувати плани забезпечення безперервності надання послуг IT, використовувати віддалене сховище даний для резервування та проводити періодичне навчання з питань забезпечення безперервності надання послуг. Ефективний процес забезпечення безперервності надання послуг зводить до мінімуму імовірність виникнення та наслідки перебоїв у наданні основних IT послуг для ключових бізнес-функцій та бізнес-процесів.





Контроль IT процесу

Забезпечувати безперервність надання послуг

який задовольняє бізнес-вимоги до IT, а саме:

гарантування мінімального рівня наслідків для бізнесу у випадку перебоїв у наданні IT послуг

зосереджений на

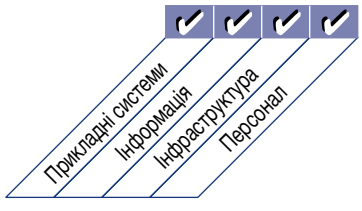
забезпеченні стійкості до відмов автоматизованих рішень та розробці, підтримці та тестуванні планів забезпечення безперервності надання IT послуг

реалізується шляхом

- розробки та підтримки (вдосконалення) механізмів функціонування IT під час аварій
- проведення навчання та тестування планів забезпечення відновлення функціонування IT під час аварій
- збереження копій планів забезпечення відновлення функціонування IT під час аварій та резервний даних у віддаленому приміщенні

та вимірюється

- кількістю втрачених годин з розрахунку на одного користувача на рік внаслідок незапланованих перебоїв у роботі систем
- кількістю критичних бізнес-процесів, в яких задіяні IT, не включених до плану забезпечення безперервності діяльності та відновлення функціонування IT



Цілі контролю

DS4 Забезпечувати безперервність надання послуг

DS4.1 Система забезпечення безперервності надання IT послуг
Розробити систему забезпечення безперервності надання IT послуг з метою підтримки управління безперервністю бізнесу в масштабах всієї організації та з використанням відповідного узгодженого процесу. Метою впровадження вказаної системи є допомога у визначення необхідного рівня стійкості інфраструктури до відмов та сприяння розробці планів забезпечення безперебійності роботи та відновлення функціонування IT після аварій. Система повинна передбачити організаційну структуру для управління неперервністю діяльності, що включає розподіл ролей, завдань та обов'язків внутрішніх та зовнішніх постачальників послуг, їх керівництво та їх замовників, а також процеси планування, які формують правила та структури документального оформлення, тестування та виконання планів забезпечення безперервності роботи та відновлення функціонування IT після аварій. У плані також потрібно розглянути такі питання, як виявлення критичних ресурсів, зазначення ключових залежностей, здійснення моніторингу та надання звітності щодо придатності критичних ресурсів, наявність резервних засобів обробки даних, а також принципи резервування та відновлення системи.

.

DS4.2 Плани забезпечення безперервності надання IT послуг
Розробити плани забезпечення безперервності надання IT послуг на основі вищезазначеної системи, що передбачені для послаблення наслідків суттєвих перебоїв у наданні IT послуг для ключових бізнес-функцій та бізнес-процесів. В основу подібних планів має бути покладене осмислення можливих наслідків для бізнесу та передбачені вимоги стосовно стійкості до відмов, існування резервних засобів обробки даних та можливості по відновленню для всіх критичних IT послуг. В планах також необхідно передбачити наявність посібників для використання, розподіл ролей та обов'язків, відповідні процедури, процеси комунікації та підходи до тестування.

DS4.3 Критичні IT ресурси
Сконцентрувати увагу на елементах, що вказані в плані забезпечення безперервності надання IT послуг, якнайбільш критичні, щоб перебачити належну стійкість до відмов та встановити пріоритети відновлення. Уникати відволікання на відновлення менш критичних елементів та забезпечити реагування та відновлення функціонування згідно з пріоритетами потреб бізнесу, одночасно забезпечуючи утримання витрат до прийнятного рівня і забезпечення відповідності вимогам регулятивних органів та умовам контрактів. Передбачити класифікацію потреб у забезпеченні стійкості до відмов на різних рівнях, наприклад, відновлення у період від 1 до 4 годин, відновлення у період від 4 до 24 годин, відновлення у період більше 24 годин, класифікацію по періодам критичних бізнес-операцій.

DS4.4 Підтримка плану забезпечення безперервності надання IT послуг
Заохочувати керівництво IT служби до визначення та здійснення процедур контролю за змінами з метою підтримки актуальності плану забезпечення безперервності надання IT послуг та постійного відображення в ньому діючих потреб бізнесу. Повідомляти про зміни, внесені до процедур та обов'язків чітко та своєчасно.

DS4.5 Тестування плану забезпечення безперервності надання IT послуг
Регулярно тестувати план забезпечення безперервності надання IT послуг для забезпечення ефективного відновлення IT систем, усунення недоліків та забезпечення актуальності плану. Для цього необхідно ретельно готувати, документувати та повідомляти результати тестування, а також, згідно з вказаними результатами, впроваджувати план відповідних заходів. Передбачити необхідний обсяг тестування від окремих прикладних продуктів до комплексного тестів, тестів всіх компонент системи, та тестів з участю виробників.

DS4.6 IT Навчання, що стосуються плану забезпечення безперервності надання IT послуг
Для всіх зацікавлених сторін забезпечити регулярне навчання з питань, що стосуються відповідних процедур та їх ролей і обов'язків у випадку інциденту або аварії. Здійснювати перевірку рівня навчання та його підвищення згідно з результатами тестів планів забезпечення безперервності діяльності.

DS4.7 Розповсюдження плану забезпечення безперервності надання IT послуг
Встановити визначену та керовану стратегія розповсюдження плану, яка забезпечує належне та безпечне розповсюдження планів і їх доступність для належним чином уповноважених зацікавлених сторін за необхідності. Слід приділити увагу забезпеченню доступу до планів у всіх випадках виникнення всіх аварійних ситуацій.

DS4.8 Відновлення процесу надання IT послуг
Скласти план заходів, які необхідно вживати у період відновлення IT та процесу надання послуг. В цьому плані можна передбачити введення в дію резервних приміщень (площадок), ініціацію використання резервних засобів обробки даних, комунікації з замовниками та зацікавленими сторонами та процедури відновлення. Забезпечити розуміння представниками бізнес-підрозділів часу,що потрібен для відновлення IT послуг, та необхідних інвестицій у технології, які

задовольнять потребу у відновленні бізнесу.

DS4.9 Резервні засоби зберігання даних поза об'єктом
Зберігати у віддаленому приміщенні всі критичні резервні носії інформації, документацію та інші IT ресурси, необхідні для відновлення IT послуг і виконання планів забезпечення безперервності бізнесу. Визначити контент , що підлягає зберіганню у резервних місцях під час співпраці між власниками бізнес-процесів та персоналом IT служби. Управління засобами віддаленого збереження резервної інформації повинно узгоджуватись з політикою щодо класифікації інформації та з практиками відносно носіїв інформації. Керівництво IT служби повинно забезпечити проведення періодичної перевірки засобів віддаленого збереження резервної інформації (як мінімум один раз на рік) з точки зору наявності контенту, захисту від впливу оточуючого середовища та безпеки. Забезпечити сумісність апаратного та програмного забезпечення, призначених для відновлення архівованих даних, здійснювати періодичну перевірку та оновлення архіву даних.

DS4.10 Аналіз функціонування систем після відновлення
Встановити, чи впровадило керівництво IT служби процедури оцінки адекватності плану з точки зору можливості успішного відновлення функціонування IT після аварії, та відповідного оновлення вказаного плану.

Сторінку навмисне залишено вільною

Керівні принципи управління

DS4 Забезпечувати безперервність надання послу

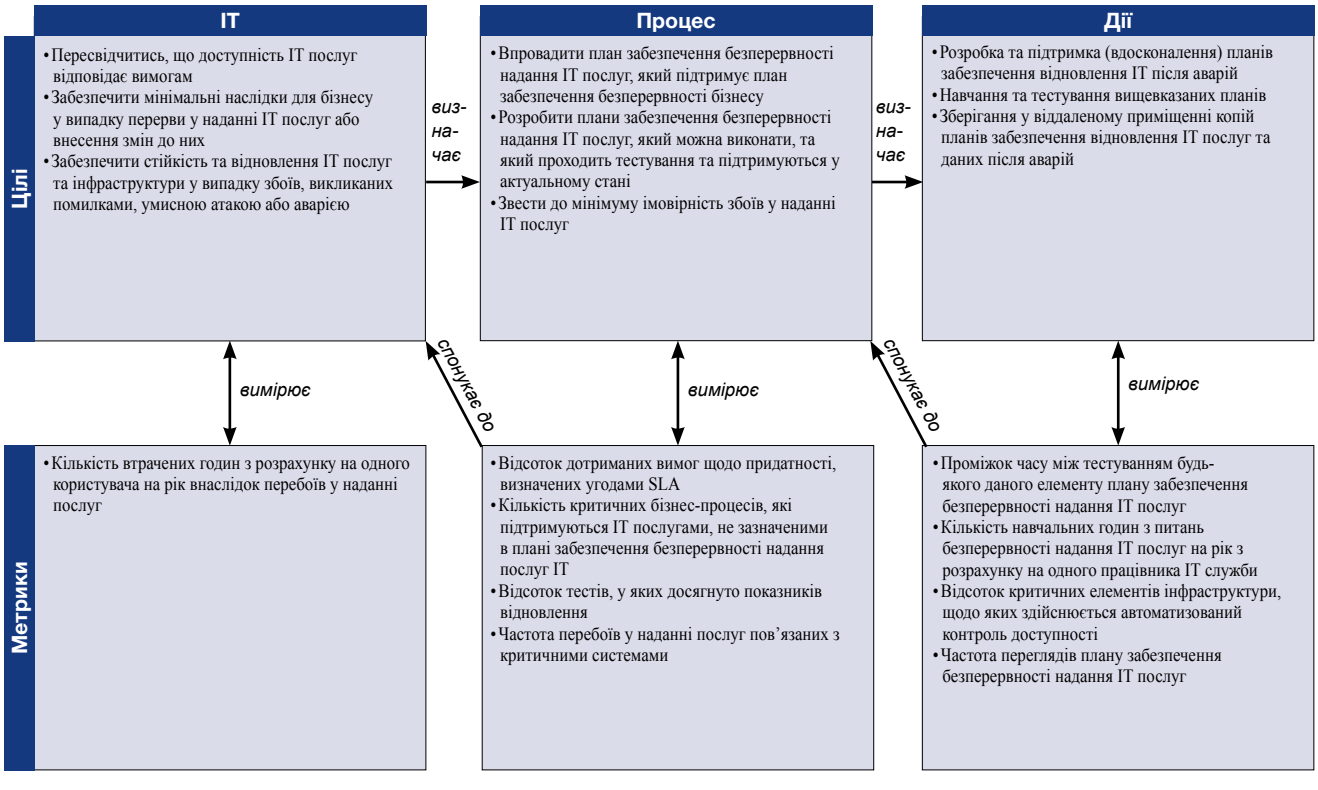
Від	Вхідні дані
PO2	Призначені класифікатори до інформації
PO9	Оцінка ризиків
AI2	Вимоги щодо доступності, безперервності та відновлення
AI4	Посібники користувача, з експлуатації, підтримки, технічний, адміністратора та ін.
DS1	Угоди SLA та OLA

Вихідні дані	Для						
Результати тестів відновлення під час аварій	PO9						
Критичність елементів конфігурації IT	DS9						
План резервного зберігання даних та їх захисту	DS11	DS13					
Порогові параметри інциденту/аварії	DS8						
Вимоги до обслуговування за умов аварії, в тому числі ролі та обов'язки	DS1	DS2					
Звіти щодо результативності процесу	ME1						

RACI-діаграма

Дії \ Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Розробка системи безперервності надання IT послуг		C	C	A	C	R	R	R	C	C	R
Проведення аналізу наслідків для бізнесу та оцінки ризиків		C	C	C	C	A/R	C	C	C	C	C
Розробка та підтримка у робочому стані планів забезпечення безперервності надання IT послуг	I	C	C	C	I	A/R		C	C	C	C
Визначення та розподіл за категоріями IT ресурсів, виходячи з показників відновлення				C		A/R		C	I	C	I
Визначення та виконання процедури контролю за змінами з метою підтримки актуальності плану забезпечення безперервності надання IT послуг				I		A/R		R	R	R	I
Регулярне проведення тестування плану забезпечення безперервності надання IT послуг				I	I	A/R		C	C	I	I
Розробка плану подальших заходів, виходячи з результатів тестування				C	I	A/R	C	R	R	R	I
Складення плану навчальних заходів з питань забезпечення безперервності надання IT послуг та здійснення цих заходів				I	R	A/R		C	R	I	I
Складення плану відновлення IT послуг		I	I	C	C	A/R	C	R	R	R	C
Складення плану та впровадження системи резервного зберігання та захисту інформації				I		A/R		C	C	I	I
Впровадження процедури проведення аналізу функціонування системи після відновлення				C	I	A/R		C	C		C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS4 Забезпечувати безперервність надання послуг

Рівні зрілості управління процесом *«Забезпечувати безперервність надання послуг»*, які задовольняють бізнес-вимоги до IT *«гарантувати мінімальний рівень наслідків для бізнесу у випадку перебоїв у наданні IT послуг»*, є такими:

0 Не існуючий, якщо
Відсутнє усвідомлення ризиків, уразливих місць та загроз для IT операцій, або розуміння наслідків збоїв у наданні IT послуг для бізнесу. Керівництво вважає, що забезпечення безперервності надання послуг IT не потребує його уваги.. . . . .

1 Початковий, якщо
Відповідальність за забезпечення безперебійності IT послуг офіційно не визначена, а повноваження щодо виконання відповідних обов'язків є обмеженими. Керівництво починає усвідомлювати значення відповідних ризиків та потребу у безперервному наданні IT послуг. Увага керівництва у забезпеченні безперебійного обслуговування сконцентрована на ресурсах інфраструктури, а не на IT послугах. Користувачі винаходять тимчасові рішення та обхідні шляхи у відповідь на виникнення збоїв у наданні IT послуг. Служба IT реагує на суттєві перебої в конкретному випадку та без належної підготовки. Існує графік планових перерв в обслуговування з урахуванням потреб IT, але при цьому не враховуються потреби бізнесу.

2 Повторюваний але інтуїтивний, якщо
Існує розподіл обов'язків по забезпеченню безперервного надання IT послуг. Методи забезпечення безперервності обслуговування мають фрагментарний характер. Звіти щодо придатності систем є поодинокими, можуть бути неповними та не враховують наслідків для бізнесу. Немає документально оформленого плану забезпечення безперервності надання IT послуг, хоча існує курс на забезпечення постійної придатності послуг та усвідомлені його основні принципи. Існує перелік критичних систем та елементів, але він може бути недостовірним. Зароджуються практики забезпечення безперервності надання IT послуг, але позитивні результати від їх реалізації залежать від окремих осіб.

3 Визначений, якщо
Має місце чітка індивідуальна відповідальність за управління безперервністю надання послуг IT. Обов'язки стосовно планування та тестування заходів із забезпечення безперебійної роботи чітко визначені та розподілені. План забезпечення безперервності надання IT послуг оформлений документально та складений з врахуванням критичності систем та наслідків для бізнесу. Має місце періодична звітність щодо результатів тестування на безперервність надання послуг. Окремі особи проявляють ініціативу у дотриманні стандартів та проходженні навчання з питань поводження у випадку суттєвих інцидентів або аварій. Керівництво постійно доводить до відома працівників необхідність складання планів для забезпечення безперервності надання послуг. Застосовуються компоненти, що забезпечують високу доступність, та резервні системи. Постійно ведеться облік критичних систем та компонент.

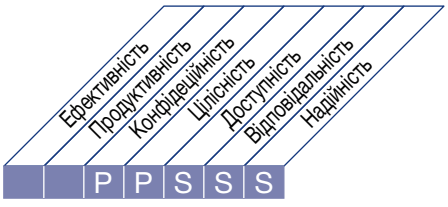
4 Керований та вимірюваний, якщо
Забезпечується виконання обов'язків та дотримання стандартів безперебійності надання IT послуг. Призначена відповідальність за підтримку на належному рівні плану забезпечення безперервності надання IT послуг. Діяльність з вказаної підтримки базується на результатах тестування безперервності надання послуг, власних провідних практиках а також з врахуванням змін в IT та бізнес-середовищі. Здійснюється накопичення, аналіз, надання структурованих даних щодо безперервності надання послуг, відповідно до яких вживаються заходи. Проводиться формальне та обов'язкове навчання з питань, що стосуються процесів забезпечення безперебійності роботи. Постійно впроваджуються провідні практики у сфері забезпечення доступності систем. Практики із забезпечення доступності систем та процеси планування безперебійності роботи взаємопов'язані. Здійснюється класифікація випадків виникнення збоїв, і для кожного типу збоїв шлях ескалації інциденту відомий всім задіяним особам. Розроблені та узгоджені цілі та метрики для процесу забезпечення безперервності надання IT послуг, але вимірювання може мати непослідовний характер.

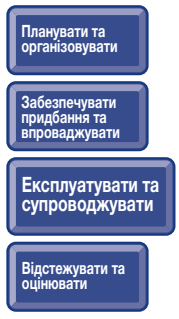
5 Оптимізований, якщо
Інтегровані процеси забезпечення безперервності надання IT послуг передбачають проведення порівняльного аналізу та врахування найкращих зовнішніх практик. План забезпечення безперервності надання IT послуг інтегровано у плани забезпечення безперервності бізнесу, постійно підтримується його актуальність. Вимога щодо забезпечення безперервності надання IT послуг гарантується виробниками та основними постачальниками. Проводиться глобальне тестування плану забезпечення безперервності надання IT послуг, результати цих випробувань використовуються для оновлення цього плану. Накопичення та аналіз даних слугують постійному вдосконаленню процесу. Практики, що стосуються забезпечення доступності систем та процеси планування заходів із забезпечення безперервності надання IT послуг повністю узгоджені між собою. Керівництво організації гарантує, що аварія або суттєвий інцидент не стануться в результаті поодинокої відмови системи. Практики ескалації проблем є зрозумілими, забезпечено їх чітке дотримання. Цілі та метрики результатів із забезпечення безперервності надання IT послуг вимірюються систематично. Керівництво організації коригує план безперебійної роботи з надання послуг на підставі вказаних результатів вимірювання.

Опис процесу

DS5 Забезпечувати безпеку систем

Щоб підтримувати цілісність інформації та забезпечити захист IT ресурсів, необхідно впровадити процес управління безпекою. Цей процес передбачає введення та дотримання розподілу ролей та обов'язків щодо безпеки IT, політик, стандартів та процедур. Управління безпекою також повинно включати здійснення моніторингу та періодичної перевірки інформаційної безпеки, а також вжиття коригувальних заходів для виявлення слабких місць та інцидентів інформаційної безпеки. Ефективне управління безпекою дозволяє організувати захист всіх IT ресурсів з метою зведення до мінімуму наслідків для бізнесу, спричинених наявністю вразливостей та інцидентів.





Контроль IT процесу

Забезпечувати безпеку систем

який задовольняє бізнес-вимоги до IT, а саме:

підтримка цілісності інформації та інфраструктури системи обробки інформації, а також зведення до мінімуму наслідки від вразливостей та інцидентів інформаційної безпеки

зосереджений на

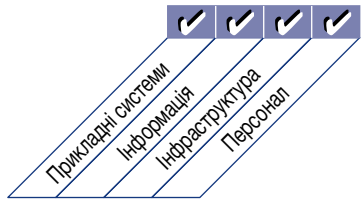
визначенні політик, планів та процедур в сфері забезпечення безпеки IT, а також здійсненні моніторингу, виявлення, надання інформації а також вжиття коригувальних заходів щодо вразливостей та інцидентів інформаційної безпеки

реалізується шляхом

- осмислення вимог інформаційної безпеки, вразливостей та загроз
- управління ідентифікаційною інформацією та процесом авторизації користувачів у стандартний спосіб
- регулярного тестування системи безпеки

та вимірюється

- кількістю інцидентів, які шкодять репутації підприємства
- кількістю систем, які не задовольняють вимоги інформаційної безпеки
- кількістю порушень правил розподілу обов'язків



Цілі контролю

DS5 Забезпечувати безпеку систем

DS5.1 Управління безпекою IT
Управляти безпекою IT на найвищому відповідному організаційному рівні, таким чином узгоджуючи управління заходами із забезпечення безпеки з потребами бізнесу. . .
.

DS5.2 План забезпечення безпеки IT
Трансформувати бізнес-вимоги, а також вимоги, продиктовані управлінням ризиками та необхідністю дотримання відповідності, у загальний план забезпечення безпеки IT, виходячи з інфраструктури IT та культури інформаційної безпеки. Забезпечити реалізацію цього плану у політиках та процедурах інформаційної безпеки разом з необхідними інвестиціями в послуги, персонал, програмне та апаратне забезпечення. Довести політики та процедури інформаційної безпеки, до відома зацікавлених сторін та користувачів.

DS5.3 Управління ідентифікаційною інформацією
Забезпечити однозначну ідентифікацію всіх користувачів (внутрішніх, зовнішніх та тимчасових) та дії, які вони виконують в IT системах (використання прикладних програмних продуктів для бізнесу, підтримка IT оточення, експлуатація системи, розробка та технічне обслуговування). Надавати ідентифікаційну інформацію користувача з використанням механізмів аутентифікації. Підтверджувати те, що всі права доступу користувачі до систем та даних відповідають визначеним та документально оформленим вимогам бізнесу, а також той факт, що посадові вимоги прив'язані до ідентифікаційної інформації користувача. Забезпечити те, що права користувача надаються за запитом керівника користувача, затверджуються власниками системи та впроваджуються особою, відповідальною за питання інформаційної безпеки. Зберігати ідентифікаційну інформацію користувача та права доступу в центральному сховищі даних. Вживати ефективних з точки зору затрат заходів технічного та процедурного характеру та підтримувати їх в робочому стані з метою визначення ідентифікаційної інформації користувача, впровадження аутентифікації та забезпечення дотримання прав доступу.

DS5.4 Управління обліковими записами користувача
Забезпечити виконання процедур запиту, визначення, видачі, призупинення повноважень, зміни та закриття облікових даних користувача та пов'язаних з ними повноважень користувача шляхом введення сукупності процедур з управління обліковими даними користувача. Передбачити процедуру затвердження, у якій зазначити власника даних або системи, що надає права доступу до них. Вказані процедури слід застосовувати по відношенню до всіх користувачів, в тому числі адміністраторів (привілейованих користувачів), а також внутрішніх та зовнішніх користувачів за умов звичайної роботи систем та у випадку виникнення аварійних ситуацій. Права та обов'язки, які стосуються реалізації доступу до систем та даних підприємства повинні бути закріплені контрактами, укладеними з усіма категоріями користувачів. Здійснювати регулярну перевірку керівництвом всіх облікових записів та відповідних прав.

DS5.5 Тестування системи безпеки, здійснення огляду та моніторингу
Здійснювати проактивне тестування та моніторинг впровадження системи безпеки IT. Система безпеки IT повинна своєчасно проходити повторну акредитацію, яка має підтвердити дотримання затвердженого організацією рівня інформаційної безпеки. Ведення реєстраційного журналу та здійснення моніторингу дадуть змогу на ранньому етапі попереджати та/або виявляти факти нестандартних та/ або аномальних дій, на які потрібно звернути належну увагу, а також надавати своєчасну інформацію щодо вказаних подій.

DS5.6 Визначення поняття інциденту в системі безпеки
Чітко визначити та довести до загального відома характеристики потенційних інцидентів у системі безпеки, щоб мати змогу здійснити відповідну класифікацію таких подій та забезпечити належну реалізацію процесу управління інцидентами та проблемами.

DS5.7 Захист технології забезпечення безпеки
Забезпечити стійкість до можливого злочинного використання технології, задіяної у забезпечення безпеки, та не розголошувати зміст документації, що стосуються питань безпеки, якщо в цьому немає потреби.

DS5.8 Управління криптографічними ключами
Забезпечити введення політик та процедур, які дозволяють організувати генерацію, зміну, анулювання, знищення, розповсюдження, сертифікацію, зберігання, введення, використання та архівування криптографічних ключів для забезпечення захисту від модифікації та несанкціонованого розкриття.

DS5.9 Попередження проникнення шкідливого програмного забезпечення, виявлення подібних фактів та вжиття коригувальних заходів
Ввести в дію систему заходів з попередження, виявлення та корегування розповсюдження шкідливого програмного забезпечення (зокрема, сучасних оновлень системи безпеки та антивірусних програм) в масштабах всієї організації з метою захисту інформаційних систем та технологій від шкідливих програмних засобів (наприклад, вірусів, вірусних програм само тиражування, спаму).

DS5.10 Безпека мережі
Використовувати належні методи забезпечення безпеки та відповідні процедури управління (наприклад, системи мережевого захисту типу брандмауер, програмно-апаратні комплекси забезпечення захисту, методи сегментації мережі, методи виявлення вторгнення) з метою авторизації доступу та контролю інформаційних потоків, що виходять з мереж та надходять до них.

DS5.11 Обмін конфіденційними даними
Здійснювати обмін конфіденційною інформацією тільки з використанням захищеного каналу або середовища, із застосуванням засобів контролю, які дозволяють забезпечити автентичність змісту, підтвердження передачі, підтвердження отримання та неможливість зречення від походження інформації.

Сторінку навмисне залишено вільною

Керівні принципи управління

DS5 Забезпечувати безпеку систем

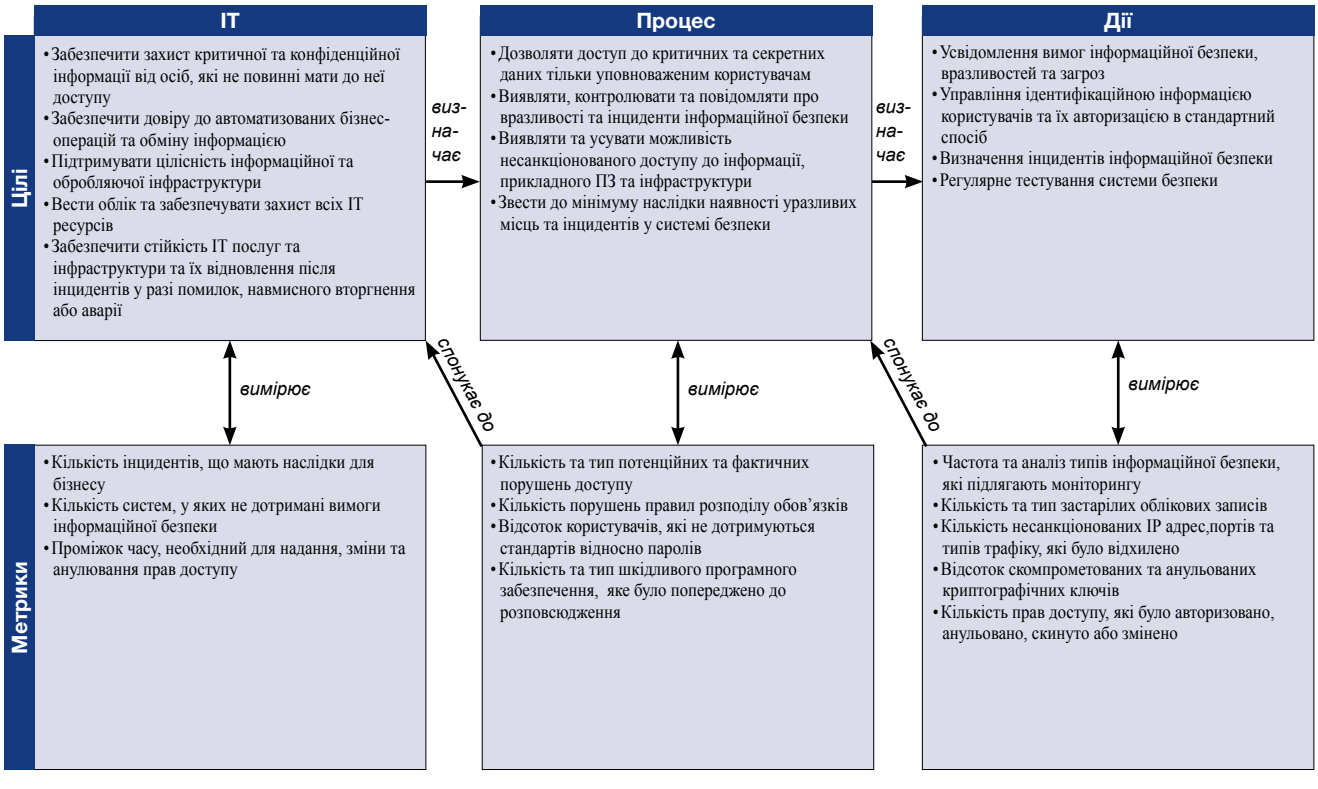
Від	Вхідні дані
PO2	Інформаційна архітектура; визначені класифікатори даних
PO3	Технологічні стандарти
PO9	Оцінка ризиків
AI2	Вимоги до заходів контролю безпеки прикладного ПЗ
DS1	Угоди OLA

Вихідні дані	Для						
Визначення інциденту інформаційної безпеки	DS8						
Конкретні вимоги до навчання з питань усвідомлення інформаційної безпеки	DS7						
Звіти щодо результативності процесу	ME1						
Необхідні зміни у системі безпеки	AI6						
Загрози та уразливі місця системи безпеки	PO9						
План та політики IT безпеки	DS11						

RACI-діаграма

Дії \ Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Складання плану забезпечення безпеки IT та підтримка його актуальності	I	C	C	A	C	C	C	C	I	I	R
Визначення, впровадження та виконання процесу управління ідентифікаційною інформацією користувача (або обліковими даними)			I	A	C	R	R	I			C
Здійснення моніторингу потенційних та реальних інцидентів у системі безпеки				A	I	R	C	C			R
Здійснення періодичної перевірки та підтвердження прав доступу користувачів та їх привілеїв				I	A	C					R
Встановлення та підтримка у робочому стані процедури збереження та захисту криптографічних ключів				A		R			I		C
Впровадження та підтримка в робочому стані заходів технічного та процедурного контролю з метою забезпечення захисту інформаційних потоків при переміщенні між мережами				A	C	C	R	R			C
Здійснення регулярних заходів з оцінки вразливостей		I		A	I	C	C	C			R

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS5 Забезпечувати безпеку систем

Рівні зрілості управління процесом *«Забезпечувати безпеку систем»*, які задовольняють бізнес-вимоги до IT *«підтримувати цілісність інформації та інфраструктури системи обробки інформації а також звести до мінімуму наслідки від вразливостей та інцидентів інформаційної безпеки»*, є такими:

0 Не існуючий, якщо
Організація не усвідомлює необхідності забезпечення безпеки IT. Обов'язки та індивідуальна відповідальність щодо забезпечення безпеки не визначені та не розподілені. Не впроваджено заходи стосовно підтримки управління безпекою IT. Не існує звітності щодо стану системи забезпечення безпеки IT, відсутній процес реагування на порушення системи безпеки IT. Повністю відсутній виділений процес управління системою безпеки.

1 Початковий, якщо
Організація усвідомлює необхідність забезпечення безпеки IT. Усвідомлення потреби в безпеці залежить в основному від окремих осіб. Вирішення питань інформаційної безпеки має реактивний характер. Стан безпеки IT не оцінюється. У разі виявлення порушення безпеки IT ведеться пошук винуватців, оскільки відповідальність та обов'язки не є чітко визначеними. Реакція на порушення безпеки IT має непередбачений характер.

2 Повторюваний але інтуїтивний, якщо
Обов'язки та індивідуальна відповідальність за забезпечення безпеки IT покладено на координатора заходів із забезпечення безпеки IT, хоча повноваження подібного координатора мають обмежений характер. Усвідомлення необхідності забезпечення безпеки IT є фрагментарним та обмеженим. Хоча системи формують дані, що стосуються безпеки, цю інформацію не аналізують. Послуги сторонніх організацій можуть не відповідати конкретним потребам організації з точки зору безпеки. Політики у сфері забезпечення безпеки розроблені, але кваліфікація персоналу та наявні засоби не відповідають висунутим вимогам. Звітність щодо стану безпеки IT є неповноцінною, недостовірною або не маючою відношення до справи. Навчання з питань безпеки проводяться, але головним чином з ініціативи окремих осіб. Вважається, що забезпечення безпеки у сфері IT є обов'язком служби IT та належить до сфери IT, а бізнес-підрозділи не вважають, що це питання належить до сфери інтересів бізнесу.

3 Визначений, якщо
Усвідомлення потреби у інформаційній безпеці підтримується керівництвом організації. Процедури забезпечення безпеки IT визначені та узгоджені з політикою у сфері безпеки IT. Обов'язки щодо забезпечення безпеки IT розподілені та усвідомлені, але не забезпечене їх послідовне виконання. План забезпечення безпеки IT та рішення, які дозволяють реалізувати безпеку IT спричинені результатом аналізу ризиків. Звітність щодо стану системи безпеки не має чіткої орієнтації на потреби бізнесу. Здійснюється епізодичне тестування системи безпеки (наприклад, тестування з моделюванням вторгнення в систему). Для бізнес-підрозділів та IT служби проводиться навчання з питань безпеки IT,але планування та організація таких заходів є неформальними.

4 Керований та вимірюваний, якщо
Обов'язки із забезпечення безпеки IT чітко розподілені, організовані та виконуються. Постійно здійснюється аналіз ризиків IT безпеки та їх наслідків. Політики та процедури у сфері забезпечення безпеки доповнені базовими прикладами. Обов'язковим є знайомство з методами підвищення рівня усвідомлення безпеки. Процедури ідентифікації, аутентифікації та авторизації користувачів мають стандартний характер. Здійснюється процедура сертифікації для персоналу, який несе відповідальність за аудит та управління системою безпеки. Тестування системи безпеки здійснюється з використанням стандартних та формалізованих процесів, що дає змогу підвищити рівень захисту. Процеси забезпечення безпеки IT координуються з процесами забезпечення загальної безпеки організації. Звітність щодо стану системи безпеки IT узгоджена з бізнес-цілями. Навчання з питань безпеки у сфері IT проводиться як для бізнес-підрозділів, так і для IT служби. Навчальні заходи з питань безпеки IT плануються та організовуються в спосіб, який враховує потреби бізнесу та визначені профілі ризиків, пов'язаних з безпекою. Цілі та метрики процесу управління забезпеченням безпеки визначені, але вимірювання не здійснюються.

5 Оптимізований, якщо
Забезпечення безпеки IT є спільним обов'язком керівництва бізнес-підрозділів та IT служби та інтегровано з бізнес-цілями забезпечення корпоративної безпеки. Вимоги до IT безпеки чітко визначені, оптимізовані та включені у затверджений план інформаційної безпеки. Користувачі та замовники все частіше беруть участь у визначенні вимог до системи безпеки, а функції забезпечення безпеки інтегровані з прикладними програмними продуктами на стадії проектування. Інциденти в системі безпеки оперативно аналізуються з використанням формалізованих процедур реагування на інциденти із залученням автоматизованих (програмних) засобів. Проводяться періодичні перевірки системи безпеки з метою оцінки ефективності впровадження плану інформаційної безпеки. Дані щодо загроз та

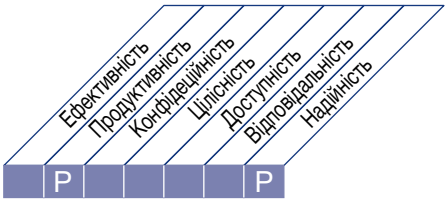
вразливостей системи безпеки систематично накопичуються та аналізуються. Терміново доводяться до відома та впроваджуються належні заходи із зменшення ризиків.
Тестування безпеки, аналіз ключової причини інцидентів безпеки на проактивне визначення ризиків використовуються для постійного вдосконалення процесу. Процеси та технології забезпечення безпеки інтегровані в масштабах всієї організації. Метрики процесу управління інформаційною безпекою регулярно вимірюються, накопичуються та доводяться до відома. Керівництво використовує ці метрики для коригування плану заходів із забезпечення безпеки в ході процесу безперервного вдосконалення.

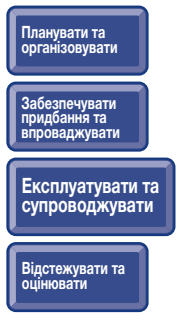
Сторінку навмисне залишено вільною

Опис процесу

DS6 Визначати та розподіляти витрати

Щоб створити чесну та справедливу систему розподілу витрат на IT бізнес-підрозділами, необхідно здійснювати точний вимір витрат на IT, а також домовитись з користувачами з бізнес-підрозділів щодо чесного віднесення та розподілу витрат. Цей процес передбачає побудову та експлуатацію системи фіксації, розподілу, та звітування користувачам витрат на IT. Чесна система розподілу дає змогу бізнес-підрозділам приймати максимально обґрунтовані рішення стосовно користування IT послугами.





Контроль IT процесу

Визначати та розподіляти витрати

який задовольняє бізнес-вимоги до IT, а саме:

забезпечення прозорості та зрозумілості витрат на IT та підвищення економічної ефективності шляхом надання вичерпної інформації щодо користування IT послугами

зосереджений на

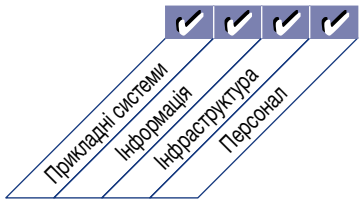
накопичені повної та точної інформації стосовно витрат на IT, створенні чесної системи розподілу витрат, узгодженої з користувачами з бізнес-підрозділів, та системи, що забезпечить вчасне надання звітності щодо користування IT послугами та розподілу відповідних витрат

реалізується шляхом

- узгодження витрат з рівнем якості та обсягом наданих послуг
- створення та узгодження повноцінної моделі витрат
- здійснення розподілу витрат згідно з узгодженою політикою

та вимірюється

- відсотком рахунків-фактур із зазначенням витрат на IT послуги, прийнятих/оплачених керівництвом бізнес-підрозділів
- відсотком розбіжностей між даними щодо витрат, закладеними до бюджетів, прогнозованими даними та фактичними витратами
- відсотком загальних витрат на IT, які розподілені відповідно до узгоджених моделей витрат



Цілі контролю

DS6 Визначати та розподіляти витрати

DS6.1 Визначення послуг
Визначити всі витрати на IT, та поставити їх у відповідність до IT послуг з метою підтримки прозорої моделі витрат. IT послуги повинні бути прив'язані до бізнес-процесів в такий спосіб, щоб бізнес-підрозділи могли ототожнити з послугами відповідні рівні рахунків, виставлених за надання послуг.

DS6.2 Ведення обліку та звітності у сфері IT
Накопичувати інформацію та розподіляти фактичні витрати згідно з моделлю витрат, прийнятою на підприємстві. Розбіжності між прогнозованими даними та фактичними витратами слід аналізувати та відображати у звітах звіти відповідно до системи оцінки фінансових показників,прийнятої в організації. . .

DS6.3 Створення моделі витрат та нарахування витрат
Створити та використовувати модель витрат у сфері IT на базі визначень послуг, яка дозволяє здійснювати розрахунок частки претензійних платежів на одну послугу. Модель витрат у сфері IT повинна забезпечувати нарахування витрат таким чином, щоб користувачі могли їх розпізнати, виміряти та спрогнозувати з метою належного використання ресурсів.

DS6.4 Підтримка актуальності моделі витрат
Регулярно аналізувати та виконувати порівняльний аналіз моделі витрат/моделі перерозподілу витрат з метою збереження її актуальності та відповідності новим напрямкам бізнесу та IT.

Керівні принципи управління

DS6 Визначати та розподіляти витрати

Від	Вхідні дані
PO4	Власники систем, зазначені в документації
PO5	Звіти про співвідношення вигод/витрат, бюджети IT
PO10	Детальні проектні плани
DS1	Угоди SLA та OLA

Вихідні дані	Для						
Фінансові показники у сфері IT	PO5						
Звіти щодо результативності процесу	ME1						

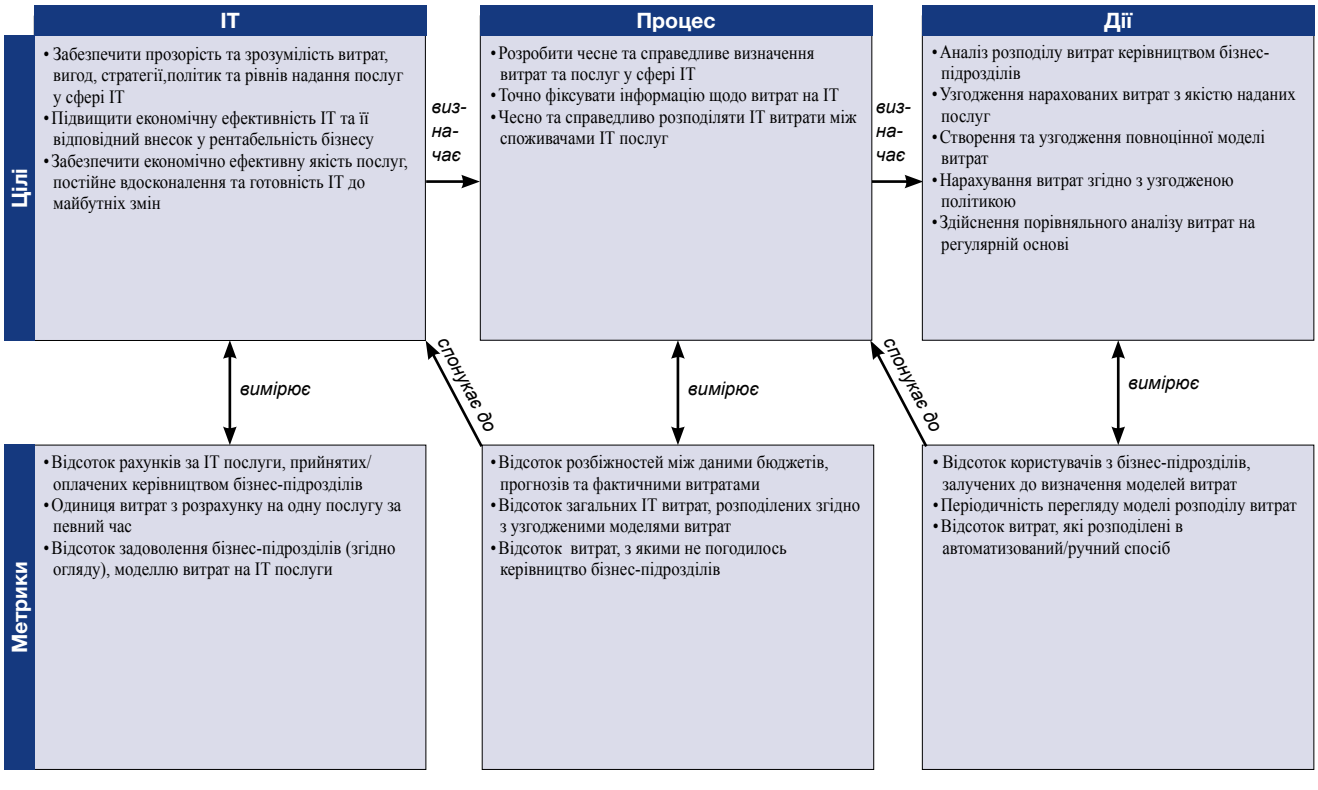
RACI-діаграма

Функції / **Дії**

Співставлення IT інфраструктури з наданими послугами/підтриманими бізнес-процесами		C	C	A	C	C	C	C	R	C	
Визначення всіх IT витрати (наприклад, на персонал, технології) та співставлення їх з IT послугами, виходячи з одиниці витрат		C		A		C	C	C	R	C	
Впровадження та підтримка обліку в IT та процесу контролю витрат		C	C	A	C	C	C	C	R	C	
Впровадження та виконання політик та процедур нарахування витрат		C	C	A	C	C	C	C	R	C	

CEO | CFO | Керівник бізнес-підрозділу | CIO | Власник бізнес-процесу | Директор з операційних питань | Директор з питань архітектури | Керівник підрозділу розробки | Керівник служби адміністрування IT | PMO | Служба контролю дотримання вимог, аудиту, ризиків та безпеки

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS6 Визначати та розподіляти витрати

Рівні зрілості управління процесом *«Визначати та розподіляти витрати»*, які задовольняють бізнес-вимоги до IT *«забезпечити прозорість та зрозумілість витрат на IT та підвищити економічну ефективність шляхом надання вичерпної інформації щодо користування IT послугами»*, є такими:

0 Не існуючий, якщо
Повністю відсутній процес визначення та розподілу витрат згідно з наданими інформаційними послугами. Організація навіть не усвідомлює, що потрібно займатись проблемою обліку та аналізу витрат, комунікації з цього питанні відсутні.. .

1 Початковий, якщо
Присутнє загальне розуміння всіх витрат на інформаційні послуги, але немає розбивки витрат за користувачами, замовниками, департаментами, групами користувачів, сервісними групами, проектами або кінцевими результатами. Фактично немає контролю витрат, має місце лише звітність стосовно сукупних витрат перед керівництвом. Витрати на IT послуги відносяться на експлуатаційні витрати. Бізнес-підрозділи не отримують жодної інформації щодо витрат або вигод від надання послуг.

2 Повторюваний але інтуїтивний, якщо
Має місце загальне усвідомлення необхідності визначення та розподілу витрат. Розподіл витрат базується на неформальних або застарілих припущеннях щодо витрат, наприклад, оцінці витрат на апаратне забезпечення, і вони, фактично, жодними чином не пов'язані з чинниками цінності. Процеси, що описують розподіл витрат, є відтворюваними. Відсутні заходи з навчання або комунікацій з питань стандартних процедур визначення або розподілу витрат. Відповідальність за накопичення інформації або розподіл витрат не покладена на конкретних осіб.

3 Визначений, якщо
Створено визначену та оформлену документально модель витрат на інформаційні послуги. Визначено процес, що описує зв'язок IT витрат з послугами, наданими користувачам. Має місце належне розуміння того, що витрати співвідносяться з певними інформаційними послугами. Бізнес-підрозділи отримують часткову інформацію щодо витрат.

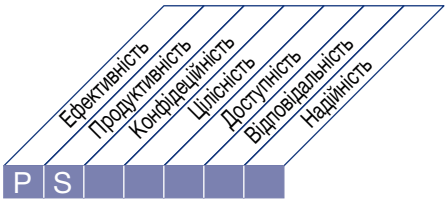
4 Керований та вимірюваний, якщо
Обов'язки та індивідуальна відповідальність щодо управління витратами на інформаційні технології визначена та зрозуміла на всіх рівнях організації, а також підтримується офіційними навчаннями. Визначаються прямі та непрямі витрати; керівництво, власники бізнес-процесів та користувачі вчасно отримують відповідні звіти та із застосуванням автоматизованих методів. В більшості випадків здійснюється моніторинг та оцінювання витрат, вживаються заходи у разі виявлення відхилень у витратах. Звітність щодо витрат на інформаційні послуги пов'язана з бізнес-цілями та угодами про рівень надання послуг, та знаходиться під моніторингом власників бізнес-процесів. Фінансова служба здійснює аналіз прийнятності процесу розподілу витрат. Впроваджено автоматизовану систему обліку витрат, але вона орієнтована на задачі надання інформаційних послуг, а не на бізнес-процеси. Цілі та метрики узгоджені з процесом вимірювання витрат, але подібне вимірювання здійснюється непослідовно.

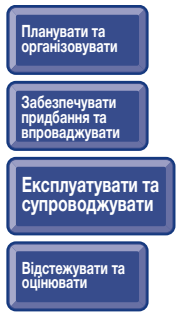
5 Оптимізований, якщо
Здійснюється визначення, фіксація, агрегація і формування звітності для власників бізнес-процесів та користувачів відносно витрат пов'язаних з наданням послуг. Витрати визначаються як позиції, що підлягають оплаті, та можуть підтримувати систему претензійних (зворотних) платежів, яка дозволяє належним чином виставити рахунки користувачам за надані послуги, виходячи з використання. Детальні витрати використовуються в угодах SLA. Здійснюється моніторинг та оцінка витрат з метою оптимізації вартості IT ресурсів. Отримані дані щодо витрат використовуються для оцінювання результатів з точки зору отримання вигод в ході процесу формування бюджету організації. Звітність щодо витрат на інформаційні послуги дозволяє заздалегідь попереджати про зміни у бізнес-вимогах завдяки використанню інтелектуальних систем формування звітності. Застосовується модель змінних витрат, яку отримують на підставі обсягів робіт, виконаних для кожної наданої послуги. Процес управління втратами доведений до рівня галузевих практик в результаті постійного вдосконалення та порівняння з показниками інших організацій. Постійно здійснюється процес оптимізації витрат. Керівництво організації здійснює критичний перегляд цілей та метрик в межах постійно діючого процесу вдосконалення, орієнтованого на реорганізацію систем вимірювання витрат.

Опис процесу

DS7 Навчати користувачів

Для здійснення ефективного навчання всіх користувачів IT систем, в тому числі ITперсоналу, необхідно визначити потреби у навчанні кожної групи користувачів. На додаток до визначення потреб даний процес передбачає формування та реалізацію стратегії ефективного навчання та оцінки результатів. Програма ефективного навчання сприяє підвищенню ефективності використання технологій за рахунок зменшення кількості помилок користувачів, підвищення продуктивності та ступеня відповідності вимогам основних контролів, наприклад, заходів з інформаційної безпеки по відношенню до користувачів.





Контроль IT процесу

Навчати користувачів

який задовольняє бізнес-вимоги до IT, а саме:

ефективне та продуктивне використання прикладних програмних засобів та технологічних рішень, а також забезпечення дотримання користувачами політик та процедур

зосереджений на

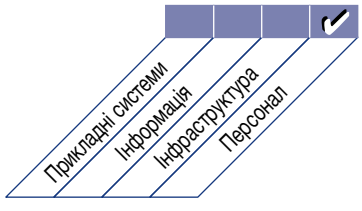
чіткому усвідомленні потреби у проведення навчання користувачів IT, реалізації стратегії ефективного навчання та вимірюванні результатів

реалізується шляхом

- створення учбового плану
- організації навчання
- проведення навчання
- здійснення моніторингу ефективності навчання на надання відповідної звітності

та вимірюється

- кількістю дзвінків до служби підтримки користувачів, викликаних відсутністю навчання користувачів
- відсотком зацікавлених сторін, задоволених наданим навчанням
- проміжком часу між моментом визначення потреб у навчанні та моментом здійснення відповідного навчального заходу



Цілі контролю

DS7 Навчати користувачів

DS7.1 Визначення потреб у навчанні та проведенні інструктажу
Скласти та регулярно оновлювати учбову програму або план для кожної цільової групи працівників з врахуванням:
- поточних та майбутніх потреб бізнесу та бізнес-стратегії
- цінності інформації як ресурсу
- корпоративних цінностей (етичних цінностей, культури у сфері забезпечення контролю та безпеки тощо)
- впровадження нової IT інфраструктури та програмного забезпечення (тобто пакетних програмних засобів, прикладних програмних засобів)
- поточного та майбутнього рівня кваліфікації, даних щодо компетентності, а також необхідності у проведенні акредитації (сертифікації), атестації а також повторної акредитації спеціалістів
- методів подання навчального матеріалу (наприклад, учбові приміщення, веб-технології), розміру цільової групи, доступності та належного розкладу.

DS7.2 Проведення навчання та інструктажу
Виходячи з визначених потреб у навчанні, визначити цільові групи та їх учасників, ефективні способи подання навчального матеріалу, склад викладачів, інструкторів та кураторів. Призначити викладачів та організувати навчальні заняття відповідно до розкладу. Здійснювати реєстрацію учасників (в тому числі фіксувати передумови для навчання), відвідуваність занять та оцінювання ефективності навчання.

DS7.3 Оцінка результатів проведеного навчання
Оцінювати процес подання інформаційного наповнення навчальних курсів після їх завершення з точки зору відповідності, якості, ефективності, запам'ятовування інформації, вартості та цінності. Результати подібного оцінювання слід використовувати з метою подальшої розробки учбових програм та проведення навчальних занять.

Керівні принципи управління

DS7 Навчати користувачів

Від	Вхідні дані
PO7	Кваліфікація та компетентність користувачів в тому результати індивідуального навчання, конкретні вимоги до навчання
AI4	Навчальні матеріали, вимоги до передачі знань з метою впровадження рішень
DS1	Угоди OLA
DS5	Конкретні вимоги до навчання з питань усвідомлення необхідності захисту
DS8	Звіти про задоволення користувачів

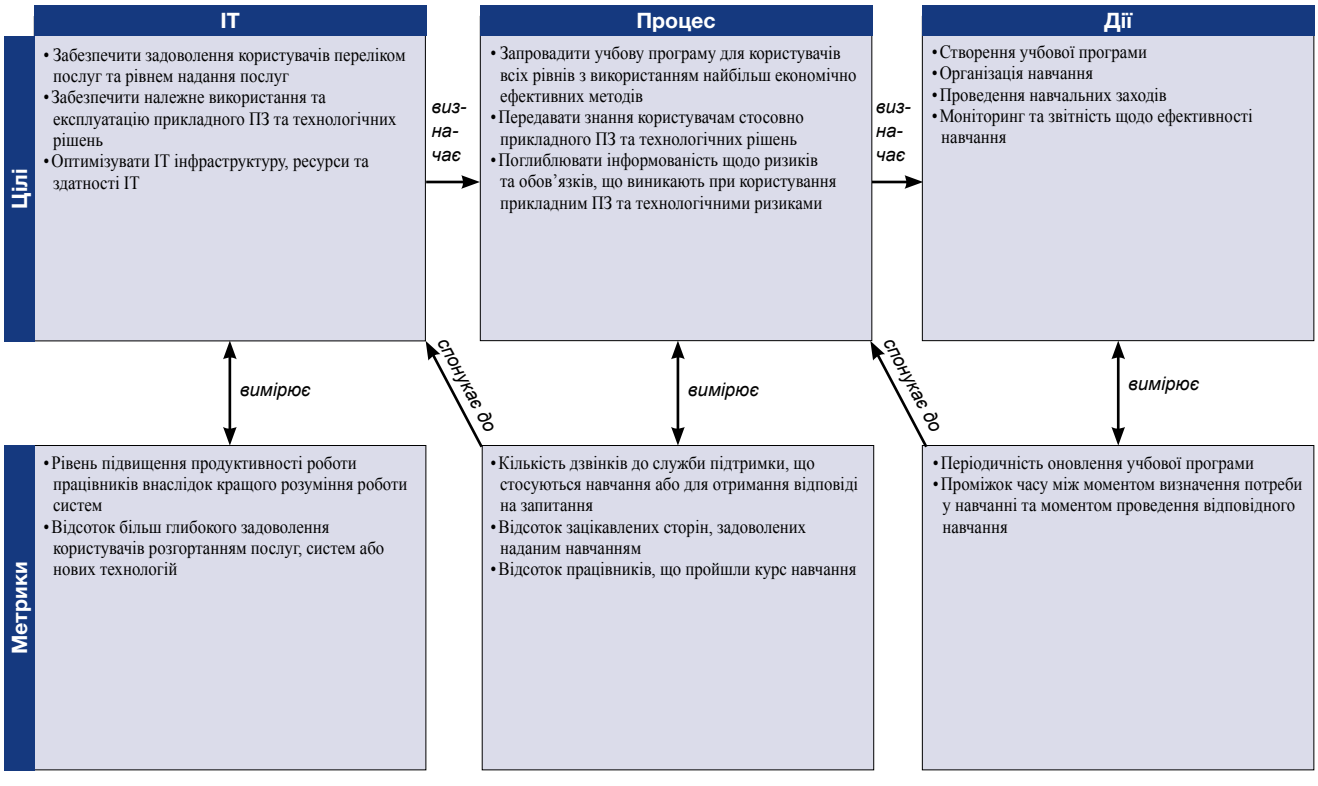
Вихідні дані	Для						
Фінансові показники у сфері IT	PO5						
Звіти щодо результативності процесу	ME1						

RACI-діаграма

Функції

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки	Департамент навчання
Визначення та характеризування потреби користувачів у навчанні			C	A	R	C	C	C	C	C	C	R
Створення навчальної програми			C	A	R	C	I	C	C	C	I	R
Здійснювати діяльність із забезпечення підвищення усвідомлення, інструктажу та навчання			I	A	C	C	I	C	C	C	I	R
Здійснення оцінки результатів навчання			I	A	R	C	I	C	C	C	I	R
Визначення та оцінка найкращих методів та засобів навчання			I	A/R	R	C	C	C	C	C	C	R

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS7 Навчати користувачів

Рівні зрілості управління процесом *«Навчати користувачів»*, які задовольняють бізнес-вимоги до IT *«ефективно та продуктивно використовувати прикладні програмні засоби та технологічні рішення, а також забезпечити дотримання користувачами політик та процедур»*, є такими:

0 Не існуючий, якщо
Програма навчання та інструктажу працівників відсутня взагалі. В організації навіть не існує усвідомлення того, що проблемою навчання необхідно займатись, комунікації з цього питання також відсутні.

1 Початковий, якщо
Організація усвідомлює потребу у створенні програми навчання та інструктажу працівників, але немає відповідних стандартних процесів. Внаслідок відсутності чіткої програми працівники визначають свої потреби у навчанні та відвідують навчальні заходи з власної ініціативи та на свій розсуд. Деякі з навчальних заходів орієнтовані на проблеми етичної поведінки, усвідомлення важливості забезпечення безпеки систем та вивчення практик інформаційної безпеки. У підходах керівництва до цього питання немає злагодженості, комунікації мають хаотичний та непослідовний характер, так само як і підходи до проведення навчання та інструктажу.

2 Повторюваний але інтуїтивний, якщо
Має місце усвідомлення потреби у створення програми з навчання та інструктажу та відповідних процесів в масштабах всієї організації. Працівники починають зазначати необхідність навчання у своїх індивідуальних робочих планах. Процеси розвинуті до рівня, на якому неформальні учбові курси подаються різними викладачами, при цьому аналогічні предмети навчання подаються різними методами. Деякі з навчальних курсів орієнтовані на розгляд питань етичної поведінки та усвідомлення важливості забезпечення безпеки систем, а також відповідних практик. Існує високий ступінь залежності від знань окремих осіб. Однак, мають місце послідовні комунікації з проблем загального характеру та способів їх вирішення.

3 Визначений, якщо
Програму навчання та інструктажу впроваджено та доведено до відома працівників, працівники та керівники визначають та документально закріплюють свої потреби у навчанні. Процеси, що стосуються навчання та інструктажу, стандартні та оформлені документально. На підтримку програми навчання та інструктажу складаються відповідні бюджети, виділяються ресурси, засоби та призначаються викладачі. Працівники проходять формальне навчання з питань етичної поведінки та усвідомлення важливості забезпечення безпеки систем та відповідних практик. Здійснюється моніторинг більшості процесів, що стосуються навчання та інструктажу, але не всі відхилення можуть бути виявлені керівництвом. Аналіз проблем, пов'язаних з навчанням та інструктажем, проводиться лише в окремих випадках.

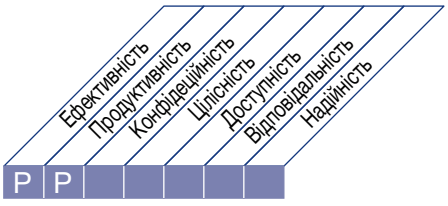
4 Керований та вимірюваний, якщо
Існує всебічна програма навчання та інструктажу, яка дає результати, що піддаються вимірюванню. Обов'язки чітко визначені, визначено власників процесів. Навчання та інструктаж є елементами професійного росту та просування працівників по службі. Керівництво підтримує та відвідує навчальні заняття та заходи з інструктажу. Всі працівники проходять навчання з питань етичної поведінки а також стосовно знання та розуміння заходів безпеки. Всі працівники проходять навчання належного рівня з питань, що стосуються практик інформаційної безпеки, які дозволяють гарантувати захист від шкоди, спричиненої відмовами, що може мати наслідки для доступності, конфіденційності та цілісності даних. Керівництво контролює відповідність програм існуючим вимогам, здійснюючи постійний аналіз та оновлення програм та процесів, що стосуються навчання та інструктажу. Процеси постійно вдосконалюються, забезпечується дотримання найкращих власних практик.

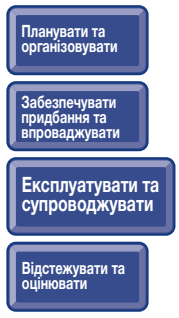
5 Оптимізований, якщо
Проведення навчання та інструктажу сприяє підвищенню індивідуальних показників діяльності працівників. Навчання та інструктаж є критичними чинниками професійного росту працівників. Для реалізації програм навчання та інструктажу виділяють достатні бюджетні кошти, ресурси, засоби та призначаються викладачі. Процеси чітко визначені, постійно вдосконалюються., застосовуються найкращі зовнішні практики та здійснюється формування моделей зрілості з проведенням порівняльного аналізу з показниками інших організацій. Всі проблеми та відхилення аналізуються з метою виявлення першопричин, негайно визначаються та вживаються ефективні коригувальні заходи. Має місце позитивне ставлення до дотримання принципів етичної поведінки та забезпечення безпеки систем. IT використовуються в екстенсивний, інтегрований та оптимізований спосіб, що дозволяє автоматизувати та надати засоби для реалізації програми навчання та інструктажу. Ефективно використовується допомога сторонніх спеціалістів з навчання, для подальшого керівництва застосовується порівняльний аналіз відповідних показників.

Опис процесу

DS8 Управляти службою підтримки та інцидентами

Щоб забезпечити своєчасне та ефективне реагування на запити та проблеми користувачів IT, необхідно впровадити правильно розроблений процес управління службою технічної підтримки та інцидентами, який належним чином виконується. Вказаний процес передбачає введення в дію служби технічної підтримки, яка здійснює реєстрацію запитів, ескалацію інцидентів, аналіз тенденцій та першопричин, а також врегулювання інцидентів. Серед вигод для бізнесу – підвищення продуктивності завдяки швидкому вирішенню проблем користувачів. Крім цього, бізнес-підрозділи мають можливість аналізувати першопричини інцидентів (наприклад, низький рівень навчання користувачів), завдяки наявності ефективної звітності.





Контроль IT процесу

управляти службою технічної підтримки та інцидентами

який задовольняє бізнес-вимоги до IT, а саме:

забезпечення ефективного використання IT систем за рахунок врегулювання та аналізу запитів, запитань кінцевих користувачів, а також інцидентів, що трапляються в системах

зосереджений на

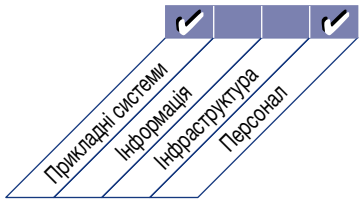
організації професійної служби технічної підтримки з швидким реагуванням, процедурами ескалації, вирішенням інцидентів, та проведенням аналізу тенденцій

реалізується шляхом

- організації та експлуатації служби технічної підтримки
- моніторингу та звітності щодо наявних тенденцій
- визначення чітких критеріїв та процедур ескалації

та вимірюється

- ступенем задоволення користувачів службою оперативної підтримки
- відсотком інцидентів, вирішених в межах узгодженого/прийнятного проміжку часу
- відсотком дзвінків, залишений без відповіді



Цілі контролю

DS8 Управляти службою підтримки та інцидентами

DS8.1 Служба технічної підтримки
Організувати службу технічної підтримки, яка є засобом взаємодії користувача зі службою IT, з метою реєстрації, інформування, диспетчерського управління та аналізу всіх дзвінків, повідомлень про інциденти, заявки на сервісне обслуговування та запитів щодо надання інформації. Необхідно впровадити процедури моніторингу та ескалації, виходячи з узгоджених рівнів надання послуг, визначених відповідними угодами SLA, які дозволяють здійснити класифікацію та встановити пріоритети будь-яких повідомлених проблем, та віднести їх до категорій інцидентів, заявок на сервісне обслуговування або запитів щодо надання інформації. Оцінювати ступінь задоволення кінцевих користувачів якістю роботи служби технічної підтримки та рівнем надання IT послуг. . .

DS8.2 Реєстрація запитів замовників
Встановити функцію та систему, які дозволяють здійснювати реєстрацію та відстеження дзвінків, інцидентів, заявок на сервісне обслуговування та запитів щодо надання інформації. Вказана функція повинна працювати у тісному зв'язку з такими процесами як управління інцидентами, управління проблемами, управління змінами, управління потужностями та управління доступністю. Необхідно здійснювати класифікацію інцидентів згідно з пріоритетами напрямків діяльності та обслуговування, а також, у разі необхідності, направляти їх на розгляд відповідної групи з управління інцидентами. Необхідно постійно інформувати замовників стосовно статусу їх запитів. . .

DS8.3 Ескалація інцидентів (Передача вирішення проблем на більш високий рівень підтримки)
Впровадити процедури, що стосуються дій служби технічної підтримки на той випадок, коли інцидент не може бути врегульований негайно, які передбачають відповідну ескалацію згідно з обмеженнями, визначеними в угоді про рівень надання послуг, а також, якщо це доцільно, забезпечують тимчасові рішення та обхідні шляхи. Забезпечити те, що у випадку виникнення інцидентів, пов'язаних з користувачами, власність інциденту та моніторинг під час вирішення залишаються в службі технічної підтримки, незалежно від того, яка група спеціалістів IT служби здійснює заходи з його вирішення.

DS8.4 Вирішення («закриття») інциденту
Впровадити процедури, які передбачають здійснення регулярного моніторингу процесу вирішення запитів користувачів. Після вирішення інциденту впевнитись, що служба технічної підтримки реєструє всі етапи процесу вирішення, та підтвердити, що вжиті заходи були узгоджені з користувачем. Також реєструвати та повідомляти про невирішені інциденти (відомі помилки та обхідні шляхи) для забезпечення інформацію процесу управління проблемами.

DS8.5 Звітність та аналіз тенденцій
Формувати звіти про діяльність служби технічної підтримки щоб дати можливість керівництву оцінити результативність роботи та швидкість реагування служби та визначити тенденції і повторювані проблеми для постійного вдосконалення послуг.

Керівні принципи управління

DS8 Управляти службою підтримки та інцидентами

Від	Вхідні дані
AI4	Інструкції з питань експлуатації, підтримки, технічного обслуговування та адміністрування
AI6	Авторизація змін
AI7	Випущені елементи конфігурації
DS1	Угоди SLA та OLA
DS4	Пороги інциденту/аварії
DS5	Визначення інциденту в системі безпеки
DS9	Детальні дані щодо конфігурації IT/IT ресурсів
DS10	Відомі проблеми,помилки та обхідні способи
DS13	Заявки про відкриття інцидентів

Вихідні дані	Для						
Заявки на обслуговування/запит на внесення змін (RFC)	AI6						
Звіти про інциденти	DS10						
Звіти щодо результативності процесу	ME1						
Звіти щодо задоволення користувачів	DS7	ME1					

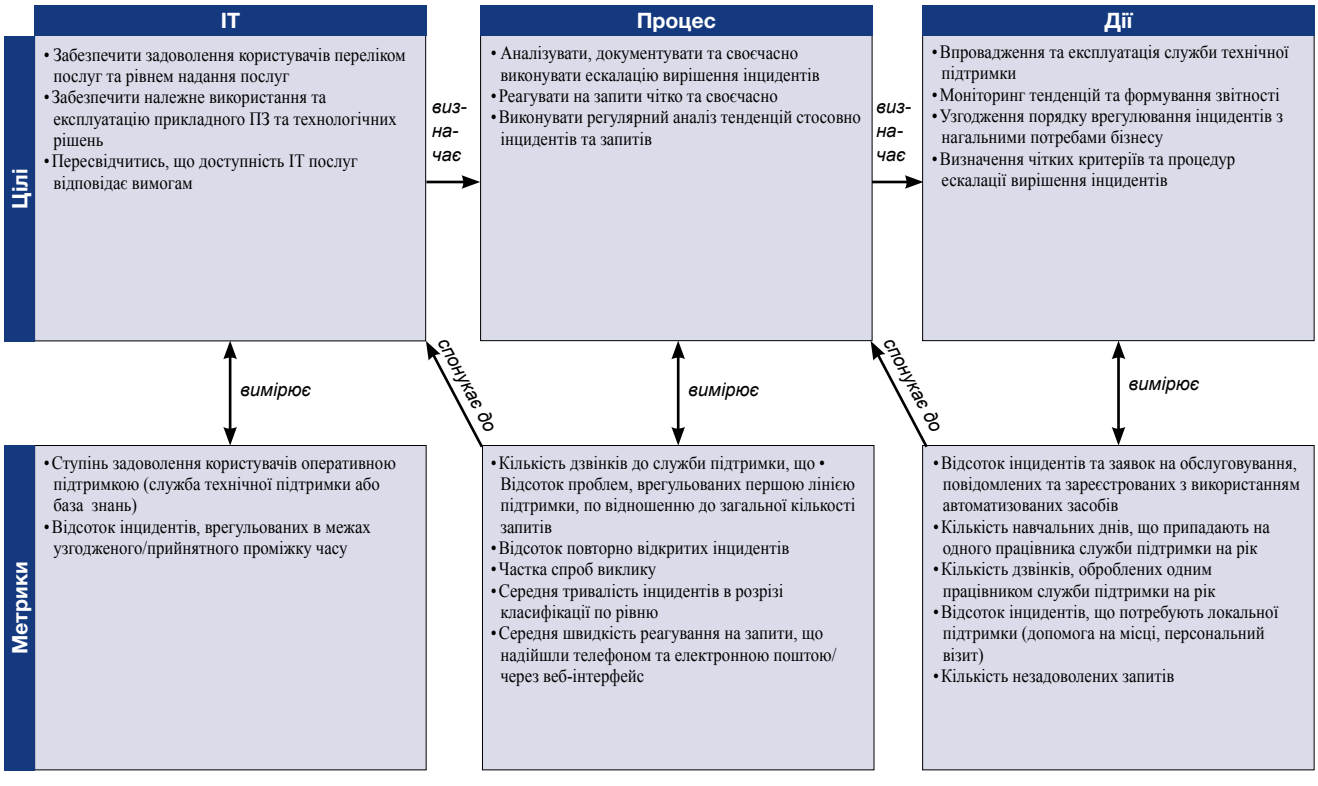
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки	Служба технічної підтримки / керівник з питань управління інцидентами
Створення процедури класифікації (за серйозністю та можливими наслідками) та передачі вирішення проблем на більш високий рівень ієрархії (функціональну та ієрархічну)				C	C	C	C	C	C		C	A/R
Виявлення та реєстрація інцидентів/заяв на обслуговування/запити щодо надання інформації												A/R
Здійснення класифікації, розслідування та діагностики запитів				I		C	C	C			I	A/R
Врегулювання, коригування та закриття інцидентів					I	R	R	R			C	A/R
Інформування користувачів (наприклад, надання нової інформації щодо статусу запиту)				I	I							A/R
Оформлення звітності для керівництва	I			I	I	I			I		I	A/R

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS2 Управляти службою підтримки та інцидентами

Рівні зрілості управління процесом *«Управляти службою підтримки та інцидентами»*, які задовольняють бізнес-вимоги до IT *«забезпечити ефективне використання IT систем за рахунок врегулювання та аналізу запитів, запитань кінцевих користувачів, а також інцидентів, що трапляються в системах»*, є такими:

0 Не існуючий, якщо
Не існує служби підтримки, що відповідає на запити користувачів та вирішує їх проблеми. Повністю відсутній процес управління інцидентами. Організація не усвідомлює, що цією проблемою необхідно займатись.. . . . . .

1 Початковий, якщо
Керівництво усвідомлює, що необхідно впровадити процес, підтриманий відповідними засобами та персоналом, з метою реагування на запити користувачів та управління вирішенням інцидентів. Однак, відсутній стандартизований процес, та має місце лише реактивна підтримка. Керівництво не здійснює моніторингу запитів користувачів, інцидентів або тенденцій. Немає процесу передачі вирішення проблем на більш високий рівень ієрархії, який би забезпечив гарантоване врегулювання проблем.

2 Повторюваний але інтуїтивний, якщо
В організації усвідомлюють потребу в організації служби технічної підтримки та впровадженні процесу управління інцидентами. Допомога надається на неформальній основі через мережу окремих відомих спеціалістів. Ці особи мають у розпорядженні деякі загальні інструменти, що дозволяють вирішувати інциденти. Формальне навчання та комунікації, які стосуються стандартних процедур, відсутні, це залишено на розсуд окремих осіб.

3 Визначений, якщо
Потребу в організації служби технічної підтримки та впровадженні процесу управління інцидентами усвідомлено та прийнято. Процедури стандартизовані та оформлені документально, проводиться неформальне навчання. Однак, працівники на свій розсуд приймають рішення щодо проходження навчання та дотримання стандартів. Відповіді на популярні запитання (FAQ) та інструкції для користувача розроблені, але працівники повинні відшукувати їх та можуть їх не дотримуватись. Запити та інциденти відстежуються в ручному режимі, здійснюється індивідуальний моніторинг, але не існує системи формальної звітності. Своєчасність реагування на запити та інциденти не оцінюється, інциденти можуть залишитись неврегульованими. Користувачі отримали чітку інформацію стосовно того, де, коли та в який спосіб повідомляти про інциденти та проблеми.

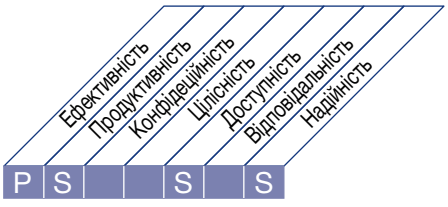
4 Керований та вимірюваний, якщо
Існує повне розуміння вигод від впровадження процесу управління інцидентами на всіх рівнях організації, службу технічної підтримки впроваджено у відповідних підрозділах організації. Засоби та методи автоматизовані, використовується централізована база знань. Персонал служби підтримки працює в тісні взаємодії з персоналом підрозділу управління проблемами. Обов'язки чітко визначені, виконується моніторинг ефективності роботи. Впроваджено та доведено до відома всіх зацікавлених сторін процедури комунікацій, ескалації та вирішення проблем. Персонал служби технічної підтримки проходить навчання, процеси вдосконалюються шляхом використання спеціалізованого програмного забезпечення. Керівництво розробляє метрики для оцінки результатів роботи служби технічної підтримки.

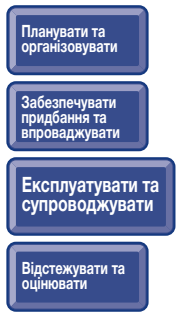
5 Оптимізований, якщо
Процес управління інцидентами та служба технічної підтримки впроваджені та добре організовані, орієнтовані на високоякісне обслуговування користувачів завдяки глибоким знанням персоналу, орієнтації на інтереси користувача та користь. Метрики систематично вимірюються та доводяться до відома відповідних осіб. Повноцінні посібники з відповідями на популярні запитання (FAQ) є невід'ємною частиною бази знань. Впроваджено в дію інструменти, які дозволяють користувачеві здійснювати самодіагностику проблем та вирішувати інциденти. Рекомендації є змістовними, інциденти вирішуються швидко в межах структурованого процесу ескалації. Керівництво використовує інтегровані засоби для отримання статистичних даних щодо результативності процесу управління інцидентами та роботи служби технічної підтримки. Процеси доведені до рівня найкращих галузевих практик в результаті аналізу показників ефективності, постійного вдосконалення та порівняльного аналізу інших організацій.

Опис процесу

DS9 Управляти конфігураціями

Щоб забезпечити цілісність конфігурацій апаратного та програмного забезпечення, необхідно впровадити тат підтримувати в робочому стані точний та повний репозиторій конфігурації. Цей процес передбачає накопичення інформації щодо початкової конфігурації, визначення базових прикладів, перевірку та аудит інформації щодо конфігурації та оновлення репозиторію конфігурацій в разі необхідності. Ефективне управління конфігураціями забезпечує більш високу доступність систем, зводить до мінімуму проблеми виробництва та дозволяє вирішувати проблеми більш оперативно.





Контроль IT процесу

Управляти конфігураціями

який задовольняє бізнес-вимоги до IT, а саме:

оптимізація IT інфраструктури, ресурсів та здатності IT, а також ведення обліку IT ресурсів

зосереджений на

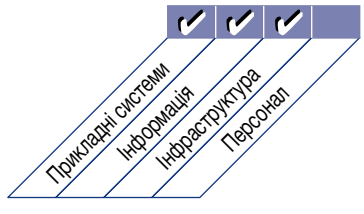
впровадженні та підтримці точного та повного репозиторію конфігурації ресурсів та базових прикладів конфігурації ресурсів та порівнянні їх з поточною конфігурацією ресурсів

реалізується шляхом

- впровадження центрального репозиторію всіх елементів конфігурації
- визначення елементів конфігурації та підтримки їх актуальності
- аналізу цілісності даних щодо конфігурації

та вимірюється

- кількістю проблем з дотриманням бізнес-вимог, викликаних неналежною конфігурацією ресурсів
- кількістю розбіжностей, виявлених між даними щодо конфігурації, які зберігаються в репозиторії, та даними щодо поточної конфігурації ресурсів
- відсотком ліцензій, придбаних та не врахованих в репозиторії



Цілі контролю

DS9 Управляти конфігураціями

DS9.1 Репозиторій даних щодо конфігурацій та базові приклади
Впровадити допоміжні засоби та центральний репозиторій для зберігання всієї належної інформації щодо елементів конфігурації. Контролювати та реєструвати всі ресурси та зміни до ресурсів. Зберігати базовий приклад для елементів конфігурації кожної системи та послуги, який слугуватиме контрольною точкою, до якої необхідно повертатись після внесення змін.

DS9.2 Визначення елементів конфігурацій та підтримка їх актуальності
Впровадити процедури для підтримки управління та реєстрації всіх змін, внесених до репозиторію конфігурації. Інтегрувати ці процедури з процедурами управління змінами, управління інцидентами та управління проблемами. . .

DS9.3 Аналіз цілісності конфігурацій
Здійснювати періодичний аналіз даних конфігурацій з метою перевірки та підтвердження цілісності поточної та історичних конфігурацій. Періодично перевіряти встановлене програмне забезпечення згідно з політикою використання програмного забезпечення з метою виявлення особистого або неліцензійного програмного забезпечення, або всіх інших версій програмного забезпечення, що виходять за межі діючих ліцензійних угод. Надавати звіти, вживати відповідних заходів та усувати помилки та розбіжності.

Керівні принципи управління

DS9 Управляти конфігураціями

Від	Вхідні дані
AI4	Інструкції з питань експлуатації, підтримки, технічного обслуговування та адміністрування
AI7	Фінальні елементи конфігурацій
DS4	Критичність елементів IT конфігурацій

Вихідні дані	Для						
Детальні дані щодо IT конфігурацій/ресурсів	DS8	DS10	DS13				
Запит на внесення змін (RFC, де та як застосовувати виправлення)	AI6						
Звіти щодо результативності процесу	ME1						

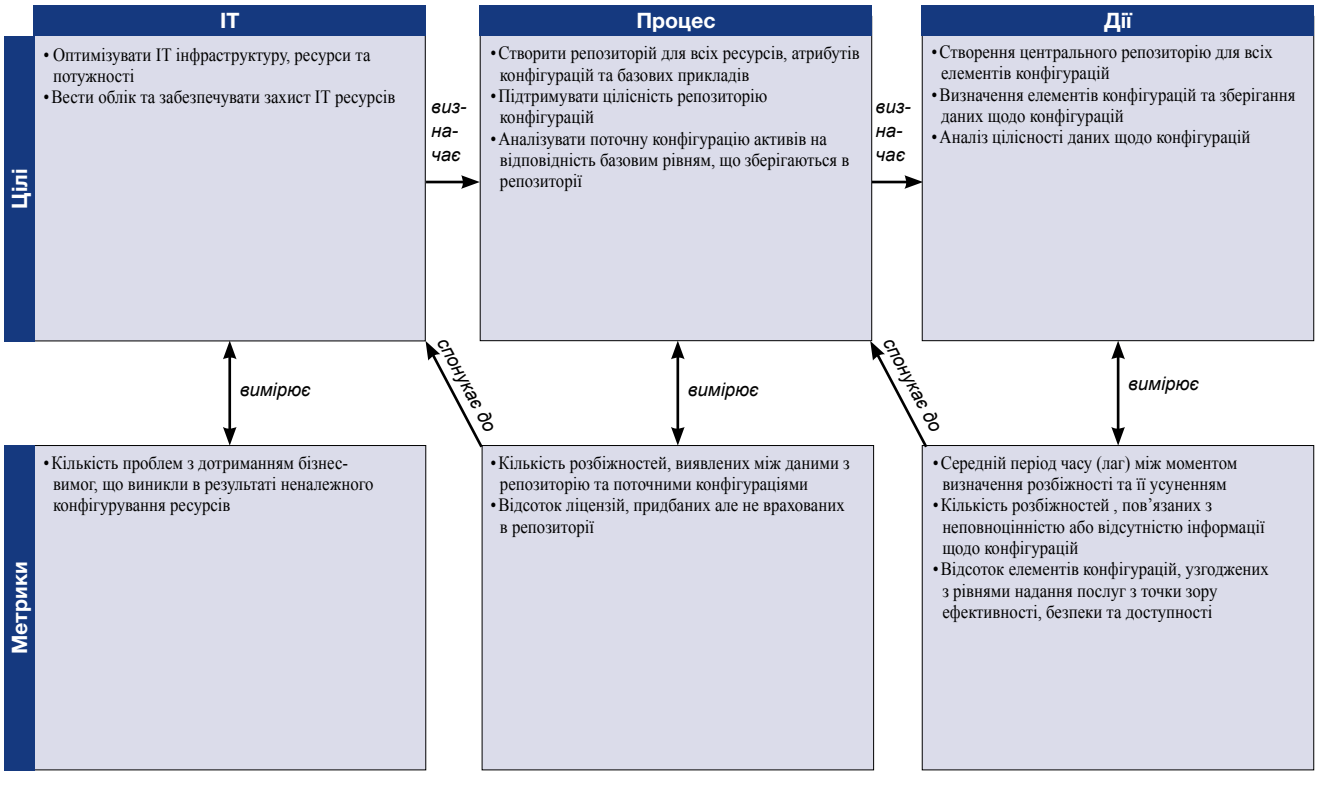
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки	Менеджер з управління конфігураціями
Розробка процедур планування управління конфігураціями					C	A	C	I	C		C	A/R
Накопичення інформації щодо початкових конфігурацій та встановлення базових прикладів						C	C	C			I	A/R
Здійснення перевірки та аудиту інформації стосовно конфігурацій (в тому числі виявлення несанкціонованого програмного забезпечення)		I				A			I		I	A/R
Оновлення репозиторію даних щодо конфігурацій						R	R	R			I	A/R

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS2 Управляти конфігураціями

Рівні зрілості управління процесом *«Управляти конфігураціями»*, які задовольняють бізнес-вимоги до IT *«оптимізувати IT інфраструктуру, ресурси та здатності IT а також вести облік IT ресурсів»*, є такими:

0 Не існуючий, якщо
Керівництво не усвідомлює вигод від впровадження процесу, який би передбачав можливість отримання інформації щодо IT інфраструктури та управління нею, це стосується конфігурацій як апаратного, так і програмного забезпечення.. . . . . .

1 Початковий, якщо
Усвідомлено потребу в управлінні конфігураціями. Основні завдання з управління конфігураціями, а саме, ведення обліку апаратного та програмного забезпечення, виконуються в окремих випадках. Стандартні практики не введені.

2 Повторюваний але інтуїтивний, якщо
Керівництво усвідомлює потребу в управлінні IT конфігураціями та розуміє вигоди від зберігання точної та повної інформації щодо конфігурацій, але є неявне покладання на знання та досвід технічного персоналу. До певної міри застосовуються засоби управління конфігураціями, але для різних платформ вони різні. Крім того, немає визначених стандартних робочих практик. Обсяг даних щодо конфігурацій обмежений та не використовується такими взаємопов'язаними процесами, як управління змінами та управління проблемами.

3 Визначений, якщо
Процедури та робочі практики документально оформлені, стандартизовані та доведені до відома всіх зацікавлених сторін, але навчання та застосування вказаних стандартів здійснюється на розсуд окремих осіб. Крім того одній ті самі засоби управління конфігураціями використовуються для різних платформ. Дуже мала імовірність того, що будуть виявлені відхилення від процедур, а фізичні перевірки проводяться непослідовно. До деякої міри використовуються автоматизовані засоби, які дозволяють відстежувати зміни в обладнанні та програмному забезпеченні. Дані щодо конфігурацій використовуються взаємопов'язаними процесами.

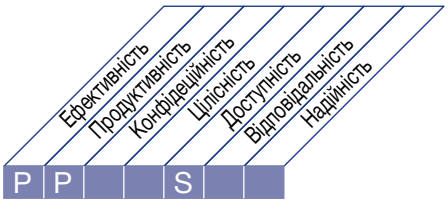
4 Керований та вимірюваний, якщо
Потребу в управлінні конфігурацією усвідомлено на всіх рівнях організації, продовжується розгортання найкращих практик. Процедури та стандарти доведені до відома працівників, є предметом навчання, відхилення від процедур відстежуються, контролюються та фіксуються в звітах. З метою забезпечення дотримання стандартів та підвищення стабільності застосовуються автоматизовані засоби , наприклад, технологія «проштовхування» інформації. Системи управління конфігураціями охоплюють більшість IT ресурсів та дозволяють здійснювати управління версіями та контроль за їх розповсюдженням в належний спосіб. Послідовно здійснюються аналіз нестандартних ситуацій та фізичні перевірки, ретельно вивчають першопричини виникнення таких ситуацій.

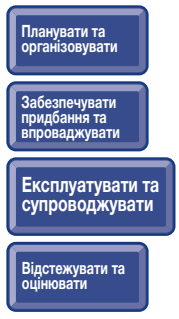
5 Оптимізований, якщо
Здійснюється управління всіма IT ресурсами в центральній системі управління конфігураціями, яка містить всю необхідну інформацію стосовно елементів конфігурацій, їх взаємозв'язків та подій. Дані щодо конфігурацій узгоджені з каталогами постачальників. Має місце повна інтеграція взаємопов'язаних процесів, вони використовують та оновлюють дані щодо конфігурації в автоматизований спосіб. У звітах аудиту базового рівня міститься основна інформація щодо апаратного та програмного забезпечення, а саме та, що стосується ремонту, обслуговування, гарантійних умов, модифікації та технічної оцінки кожного окремого блоку. Забезпечується виконання правил обмеження інсталяції несанкціонованого програмного забезпечення. Керівництво складає прогнози щодо проведення ремонту та здійснення модифікацій на підставі звітів щодо аналізу конфігурацій, надаючи графік встановлення оновлення та оцінку здатності до оновлення технології. Завдяки відстеженню ресурсів та моніторингу окремих IT ресурсів забезпечується їх захист та попереджаються крадіжки, неправильне та зловмисне використання.

Опис процесу

DS10 Управляти проблемами

Ефективне управління проблемами вимагає ідентифікації та класифікації проблем, аналізу першопричин та вирішення проблем. Процес управління проблемами також передбачає формулювання рекомендацій щодо покращення, ведення записів щодо проблем та аналізу статусу коригуючих заходів. Ефективний процес управління проблемами забезпечує максимальну доступність системи, підвищує рівні надання послуг, сприяє зниженню втрат та підвищенню ступеня зручності у використанні системи та задоволення користувачів.





Контроль IT процесу

Управляти проблемами

який задовольняє бізнес-вимоги до IT, а саме:

забезпечення задоволення кінцевих користувачів переліком послуг та рівнем надання послуг, а також зменшення кількості недоліків та обсяг повторних робіт при впровадженні рішень та наданні послуг

зосереджений на

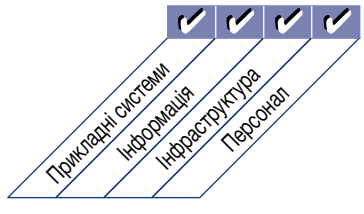
реєстрації, відстеженні та врегулюванні експлуатаційних проблем; розслідуванні першопричин всіх суттєвих проблем та визначенні рішень, призначених для усунення виявлених експлуатаційних недоліків

реалізується шляхом

- здійснення аналізу першопричин повідомлених проблем
- аналізу тенденцій
- прийняття власності на проблеми та вдосконалення механізмів вирішення проблем

та вимірюється

- кількістю повторних проблем, що мають наслідки для бізнесу
- відсотком проблем, вирішених в межах запланованого проміжку часу
- періодичністю надання звітів або нової інформації щодо проблеми, яка продовжує існувати, виходячи з серйозності проблеми



Цілі контролю

DS10 Управляти проблемами

DS10.1 Ідентифікація та класифікація проблем
Впровадити процеси надання звітності та здійснення класифікації проблем, які були виявлені в ході управління інцидентами. Етапи класифікації проблем аналогічні етапам класифікації інцидентів; вони передбачають визначення категорії проблеми, її наслідків, терміновості врегулювання та пріоритету. Розподілити проблеми за категоріями, як належить, на відповідні групи або домени (наприклад, апаратне забезпечення, програмне забезпечення, допоміжне програмне забезпечення). Вказані групи можуть відповідати організаційним обов'язкам користувачів та клієнтів, та провинні слугувати базисом розподілу проблем між спеціалістами служби підтримки. . .

DS10.2 Відстеження та врегулювання проблеми
Впевнитись, що система управління проблемами має належні засоби ведення журналу аудиту, які дозволяють здійснювати стеження, аналіз та визначення першопричин всіх повідомлених проблем, з врахуванням:
- всіх відповідних елементів конфігурації
- суттєвих проблем та інцидентів
- відомих та підозрюваних помилок
- результатів відстеження тенденцій розвитку проблеми.

Визначати та ініціювати створення раціональних рішень, що дозволяють усунути першопричини проблеми та подати заявку на внесення змін за допомогою встановленого процесу управління змінами. За допомогою процесу врегулювання проблем, керівництво підрозділу з питань управління проблемами повинно отримувати регулярні звіти від керівництва підрозділу з управління змінами щодо успіхів у врегулювання проблем та усуненні помилок. Керівництво підрозділу з питань управління проблемами повинно контролювати наслідки проблем та відомих помилок для послуг користувачам. В тому разі, коли такі наслідки стають суттєвими, керівництво підрозділу з питань управління проблемами повинно виконати ескалацію вирішення проблеми, можливо, звернувшись до відповідного комітету в організації, щоб підвищити ступінь пріоритетності запиту на зміну або з метою впровадження відповідних термінових змін в належний спосіб. Контролювати хід вирішення проблеми, орієнтуючись на вимоги, визначені угодами про рівень надання послуг.

DS10.3 Закриття проблеми
Впровадити процедуру закриття реєстраційних записів щодо проблеми або після підтвердження успішного усунення відомої помилки, або після узгодження з бізнес-підрозділами альтернативного способу вирішення проблеми.

DS10.4 Інтеграція процесів управління конфігурацією, інцидентами та проблемами
Інтегрувати відповідні процеси управління конфігурацією, інцидентами та проблемами з метою забезпечення ефективного управління проблемами та здійснення вдосконалень.

Керівні принципи управління

DS10 Управляти проблемами

Від	Вхідні дані
AI6	Авторизація змін
DS8	Повідомлення про інциденти
DS9	Дані щодо IT конфігурації/ресурсів
DS13	Реєстраційні дані щодо помилок

Вихідні дані	Для						
Заявки на зміни (де та як застосовувати виправлення)	AI6						
Реєстраційні дані щодо проблем	AI6						
Звіти щодо продуктивності процесу	ME1						
Відомі проблеми, відомі помилки та обхідні шляхи	DS8						

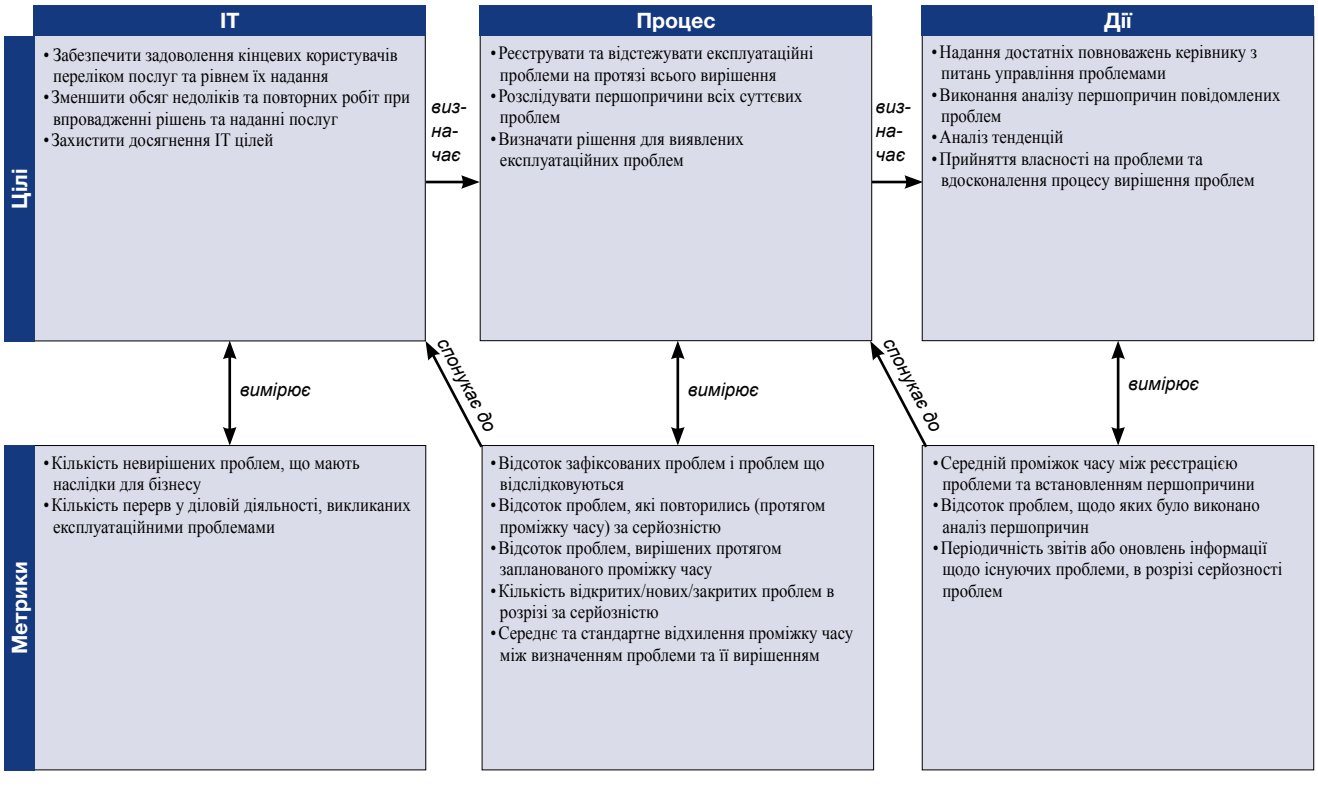
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки	Менеджер з управління проблемами
Виявлення та класифікація проблем			I	I	C	A	C	C			I	R
Виконання аналізу першопричин						C		C				A/R
Вирішення проблеми					C	A	R	R		R	C	C
Аналіз статусу проблем			I	I	C	A/R	C	C		C	C	R
Надання рекомендацій щодо виправлень та створення відповідних запитів на зміни					I	A	I	I		I		R
Ведення записів щодо проблем					I	I		I			I	A/R

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS10 Управляти проблемами

Рівні зрілості управління процесом *«Управляти проблемами»*, які задовольняють бізнес-вимоги до IT *«забезпечити задоволення кінцевих користувачів переліком послуг та рівнем надання послуг, а також зменшити кількість недоліків та обсяг повторних робіт при впровадженні рішень та наданні послуг»*, є такими:

0 Не існуючий, якщо
Не існує усвідомлення потреби в управлінні проблемами, так само як не існує процедури диференціації проблем та інцидентів. Як наслідок не робляться спроби встановлення першопричин проблем та інцидентів.

1 Початковий, якщо
Персонал усвідомлює потребу в управлінні проблемами та усуненні їх причин. Ключовий досвідчений персонал надає певну допомогу у вирішенні проблем в залежності від сфери своєї компетенції, але відповідальність за управління проблемами не визначена. Немає обміну інформацією, що призводить до виникнення додаткових проблем та втрати продуктивного часу на пошук відповідей на запитання.

2 Повторюваний але інтуїтивний, якщо
Має місце загальне усвідомлення потреби та переваг від управління IT проблемами як в бізнес-підрозділах, так і в службі надання інформаційних послуг. Процес врегулювання проблем розвинутий до того моменту, коли декілька ключових спеціалістів несуть відповідальність за виявлення та вирішення проблем. Обмін інформацією між працівниками має неформальний та реактивний характер. Рівень надання послуг користувачам є нестабільним, його важко забезпечити внаслідок того, що керівник з питань врегулювання проблем отримує неповну та фрагментарну інформацію.

3 Визначений, якщо
Потребу у впровадженні ефективно діючої інтегрованої системи управління проблемами усвідомлено та підтримано керівництвом, сформовані бюджети на комплектацію персоналу та проведення відповідного навчання. Процеси вирішення проблем та ескалації стандартизовані. Обов'язки з реєстрації та відстеження проблем в ході їх вирішення розподілені всередині групи реагування, яка діє децентралізовано, використовуючи доступні засоби. Імовірно, що відхилення від встановлених норм та стандартів можуть і не бути виявлені. Обмін інформацією між спеціалістами здійснюється у проактивний і формальний спосіб. Перегляд інцидентів керівництвом та аналіз виявлення та вирішення проблем, має обмежений та неформальний характер.

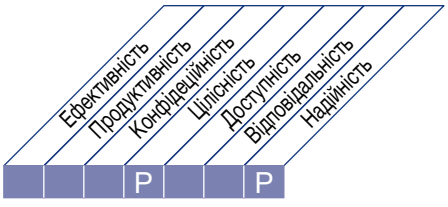
4 Керований та вимірюваний, якщо
Процес управління проблемами осмислено на всіх рівнях організації. Обов'язки та власність чітко визначені та встановлені. Методи та процедури оформлені документально, доведені до відома та оцінені з точку зору ефективності. Більшість проблем виявлені, зареєстровані та повідомлені, розпочато їх вирішення. Культивуються глибокі знання та досвід, підтримуються та розвиваються до більш високого рівня, оскільки IT служба розглядається як ресурс та основний вкладник у справу досягнення IT цілей та підвищення рівня надання IT послуг. Процес управління проблемами добре інтегрований з взаємопов'язаними процесами, такими як процеси управління інцидентами, змінами, доступністю та конфігурацією,та допомагає клієнтам в управлінні даними, засобами та операціями. Узгоджені цілі та метрики для процесу управління проблемами.

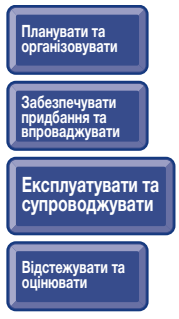
5 Оптимізований, якщо
Процес управління проблемами розвинутий до стадії, коли він працює проактивно, сприяючи досягненню IT цілей. Здійснюється передбачення та попередження проблем. Підтримується накопичення інформації стосовно минулих та майбутніх проблем шляхом регулярних контактів з постачальниками та експертами. Реєстрація, звітність та аналіз проблем, а також їх вирішення здійснюються в автоматизований спосіб, який повністю інтегровано з процесом управління конфігураціями. Виконується послідовне вимірювання цілей. Більшість систем обладнані засобами автоматичного детектування та попередження, які постійно контролюються та аналізуються. Процес управління проблемами аналізують з метою постійного вдосконалення на основі аналізу метрик, результати повідомляються зацікавленим сторонам.

Опис процесу

DS11 Управляти даними

Ефективне управління даними потребує визначення вимог до даних. Процес управління даними також передбачає впровадження ефективних процедур управління бібліотекою носіїв, резервування та відновлення даних, а також утилізації носіїв інформації в належний спосіб. Ефективне управління даними дозволяє забезпечити відповідний рівень якості, своєчасність надання та доступність інформації для бізнесу.





Контроль IT процесу

Управляти даними

який задовольняє бізнес-вимоги до IT, а саме:

оптимізація процесу використання інформації та забезпечення доступності інформації при потребі

зосереджений на

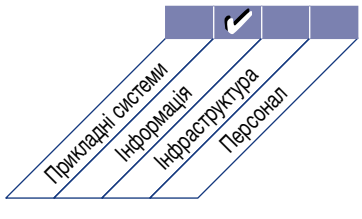
підтримці повноти, точності, доступності та забезпеченні захисту даних

реалізується шляхом

- резервування даних та перевірки можливості їх відновлення
- управління сховищами даних, розташованими в приміщенні організації та поза його межами
- надійної та безпечної утилізації даних та обладнання

та вимірюється

- відсотком користувачів, задоволених рівнем доступності даних
- відсотком успішно здійснених спроб відновлення даних
- кількістю інцидентів, у яких конфіденційні дані були відновлені після утилізації носія інформації



Цілі контролю

DS11 Управляти даними

DS11.1 Бізнес-вимоги, що стосуються управління даними
Впевнитись в тому, що всі дані, передбачені для обробки, отримані та оброблені повністю, без помилок та своєчасно, а всі кінцеві результати надані відповідно до бізнес-вимог. Надавати відповідну допомогу у разі виникнення потреби повторного запуску та повторної обробки. .

DS11.2 Механізми зберігання та запам'ятовування інформації
Визначити та впровадити процедури ефективного та продуктивного запису даних, їх збереження та архівації, які відповідають бізнес-цілям, політиці інформаційної безпеки, прийнятій в організації та вимогам регулятивних органів. . .
.

DS11.3 Система управління бібліотекою носіїв інформації
Визначити та впровадити процедури ведення обліку носіїв записаної та за архівованої інформації, щоб забезпечити їх доступність та придатність до використання, а також цілісність. . .

DS11.4 Утилізація носіїв інформації
Визначити та впровадити процедури, які забезпечують задоволення бізнес-вимог щодо захисту конфіденційної інформації та програмного забезпечення у випадку знищення або передачі даних та апаратного забезпечення. . .

DS11.5 Резервування та відновлення
Визначити та впровадити процедури, які забезпечують резервування та відновлення систем, прикладного програмного забезпечення, даних та документації згідно з бізнес-вимогами та планом забезпечення безперервності бізнесу. . .

DS11.6 Вимоги з безпеки при управлінні даними
Визначити та впровадити політики та процедури, які дозволяють визначати та накладати вимоги з безпеки до процедур отримання, обробки, запису та виводу даних з метою забезпечення відповідності бізнес-цілям, політиці інформаційної безпеки та регулятивним вимогам.

Керівні принципи управління

DS11 Управляти даними

Від	Вхідні дані
PO2	Словник даних, визначені класифікатори даних
AI4	Інструкції з питань експлуатації, підтримки, технічного обслуговування та адміністрування
DS1	Угоди OLA
DS4	План резервування та захисту даних
DS5	План та політики у сфері безпеки IT

Вихідні дані	Для						
Звіти щодо результативності процесу	ME1						
Інструкції для операторів з управління даними	DS13						

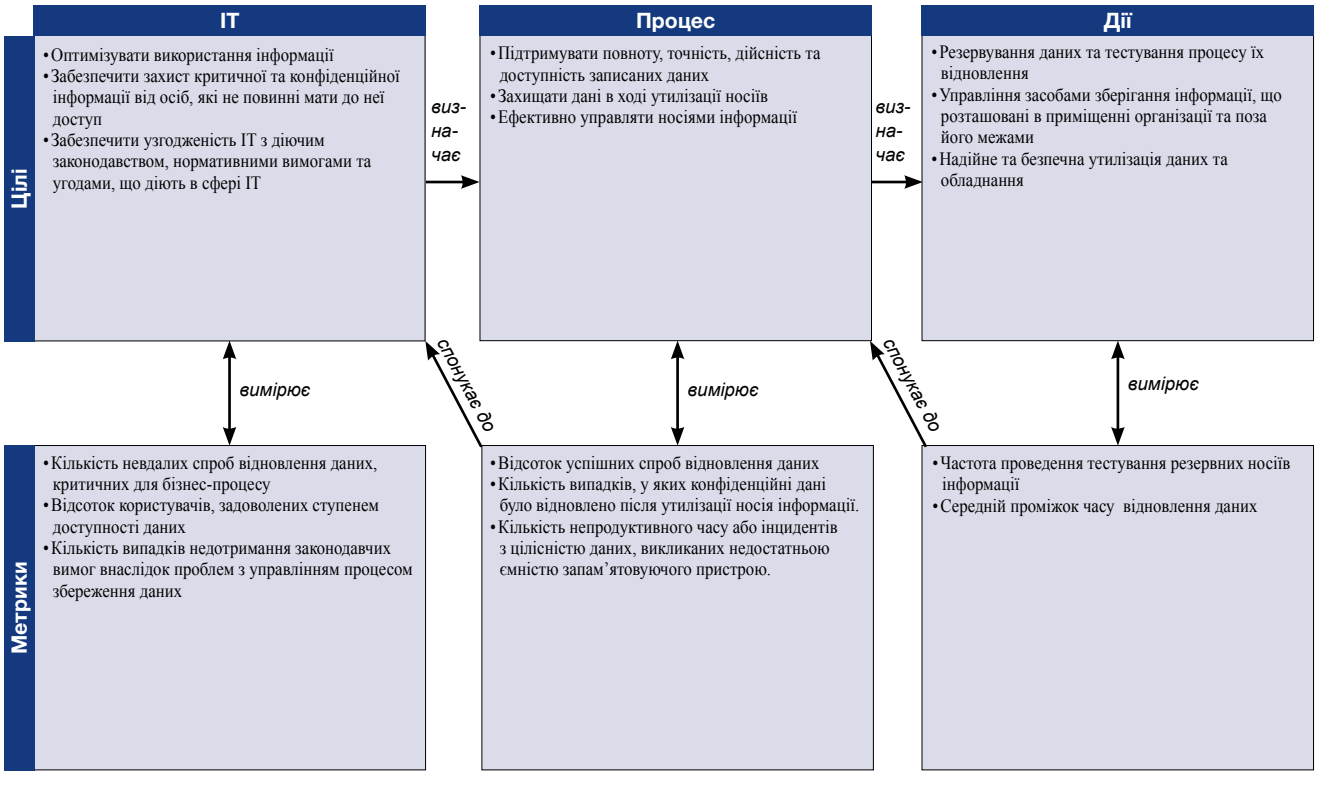
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог аудиту, ризиків та безпеки
Втілення вимог до запису та відновлення даних у відповідні процедури				A	I	C	R				C
Визначення, підтримка та впровадження процедур управління бібліотекою носіїв інформації				A		R	C	C	I		C
Визначення, підтримка та впровадження процедур безпечної утилізації носіїв інформації та обладнання.				A	C	R			I		C
Резервування даних згідно зі схемою				A		R					
Визначення, підтримка та впровадження процедури відновлення даних				A	C	R	C	C			I

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS11 Управляти даними

Рівні зрілості управління процесом *«Управляти даними»*, які задовольняють бізнес-вимоги до IT *«оптимізувати процес використання інформації та забезпечити доступність інформації при потребі»*, є такими:

0 Не існуючий, якщо
Дані не визнаються корпоративними ресурсами та активами. Не призначені власники даних, відсутня індивідуальна відповідальність за управління даними. Якість даних та їх безпека знаходяться на низькому рівні або відсутні зовсім.

1 Початковий, якщо
Організація усвідомлює потребу в ефективному управлінні даними. Визначення вимог до безпеки на випадок управління даними здійснюється к кожному конкретному випадку, але не введені жодні формальні процедури, що стосуються комунікацій. Не проводиться спеціалізоване навчання з питань управління даними. Немає чіткого розподілу обов'язків з управління даними. Введені процедури резервування/відновлення даних, а також схеми утилізації носіїв.

2 Повторюваний але інтуїтивний, якщо
Усвідомлення потреби в ефективному управління даними існує в масштабах всієї організації. Починає зароджуватись процес встановлення власності щодо даних на високому рівні. Вимоги до безпеки при управлінні даними документально оформляються ключовими особами. До деякої міри здійснюється моніторинг службою IT ключових заходів з управління даними (наприклад, процесів резервування, відновлення, утилізації). Обов'язки з управління даними неформально покладені на ключових працівників IT служби.

3 Визначений, якщо
Потребу в управлінні даними розуміють та сприймають як в службі IT, так і в масштабах всієї організації. Встановлено відповідальність за управління даними. Право власності на дані надане відповідальній особі, яка контролює їх цілісність та безпеку. Процедури управління даними формалізовані в межах IT служби, використовуються деякі засоби резервування/відновлення та утилізації обладнання. До деякої міри здійснюється моніторинг процесу управління даними. Визначені базові метрики результативності. Зароджується процес навчання працівників, що займаються управлінням даними.

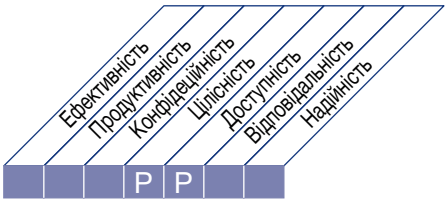
4 Керований та вимірюваний, якщо
Потребу в управлінні даними усвідомлено, в організації здійснюються необхідні заходи. Чітко визначені, розподілені та доведені до відома співробітників організації обов'язки щодо володіння та управління даними. Процедури формалізовані та широко відомі, здійснюється обмін знаннями. Починається застосування сучасних інструментів та засобів. Показники цілей та продуктивності узгоджені з клієнтами та контролюються із застосуванням чітко визначеного процесу. Проводиться формальне навчання працівників, що залучені до управління даними.

5 Оптимізований, якщо
Потребу в управлінні даними та в осмисленні всіх необхідних заходів розуміють та сприймають в масштабах всієї організації. Вивчаються майбутні потреби та вимоги з елементами прогнозування. Відповідальність за володіння та управління даними чітко визначена, широко відома всім працівникам організації та своєчасно переглядається. Процедури формалізовані та широко відомі, обмін знаннями є стандартною практикою. Управління даними здійснюється з максимальним ступенем автоматизації з використанням інтелектуальних засобів. Показники цілей та результативності узгоджені з користувачами та клієнтами, пов'язані з бізнес-цілями та постійно контролюються за допомогою чітко визначеного процесу. Здійснюється постійний пошук можливостей для вдосконалення. Впроваджено навчання для персоналу, залученого до управління даними.

Опис процесу

DS12 Управляти фізичним середовищем

Щоб забезпечити захист комп'ютерного обладнання та персоналу, необхідно мати добре спроектовані та під надійним управлінням засоби праці. Процес управління фізичним середовищем передбачає визначення фізичних вимог до місця розташування обладнання та персоналу, вибір відповідної матеріально-технічної бази та розробку ефективних процесів моніторингу оточуючого середовища та управління фізичним доступом. Ефективне управління фізичним середовищем дає змогу зменшити кількість перерв у веденні бізнесу внаслідок шкоди, нанесеної комп'ютерному обладнанню та персоналу.



Контроль IT процесу

Управляти фізичним середовищем

який задовольняє бізнес-вимоги до IT, а саме:

забезпечення захисту комп'ютерних ресурсів та бізнес інформації та зведення до мінімуму ризику порушення нормального ходу бізнесу

зосереджений на

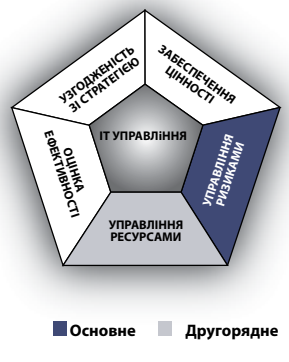
створенні та підтримці в належному стані відповідного фізичного середовища з метою захисту IT ресурсів від несанкціонованого доступу, пошкоджень або крадіжки

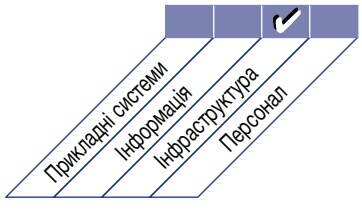
реалізується шляхом

- впровадження заходів фізичного захисту
- вибору засобів праці та їх управління

та вимірюється

- обсягом непродуктивних втрат часу, викликаних інцидентами у фізичному середовищі
- кількістю інцидентів, обумовлених порушенням системи фізичного захисту або недоліками в її функціонуванні
- періодичністю здійснення оцінки ризиків та заходів з контролю





Цілі контролю

DS12 Управляти фізичним середовищем

DS12.1 Вибір місця розташування та схема розміщення
Охарактеризувати та здійснити вибір місця розміщення IT обладнання відповідно до технологічної стратегії, яка пов'язана з бізнес-стратегією. Здійснюючи вибір місць та проектування схем розміщення обладнання, необхідно враховувати ризик, пов'язаний зі стихійними лихами та техногенними катастрофами, водночас з цим беручи до уваги відповідне діюче законодавство та нормативно-правові акти, наприклад, правила техніки безпеки та охорони праці. . .

DS12.2 Заходи фізичного захисту
Визначити та впровадити заходи фізичного захисту, що відповідають бізнес-умовам, з метою забезпечення захисту приміщення та фізичних ресурсів. Заходи фізичного захисту повинні бути здатними до ефективного попередження, виявлення та зменшення наслідків ризиків, пов'язаних з крадіжкою, впливом температури, пожежею, задимленням, дією води, вібраціями, терористичними діями, вандалізмом, відключеннями електроенергії, наявністю хімічних або вибухових речовин.

DS12.3 Фізичний доступ
Визначити та впровадити процедури надання, обмеження та анулювання доступу до приміщень, споруд та зон відповідно до потреб бізнесу, в тому числі у надзвичайних ситуаціях. Доступ до приміщень, споруд та зон необхідно обґрунтовувати, санкціонувати, реєструвати та контролювати. Вищесказане стосується всіх осіб, які заходять до приміщень, включаючи штатних працівників, тимчасовий персонал, клієнтів, постачальників, відвідувачів або будь-яких інших сторонніх осіб. . .

DS12.4 Захист від чинників зовнішнього середовища
Розробити тат впровадити заходи захисту від чинників оточуючого середовища. Встановити спеціальне обладнання та пристрої для здійснення моніторингу та контролю стану оточуючого середовища. . .

DS12.5 Управління фізичними засобами
Здійснювати управління фізичними засобами, в тому числі обладнанням електроживлення та засобами зв'язку згідно із законодавчими та нормативними актами, технічними вимогами та бізнес-вимогами, вимогами виробників а також інструкціями з охорони праці та техніки безпеки.

Керівні принципи управління

DS12 Управляти фізичним середовищем

Від	Вхідні дані
PO2	Призначені класифікатори даних
PO9	Оцінка ризиків
AI3	Вимоги до фізичного середовища

Вихідні дані	Для						
Звіти щодо результативності процесу	ME1						

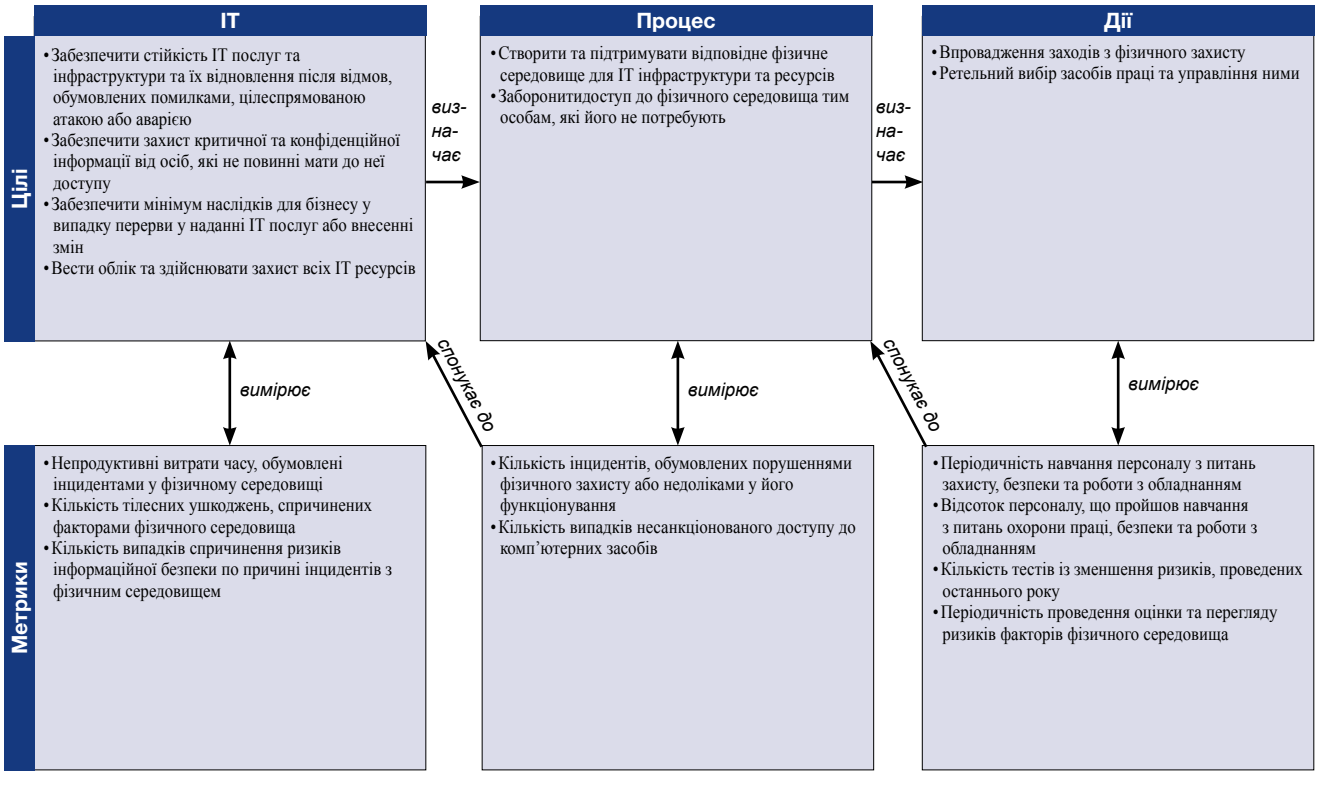
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Визначити необхідний ступінь фізичного захисту					C	A/R	C				C
Вибрати та здати в експлуатацію об'єкт (центр обробки даних, офіс, тощо)	I	C	C	C	C	A/R	C		C	C	C
Запровадити заходи з покращення фізичних умов					I	A/R	I	I			C
Здійснювати управління фізичним середовищем (підтримання, моніторинг та звітність)						A/R	C				
Визначити та запровадити процедури авторизації та супроводу фізичного доступу				C	I	A/R	I	I	I		C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS12 Управляти фізичним середовищем

Рівні зрілості управління процесом *«Управляти фізичним середовищем»*, які задовольняють бізнес-вимоги до IT *«забезпечити захист комп'ютерних ресурсів та бізнес інформації та звести до мінімуму ризик порушення нормального ходу бізнесу»*, є такими:

0 Не існуючий, якщо
Немає усвідомлення потреби у захисті засобів праці або інвестицій в обчислювальні ресурси. Параметри оточуючого середовища, в тому числі протипожежний захист, наявність пилу, стан електропостачання, наявність надлишкового тепла та вологості не відстежуються та не контролюються.

1 Початковий, якщо
Організація визнає бізнес-вимогу щодо створення відповідного фізичного середовища, яке забезпечує захист ресурсів та персоналу від штучних та природних загроз. Рівень управління спорудами та обладнанням залежить від кваліфікації та компетентності ключових осіб. Персонал може пересуватись приміщеннями без обмежень. Керівництво не здійснює моніторингу засобів контролю оточуючих умов в приміщеннях або пересування персоналу.

2 Повторюваний але інтуїтивний, якщо
Введені в дію засоби контролю оточуючих умов, експлуатаційний персонал здійснює моніторинг їх функціонування. Забезпечення фізичного захисту є неформальним процесом, керованим невеликою групою спеціалістів, які дуже переймаються проблемою захисту засобів праці. Процедури технічного обслуговування приміщень та обладнання недостатньо добре документовані, вони ґрунтуються на найкращому досвіді кількох окремих осіб. Цілі фізичного захисту не мають під собою жодних формальних стандартів, керівництво не забезпечує досягнення цілей безпеки.

3 Визначений, якщо
Потребу в управлінні обчислювальним середовищем в організації розуміють та сприймають. Засоби контролю оточуючих умов, превентивні заходи та фізична безпека є затвердженими позиціями бюджету, які контролюються керівництвом. Застосовуються процедури обмеження доступу, доступ до обчислювальних засобів дозволено лише затвердженому персоналу. Відвідувачів реєструють та супроводжують, в залежності від їх особи. Засоби праці залишаються в тіні, їх важко ідентифікувати. Цивільна влада стежить з дотриманням техніки безпеки та охорони праці. Ризики застраховано на умовах докладання мінімальних зусиль з оптимізації витрат на страхування.

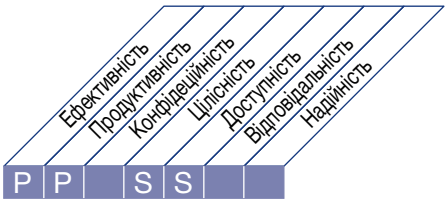
4 Керований та вимірюваний, якщо
Необхідність підтримання у робочому стані обчислювального середовища цілком та повністю розуміють в організації, як видно з відповідної організаційної структури та розподілу бюджетних коштів. Вимоги до оточуючих умов та фізичного захисту документально оформлені, а доступ суворо контролюється та відстежується. Відповідальність та право власності чітко визначені та доведені до відома персоналу організації. Персонал, що працює на об'єктах, проходить всебічне навчання з питань поводження в надзвичайних ситуаціях а також з практик охорони здоров'я. Введені стандартні механізми контролю, які дозволяють обмежувати доступ до приміщень та слідкувати за параметрами оточуючого середовища та системи безпеки. Керівництво контролює ефективність функціонування засобів контролю та дотримання встановлених стандартів. Керівництво визначило цілі та метрики для оцінювання процесу управління середовищем, в якому знаходиться обчислювальне обладнання. Здатність обчислювальних ресурсів до відновлення враховується у процесі управління організаційними ризиками. Для оптимізації страхового покриття та відповідних витрат використовується інтегрована інформація.

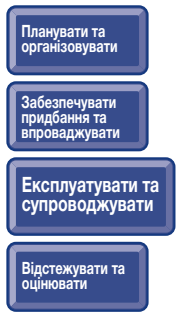
5 Оптимізований, якщо
Існує узгоджений довгостроковий план, що стосується споруд та обладнання, необхідних для підтримки обчислювального середовища організації. Визначено стандарти для всіх об'єктів, що охоплюють вибір місця розташування, побудову конструкції, організацію охорони, організацію безпеки персоналу, побудову механічних та електричних систем, а також захист від чинників оточуючого середовища (наприклад, вогню, блискавки, повені). Всі приміщення та засоби поставлені на облік та розподілені за категоріями відповідно до існуючого в організації процесу оцінки ризиків. Доступ суворо контролюється та дозволяється тим особам, як мають в ньому службову потребу, здійснюється постійний моніторинг доступу, всіх відвідувачів завжди супроводжують. Здійснюється моніторинг та контроль стану оточуючого середовища за допомогою спеціального обладнання, приміщення з обладнанням працюють без обслуговуючого персоналу. Цілі постійно вимірюються та оцінюються. Програми превентивного технічного обслуговування передбачають суворе дотримання плану, проводиться регулярне тестування чутливого обладнання. Стратегії та стандарти, що стосуються приміщень та засобів праці, узгоджені із цілями щодо забезпечення доступності IT послуг та інтегровані з процесами планування безперервності бізнесу та управління кризовими ситуаціями. Керівництво постійно здійснює критичний аналіз та оптимізацію приміщень та засобів з використанням цілей та метрик, намагаючись підвищення ефективність бізнесу.

Опис процесу

DS13 Управляти операційною діяльністю

Щоб забезпечити повноцінну та точну обробку даних, необхідно здійснювати ефективне управління процедурами обробки даних та належне технічне обслуговування апаратного забезпечення. Цей процес передбачає визначення робочих політик та процедур, що стосуються ефективного управління плановою обробкою даних, захисту конфіденційної вихідної інформації, моніторингу функціонування та продуктивності інфраструктури та здійснення планового технічного обслуговування. Ефективне управління операційною діяльністю сприяє збереженню цілісності даних та зменшує перерви у бізнесі і операційні витрати у сфері IT.





Контроль IT процесу

Управляти операційною діяльністю

який задовольняє бізнес-вимоги до IT, а саме:

підтримка цілісності даних та гарантія того, що IT інфраструктура зберігає стійкість та може відновлюватись після помилок та відмов

зосереджений на

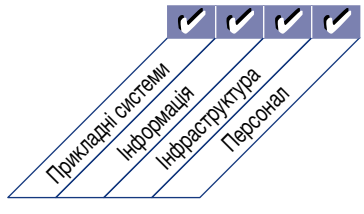
забезпеченні відповідного рівня експлуатаційного обслуговування відносно планової обробки даних, захисту конфіденційних вихідних даних, моніторингу та профілактичного технічного обслуговування інфраструктури

реалізується шляхом

- експлуатації IT середовища відповідно до узгоджених рівнів обслуговування та встановлених інструкцій
- підтримки IT інфраструктури

та вимірюється

- кількістю рівнів обслуговування, на які вплинули інциденти, що стосуються питань експлуатації
- кількістю годин незапланованих непродуктивних втрат часу, викликаних інцидентами, що стосуються експлуатації
- відсотком активів у вигляді апаратного забезпечення, внесених до планів здійснення профілактичного технічного обслуговування



Цілі контролю

DS13 Управляти операційною діяльністю

DS13.1 Процедури та інструкції, що стосуються операцій
Визначити, впровадити та підтримувати в робочому стані процедури, що стосуються IT операцій, слідкуючи за тим, щоб оперативний персонал добре опанував всі операції що на нього покладені. Процедури, що регламентують експлуатацію, повинні передбачати порядок передачі змін (формальна передача справ, звітів щодо поточного статусу, даних щодо експлуатаційних проблем, процедури ескалації та звітів щодо поточних обов'язків) з метою забезпечення узгоджених рівнів обслуговування та безперервності операцій. . ..

DS13.2 Планування робіт
Організувати планування робіт, процесів та завдань в максимально ефективній послідовності, яка забезпечить максимальну продуктивність та ефективне використання систем відповідно до бізнес-вимог.

DS13.3 Моніторинг IT інфраструктури
Визначити та запровадити процедури, які регламентують здійснення моніторингу IT інфраструктури та відповідних подій. Забезпечити реєстрацію достатньої хронологічної інформації в журналах обліку робіт з метою відновлення, аналізу та вивчення послідовності здійснення операцій в часі, а також інших дій, які здійснюються у зв'язку або на підтримку операцій.

DS13.4 Документи, які потребують захисту, та пристрої виводу інформації
Впровадити фізичні заходи захисту з врахуванням практик обліку та управління реєстрами критичних IT ресурсів, наприклад, спеціальних форм, інструментів переговорів, принтерів спеціального призначення або брелоків для забезпечення безпеки.

DS13.5 Профілактичне технічне обслуговування апаратного забезпечення
Визначити та запровадити процедури, які забезпечать своєчасне проведення технічного обслуговування інфраструктури з метою зниження частоти та зменшення наслідків відмов або зниження продуктивності.

Керівні принципи управління

DS13 Управляти операційною діяльністю

Від	Вхідні дані
AI4	Інструкції з питань експлуатації, підтримки, технічного обслуговування та адміністрування
AI7	Передача в експлуатацію та плани випуску та розповсюдження ПЗ
DS1	Угоди SLA та OLA
DS4	План резервування та захисту даних
DS9	Дані щодо IT конфігурації/ресурсів
DS11	Інструкції для операторів щодо управління даними

Вихідні дані	Для						
Форми обробки інцидентів	DS8						
Журнали реєстрації помилок	DS10						
Звіти щодо продуктивності систем	ME1						

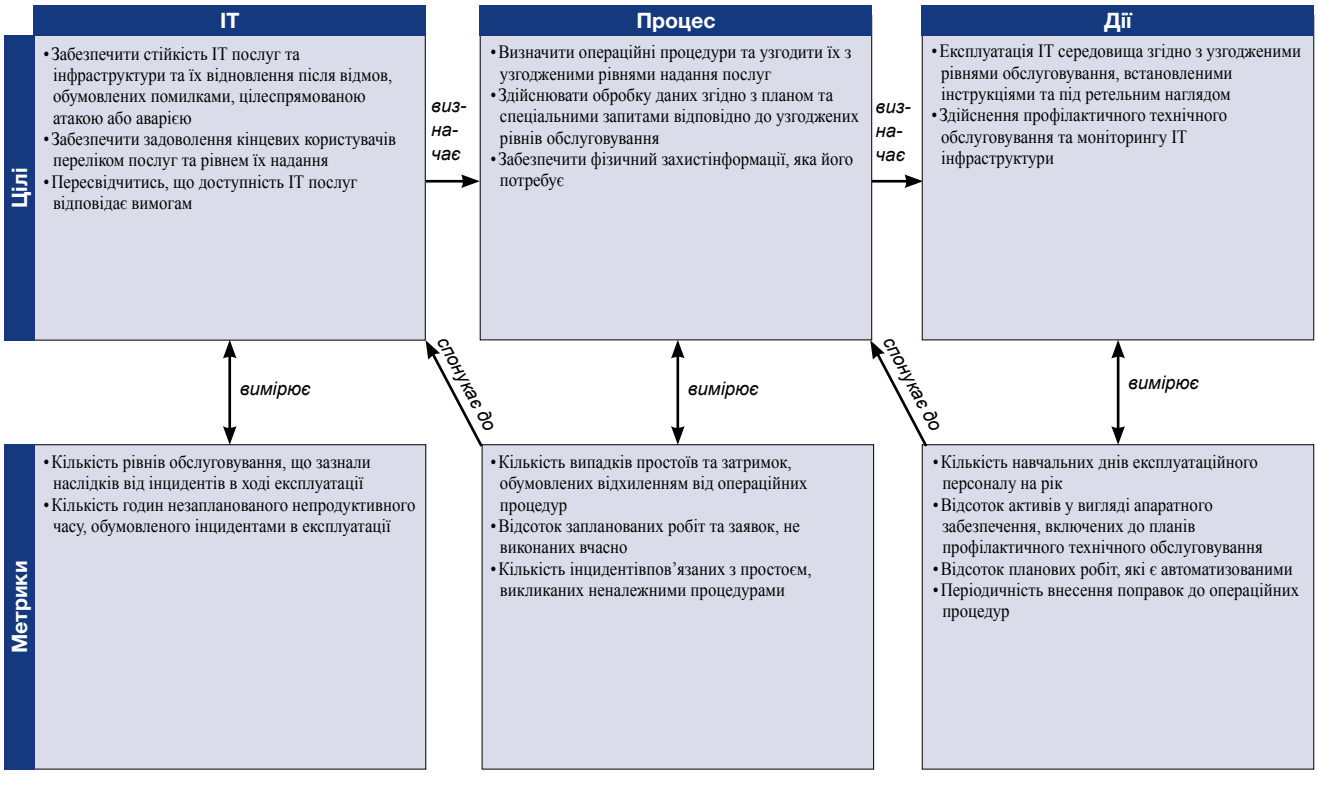
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Створення/зміна процедур експлуатації (в тому числі, інструкції, контрольні списки, плани роботи по змінам, передача документації, процедури ескалації проблем, тощо)						A/R					I
Складення графіку завантаження та пакетних завдань					C	A/R	C	C			
Моніторинг інфраструктури та обробки даних, вирішення проблем						A/R					I
Управління та захист фізичних вихідних документів (на папері, на носіях інформації)						A/R					C
Виправлення або зміни до плану-графіку та інфраструктури					C	A/R	C	C			C
Впровадження/встановлення процесу захисту пристроїв аутентифікації від зовнішнього впливу, втрати та крадіжки				A		R			I		C
Складення плану профілактичного технічного обслуговування та здійснення його						A/R					

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

DS13 Управляти операційною діяльністю

Рівні зрілості управління процесом *«Управляти операційною діяльністю»*, які задовольняють бізнес-вимоги до IT *«підтримувати цілісність даних та гарантувати те, що IT інфраструктура зберігає стійкість та може відновлюватись після помилок та відмов»*, є такими:

0 Не існуючий, якщо
Організація не приділяє часу та не виділяє ресурсів для вжиття базових заходів з підтримки та експлуатації IT.

1 Початковий, якщо
Організація усвідомлює потребу в структуризації функцій з підтримки IT. Впроваджено кілька стандартних процедур, заходи, що мають стосунок до експлуатації, носять реактивний характер. Більшість робочих процесів неформально сплановані, запити на обробку даних приймаються без попередньої перевірки. Комп'ютери, системи та прикладне програмне забезпечення, які підтримують бізнес-процеси, часто зазнають перерв у роботі, затримок та бувають недоступними. Втрачається час, коли працівники очікують на ресурси. Вихідні документи часто опиняються в неочікуваних місцях, або їх немає зовсім.

2 Повторюваний але інтуїтивний, якщо
Організація усвідомлює ключову роль, яку заходи з підтримки IT операцій відіграють у забезпечення функціонування IT. В кожному окремому випадку виділяються бюджетні кошти на засоби. Операції з підтримки IT є неформальними та інтуїтивними. Має місце високій ступінь залежності від кваліфікації та досвіду окремих спеціалістів. Інструкції, які передбачають, що треба зробити, коли та в якому порядку, не оформлені документально. Має місце епізодичне навчання персоналу, існують деякі формальні нормативи діяльності.

3 Визначений, якщо
Потребу в управлінні комп'ютерними операціями в організації розуміють та сприймають. Виділяються відповідні ресурси, іноді проводиться практичне навчання на робочому місці. Функції, що повторюються, формально визначені, стандартизовані, оформлені документально та доведені до відома співробітників організації. Події та результати виконаних завдань реєструються, але звітність керівництву щодо цих завдань має обмежений характер. Застосовується процедура автоматизованого планування та інші засоби, що дозволяє обмежити втручання оператора. Впроваджуються засоби контролю на випадок введення в роботу нових завдань. Розробляється формальна політика зменшення кількості незапланованих подій. Угоди з виробниками щодо технічного забезпечення та обслуговування і досі мають неформальний характер.

4 Керований та вимірюваний, якщо
Обов'язки щодо здійснення комп'ютерних операцій та їх супроводу чітко визначені, призначені відповідні власники. Операції мають підтримку у вигляді складання бюджету на ресурси з точки зору капітальних витрат та кадрових ресурсів. Навчання формалізоване та проводиться постійно. Плани-графіки та відповідні завдання оформлені документально та доведені до відома як працівників IT служби, так і користувачів у бізнес-підрозділах. Є можливість здійснювати оцінку та моніторинг поточної діяльності за допомогою стандартних угод відносно продуктивності та встановлених рівнів обслуговування. Будь-які відхилення від встановлених норм негайно фіксуються та коригуються. Керівництво контролює використання обчислювальних ресурсів та виконання роботи або поставлених завдань. Докладаються постійні зусилля до підвищення рівня автоматизації процесів, як фактору постійного вдосконалення. З постачальниками укладаються формальні угоди щодо технічного забезпечення та обслуговування. Існує повна узгодженість з процесами управління проблемами, здатностями та доступністю, на їх підтримку проводиться аналіз причин виникнення помилок та відмов.

5 Оптимізований, якщо
Операції з підтримки IT є ефективними, продуктивними та достатньо гнучкими, щоб відповідати вимогам дотримання рівня обслуговування з мінімальними втратами продуктивності. Процеси управління операціями IT стандартизовані та оформлені документально в базі знань, вони постійно вдосконалюються. Автоматизовані процеси, що підтримують роботу систем, працюють як єдине ціле та сприяють стабільності середовища. Всі проблеми та відмови аналізуються на предмет визначення першопричин. Регулярні наради за участю керівництва з питань внесення змін дозволяють вчасно включати внесення змін до виробничих планів. У співпраці з виробниками здійснюється аналіз обладнання на наявність симптомів старіння та неправильного функціонування, технічне обслуговування здебільшого має превентивний характер.

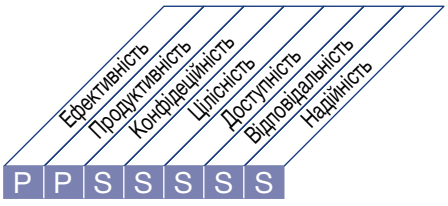
Відстежувати та оцінювати

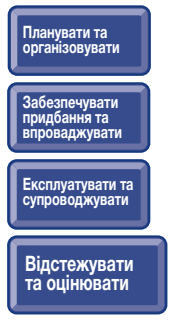
ME1 Відстежувати та оцінювати ефективність IT
ME2 Відстежувати та оцінювати ефективність внутрішнього контролю
ME3 Забезпечувати відповідність зовнішнім нормативним вимогам
ME4 Запровадити систему IT-управління

Опис процесу

ME1 Відстежувати та оцінювати ефективність IT

Ефективне управління продуктивністю IT потребує введення процесу моніторингу. Цей процес передбачає визначення відповідних показників продуктивності, систематичну та своєчасну звітність щодо продуктивності та негайне вжиття заходів у разі виникнення відхилень. Моніторинг дозволяє впевнитись в тому, що вживаються саме ті заходи, які узгоджуються з визначеними напрямками та політиками.





Контроль IT процесу

Відстежувати та оцінювати ефективність IT

який задовольняє бізнес-вимоги до IT, а саме:

забезпечення прозорості та зрозумілості витрат, вигод, стратегії, політик та рівнів обслуговування в сфері IT відповідно до вимог корпоративного управління

зосереджений на

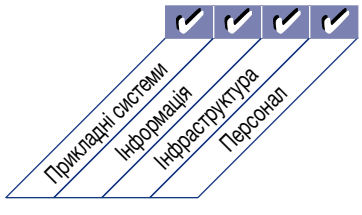
метриках процесів моніторингу та звітності а також визначенні та впровадженні заходів з підвищення продуктивності

реалізується шляхом

- Упорядкування та перетворення звітів щодо продуктивності процесу у звіти з питань управління
- Аналізу продуктивності у порівнянні з узгодженими плановими показниками та ініціації необхідних коригувальних заходів

та вимірюється

- Ступенем задоволення керівництва та керуючого органу звітністю щодо продуктивності
- Кількістю заходів з підвищення продуктивності, вжитих на підставі результатів моніторингу
- Відсотком критичних процесів, які відстежуються



Цілі контролю

ME1 Відстежувати та оцінювати ефективність IT

ME1.1 Концепція моніторингу
Створити загальну концепцію моніторингу та підхід до визначення обсягу, методології та процесу, яких слід дотримуватись при оцінюванні результатів надання IT рішень та IT послуг, а також здійснювати моніторинг внеску IT у бізнес. Інтегрувати цю концепцію у систему управління корпоративною продуктивністю.

ME1.2 Визначення та накопичення даних моніторингу
Співпрацювати з бізнес-підрозділами з метою визначення збалансованої сукупності планових показників продуктивності, отримати їх затвердження з боку бізнес-підрозділів та інших відповідних зацікавлених сторін. Визначити орієнтовні показники для порівняльної оцінки планових показників та охарактеризувати придатні дані, які слід накопичувати для вимірювання планових показників. Ввести в дію процеси, які передбачають накопичення актуальних та точних даних, на підставі яких буде складатись звітність щодо досягнень у реалізації планових показників.. .

ME1.3 Метод моніторингу
Впровадити в дію метод моніторингу продуктивності (наприклад, систему збалансованих показників), який дозволяє реєструвати планові показники та фіксувати результати вимірювань, забезпечує вичерпну та всебічну картину продуктивності IT та вписується в систему моніторингу продуктивності, введену в організації.

ME1.4 Оцінка продуктивності
Здійснювати періодичне порівняння ефективності з плановими показниками, аналізувати причини виникнення всіх відхилень та вживати коригувальних заходів щодо усунення виявлених причин. У відповідний час здійснювати аналіз першопричин всіх відхилень.

ME1.5 Звітність для Ради директорів та виконавчого керівництва
Організувати процес надання звітності вищому керівництву щодо внеску IT у розвиток бізнесу, зокрема, стосовно продуктивності портфелю підприємства, інвестиційних програм, передбачених в сфері IT, а також результатів реалізації окремих програм надання рішень та послуг. Відображати у звітах про хід справ той рівень, якого було досягнуто в реалізації запланованих цілей, перелік використаних ресурсів, передбачених бюджетом, рівень відповідності заданим плановим показникам продуктивності та перелік виявлених ризиків, які вдалося знизити. Передбачити оцінку вищого керівництва шляхом пропонування коригувальних заходів з усунення основних відхилень. Надавати звіт вищому керівництву та клопотати про надання у відповідь інформації щодо оцінки звіту керівництвом.. . . .

ME1.6 Коригувальні заходи
Визначати та ініціювати вжиття коригувальних заходів, виходячи з результатів моніторингу продуктивності, оцінки показників та звітів. Це передбачає вжиття подальших заходів на виконання всіх результатів моніторингу, звітності та оцінок шляхом:
- Аналізу, обговорення та втілення в життя відгуків керівництва
- Розподілу обов’язків щодо вжиття коригувальних заходів
- Відстеження результатів вжитих заходів

Керівні принципи управління

ME1 Відстежувати та оцінювати ефективність IT

Від	Вхідні дані
PO5	Звіти щодо втрат та вигод
PO10	Звіти щодо реалізації проекту
AI6	Звіти щодо статусу змін
DS1-13	Звіти щодо продуктивності процесу
DS3	План щодо продуктивності та потужностей
DS8	Звіти щодо задоволення користувачів
ME2	Звіт щодо ефективності заходів з контролю IT
ME3	Звіт щодо відповідності діяльності у сфері IT законодавчим та нормативним вимогам
ME4	Звіт щодо стану справ з управлінням IT

Вихідні дані	Для						
Вхідні дані щодо продуктивності для IT	PO1	PO2	DS1				
Плани коригувальних заходів	PO4	PO8					
Тенденції та події стосовно ризиків, які прослідкуються	PO9						
Звіт щодо продуктивності процесу	ME2						

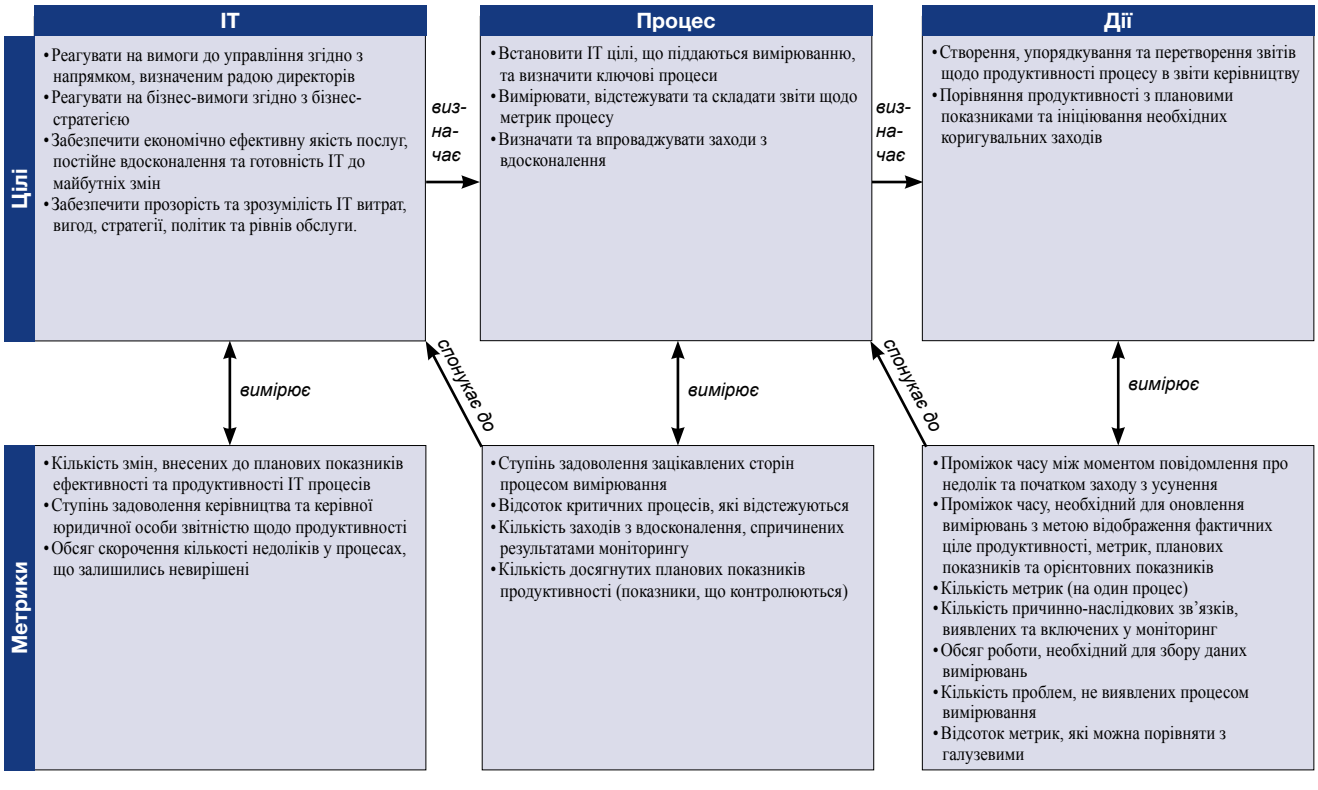
RACI-діаграма

Функції

Дії

	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Побудувати концепцію моніторингу	A	R	C	R	I	C	I	C	I		C
Визначити вимірні цілі, які підтримують бізнес-цілі	C	C	C	A	R	R		R			
Створити систему збалансованих показників				A		R	C	R	C		
Здійснювати оцінку продуктивності		I	I	A	R	R	C	R	C		
Складати звіти щодо продуктивності	I	I	R	A	R	R	C	R	C		I
Визначати та контролювати дії з підвищення продуктивності				A	R	R	C	R	C		C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

ME1 Відстежувати та оцінювати ефективність IT

Рівні зрілості управління процесом *«Відстежувати та оцінювати ефективність IT»*, які задовольняють бізнес-вимоги до IT стосовно *забезпечення прозорості та зрозумілості витрат, вигод, стратегії, політик та рівнів обслуговування в сфері IT відповідно до умов, необхідних для управління*, є такими:

0 Не існуючий, якщо
В організації не впроваджено процес моніторингу. IT служба не здійснює незалежного моніторингу проектів або процесів. Змістовна, своєчасна та точна звітність відсутня. Не визнано потребу у чіткому усвідомленні цілей процесу.

1 Початковий, якщо
Керівництво визнає необхідність збору та оцінки інформації стосовно процесів моніторингу. Стандартні процеси збору інформації та їх оцінки не визначені. Здійснення моніторингу та вибір метрик відбуваються в кожному конкретному випадку, згідно з потребами конкретних IT проектів та процесів. Як правило, моніторинг впроваджується у відповідь на інцидент, який спричинив якусь шкоду або труднощі для організації. Служба бухгалтерського обліку відстежує базові фінансові метрики у сфері IT.

2 Повторюваний але інтуїтивний, якщо
Визначені базові вимірювання, які необхідно відстежувати. Існують методи та технології накопичення даних та їх оцінки, але процеси не впроваджені в масштабах всієї організації. Інтерпретація результатів моніторингу ґрунтується на досвіді ключових спеціалістів. Для збору інформації вибрано та впроваджено обмежену кількість інструментів, але накопичення інформації немає планового підходу.

3 Визначений, якщо
Керівництво доводить до відома та впроваджує стандартні процеси моніторингу. Діють програми інструктажу та навчання з питань моніторингу. Розробляється формалізована база знань, у якій міститься інформація щодо продуктивності за попередні роки. Оцінку все же здійснюють на рівні окремих IT процесів та проектів немає інтеграції з усіма процесами. Визначено засоби моніторингу IT процесів та рівні обслуговування. Вимірювання внеску служби інформаційних технологій у продуктивність організації визначається із застосуванням традиційних фінансових та операційних критеріїв. Визначено показники IT продуктивності, не фінансові показники, показники ступеню задоволення користувачів та рівні обслуговування. Створено схему вимірювання продуктивності.

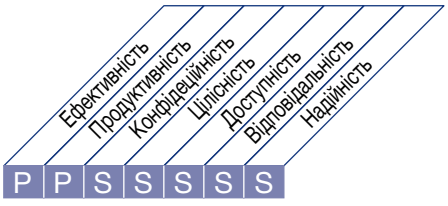
4 Керований та вимірюваний, якщо
Керівництво встановлює допуски, в межах яких повинні працювати процеси. Стандартизовано та нормалізовано звітність щодо результатів моніторингу. Має місце інтеграція показників за всіма IT проектами та процесами. Системи звітності щодо управління IT формалізовані. Автоматизовані засоби інтегровані та ефективно використовуються в масштабах всієї організації для збору та відстеження інформації стосовно роботи прикладних програмних продуктів, систем та процесів. Керівництво здатне оцінити продуктивність згідно з узгодженими критеріями, затвердженими зацікавленими сторонами. Вимірювання, які здійснює служба IT, узгоджуються з цілями організації в цілому.

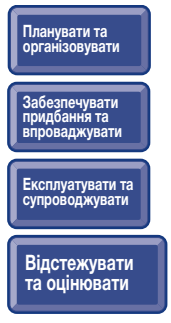
5 Оптимізований, якщо
Розробляється процес постійного підвищення якості для оновлення стандартів та політик, що діють в масштабах всієї організації, та з метою врахування найкращих галузевих практик. Всі процеси моніторингу оптимізовані та підтримують цілі організації в цілому. Метрики, визначені на підставі потреб бізнесу, регулярно використовуються для вимірювання продуктивності та інтегровані у схеми стратегічного оцінювання, такі як збалансовані системи показників IT. Моніторинг процесів та постійне їх перепроектування узгоджені з планами вдосконалення бізнес-процесів в масштабах всієї організації. Порівняльний аналіз показників з результатами, що існую в дані галуза та показниками ключових конкурентів набуває формалізованого характеру, застосовуються добре зрозумілі критерії порівняння.

Опис процесу

ME2 Відстежувати та оцінювати ефективність внутрішнього контролю

Впровадження ефективної програми внутрішнього контролю IT потребує введення в дію добре визначеного процесу моніторингу. Цей процес передбачає здійснення моніторингу та надання звітності щодо відхилень від вимог контролів, результатів самооцінювання та перевірок з боку третіх осіб. Основною вигодою моніторингу внутрішнього контролю є забезпечення продуктивних та ефективних операцій та дотримання відповідності до діючого законодавства та нормативних вимог.





Контроль IT процесу

Відстежувати та оцінювати ефективність внутрішнього контролю

який задовольняє бізнес-вимоги до IT, а саме:

забезпечення досягнення IT цілей та дотримання законодавства, нормативних вимог та контрактів, що діють у сфері IT

зосереджений на

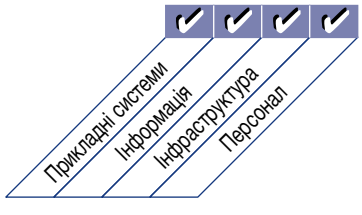
Здійсненні моніторингу процесів внутрішнього контролю діяльності, пов'язаної з IT, та визначенні заходів з їх вдосконалення

реалізується шляхом

- Створення системи внутрішнього контролю, вбудованої в структуру IT процесу
- Моніторингу та надання звітності щодо ефективності системи внутрішнього контролю за IT
- Надання керівництву звітності щодо відхилень від вимог внутрішнього контролю з метою вжиття необхідних заходів

та вимірюється

- Кількістю суттєвих порушень системи внутрішнього контролю
- Кількістю пропозицій щодо вдосконалення системи
- Кількістю фактів само оцінювання у системі контролю та повнотою охоплення



Цілі контролю

ME2 Відстежувати та оцінювати ефективність внутрішнього контролю

ME2.1 Моніторинг системи внутрішнього контролю
Здійснювати постійний моніторинг, порівняльний аналіз та вдосконалення контрольного середовища IT та системи контролю з метою досягнення організаційних цілей.

ME2.2 Перевірка в наглядовому порядку
Здійснювати моніторинг та оцінку продуктивності та ефективності внутрішніх перевірок з боку керівництва IT.

ME2.3 Відхилення від вимог контролю
Виявляти виключні ситуації в системі контролю, аналізувати та встановлювати першопричини їх виникнення. Здійснювати передачу виключних ситуацій в системі контролю для врегулювання на більш високий рівень ієрархії та надавати звіти зацікавленим сторонам в належний спосіб. Вживати необхідних коригуючи заходів.

ME2.4 Самооцінка контролю
Оцінювати повноту та ефективність контролю керівництва над IT процесами, політиками та контрактами за допомогою постійно діючої програми самооцінки.

ME2.5 Гарантія адекватності внутрішнього контролю
Отримувати в разі необхідності додаткові гарантії повноти та ефективності системи внутрішнього контролю шляхом проведення перевірок третіми сторонами.

ME2.6 Система внутрішнього контролю, що діє у третіх осіб
Оцінювати стан систем внутрішнього контролю в сторонніх організаціях, що надають послуги. Підтверджувати, що сторонні організації, які надають послуги, дотримуються законодавчих та нормативних вимог та виконують договірні зобов'язання.

ME2.7 Коригувальні заходи
Визначати, ініціювати, відстежувати та впроваджувати коригувальні заходи, які випливають з результатів оцінки системи контролю та відповідних звітів.

Керівні принципи управління

ME2 Відстежувати та оцінювати ефективність внутрішнього контролю

Від	Вхідні дані
AI7	Моніторинг системи внутрішнього контролю
ME1	Звіт щодо продуктивності процесу

Вихідні дані	Для						
Звіт про ефективність IT контролів	PO4	PO6	ME1	ME4			

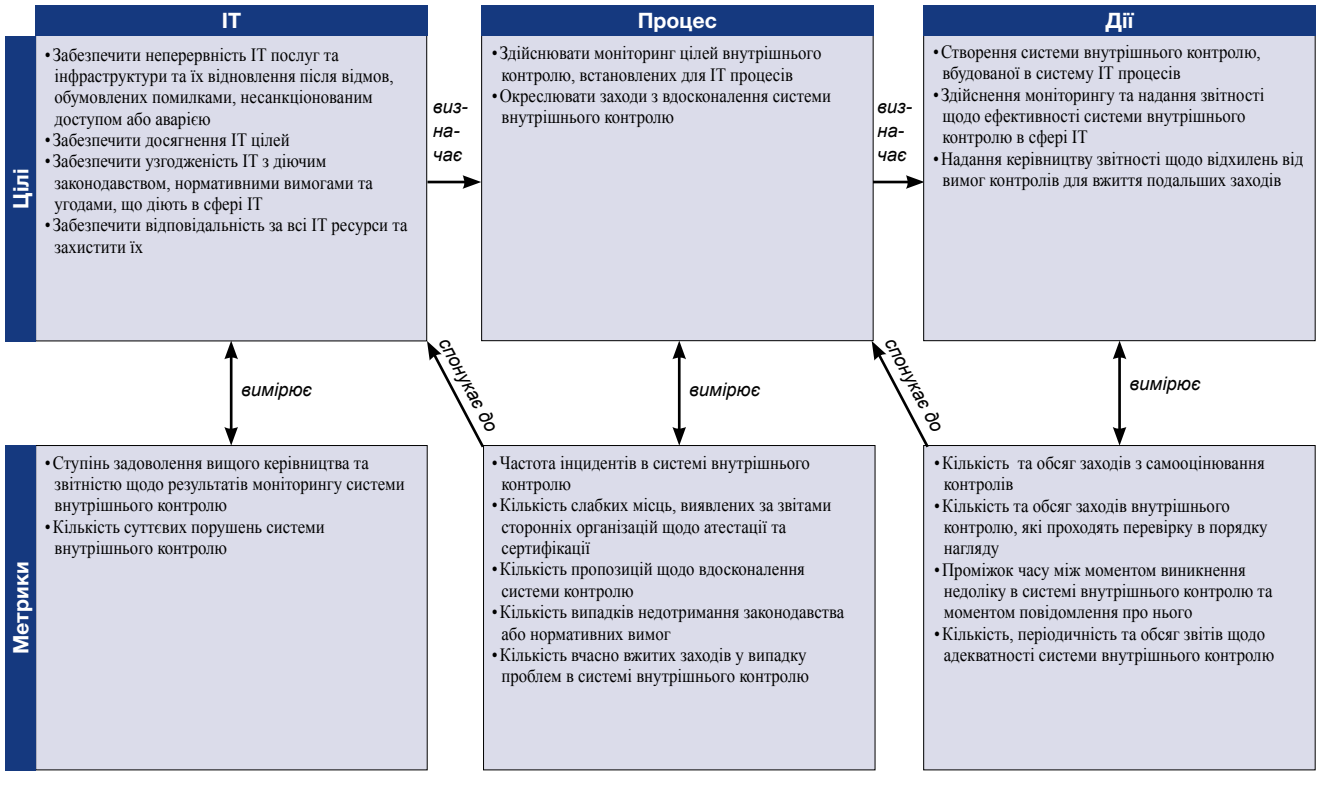
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог аудиту, ризиків та безпеки
Здійснювати моніторинг та контроль діяльності системи внутрішнього контролю в сфері IT				A		R		R	R		R
Здійснювати моніторинг процесу самооцінки			I	A		R		R	R		C
Здійснювати моніторинг виконання незалежних перевірок, аудитів та розслідувань			I	A		R		R	R		C
Здійснювати моніторинг процесу з метою отримання гарантій щодо адекватності систем контролю, які діють в сторонніх організаціях	I	I	I	A	I	R		R	R		C
Здійснювати моніторинг процесу з метою визначення та оцінки виключних ситуацій в системі контролю	I	I	I	A	I	R		R	R		C
Здійснювати моніторинг процесу з метою виявлення та коригування виключних ситуацій в системі контролю	I	I	I	A	I	R		R	R		C
Надавати звіти ключовим зацікавленим сторонам	I	I		A/R							I

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

ME2 Відстежувати та оцінювати ефективність внутрішнього контролю

Рівні зрілості управління процесом *«Відстежувати та оцінювати ефективність внутрішнього контролю»*, які задовольняють бізнес-вимоги до IT стосовно *забезпечення досягнення IT цілей та дотримання законодавства, нормативних вимог та контрактів, що діють у сфері IT*, є такими:

0 Не існуючий, якщо
В організації не введені процедури моніторингу ефективності системи внутрішнього контролю. Відсутні методи звітності щодо адекватності внутрішнього контролю перед керівництвом. Необхідність забезпечення безпеки IT операцій та потреба у системі внутрішнього контролю не усвідомлюються взагалі. Керівництво та співробітники організації абсолютно не усвідомлюють потреби у системі внутрішнього контролю.

1 Початковий, якщо
Керівництво усвідомлює потребу у регулярному підтвердженні адекватності управління та контролю за IT. В кожному конкретному випадку використовується досвід окремих осіб з оцінки адекватності внутрішнього контролю. На керівництво служби IT не покладено формальної відповідальності за здійснення моніторингу ефективності системи внутрішнього контролю. Оцінку адекватності внутрішнього контролю здійснюють в межах звичайного фінансового аудиту, користуючись методами та набором навичок, які не відображають потреби служби інформаційного обслуговування.

2 Повторюваний але інтуїтивний, якщо
В організації застосовується система неформальної звітності щодо адекватності контролю з метою ініціації коригуючи заходів. Оцінка адекватності внутрішнього контролю залежить від набору навичок ключових спеціалістів. В організації зростає ступінь усвідомлення необхідності моніторингу системи внутрішнього контролю. Керівництво служби інформаційних технологій здійснює регулярний моніторинг ефективності тих видів внутрішнього контролю, які воно вважає критичними. Починається застосування методологій та засобів моніторингу адекватності внутрішнього контролю, але відповідного плану немає. На базі досвіду окремих спеціалістів здійснюється виявлення чинників ризику, пов'язаних із IT оточенням.

3 Визначений, якщо
Керівництво підтримує та впроваджує процес моніторингу системи внутрішнього контролю. Розробляються політики та процедури, що передбачають оцінку та надання звітності щодо діяльності у сфері моніторингу системи внутрішнього контролю. Складено програми інструктажу та навчання з питань внутрішнього контролю. Визначено процес для здійснення самооцінки та перевірки адекватності внутрішнього контролю, з розподілом ролей та обов'язків відповідальних керівників бізнес-підрозділів та служби IT. Відповідні інструменти та засоби застосовуються, але вони не обов'язково інтегровані у всі процеси. Політики оцінки ризиків, пов'язаних з IT процесами, використовуються в системах контролю, розроблених конкретно для IT організації. Визначено ризики, пов'язані з конкретними процесами, та політики пом'якшення їх наслідків.

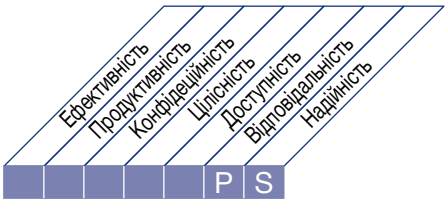
4 Керований та вимірюваний, якщо
Керівництво впроваджує концепцію моніторингу системи внутрішнього контролю IT. Організація встановлює величину допусків для процесу, що описує моніторинг системи внутрішнього контролю. З метою стандартизації оцінок та автоматичного виявлення виключних ситуацій в системі контролю застосовуються відповідні інструменти та засоби. Засновано офіційну службу внутрішнього контролю IT, в якій працюють атестовані спеціалісти, які застосовують формальну систему контролю, затверджену вищим керівництвом. Кваліфікований персонал IT служби регулярно бере участь в оцінці адекватності внутрішнього контролю. Засновано базу знань, в якій зберігаються статистичні дані за попередні періоди, що стосуються метрик, застосовних у моніторингу внутрішнього контролю. Застосовується підхід огляду результатів роботи колегами при здійсненні моніторингу системи внутрішнього контролю.

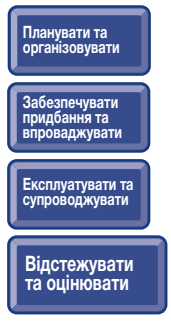
5 Оптимізований, якщо
Керівництво впроваджує постійно діючу в масштабах всієї організації програму вдосконалення, в реалізації якої бере до уваги набутий досвід та найкращі практики, що діють в галузі моніторингу систем внутрішнього контролю. Організація застосовує інтегровані та сучасні засоби та інструменти, коли це доцільно, які дозволяють здійснити ефективну оцінку критично важливих засобів IT контролю та швидко виявити інциденти у схемі моніторингу внутрішнього контролю. Формально запроваджений обмін знаннями, які конкретно стосуються діяльності служби інформаційних технологій. Офіційно здійснюється порівняльний аналіз показників з галузевими стандартами та найкращими практиками.

Опис процесу

МЕ3 Забезпечувати відповідність зовнішнім нормативним вимогам

Ефективний нагляд за дотриманням нормативних вимог потребує введення процесу перевірки з метою забезпечення відповідності діючим законам, нормативним вимогам та виконання договірних умов. Цей процес передбачає визначення вимог щодо відповідності нормативам, оптимізацію та оцінку відповідності, отримання підтвердження того, що вимоги були дотримані, а також, насамкінець, інтеграція звітності щодо відповідності ІТ існуючим вимогам зі звітністю решти бізнес-підрозділів.





Контроль ІТ процесу

Забезпечувати відповідність зовнішнім нормативним вимогам

який задовольняє бізнес-вимоги до ІТ, а саме:

забезпечення відповідності діючому законодавству, нормативним вимогам та умовам контрактів

зосереджений на

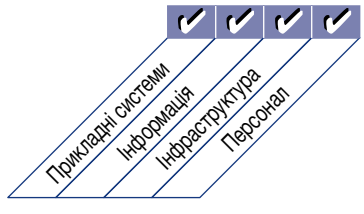
встановленні всіх застосовних законів, нормативних вимог та контрактів, а також відповідного рівня відповідності ІТ, та оптимізації ІТ процесів з метою зменшення ризику, пов'язаного з недотриманням існуючих вимог

реалізується шляхом

- Визначення законодавчих, регулятивних та договірних вимог, що мають стосунок до ІТ
- Оцінки наслідків застосування вимог щодо відповідності
- Здійснення моніторингу та надання звітності щодо відповідності вказаним вимогам

та вимірюється

- Витратами, пов'язаними з невідповідністю ІТ існуючим вимогам, включаючи врегулювання платежів та взаєморозрахунки, а також штрафи
- Середній проміжок часу між моментом встановлення проблем з відповідністю нормативним вимогам та моментом їх врегулювання
- Періодичністю перевірки відповідності існуючим вимогам



Цілі контролю

ME3 Забезпечувати відповідність зовнішнім нормативним вимогам

ME3.1 Визначення законодавчих, регулятивних та договірних вимог, яких необхідно дотримуватись
Постійно виявляти основні, місцеві та міжнародні закони, правові норми ті інші зовнішні вимоги, яких потрібно дотримуватись в обов'язковому порядку та включати в політики, стандарти, процедури та методології, прийняті в організації у сфері IT.

ME3.2 Оптимізація реагування на зовнішні вимоги
Здійснювати перегляд та коригування політик, стандартів, процедур та методологій IT з врахуванням діючих законодавчих та нормативних вимог.

ME3.3 Оцінка відповідності зовнішнім вимогам
Підтверджувати відповідність політик, стандартів, процедур та методологій IT законодавчим та нормативним вимогам.

ME3.4 Позитивне підтвердження відповідності вимогам
Отримувати та доводити до відома інформацію про позитивне підтвердження відповідності вимогам та дотримання всіх внутрішніх політик, вироблених на базі внутрішніх директив або зовнішніх законодавчих, регулятивних тат договірних вимог, на підтвердження того, що відповідальний власник процесу своєчасно вжив всіх коригуючи заходів з метою усунення всіх невідповідностей вимогам.

ME3.5 Інтегрована система звітності
Інтегрувати систему звітності щодо відповідності IT законодавчим, регулятивним та договірним вимогам з аналогічними системами інших підрозділів організації.

Керівні принципи управління

ME3 Забезпечувати відповідність зовнішнім вимогам

Від	Вхідні дані
*	Вимоги щодо відповідності законодавчим та нормативним вимогам
PO6	IT-політики

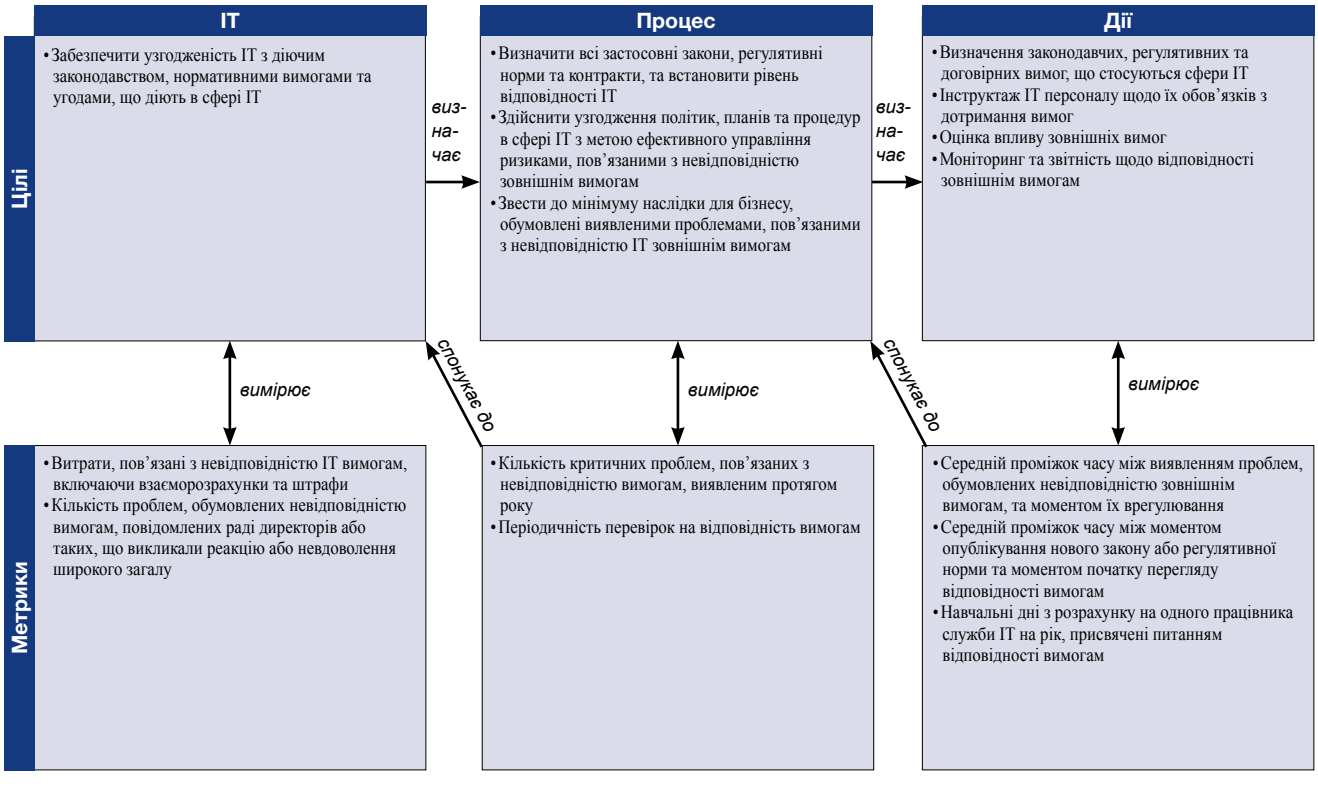
* Вхідні ресурси, що надходять з джерел поза межами стандарту CobiT®.

Вихідні дані	Для						
Перелік законодавчих та нормативних вимог, що стосуються надання IT послуг	PO4	ME4					
Звіт щодо відповідності функціонування IT законодавчим та регулятивним вимогам	ME1						

RACI-діаграма

Дії \ Функції	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Визначити та виконати процес встановлення законодавчих, договірних, регулятивних вимог та політик, яких треба дотримуватись				A/R	C	I	I	I	C	I	R
Оцінювати ступінь відповідності діяльності у сфері IT політикам, планам та процедурам, прийнятим для IT	I	I	I	A/R	I	R	R	R	R	R	R
Доповідати про позитивне підтвердження відповідності діяльності в сфері IT політикам, планам та процедурам, прийнятим для IT				A/R	C	C	C	C	C	C	R
Надавати вхідні дані для узгодження політик, планів та процедур, прийнятих для IT, з вимогами відповідності				A/R	C	C	C	C	C		R
Інтегрувати систему звітності щодо відповідності IT регулятивним вимогам з аналогічними системами інших підрозділів організації				A/R		I	I	I	R	I	R

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

ME3 Забезпечувати відповідність зовнішнім нормативним вимогам

Рівні зрілості управління процесом *«Забезпечувати відповідність зовнішнім нормативним вимогам»*, які задовольняють бізнес-вимоги до IT стосовно *відповідності діючому законодавству, нормативним вимогам та умовам контрактів*, є такими:

0 Не існуючий, якщо
Погано усвідомлені зовнішні вимоги, які впливають на функціонування IT, не впроваджено процес, що стосується дотримання відповідності законодавчим, регулятивним та договірним вимогам.

1 Початковий, якщо
Має місце розуміння впливу регулятивних, контрактних та законодавчих вимог на діяльність організації. Виконуються неформальні процеси, що забезпечують відповідність вимогам, але тільки тоді, коли виникає в цьому виникає потреба при виконанні нових проектів або у відповідь на проведені аудити або перевірки.

2 Повторюваний але інтуїтивний, якщо
Існує розуміння потреби у дотримання зовнішніх вимог, цю потребу доведено до відома в організації. Там, де необхідність дотримання вимог виникає періодично, як, наприклад, при застосування фінансових регулятивних норм або законодавства, що регулює питання конфіденційності, були розроблені окремі процедури перевірки на відповідність, які застосовуються рік від року. Однак, немає стандартного підходу. Має місце високі ступінь залежності від знань та відповідальності окремих осіб, існує імовірність виникнення помилок. Проводиться формальне навчання з питань відповідності зовнішнім вимогам.

3 Визначений, якщо
Політики, плани та процедури розробляються, оформляються документально та доводяться до відома працівників з метою забезпечення дотримання регулятивних норм а також договірних та законодавчих зобов'язань, але деякі з них не завжди бувають дотримані а деякі можуть бути застарілими або непридатними до застосування. Моніторинг здійснюється рідко, є вимого щодо відповідності, які не були дотримані. Проводиться навчання з питань законодавчих та регулятивних вимог, що стосуються діяльності організації та з питань застосування визначених процесів перевірки відповідності. Введені типові форми контрактів та стандартні юридичні процеси, що дозволяє звести до мінімуму ризики, пов'язані з відповідальністю через контракти.

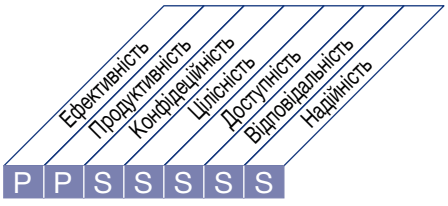
4 Керований та вимірюваний, якщо
Проблеми та ризики, пов'язані з невідповідністю нормативним вимогам, а також потреба у забезпеченні вказаної відповідності усвідомлені на всіх рівнях. Впроваджено формальну систему навчання з метою гарантії того, що всі співробітники усвідомлюють свої обов'язки щодо дотримання відповідності. Обов'язки чітко розподілені,приналежність процесів усвідомлена. Цей процес передбачає аналіз середовища з метою визначення зовнішніх нормативних вимог та слідкування за постійними змінами до них. Введено механізм виявлення невідповідності вимогам, забезпечення реалізації внутрішніх практик та запровадження коригуючи заходів. Проблеми, пов'язані з невідповідністю вимогам, аналізують на предмет виявлення першопричин у стандартний спосіб, з метою знаходження раціональних рішень. Найкращі внутрішні практики застосовуються для конкретних потреб, наприклад, для поточних змін у законодавстві та регулярно поновлюваних угод.

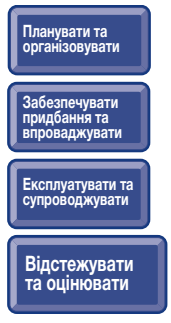
5 Оптимізований, якщо
Введено добре організований, ефективний процес, виконання якого забезпечено, що передбачає дотримання зовнішніх нормативних вимог. Робота процесу організована спеціальною центральною службою, яка забезпечує керівництво та координацію роботи всієї організації. Має місце широка поінформованість у сфері застосовного законодавства та нормативних вимог, в тому числі майбутніх тенденцій їх розвитку та очікуваних змін, а також усвідомлено потребу у пошуку нових рішень. Організація бере участь у спільних обговорення питань, пов'язаних з зовнішніми нормативними вимогами, які чинять вплив на її діяльність, з регулятивними обговорення з представниками своєї галузі. Розгортаються найкращі практики, які забезпечують ефективне дотримання нормативних вимог, що призводить до дуже малої кількості виключних ситуацій в частині відповідності вимогам. Існує централізована система контролю, яка дозволяє керівництву документувати робочий процес, а також вимірювати та підвищувати якість та ефективність процесу моніторингу відповідності вимогам. Впроваджено процес самооцінки відповідності нормативним вимогам, який доведено до рівня найкращої практики. Стиль управління та культура, які практикує керівництво у сфері забезпечення відповідності нормативним вимогам приймається більшістю співробітників, а процеси описані та запроваджені достатньо добре для того, щоб навчання проводилось тільки у випадку набору нового персоналу та при внесенні суттєвих змін.

Опис процесу

ME4 Запровадити систему IT-управління

Створення ефективної системи управління передбачає визначення організаційних структур, процесів, керівників, розподілу ролей та обов'язків з метою гарантії того, що інвестиції, які організація родить у сферу IT, узгоджуються та надаються відповідно до стратегій та цілей підприємства.





Контроль IT процесу

Запровадити систему IT-управління

який задовольняє бізнес-вимоги до IT, а саме:

здійснення інтеграції системи управління IT з системою корпоративного управління згідно з її цілями, а також забезпечити відповідність діючому законодавству, регулятивним вимогам та умовам діючих контрактів

зосереджений на

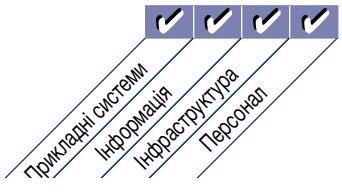
підготовці звітів для ради директорів щодо стратегії у сфері IT, продуктивності та ризиків, пов'язаних з IT, а також на забезпеченні відповідності вимогам щодо управління згідно з вказівками ради директорів

реалізується шляхом

- Впровадження системи управління IT, інтегрованої із системою корпоративного управління
- Отримання незалежного позитивного підтвердження статусу системи управління IT

та вимірюється

- Періодичністю наданні звітів радою директорів щодо стану справ у сфері IT зацікавленим сторонам (в тому числі інформації щодо ступеню зрілості процесів)
- Періодичністю надання звітів службою IT раді директорів (в тому числі інформації щодо ступеню зрілості процесів)
- Періодичністю незалежних перевірок відповідності IT існуючим вимогам



Цілі контролю

ME4 Запровадити систему IT-управління

ME4.1 Впровадження системи управління IT
Створити, впровадити в дію та узгодити систему управління IT із загальною системою корпоративного управління, наявною в організації, та контрольним середовищем. В основу такої системи покласти прийнятний IT процес та модель контролю, а також забезпечити абсолютно однозначну індивідуальну відповідальність та впровадити відповідні практики з метою уникнення порушень системи внутрішнього контролю та нагляду. Підтверджувати той факт, що система управління IT забезпечує відповідність законам та регулятивним нормам, узгоджується та підтверджує реалізацію стратегій та цілей організації. Надавати звіти щодо статусу системи управління IT та проблем, що у ній виникають.

ME4.2 Відповідність на стратегічному рівні
Забезпечити для ради директорів та виконавчого керівництва можливість усвідомлення таких стратегічних питань, пов'язаних зі сферою IT, як роль IT, правильне уявлення про IT та розуміння потужностей IT. Впевнитись в тому, що відбувається обмін знаннями між бізнес-підрозділами та службою IT стосовно потенційного внеску IT в реалізацію бізнес-стратегії. Працювати з радою директорів та запровадженими органами управління, наприклад, з комітетом з питань IT стратегії, з метою визначення стратегічного напрямку роботи керівництва стосовно IT, гарантувати надходження інформації щодо стратегії та цілей зверху донизу до усіх бізнес-підрозділів та служб IT, а також впевнитись в тому, що між бізнес-підрозділами та службами IT розвиваються стосунки, що ґрунтуються на взаємній довірі. Забезпечити узгодження IT з бізнес-стратегією та бізнес-операціями, заохочувати спільну відповідальність бізнес-підрозділів та служби IT за прийняття стратегічних рішень та отримання вигод від інвестицій, зроблених у сфері IT.

ME4.3 Забезпечення цінності
Здійснювати управління програмами інвестування в розвиток IT та іншими IT ресурсами та послугами з метою надання ними максимально можливої цінності у підтримці стратегій та цілей підприємства. Впевнитись в тому, що організація усвідомлює та розуміє очікувані кінцеві результати ділової діяльності, обумовлені інвестиціями в IT, та повний обсяг робіт, необхідних для досягнення вказаних кінцевих результатів, в тому, що підготовлені всебічні та послідовні економічні обґрунтування, схвалені зацікавленими сторонами, в тому, що управління ресурсами та інвестиціями здійснюється протягом всього їх економічного життєвого циклу, а також в тому, що здійснюється активне управління процесом реалізації вигод, наприклад, сприяння розвитку нових послуг, підвищення продуктивності та вдосконалення системи реагування на потреби користувачів та клієнтів. Забезпечити обов'язкове здійснення упорядкованого підходу до вирішення питань у сфері управління портфелями, програмами та проектами, наполягаючи на тому щоб бізнес-підрозділи приймали на себе право власності на всі інвестиції, зроблені в IT, а служба IT забезпечувала б оптимізацію витрат, понесених у зв'язку з наданням IT потужностей та IT послуг.

ME4.4 Управління ресурсами
Здійснювати нагляд за здійсненням інвестицій, використанням та розподілом IT ресурсів шляхом проведення регулярних оцінок IT проектів та поточної діяльності з метою забезпечення належного надання ресурсів та узгодженості з поточними та майбутніми стратегічними цілями а також нагальними потребами бізнесу.

ME4.5 Управління ризиками
Працювати з радою директорів над визначенням прийнятного для підприємства рівня ризиків, пов'язаних з використанням IT, та отримати розумне позитивне підтвердження того факту, що практики управління IT ризиками, можуть гарантувати, що фактична величина IT ризику не перевищать рівня прийнятного ризику, визначеного радою директорів. Здійснити в організації розподіл обов'язків щодо управління ризиками, щоб забезпечити регулярність оцінки та надання звітності бізнес-підрозділами та IT службою щодо ризиків, пов'язаних з використанням IT, та інших їх наслідків, а також гарантувати прозорість картини щодо IT ризиків, до яких схильна організація, для всіх зацікавлених сторін.

ME4.6 Оцінка ефективності
Підтверджувати, що узгоджені IT цілі були досягнуті або перевершені, або той факт, що вигоди, досягнуті шляхом реалізації IT цілей, відповідають очікуванням. Якщо узгоджені цілі не були реалізовані, або якщо вигоди від їх реалізації не такі, як очікувалось, здійснювати критичний перегляд коригувальних заходів, вжитих керівництвом. Надавати звіти раді директорів стосовно продуктивності портфелів, програм та IT взагалі, які підкріплюються звітами, що дають можливість вищому керівництву здійснювати аналіз ходу просування організації у напрямку досягнення визначених цілей.

ME4.7 Незалежне позитивне підтвердження
Отримувати незалежне позитивне підтвердження (внутрішнє або зовнішнє) щодо відповідності IT діючому законодавству та нормативним вимогам, політикам, стандартам та процедурам, прийнятим в організації, загальноприйнятим практикам, а також ефективного та продуктивного функціонування IT.

Керівні принципи управління

ME4 Запровадити систему IT-управління

Від	Вхідні дані
PO4	Структура IT процесу
PO6	Звіти щодо вигод та витрат
PO9	Оцінка ризиків та звітність
ME2	Звіт щодо ефективності IT контролю
ME3	Перелік законодавчих та регулятивних вимог щодо надання IT послуг

Вихідні дані	Для						
Вдосконалення структури процесу	PO4						
Звіт щодо статусу системи управління IT	PO1	ME1					
Очікувані результати ділової діяльності, обумовлені інвестиціями бізнесу в IT	PO5						
Стратегічний напрямок розвитку IT в організації	PO1						
Схильність організації до IT ризиків	PO9						

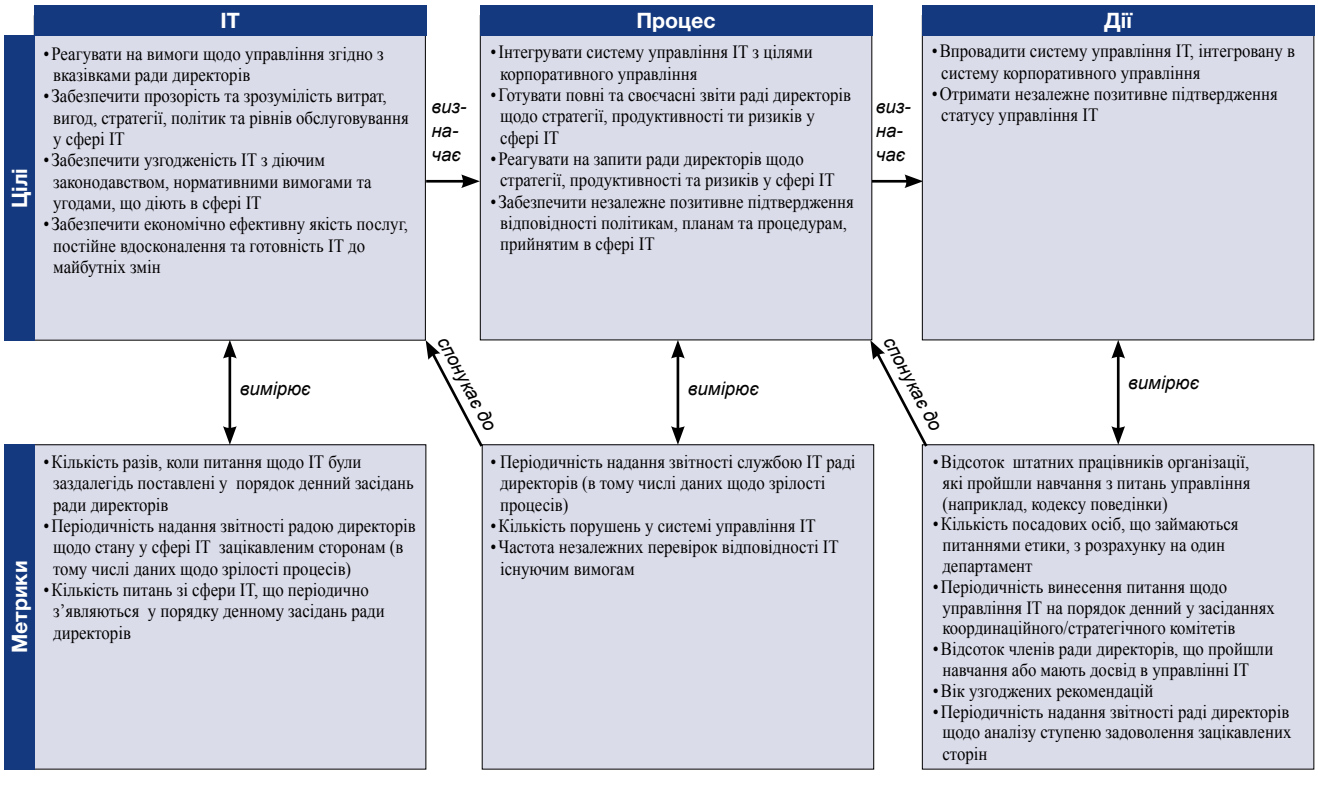
RACI-діаграма

Функції

Дії

Дії	CEO	CFO	Керівник бізнес-підрозділу	CIO	Власник бізнес-процесу	Директор з операційних питань	Директор з питань архітектури	Керівник підрозділу розробки	Керівник служби адміністрування IT	PMO	Служба контролю дотримання вимог, аудиту, ризиків та безпеки
Встановити нагляд з боку виконавчого керівництва та ради директорів за діяльністю у сфері IT та здійснювати відповідне сприяння	R	C	C	C							C
Здійснювати аналіз, орієнтування та інформування щодо продуктивності IT, IT стратегії а також управління ризиками та ресурсами відповідно до бізнес-стратегії	R	I	I	R							C
Отримувати періодичну незалежну оцінку продуктивності та відповідності політикам, планам та процедурам	R	C	I	C		I	I	I	I	I	R
Вирішувати питання, пов'язані з результатами незалежного оцінювання та забезпечити впровадження керівництвом узгоджених рекомендацій	R	C	I	C		I	I	I	I	I	R
Формувати звіт щодо управління IT	C	C	C	R	C	I	I	I	I	I	C

В **RACI** – діаграмі вказано, хто є відповідальним (**R**), перед ким потрібно звітувати (**A**), з ким консультуватись (**C**) та кого інформувати (**I**).



Модель зрілості

ME4 Запровадити систему IT-управління

Рівні зрілості управління процесом *«Запровадити систему IT-управління»*, які задовольняють бізнес-вимоги до IT стосовно *здійснення інтеграції системи управління IT з системою корпоративного управління згідно з її цілями, а також забезпечення відповідності діючому законодавству, регулятивним вимогам та умовам діючих контрактів*, є такими:

0 Не існуючий, якщо
Повністю відсутній будь-який процес управління IT, який можна було б розпізнати. Організація навіть не усвідомлює того, що цією проблемою потрібно опікуватись. Як наслідок, немає комунікацій з цього питання.

1 Початковий, якщо
Має місце усвідомлення того, що проблема створення системи управління IT існує, і її потрібно вирішувати. В кожному конкретному випадку застосовуються конкретні підходи до вирішення проблеми. Підхід керівництва до управління має реактивний та епізодичний характер, комунікації щодо проблем та способів їх вирішення також мають епізодичний та непослідовний характер. Керівництво має лиже приблизні дані щодо внеску IT у продуктивність ділової діяльності. Керівництво лише за фактом виникнення реагує не інцидент, який спричинив якусь шкоду організації або створив перепону для її діяльності .

2 Повторюваний але інтуїтивний, якщо
Існує усвідомлення потреби у створенні системи управління IT. У стадії розробки знаходяться перелік заходів з управління IT та показники продуктивності, які передбачають IT планування, процеси надання послуг та моніторингу. Вибрані IT процеси призначені для вдосконалення на підставі рішень окремих спеціалістів. Керівництво встановлює основні вимірювання у сфері управління IT та методи та способи оцінки; однак, цей процес не прийнятий в масштабах всієї організації. Здійснення комунікацій з питань стандартів управління та відповідних обов'язків залишене на розсуд окремих осіб. Окремі особи керують процесами управління за допомогою різноманітних IT проектів та процесів. Процеси, інструменти та метрики, призначені для вимірювання результатів Управління IT, обмежені та можуть не використовуватись в повному обсязі та на повну потужність внаслідок відсутності досвіду щодо їх функціональних можливостей.

3 Визначений, якщо
Важливість системи управління IT та потребу у її створенні керівництво розуміє та доводить до відома всіх в організації. Розробляється сукупність базових показників управління IT, у якій встановлені та документально оформлені зв'язки між вихідними метриками та показниками продуктивності. Процедури стандартизовані та документально оформлені. Керівництво доводить до відома всіх працівників стандартні процедури, проводиться відповідне навчання. Визначено засоби підтримки здійснення нагляду за управлінням IT. Панелі нагляду передбачені в межах системи збалансованих показників IT-бізнес. Однак, працівники самі визначають, чи потрібно їм проходити навчання, дотримуватись стандартів та застосовувати їх. Процеси можуть контролюватись, але відхилення, які головним чином відбуваються з провини окремих працівників, практично не виявляються керівництвом.

4 Керований та вимірюваний, якщо
Має місце абсолютне розуміння проблем, пов'язаних з управлінням IT, на всіх рівнях. Існує чітке уявлення про те, що собою являє замовник (клієнт), обов'язки визначені та контролюються за допомогою угод про рівень обслуговування. Існує чіткий розподіл обов'язків, встановлено власників процесів. IT процеси та система управління IT узгоджені та інтегровані у бізнес-стратегію та IT стратегію. Вдосконалення IT процесів відбувається головним чином в результаті розуміння кількісних показників, існує можливість відстеження відповідності процедурам та вимірювання метрик процесу. Всі зацікавлені сторони процесів усвідомлюють відповідні ризики, важливість IT та можливості, які IT можуть запропонувати. Керівництво визначає допуски, в межах яких мають працювати процеси. Має місце обмежене, головним чином, тактичне, використання технології, що ґрунтується на методах оцінювання зрілості та впроваджених стандартних засобах. Систему управління IT інтегровано у процеси стратегічного та оперативного планування, а також у процес моніторингу. Показники продуктивності всіх видів діяльності з управління IT реєструються та контролюються, що дає підґрунтя для здійснення вдосконалень у масштабах всього підприємства. Чітко визначена повна індивідуальна відповідальність за здійснення ключових процесів, керівництво отримує винагороду на підставі ключових метрик продуктивності.

5 Оптимізований, якщо
Має місце глибоке та перспективне розуміння проблем, пов'язаних з управлінням IT, та способів їх вирішення. Навчання та комунікації здійснюються з використанням найсучасніших концепцій та методик. Процеси вдосконалено до рівня найкращих галузевих практик в результаті постійного вдосконалення та застосування моделей зрілості у порівнянні з

результатами інших організацій. Результатом впровадження IT політик є те, що організація, люди та процеси швидко пристосовуються та повністю підтримують вимоги щодо управління IT. Здійснюється аналіз першопричин всіх проблем та відхилень, негайно визначаються та ініціюються ефективні коригувальні заходи. IT широко використовуються в інтегрований та оптимізований спосіб, який дозволяє автоматизувати робочий процес та надати засоби підвищення якості та ефективності. Ризики та повернення IT процесів чітко визначені, збалансовані та доведені до відома в масштабах всього підприємства. Ефективно використовується допомога сторонніх експертів, застосовується порівняльний аналіз показників з еталонами, що дає змогу виробляти відповідні орієнтири. В організації широко розповсюджені підходи моніторингу, самооцінки та комунікацій щодо очікувань від системи управління IT, технології в оптимальний спосіб використовуються на підтримку вимірювань, аналізу, повідомлення інформації та проведення навчання. Система корпоративного управління та система управління IT пов'язані між собою на стратегічному рівні, що дає змогу максимально використати технології, кадрові та фінансові ресурси для підвищення конкурентоздатності підприємства. Заходи з управління IT інтегровані у процес управління підприємством.

Сторінку навмисне залишено вільною

Додаток I

Таблиці, що відображають зв'язок між цілями та процесами

У цьому додатку в загальних рисах показано, як стандартні бізнес-цілі пов'язані з IT цілями, IT процесами та інформаційними критеріями. Додаток містить три таблиці:

1. В першій таблиці відображено відповідність між бізнес-цілями, організованими згідно з системою збалансованих показників, IT цілями та інформаційними критеріями. Вона дає змогу побачити, які IT цілі зазвичай супроводжують стандартну бізнес-ціль, та які інформаційні критерії, застосовні у стандарті СовіТ®, мають стосунок до даної бізнес-цілі. Сукупність із 17 бізнес-цілей не слід вважати завершеним переліком всіх можливих бізнес-цілей; вказані бізнес-цілі чинять виражений вплив на сферу IT (бізнес-цілі, пов'язані з IT).
2. В другій таблиці показано відповідність між IT цілями та процесами, передбаченими стандартом СовіТ®, та інформаційними критеріями, які лежать в основі IT цілі.
3. В третій таблиці показано, яким саме IT процесом супроводжуються IT цілі.

Наведені таблиці допомагають уявити сферу застосування стандарту СовіТ® та глибокі взаємозв'язки між стандартом СовіТ® та чинниками, обумовленими бізнесом, оскільки в них типові бізнес-цілі, пов'язані з IT, поставлені у відповідність IT процесам, що необхідні для їх підтримки. Оскільки в даних таблицях наведено стандартні цілі, тіх слід використовувати як орієнтир та адаптувати на випадок конкретного підприємства.

З метою забезпечення зворотного зв'язку з інформаційними критеріями, застосовними у випадку бізнес-вимог з третього видання стандарту СовіТ®, в таблицях також вказані найважливіші інформаційні критерії, що підтримуються бізнес-цілями та IT цілями.

Примітки:

1. Інформаційні критерії (критерії інформації) у таблиці, що стосується бізнес-цілей, є результатом агрегування критеріїв для відповідних IT цілей та таких, що за суб'єктивною оцінкою максимально відповідають бізнес-цілям. Спроби виділити первинні чи вторинні критерії не робились. Вони є лише орієнтиром, тому користувачі можуть дотримуватись аналогічного процесу в ході оцінки своїх власних бізнес-цілей.
2. Розподіл інформаційних критеріїв на первинні (основні) та вторинні (другорядні) здійснено на основі агрегування критеріїв для кожного IT процесу та суб'єктивної оцінки того, що є первинним (основним), а що – вторинним (другорядним) для IT цілі, оскільки деякі процеси можуть чинити більший вплив на IT ціль, ніж інші. Цей розподіл є лише орієнтовним, тому користувачі можуть дотримуватись аналогічного процесу при здійсненні аналізу своїх власних IT цілей.

ЗВ'ЯЗОК МІЖ БІЗНЕС-ЦІЛЯМИ ТА IT ЦІЛЯМИ

		Бізнес-цілі	IT цілі								Інформаційні критерії стандарту CobiT®: Ефективність	Продуктивність	Конфіденційність	Цілісність	Доступність	Відповідність	Надійність
Фінансові перспективи	**1**	Забезпечити високу віддачу від інвестицій бізнес–підрозділів в IT	24									✔					
	2	Управляти підприємницькими ризиками, пов'язаними із застосуванням IT	2	14	17	18	19	20	21	22			✔	✔	✔		
	3	Вдосконалювати корпоративне управління та підвищувати прозорість	2	18													✔
Перспективи для користувачів	**4**	Підвищувати орієнтацію на клієнта та рівень обслуговування	3	23							✔						
	5	Пропонувати конкурентоздатні вироби та послуги	5	24							✔	✔					
	6	Забезпечити безперервність надання послуг та їх придатність	10	16	22	23					✔				✔		
	7	Швидко реагувати на зміни бізнес-вимог	1	5	25						✔	✔					
	8	Досягти оптимізації витрат при наданні послуг.	7	8	10	24						✔					
	9	Отримувати надійну та корисну інформацію для прийняття стратегічних рішень	2	4	12	20	26				✔			✔			✔
Внутрішня сфера	**10**	Вдосконалювати та підтримувати функціональність бізнес-процесів.	6	7	11						✔	✔					
	11	Зменшувати витрати, пов'язані з процесами .	7	8	13	15	24					✔					
	12	Забезпечити відповідність діючим законам, регулятивним нормам та угодам	2	19	20	21	22	26	27				✔			✔	
	13	Забезпечити дотримання внутрішніх політик.	2	13									✔			✔	
	14	Управляти змінами у бізнесі	1	5	6	11	28				✔	✔					
	15	Підвищувати та підтримувати продуктивність роботи та персоналу	7	8	11	13					✔	✔					
Навчання та проф. ріст	**16**	Управляти інноваціями у сфері продуктів та бізнесу.	5	25	28						✔	✔					
	17	Набирати та підтримувати кваліфікований та цілеспрямований персонал.	9								✔	✔					

ЗВ'ЯЗОК IT ЦІЛЕЙ З IT ПРОЦЕСАМИ

	IT цілі	Процеси											Інформаційні критерії стандарту CobiT®: Ефективність	Продуктивність	Конфіденційність	Цілісність	Доступність	Відповідність	Надійність
1	Реагувати на бізнес-вимоги згідно з бізнес-стратегією	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1		P	P		S	S		
2	Реагувати на вимоги до корпоративного управління згідно з напрямком розвитку (вказівками), визначеним Радою директорів	PO1	PO4	PO10	ME1	ME4							P	P					
3	Забезпечити задоволення кінцевих користувачів запропонованими послугами та рівнем надання послуг	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P		S	S		
4	Оптимізувати використання інформації	PO2	DS11											S		P			S
5	Забезпечити гнучкість IT (можливість швидкої перебудови)	PO2	PO4	PO7	AI3								P	P		S			
6	Визначити, як бізнес-вимоги щодо функціональних можливостей та засобів контролю перетворюються в ефективні та продуктивні рішення з автоматизації	AI1	AI2	AI6									P	P				S	
7	Отримати та підтримувати в робочому стані інтегровані та стандартизовані прикладні системи	PO3	AI2	AI5									P	P				S	
8	Комплектувати та підтримувати інтегровану та стандартизовану IT інфраструктуру	AI3	AI5										S	P					
9	Наймати IT персонал та підтримувати його кваліфікацію на рівні, що відповідає IT стратегії	PO7	AI5										P	P					
10	Забезпечити взаємне задоволення взаємовідносинами зі сторонніми організаціями	DS2											P	P	S	S	S	S	S
11	Забезпечити органічну інтеграцію прикладних програмних продуктів в бізнес-процеси	PO2	AI4	AI7									P	P		S	S		
12	Забезпечити прозорість та зрозумілість витрат, вигод, стратегії, політик та рівнів надання послуг у сфері IT	PO5	PO6	DS1	DS2	DS6	ME1	ME4					P	P				S	S
13	Забезпечити належне використання та експлуатацію прикладного програмного забезпечення та технологічних рішень	PO6	AI4	AI7	DS7	DS8							P	S					
14	Вести облік та забезпечувати захист всіх IT ресурсів	PO9	DS5	DS9	DS12	ME2							S	S	P	P	P	S	S
15	Оптимізувати IT інфраструктуру, ресурси та можливості.	PO3	AI3	DS3	DS7	DS9							S	P					
16	Знизити обсяг недоліків та робіт з їх виправлення при наданні рішень та послуг.	PO8	AI4	AI6	AI7	DS10							P	P		S	S		
17	Забезпечити досягнення IT цілей	PO9	DS10	ME2									P	P	S	S	S	S	S
18	Встановити чіткий зв'язок між наслідками ризиків для бізнесу та IT цілями,ресурсами	PO9											S	S	P	P	P	S	S
19	Забезпечити захист критичної та конфіденційної інформації від осіб, які не повинні мати до неї доступ	PO6	DS5	DS11	DS12										P	P	S	S	S
20	Гарантувати надійність автоматизованих бізнес-операцій та обміну інформацією	PO6	AI7	DS5									P			P	S	S	
21	Забезпечити стійкість IT послуг та інфраструктури, та їх відновлення після інцидентів у разі помилок, вторгнення або аварії	PO6	AI7	DS4	DS5	DS12	DS13	ME2					P	S		S	P		
22	Забезпечити мінімальні наслідки для бізнесу у випадку перерви у наданні IT послуг або внесення змін до них	PO6	AI6	DS4	DS12								P	S		S	P		
23	Пересвідчитись, що придатність IT послуг відповідає вимогам	DS3	DS4	DS8	DS13								P			P	P		
24	Підвищити економічну ефективність IT та відповідний внесок у рентабельність бізнесу	PO5	DS6										S	P					S
25	Виконувати проекти вчасно та в межах бюджету відповідно до стандартів якості	PO8	PO10										P	P		S			S
26	Підтримувати цілісність інформаційної та обробляючої інфраструктури	AI6	DS5										P	P		P	P		S
27	Забезпечити узгодженість IT з діючим законодавством, нормативними вимогами та угодами, що діють в сфері IT	DS11	ME2	ME3	ME4										S	S		P	S
28	Забезпечити економічно ефективну якість послуг, постійне вдосконалення та готовність IT до майбутніх змін	PO5	DS6	ME1	ME4								P	P					P

ТАБЛИЦЯ ВІДПОВІДНОСТІ ІТ-ПРОЦЕСІВ ІТ-ЦІЛЯМ

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Забезпечувати придбання та впроваджувати																												
PO1 розробляти стратегічний план розвитку IT	✔	✔																										
PO2 формувати архітектуру інформації	✔			✔	✔						✔																	
PO3 визначати технологічний напрямок							✔								✔													
PO4 формувати процеси, організацію та взаємозв'язки для IT	✔	✔			✔																							
PO5 управляти інвестиціями в IT												✔												✔				✔
PO6 інформувати про стратегічні цілі керівництва та напрямки розвитку												✔	✔						✔	✔	✔	✔						
PO7 управляти персоналом IT					✔				✔																			
PO8 управляти якістю			✔													✔									✔			
PO9 оцінювати та управляти IT-ризиками														✔			✔	✔										
PO10 управляти проектами	✔	✔																							✔			
Забезпечувати придбання та впроваджувати																												
AI1 визначати рішення з автоматизації	✔					✔																						
AI2 забезпечувати придбання та підтримку прикладного програмного забезпечення						✔	✔																					
AI3 забезпечувати придбання та підтримку технологічної інфраструктури					✔			✔							✔													
AI4 забезпечувати експлуатацію та використання			✔								✔		✔			✔												
AI5 закуповувати IT-ресурси							✔	✔	✔																			
AI6 управляти змінами.	✔					✔										✔						✔				✔		
AI7 впроваджувати в експлуатацію та проводити акредитацію IT-рішень та змін	✔										✔		✔			✔				✔	✔							
Експлуатувати та супроводжувати																												
DS1 визначати та управляти рівнями надання послуг	✔		✔									✔																
DS2 управляти послугами третіх сторін			✔							✔		✔																
DS3 управляти ефективністю та потужностями	✔														✔													
DS4 забезпечувати безперервність надання послуг																					✔	✔	✔					
DS5 забезпечувати безпеку систем														✔					✔	✔	✔					✔		
DS6 визначати та розподіляти витрати												✔												✔				✔
DS7 навчати користувачів			✔										✔		✔													
DS8 управляти службою підтримки та інцидентами			✔										✔										✔					
DS9 управляти конфігураціями														✔	✔													
DS10 управляти проблемами			✔													✔	✔											
DS11 управляти даними				✔															✔								✔	
DS12 управляти фізичним середовищем														✔					✔		✔	✔						
DS13 управляти операційною діяльністю			✔																		✔		✔					
Відстежувати та оцінювання																												
ME1 відстежувати та оцінювати ефективність IT	✔	✔										✔																✔
ME2 відстежувати та оцінювати ефективність внутрішнього контролю														✔			✔				✔						✔	
ME3 забезпечувати відповідність зовнішнім нормативним																											✔	
ME4 запровадити систему IT-управління		✔										✔															✔	✔

1 Реагувати на бізнес-вимоги згідно з бізнес-стратегією
2 Реагувати на вимоги до корпоративного управління згідно з напрямком розвитку (вказівками), визначеним Радою директорів
3 Забезпечити задоволення кінцевих користувачів запропонованими послугами та рівнем надання послуг
4 Оптимізувати використання інформації
5 Забезпечити гнучкість IT (можливість швидкої перебудови)
6 Визначити, які бізнес-вимоги щодо функціональних можливостей та засобів контролю перетворюються в ефективні та продуктивні рішення з автоматизації
7 Отримати та підтримувати в робочому стані інтегровані та стандартизовані прикладні системи
8 Комплектувати та підтримувати інтегровану та стандартизовану IT інфраструктуру
9 Наймати IT персонал та підтримувати його кваліфікацію на рівні, що відповідає IT стратегії
10 Забезпечити взаємне задоволення взаємовідносинами зі сторонніми організаціями
11 Забезпечити організаційну інтеграцію прикладних програмних продуктів в бізнес-процеси
12 Забезпечити прозорість та зрозумілість витрат, вигод, стратегії, політик та рівнів надання послуг у сфері IT
13 Забезпечити належне використання та експлуатацію прикладного програмного забезпечення та технологічних рішень
14 Вести облік та забезпечувати захист всіх IT ресурсів
15 Оптимізувати IT інфраструктуру, ресурси та можливості
16 Знизити обсяг недоліків та робіт з їх виправлення
17 Забезпечити досягнення IT цілей
18 Встановити чіткий зв'язок між наслідками ризиків для бізнесу та IT цілями,ресурсами
19 Забезпечити захист критичної та конфіденційної інформації від осіб, які не повинні мати до неї доступ
20 Гарантувати надійність автоматизованих бізнес-операцій та обміну інформацією
21 Забезпечити стійкість IT послуг та інфраструктури, та їх відновлення після аварії
22 Забезпечити мінімальні наслідки для бізнесу у випадку переривання або аварії
23 Переконатись, що придатність IT послуг відповідає вимогам
24 Підвищити економічну ефективність IT та відповідний внесок у рентабельність бізнесу
25 Виконувати проекти вчасно та в межах бюджету відповідно до стандартів якості
26 Підтримувати цілісність інформаційної та обробляючої інфраструктури
27 Забезпечити узгодженість IT з діючим законодавством, нормативними вимогами та угодами, що діють в сфері IT
28 Забезпечити економічно ефективну якість послуг, постійне вдосконалення та готовність IT до майбутніх змін

Додаток II

Встановлення відповідності між IT процесами та доменами стратегічного управління IT, моделлю COSO, IT-ресурсами СовіТ та інформаційними критеріями СовіТ

Цей додаток ілюструє відповідність між IT процесами стандарту СовіТ® та п'ятьма доменами стратегічного управління IT, елементами моделі COSO, IT-ресурсами та інформаційними критеріями. В наведеній таблиці також вказаний показник відносної важливості (висока (H), середня (M) та низька(L)), визначений за результатами порівняльного аналізу (бенчмаркінгу), проведеного за допомогою СовіТ Online. В цій таблиці на одній сторінці на високому рівні показано, як саме структура СовіТ відповідає вимогам стратегічного управління IT та моделі COSO, та відображено взаємозв'язки між IT процесами,IT ресурсами та інформаційними критеріями. Літерою P позначено основну (первинну) роль, а літерою S – другорядну (вторинну). Ні P, ні S не означає відсутність відповідності, вони означають лише більшу чи меншу важливість, або незначущість. Показники важливості ґрунтуються на результатах аналізу та думці експертів, вони слугують лише орієнтиром. Користувачі повинні самі оцінювати важливість процесів, що виконуються в їх організаціях.

Додаток II – Проектування IT-процесів на IT-управління
Встановлення відповідності між IT процесами та доменами стратегічного управління IT, моделлю COSO, IT ресурсами та інформаційними критеріями CobiT

	ВАЖЛИВІСТЬ	Домени стратегічного управління IT					Модель COSO					CobiT® IT Ресурси				CobiT® Критерії інформації						
		Відповідність на стратегічному рівні	Забезпечення цінності	Управління ресурсами	Управління ризиками	Оцінка ефективності	Контрольне середовище	Оцінка ризиків	Засоби контролю	Інформація та комунікації	Моніторинг	Прикладні системи	нформація	Інфраструктура	Люди	Ефективність	Продуктивність	Конфіденційність	Цілісність	Доступність	Узгодженість	Надійність
Планувати та ораганізовувати																						
PO1 розробляти стратегічний план IT	H	P		S	S			P		S	S	✓	✓	✓	✓	P	S					
PO2 формувати архітектуи інформації	L	P	S	P	S				P	P		✓	✓			S	P	S	P			
PO3 визначати технологічний напрямок	M	S	S	P	S			S	P	S		✓		✓		P	P					
PO4 формувати процеси, організацію та взаємозв'язки для IT	L	S		P	P		P			S	S				✓	P	P					
PO5 управляти інвестиціями в IT	M	S	P	S		S		S	P			✓		✓	✓	P	P					S
PO6 інформувати про стратегічні цілі керівництва та напрямки розвитку	M	P			P		P			P			✓		✓	P					S	
PO7 управляти персоналом IT	L	P		P	S	S	P			S					✓	P	P					
PO8 управляти якістю	M	P	S		S		P		P	S	P	✓	✓	✓	✓	P	P		S			S
PO9 оцінювати та управляти IT-ризиками	H	P			P			P				✓	✓	✓	✓	S	S	P	P	P	S	S
PO10 управляти проектами	H	P	S	S	S	S	S	S	P		S	✓		✓	✓	P	P					
Забезпечувати придбання та впроваджувати																						
AI1 визначати рішення з автоматизації	M	P	P	S	S				P			✓		✓		P	S					
AI2 забезпечувати придбання та підтримку прикладного програмного забезпечення	M	P	P		S				P			✓				P	P		S			S
AI3 забезпечувати придбання та підтримку технологічної інфраструктури.	L			P					P					✓		S	P		S	S		
AI4 забезпечувати експлуатацію та використання	L	S	P	S	S				P	S		✓		✓	✓	P	P		S	S	S	S
AI5 закуповувати IT-ресурси	M		S	P					P			✓	✓	✓	✓	S	P				S	
AI6 управляти змінами	H		P	S				S	P		S	✓	✓	✓	✓	P	P		P	P		S
AI7 впроваджувати в експлуатацію та проводити акредитацію IT-рішень та змін	M	S	P	S	S	S			P	S	S	✓	✓	✓	✓	P	S		S	S		
Експлуатувати та супроводжувати																						
DS1 визначати та управляти рівнями надання послуг	M	P	P	P		P	S		P	S	S	✓	✓	✓	✓	P	P	S	S	S	S	S
DS2 управляти послугами третіх сторін	L		P	S	P	S	P	S	P		S	✓	✓	✓	✓	P	P	S	S	S	S	S
DS3 управляти ефективністю та потужностями	L	S	S	P	S	S			P		S	✓		✓		P	P			S		
DS4 забезпечувати безперервність надання послуг	M	S	P	S	P	S	S		P	S		✓	✓	✓	✓	P	S			P		
DS5 забезпечувати безпеку систем	H				P				P	S	S	✓	✓	✓	✓			P	P	S	S	S
DS6 визначати та розподіляти витрати	L		S	P		S			P			✓	✓	✓	✓		P					P
DS7 навчати користувачів	L	S	P	S	S		P			S					✓	P	S					
DS8 управляти службою підтримки та інцидентами	L		P			S	S			P	P	✓			✓	P	P					
DS9 управляти конфігураціями	M		P	P	S				P			✓	✓	✓		P	S			S		S
DS10 управляти проблемами	M		P		S	S			P	S	S	✓	✓	✓	✓	P	P			S		
DS11 управляти даними	H		P	P	P				P				✓						P			P
DS12 управляти фізичним середовищем	L			S	P			S	P					✓					P	P		
DS13 управляти операційною діяльністю	L			P					P	S		✓	✓	✓	✓	P	P		S	S		
Відстежувати та оцінювання																						
ME1 відстежувати та оцінювати ефективність IT	H	S	S	S	S	P				S	P	✓	✓	✓	✓	P	P	S	S	S	S	S
ME2 відстежувати та оцінювати ефективність внутрішнього контролю	M		P		P						P	✓	✓	✓	✓	P	P	S	S	S	S	S
ME3 забезпечувати відповідність зовнішнім нормативним вимогам	H	P			P				P	S	S	✓	✓	✓	✓						P	S
ME4 запровадити систему IT-управління.	H	P	P	P	P	P	P	S		S	P	✓	✓	✓	✓	P	P	S	S	S	S	S

P=первинне (основне) S=вторинне (другорядне)

Примітка: Відповідність моделі COSO базується на початковій структурі COSO. Ця відповідність також застосовна до останньої версії моделі COSO«Управління ризиками підприємства – Інтегрована схема», яка поширюється на систему внутрішнього контролю,тим самим більш уважно зосереджуючись на розширенні об'єкту управління ризиками підприємства. Оскільки вона не передбачена для заміни початкової моделі COSO схеми внутрішнього контролю та не заміняє її, а лише вводить в неї систему внутрішнього контролю, користувачі CobiT можуть звернутись до цієї схеми управління ризиками підприємства як з метою задоволення своїх потреб у забезпеченні системи внутрішнього контролю, так і з метою просування в бік більш розширеного процесу управління ризиками.

Сторінку навмисне залишено вільною

Додаток III

Модель зрілості системи внутрішнього контролю

В цьому додатку представлено типову модель зрілості, яка відображає статус середовища внутрішнього контролю та процесу впровадження заходів внутрішнього контролю на підприємстві. З неї видно, яким чином управління системою внутрішнього контролю та усвідомлення необхідності впровадження більш досконалої системи внутрішнього контролю розвиваються від рівня «Початок» до рівня «Оптимізація». Наведена модель є узагальненим орієнтиром, за допомогою якого користувачі стандарту СовіТ можуть визначити необхідні заходи, які забезпечать ефективну роботу системи внутрішнього контролю, а також належним чином позиціонуватимуть свою організацію відповідно до шкали зрілості.

Додаток III—Модель зрілості системи внутрішнього контролю

Рівень зрілості	Статус середовища внутрішнього контролю	Впровадження заходів внутрішнього контролю
0 Не існуючий	Відсутнє усвідомлення потреби у системі внутрішнього контролю. Контроль не є частиною культури або організації, або її цільовим завданням. Існує високий ступінь ризику, пов'язаного з відсутністю системи контролю та виникненням інцидентів різного роду.	Відсутні спроби оцінити потребу у системі внутрішнього контролю, інциденти врегульовуються у разі їх виникнення.
1 Початковий /епізодичний	деякою мірою існує усвідомлення потреби у системі внутрішнього контролю. Підхід до управління ризиками та вимоги до системи контролю є епізодичними та дезорганізованими, без комунікацій та моніторингу. Недоліки не виявляються. Працівники не усвідомлюють своїх обов'язків.	Не усвідомлено потребу у визначенні заходів, необхідних з точки зору здійснення контролю у сфері IT. Якщо подібні заходи здійснюються, вони мають лише епізодичний характер, здійснюються на високому рівні та у відповідь на суттєві інциденти. Аналіз проводиться лише у випадку фактичного інциденту.
2 Повторюваний але інтуїтивний	Заходи контролю введені, але документально не оформлені. Їх здійснення залежить від знань та мотивації окремих осіб. Ефективність не оцінюється належним способом. У системі контролю багато слабких місць, якими не займаються належним чином; наслідки цього можуть виявитись значними. Дії керівництва з усунення проблем у системі контролю не мають визначених пріоритетів та є непослідовними. Працівники можуть не усвідомлювати своїх обов'язків.	Аналіз потреб у засобах контролю здійснюється лише у разі необхідності для вибраних IT процесів з метою визначення поточного рівня зрілості системи контролю, запланованого рівня, якого потрібно досягти, та невідповідності між ними, яка існує на поточний момент. Для визначення належного підходу до вжиття заходів контролю процесів та до мотивації узгодженого плану необхідних заходів застосовується неформальний підхід обговорення в робочій групі за участю керівників IT служби та членів групи, задіяної в процесі.
3 Визначений	Заходи контролю впроваджені та документально оформлені належним чином. Ефективність операцій періодично оцінюється, існує середня кількість проблем. Однак, процес оцінки не оформлений документально. Хоча керівництво і здатне прогнозувати більшість проблем, пов'язаних із системою контролю, все ще продовжують існувати слабкі місця в системі контролю, а їх наслідки можуть залишатись серйозними. Працівники усвідомлюють свої обов'язки з питань контролю.	Критичні IT процеси визначені на підставі чинників цінності та ризиків. Здійснюється детальний аналіз з метою визначення вимог до системи контролю та першопричин невідповідностей, а також з метою розробки можливостей для покращення. На додаток до обговорень у робочих групах застосовується інструментарій та система інтерв'ю на підтримку аналізу та гарантії того, що власники IT процесів управляють та керують оцінкою та процесом вдосконалення.
4 Керований та вимірюваний	Існує ефективне середовище внутрішнього контролю та управління ризиками. Часто здійснюється формальна документована оцінка заходів контролю. Багато заходів контролю автоматизовані та регулярно переглядаються. Керівництво може виявляти більшість проблем у системі контролю, але не всі проблеми регулярно виявляються. Має місце послідовне відстеження виявлених слабких місць у системі контролю. Для автоматизації заходів контролю обмежено застосовуються технології з тактичної точки зору.	Регулярно визначається критичність IT процесу за умови повної підтримки та узгодженості з відповідними власниками бізнес-процесів. Оцінка вимог до системи контролю базується на політиках і фактичному рівні зрілості вказаних процесів, та здійснюється після ретельного аналізу за участю ключових зацікавлених сторін. Підзвітність за цю оцінку чітко визначена та реалізується в обов'язковому порядку. Стратегії вдосконалення підкріплені економічним обґрунтуванням. Діяльність з досягнення бажаних кінцевих результатів постійно відстежується. Час від часу організовуються зовнішні перевірки системи контролю.
5 Оптимізований	Програма управління ризиками та системою контролю, що діє в масштабах всієї організації, забезпечує послідовне та ефективне врегулювання проблем, пов'язаних з проблемами у системі контролю та управління ризиками. Системи внутрішнього контролю та управління ризиками інтегровані у практики організації, здійснюється автоматизований моніторинг в реальному масштабі часу, забезпечується управління ризиками та дотримання існуючих вимог. Постійно здійснюється оцінка системи контролю на базі самостійної оцінки заходів контролю та аналізу невідповідностей та першопричин. Працівники заздалегідь залучені до процесу вдосконалення системи контролю.	Зміни у бізнесі враховують критичність IT процесів та охоплюють будь-яку потребу у переоцінці можливостей контролю за процесом. Власники IT процесів регулярно здійснюють самостійну оцінку заходів контролю з метою підтвердження їх належного рівня зрілості, необхідного для задоволення потреб бізнесу. Вони вважають, що ознаки зрілості можуть сприяти визначенню способів підвищення ефективності та продуктивності засобів контролю. Організація здійснює порівняльний аналіз показників з найкращими зовнішніми практиками та отримує рекомендації сторонніх осіб щодо ефективності системи внутрішнього контролю. У випадку критичних процесів проводяться незалежні опитування з метою підтвердження того, що заходи контролю мають належний рівень зрілості та працюють згідно з планом.

Сторінку навмисне залишено вільною

Додаток IV

Основні довідкові матеріали документу СовіТ 4.1

Додаток IV—Основні довідкові матеріали документу СовіТ® 4.1

Раніше в ході розробки стандарту СовіТ® та внесенні поправок і доповнень до нього використовували широкий перелік (більш як 40) міжнародних детальних ІТ-стандартів, концепцій, інструкцій та найкращих практик з метою забезпечення повноти стандарту СовіТ® з точки зору охоплення всіх сфер управління ІТ та контролю за ними.

Оскільки стандарт СовіТ® орієнтований на те, *що* необхідно реалізації належного управління та контролю за ІТ, він є стандартом високого рівня. Більш детальні ІТ-стандарти та найкращі практики на більш низькому рівні описують, *як* саме здійснювати управління та контроль конкретних аспектів сфери ІТ. Стандарт СовіТ® інтегрує всі вказані різноманітні керівні матеріали, збираючи докупи всі ключові цілі (об'єкти) в межах «парасолькової» структури, яка також прив'язана до вимог корпоративного управління та бізнес-вимог.

При створенні даної оновленої версії стандарту СовіТ® (СовіТ® 4.1) було використано шість глобальних стандартів, концепцій та практик, що мають відношення до сфери ІТ, які стали основними джерелами забезпечення адекватного охоплення всіх проблем, системності та узгодження. Це документи, наведені нижче:

- Комітет спонсорських організацій Комісії Тредуея (COSO):
  «Інтегрована схема внутрішнього контролю» (Internal Control—Integrated Framework), 1994
  «Інтегрована схема управління ризиками» (Enterprise Risk Management—Integrated Framework), 2004
- Міністерство Державної торгівлі (Office of Government Commerce (OGC®)):
  Бібліотека інфраструктури інформаційних технологій (IT Infrastructure Library® (ITIL®)), 1999-2004
- Міжнародна організація з питань стандартизації (International Organisation for Standardisation):
  Стандарт ISO/IEC 27000
- Інститут програмної інженерії (Software Engineering Institute (SEI®)):
  Модель зрілості процесів створення програмного забезпечення (SEI Capability Maturity Model (CMM®)), 1993
  Інтегрована модель досконалості та зрілості (SEI Capability Maturity Model Integration (CMMI®)), 2000
- Інститут управління проектами (Project Management Institute (PMI®)):
  «Керівництво до Зводу знань з управління проектами» (A Guide to the Project Management Body of Knowledge (PMBOK®)), 2004
- Форум з інформаційної безпеки (Information Security Forum (ISF)):
  «Стандарт найкращих практик у сфері інформаційної безпеки» (The Standard of Good Practice for Information Security), 2003

Додаткові джерела, використані при розробці стандарту СовіТ® 4.1:

- *«Цілі контролю у сфері ІТ, які відповідають вимогам Закону Сарбейнса-Окслі: Роль ІТ у розробці та впровадженні системи внутрішнього контролю фінансової звітності, 2-ге видання»* (IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition) , Інститут управління ІТ, США (IT Governance Institute, USA), 2006
- *CISA Review Manual, ISACA, 2006*

Сторінку навмисне залишено вільною

Додаток V

Перехресні посилання видань CobiT 3 та CobiT 4.1

Додаток V — Перехресні посилання видань CobiT® 3 та CobiT® 4.1

ЗМІНИ, ВНЕСЕНІ НА РІВНІ СТРУКТУРИ

Основні зміни, внесені до структури (концептуального ядра) стандарту CobiT® в процесі оновлення версії CobiT® 4.0, подані нижче:

- Домен M перетворився на домен ME, що означає «Відстежувати та оцінювати» (Monitor and Evaluate).
- Процеси M3 та M4 були процесами аудиту, а не IT процесами. Їх було вилучено, оскільки вони перекриваються низкою відповідних стандартів аудиту у сфері IT, але в оновленій структурі надано посилання, щоб привернути увагу керівництва до необхідності створення та функціонування служб гарантії якості.
- ME3 – це процес, який стосується контролю нормативно-правової відповідності, який раніше був передбачений процесом PO8.
- ME4 описує процес нагляду за стратегічним управлінням IT, відповідно до мети стандарту CobiT®, яка полягає у створенні основи для управління IT. Оскільки цей процес є останнім у ланцюжку, він є підсумком внесків, які кожний з процесів ланцюжка вносить у досягнення кінцевої цілі впровадження ефективного стратегічного управління IT на підприємстві.
- В силу вилучення процесу PO8 та необхідності зберегти нумерацію процесів PO9 *«Оцінка ризиків»* (Assess risk) та PO10 *«Управління проектами»* (Manage project), яка узгоджується з 3-м виданням стандарту CobiT®, процесом PO8 став процес, що має назву *«Управління якістю»* (Manage quality), якому відповідає старий процес PO11. Тепер до складу домену PO входить 10 процесів замість 11-ти.
- Домен AI потребував внесення двох видів змін: внесення додаткового процесу, що передбачає здійснення закупівель, та включення в процес AI5 аспектів, пов'язаних з управлінням релізами. В силу останньої зміни, вказаний процес повинен бути останнім у домені AI, тому він став процесом AI7. У проміжок, що утворився на місці процесу AI5, було додатково вставлено новий процес, що описує закупівлі. Тепер до складу домену входять сім процесів замість шести.

Стандарт COBIT 4.1, який є черговою оновленою версією стандарту CobiT® 4.0, містить:

- Розширений загальний огляд.
- Пояснення цілей та метрик у розділі, що стосується структури (методології).
- Більш детальні визначення основних концептуальних положень. Необхідно зауважити, що було внесено зміни у визначення цілей контролю (об'єктів контролю), в якому враховано практику управління.
- Оновлені цілі контролю, які стали результатом вдосконалення практик контролю, та заходи з розробки Val IT. Деякі цілі контролю були об'єднані в групи та/або перефразовані таким чином, щоб уникнути перекриття та створити перелік цілей контролю в межах одного процесу більш послідовним та узгодженим. Ці зміни призвели до зміни нумерації цілей контролю, що залишились. Деякі інші цілі контролю було перефразовано так, що вони стали більш орієнтованими на практичні дії та більш послідовно викладеними. Конкретні виправлення наведені нижче:
  - цілі контролю AI5.5 та AI5.6 було поєднано з ціллю контролю AI5.4
  - цілі контролю AI7.9, AI7.10 та AI7.11 було поєднано з ціллю контролю AI7.8
  - процес ME3 було переглянуто з метою включення відповідності вимогам контрактів на додаток до відповідності законодавчим та нормативним вимогам.
- Механізми контролю прикладних програмних продуктів було змінено з метою підвищення ефективності за рахунок введення заходів з оцінки ефективності заходів контролю та надання звітності. В результаті було створено перелік з шести механізмів контролю прикладних програмних продуктів, які замінили собою перелік з 18 механізмів контролю прикладних програмних продуктів версії CobiT® 4.0, які більш детально описані в документі *«Практики контролю стандарту CobiT, 2-ге видання»* (CobiT® Control Practices, 2nd Edition).
- Перелік бізнес-цілей та IT-цілей в додатку I було оновлено з урахуванням нових даних, отриманих в ході дослідження з метою валідації, проведеного Університетом Школи управління Антверпена (University of Antwerp Management School) (Бельгія).
- Було розширено вкладки, які ілюструють перелік процесів стандарту CobiT®, а також було переглянуто та змінено діаграму із зображенням доменів, в яку були включені посилання на процес та елементи системи контролю прикладних програмних продуктів, передбачених концепцією стандарту CobiT®.
- Уточнення, вказані користувачами стандарту CobiT® (CobiT® 4.0 та CobiT® Online), були проаналізовані та включені в оновлений стандарт належним чином.

ЦІЛІ КОНТРОЛЮ

Як можна побачити з вищевикладеного опису змін до методологічної структури та заходів з уточнення та формування змісту цілей контролю, в результаті оновлення структури стандарту CobiT®, цілі контролю суттєво змінились. Кількість цих елементів зменшилась від 215 до 210, оскільки всі стандартні теми тепер згадуються лише на рівні структури та не

повторюються в кожному процесі. Крім цього, всі посилання на механізми та заходи контролю прикладних програмних продуктів були перенесені в розділ структури, а конкретні цілі контролю були зведені докупи у нових формулюваннях. У наведених нижче двох комплектах таблиць подано перехресні посилання , що пов'язують нові та старі цілі контролю та ілюструють перехід від старих цілей контролю до нових.

КЕРІВНІ ПРИНЦИПИ УПРАВЛІННЯ

Було введено вхідні та вихідні дані (входи та виходи), які показують, що саме потрібно для даного процесу від інших процесів, та які результати зазвичай дають процеси. Також наведено дії та пов'язані з ними обов'язки. Вхідні дані та цілі діяльності замінили собою критичні чинники успіху, які фігурують в 3-му виданні стандарту CobiT®. Тепер метрики ґрунтуються на спадній узгодженій послідовності бізнес-цілей, IT цілей, цілей процесу та цілей діяльності. Метрики 3-го видання стандарту були переглянуті та вдосконалені, що підвищило ступінь їх репрезентативності та вимірюваності.

Перехресні посилання видань СовіТ® 3 та СовіТ® 4.1

СовіТ® 3-тє видання	СовіТ® 4.1
PO1 розробляти стратегічний план IT.	
1.1 IT є частиною довгострокового та короткострокового планів організації	1.4
1.2 Довгостроковий план IT	1.4
1.3 Довгострокове планування IT – підхід та структура	
1.4 Зміни довгострокового плану IT	1.4
1.5 Короткострокове планування роботи IT служби-function	1.5
1.6 Комунікації IT планів	1.4
1.7 Моніторинг та оцінка IT планів	1.3
1.8 Оцінка діючих систем	1.3
PO2 формувати архітектуру інформації.	
2.1 Модель інформаційної архітектури	2.1
2.2 Корпоративний словник даних та правила синтаксису даних	2.2
2.3 Схема класифікації даних	2.3
2.4 Рівні безпеки	2.3
PO4 формувати процеси, організацію та взаємозв'язки для IT	
4.1 Комітет з планування або координації IT	4.3
4.2 Організаційне позиціонування служби IT	4.4
4.3 Аналіз організаційних досягнень	4.5
4.4 Ролі та обов'язки	4.6
4.5 Відповідальність за гарантію якості	4.7
4.6 Відповідальність за логічну та фізичну безпеку	
logical and physical security	4.8
4.7 Власність та відповідальне зберігання	4.9
4.8 Право власності на дані та системи	4.9
4.9 Нагляд	4.10
4.10 Виділення/розділення обов'язків	4.11
4.11 Комплектація IT персоналу	4.12
4.12 Службові обов'язки або посадові інструкції IT персоналу	4.6
4.13 Ключовий IT персонал	4.13
4.14 Політики та процедури для персоналу за контрактом	4.14
4.1 Зв'язки	4.15
PO5 управляти інвестиціями в IT .	
5.1 Річний поточний бюджет IT	5.3
5.2 Моніторинг витрат та вигод	5.4
5.3 Обґрунтування витрат та вигод	1.1, 5.3, 5.4, 5.5
PO6 інформувати про стратегічні цілі керівництва та напрямки розвитку.	
6.1 Позитивне інформаційне контрольне середовище	6.1
6.2 Обов'язки керівництва щодо політик	6.3, 6.4, 6.5
6.3 Комунікації щодо політик організації	6.3, 6.4, 6.5
6.4 Ресурси впровадження політик	6.4
6.5 Підтримання політик в робочому стані	6.3, 6.4, 6.5
6.6 Відповідність політикам, процедурам та стандартам	6.3, 6.4, 6.5
6.7 Зобов'язання щодо якості	6.3, 6.4, 6.5
6.8 Політика щодо безпеки та системи внутрішнього контролю and internal control framework policy	6.2
6.9 Права інтелектуальної власності	6.3, 6.4, 6.5
6.10 Політики з конкретних проблем policies	6.3, 6.4, 6.5
6.11 Комунікації стосовно усвідомлення необхідності захисту IT	6.3, 6.4, 6.5
PO7 управляти персоналом IT.	
7.1 Найм персоналу та просування його по службі	7.1
7.2 Кваліфікація персоналу	7.2
7.3 Ролі та обов'язки	7.4
7.4 Навчання персоналу	7.5
7.5 Навчання суміжним професіям або резерву	7.6
7.6 Процедура перевірки благонадійності персоналу	
7.7 Оцінка результатів роботи персоналу	7.8
7.8 Зміна посади або звільнення	7.8
PO8 управляти якістю	
8.1 Аналіз нормативних вимог	ME3.1
8.2 Практики та процедури відповідності зовнішнім вимогам	ME3.2
8.3 Відповідність вимогам щодо безпеки та ергономіки	ME3.1
8.4 Секретність, інтелектуальна власність та потік даних	ME3.1
8.5 Електронна торгівля	ME3.1
8.6 Відповідність умовам страхових контрактів	ME3.1
PO9 оцінювати та управляти IT-ризиками.	
9.1 Оцінка підприємницького ризику	9.1, 9.2, 9.4
9.2 Підхід до оцінки ризику	9.4
9.3 Ідентифікація ризиків	9.3
9.4 Вимірювання ризику	9.1, 9.2, 9.3, 9.4
9.5 План заходів щодо ризиків action plan	9.5
9.6 Прийняття ризику accep-tance	9.5
9.7 Вибір заходів захисту selection	9.5
9.8 Здійснення оцінки ризиків	9.1
PO10 управляти пректами	
10.1 Концепція управління проектами	10.2
10.2 Участь користувачів у виконанні проектів	10.4
10.3 Склад проектної групи та обов'язки її членів	10.8
10.4 Визначення проекту	10.5
10.5 Затвердження проекту	10.6
10.6 Затвердження етапу проекту	10.6
10.7 Генеральний план проекту	10.7
10.8 План гарантії якості системи	10.10
10.9 Планування методів гарантії якості	10.12
10.10 Формальне управління ризиками проекту	10.9
10.11 Тестовий план	AI7.2
10.12 План навчання	AI7.1
10.13 План перевірки системи після інсталяції	10.14 (part)
PO11 Управління якістю	
11.1 Генеральний план гарантії якості	8.5
11.2 Підхід до гарантії якості	8.1
11.3 Планування гарантії якості	8.1
11.4 Перевірка дотримання IT стандартів та процедур службою гарантії якості	8.1, 8.2

CobiT® 3-тє видання	CobiT® 4.1
11.5 Методологія життєвого циклу розробки системи (SDLC)	8.2, 8.3
11.6 Методологія SDLC внесення основних змін до існуючої технології	8.2, 8.3
11.7 Оновлення методології SDLC	8.2, 8.3
11.8 Координація та комунікації	8.2
11.9 Концепція комплектації та підтримки технологічної інфраструктури	8.2

CobiT® 3-тє видання	CobiT® 4.1
11.10 Стосунки із сторонніми конструкторами	8.2, DS2.3
11.11 Стандарти для документації на програми	AI4.2, AI4.3, AI4.4
11.12 Стандарти тестування програмних продуктів	AI7.2, AI7.4
11.13 Стандарти тестування систем	AI7.2, AI7.4
11.14 Порівняльні/пілотні випробування	AI7.2, AI7.4

CobiT® 3-тє видання	CobiT® 4.1
11.15 Документація щодо тестування системи	AI7.2, AI7.4
11.16 Оцінка служби гарантії якості дотримання стандартів розробки	8.2
11.17 Перевірка службою ГЯ досягнення IT цілей	8.2
11.18 Метрики якості	8.6
11.19 Звіти служби ГЯ про перевірки	8.2

CobiT® 3-тє видання	CobiT® 4.1
AI1 визначати рішення з автоматизації	
1.1 Визначення вимог до інформації	1.1
1.2 Створення альтернативного плану дій	1.3, 5.1, PO1.4
1.3 Формулювання стратегії закупівель	1.3, 5.1, PO1.4
1.4 Вимоги до послуг сторонніх організацій requirements	5.1, 5.3
1.5 Вивчення технологічної здійсненності	1.3
1.6 Техніко-економічне обґрунтування	1.3
1.7 Інформаційна архітектура	1.3
1.8 Звіт про аналіз ризиків	1.2
1.9 Заходи контролю рентабельної системи безпеки	1.1, 1.2
1.10 Розробка контрольних журналів	1.1, 1.2
1.11 Ергономіка	1.1
1.12 Вибір програмного забезпечення системи	1.1, 1.3
1.13 Контроль закупівель	5.1
1.14 Придбання програмного забезпечення	5.1
1.15 Підтримка стороннього ПЗ	5.4
1.16 Прикладне програмування за контрактом programming	5.4
1.17 Приймання приміщень та засобів	5.4
1.18 Приймання технології	3.1, 3.2, 3.3, 5.4
AI2 забезпечувати придбання та підтримку прикладного програмного забезпечення	
2.1 Методи проектування methods	2.1
2.2 Суттєві зміни до існуючих систем	2.1, 2.2, 2.6

CobiT® 3-тє видання	CobiT® 4.1
2.3 Затвердження проекту approval	2.1
2.4 Вимоги до файлів, визначення та документація	2.2
2.5 Специфікації програм	2.2
2.6 Схема накопичення первинних даних	2.2
2.7 IВимоги до входів, визначення та документація	2.2
2.8 Визначення інтерфейсів	2.2
2.9 Інтерфейс користувач-машина	2.2
2.10 Вимоги до обробки даних, визначення та документація	2.2
2.11 Вимоги до виходів, визначення та документація	2.2
2.12 Контрольованість	2.3, 2.4
2.13 Доступність (придатність) як ключовий чинник проекту	2.2
2.14 Засоби забезпечення цілісності IT у прикладному програмному забезпеченні	2.3, DS11.5
2.15 Тестування прикладного програмного забезпечення	2.8, 7.4
2.16 Довідкові та супровідні матеріали для користувача	4.3. 4.4
2.17 Повторна оцінка проекту системи	2.2
AI3 забезпечувати придбання та підтримку технологічної інфраструктури	
3.1 Оцінка нового апаратного та програмного забезпечення	3.1, 3.2, 3.3
3.2 Профілактичний ремонт апаратного забезпечення	DS13.5
3.3 Безпека системного програмного забезпечення	3.1, 3.2, 3.3
3.4 Інсталяція системного програмного забезпечення	3.1, 3.2, 3.3
3.5 Супровід системного програмного забезпечення	3.3

CobiT® 3-тє видання	CobiT® 4.1
3.6 Засоби контролю змін у програмному забезпеченні систем	6.1, 7.3
3.7 Використання та моніторинг системних утиліт	3.2, 3.3, DS9.3
AI4 забезпечувати експлуатацію та використання	
4.1 Експлуатаційні вимоги та рівні обслуговування	4.1
4.2 Посібник з процедур користувача	4.2
4.3 Посібник з експлуатації	4.4
4.4 Учбові матеріали	4.3, 4.4
AI5 закуповувати IT-ресурси	
5.1 Навчання	7.1
5.2 Визначення вимог до експлуатаційних характеристик ПЗ	7.6, DS3.1
5.3 План введення в дію	7.2, 7.3
5.4 Конверсія системи	7.5
5.5 Конверсія даних	7.5
5.6 Стратегії та плани тестування	7.2
5.7 Тестування змін	7.4, 7.6
5.8 Критерії та характеристики порівняльних пілотних тестів	7.6
5.9 Остаточні випробування з приймання	7.7
5.10 Випробування та акредитація системи безпеки	7.6
5.11 Експлуатаційні випробування	7.6
5.12 Введення в експлуатацію	7.8
5.13 Оцінка відповідності вимогам користувачів	7.9
5.14 Перевірка роботи системи керівництвом після впровадження	7.9

CobiT® 3-тє видання	CobiT® 4.1
AI6 управляти змінами.	
6.1 Подання та контроль запитів на зміни	61, 6.4
6.2 Оцінка наслідків	6.2
6.3 Контроль за змінами	7.9
6.4 Аварійні зміни	6.3
6.5 Документація та процедури	6.5
6.6 Санкціонований супровід	DS5.3
6.7 Політика щодо версій ПЗ release policy	7.9
6.8 Розповсюдження ПЗ	7.9

CobiT® 3-тє видання	CobiT® 4.1
DS1 визначати та управляти рівнями надання послуг	
1.1 Концепція угод SLA	1.1
1.2 Аспекти угод SLA	1.3
1.3 Процедури функціонування	1.1
1.4 Моніторинг та звітність	1.5
1.5 Перегляд угод SLA та контрактів	1.6
1.6 Позиції, що підлягають оплаті	1.3
1.7 Програма покращення обслуговування	1.6
DS2 управляти послугами третіх сторін	
2.1 Інтерфейси постачальника	2.1
2.2 Стосунки власників	2.2
2.3 Контракти з третіми сторонами	AI5.2
2.4Кваліфікація сторонніх орг.-ій	AI5.3
2.5 Контракти зі сторонніми орг.-ями	AI5.2
2.6 Безперервність обслуговування	2.3
2.7 Стосунки з питань безпеки	2.3
2.8 Моніторинг	2.4
DS3 управляти ефективністю та потужностями	
3.1 Придатність та вимоги до продуктивності	3.1
3.2 План забезпечення придатності	3.4
3.3 Моніторинг та звітність	3.5
3.4 Інструменти моделювання	3.1
3.5 Управління продуктивністю з упередженням	3.3
3.6 Прогнозування завантаження	3.3
3.7 Управління потужністю ресурсів	3.2
3.8 Придатність ресурсів	3.4
3.9 План використання ресурсів	3.4
DS4 забезпечувати безперервність надання послуг	
4.1 Концепція безперервності IT	4.1
4.2 План безперервності IT, стратегія та філософія	4.1
4.3 Зміст плану безперервності IT послуг	4.2
4.4 Мінімізація вимог до безперервності IT послуг	4.3
4.5 Підтримання плану безперервності IT в робочому стані	4.4
4.6 Тестування плану безперервності IT послуг	4.5
4.7 Навчання з питань плану безперервності IT	4.6
4.8 Поширення плану безперервності IT послуг	4.7
4.9 Резервні процедури альтернативної обробки інформації користувачами	4.8
4.10 Критичні IT ресурси	4.3
4.11 Резервний об'єкт та апаратне забезпечення	4.8
4.12 Резервне сховище поза об'єктом	4.9
4.13 Процедури завершення	4.10
DS5 забезпечувати безпеку систем.	
5.1 Управляти заходами з безпеки	5.1
5.2 Ідентифікація, аутентифікація та доступ	5.3
5.3 Безпека доступу до даних в режимі он-лайн	5.3
5.4 Управління обліковими записами корис	5.4
5.5 Перевірка облікових записів користувачів керівництвом	5.4
5.6 Контроль облікових записів з боку користувачів	5.4, 5.5
5.7 Спостереження за безпекою	5.5
5.8 Класифікація даних	PO2.3
5.9 Централізоване управління ідентифікацією та правами доступу	5.3
5.10 Звіти про порушення безпеки та заходи безпеки	5.5
5.11 Робота з інцидентами	5.6
5.12 Повторна акредитація	5.1
5.13 Довіра до контрагентів	5.3, AC6
5.14 Авторизація тразакцій	5.3
5.15 Неможливість відмови	5.11
5.16 Захищений канал	5.11
5.17 Захист функцій безпеки	5.7
5.18 Управління криптографічними ключами	5.8
5.19 Попередження, виявлення та коригування шкідливого програмного забезпечення	5.9
5.20 Архітектури брандмауеру та підключення до мереж загального користування	5.10
5.21 Захист електронної цінності	13.4
DS6 визначати та розподіляти витрати.	
6.1 Позиції, що підлягають оплаті	6.1
6.2 Калькуляція собівартості	6.3
6.3 Виставлення рахунків користувачам та претензійні платежі	6.2, 6.4
DS7 навчати користувачів.	
7.1 Визначення потреби у навчанні	7.1
7.2 Організація навчання	7.2
7.3 Навчання з основ безпеки та усвідомлення її необхідності	PO7.4
DS8 управляти службою підтримки та інцидентами.	
8.1 Служба технічної підтримки	8.1, 8.5
8.2 Реєстрація запитів користувачів	8.2, 8.3, 8.4
8.3 Ескалація черги користувачів	8.3
8.4 Моніторинг дозволу доступу	10.3
8.5 Звітність та аналіз тенденцій	10.1
DS9 управляти конфігураціями.	
9.1 Реєстрація конфігурації	9.1
9.2 Базова конфігурація	9.1
9.3 Облік статусу	9.3
9.4 Контроль конфігурації	9.3
9.5 Несанкціоноване ПЗ	9.3
9.6 Зберігання програмного З	AI3.4
9.7 Процедури управління конфігурацією	9.2
9.8 Підзвітність щодо ПЗ	9.1, 9.2

CobiT® 3-тє видання	CobiT® 4.1
DS10 управляти проблемами.	
10.1 Система управління проблемами	10.1, 10.2, 10.3, 10.4
10.2 Ескалація проблем	10.2
10.3 Стеження за проблемою та контрольний журнал	8.2, 10.2
10.4 Авторизація аварійного та тимчасового доступу	5.4, 12.3, AI6.3
10.5 Пріоритети обробки даних в аварійних ситуаціях	10.1, 8.3
DS11 управляти даними.	
11.1 Процедури підготовки даних	AC1
11.2 Процедури авторизації документа-джерела	AC1
11.3 Накопичення даних щодо документів-джерел	AC1
11.4 Робота з помилками в документах-джерелах	AC1
11.5 Зберігання документа-джерела	DS11.2
11.6 Процедури авторизації вводу даних	AC2
11.7 Перевірки точності, повноти та авторизації	AC3
11.8 Робота з помилками при введенні даних	AC2, AC4
11.9 Цілісність обробки даних	AC4
11.10 Перевірка правильності та правка при обробці даних	AC4
11.11 Робота зх. помилками при обробці даних	AC4

CobiT® 3-тє видання	CobiT® 4.1
11.12 Обробка вихідних результатів та їх збереження	AC5, 11.2
11.13 розподіл вихідних результатів	AC5, AC6
11.14 Узгодження та співвідошення вихідних даних	AC5
11.15 Аналіз вихідних даних та робота з помилками	AC5
11.16 Забезпечення безпеки звітів щодо вихідних даних	11.6
11.17 Захист конфіденційної інформації при передачі та перенесенні	AC6, 11.6
11.18 Захист утилізованої конфіденційної інформації	11.4, AC6
11.19 Управління зберіганням даних	11.2
11.20 Періоди збереження та строки зберігання	11.2
11.21 Система управління бібліотекою носіїв	11.3
11.22 Обов'язки з управління бібліотекою носіїв	11.3
11.23 Резервування та відновлення даних	11.5
11.24 Завдання з резервування	11.4
11.25 Резервне зберігання	4.9, 11.3
11.26 Архівування	11.2
11.27 Захист секретних повідомлень	11.6
11.28 Аутентифікація та цілісність	AC6

CobiT® 3-тє видання	CobiT® 4.1
11.29 Цілісність електронних транзакцій	5.11
11.30 Безперервна цілісність збережених даних	11.2
DS12 управляти фізичним середовищем.	
12.1 Фізичний захист	12.1, 12.2
12.2 Непомітність об'єкту IT	12.1, 12.2
12.3 Супровід відвідувачів	12.3
12.4 Техніка безпеки персоналу	12.1, 12.5, ME3.1
12.5 Захист від чинників оточуючого середовища	12.4, 12.9
12.6 Безперебійне енергопостачання	12.5
DS13 управляти операційною діяльністю.	
13.1 Операції обробки, процедури та інструкції, посібники	13.1
13.2 Процес пуску в експлуатацію, інші операції, документація	13.1
13.3 Планування завдань	13.2
13.4 Відступлення від стандартних планів завдань	13.2
13.5 Безперервність обробки	13.1
13.6 Журнал обліку операцій	13.1
13.7 Спеціальні форми захисних засобів та пристрої виводу	13.4

CobiT® 3-тє видання	CobiT® 4.1
M1 відстежувати та оцінювати ефективність IT.	
1.1 Накопичення даних моніторингу	1.2
1.2 Оцінка продуктивності	1.4
1.3 Оцінка задоволення клієнтів	1.2
1.4 Звітність керівництву	1.5
M2 відстежувати та оцінювати ефективність внутрішнього контролю.	
2.1 Моніторинг внутрішнього контролю	2.2
2.2 Своєчасність заходів внутрішнього контролю	2.1
2.3 Звітність щодо рівня внутрішнього контролю	2.2, 2.3
2.4 Операційна безпека та гарантія внутрішнього контролю	2.4

CobiT® 3-тє видання	CobiT® 4.1
M3 забезпечувати відповідність зовнішнім нормативним вимогам.	
3.1 Незалежна сертифікація/ акредитація засобів безпеки та внутрішнього контролю IT послуг	2.5, 4.7
3.2 Незалежна сертифікація / акредитація засобів безпеки та внутрішнього контролю сторонніх постачальників послуг	2.5, 4.7
3.3 Незалежна оцінка ефективності IT послуг	2.5, 4.7
3.4 Незалежна оцінка ефективності сторонніх постачальників послуг	2.5, 4.7
3.5 Незалежне підтвердження відповідності законам, нормативним вимогам та умовам контрактів	2.5, 4.7

CobiT® 3-тє видання	CobiT® 4.1
3.6 Незалежне підтвердження відповідності законам, нормативним вимогам та умовам контрактів з боку сторонніх постачальників послуг	2.5, 2.6, 4.7
3.7 Компетенція служби незалежного підтвердження	2.5, 4.7
3.8 Упереджувальне залучення служби аудиту	2.5, 4.7
M4 запровадити систему IT-управління.	
4.1 Статут аудиту	2.5, 4.7
4.2 Незалежність	2.5, 4.7
4.3 Професійна етика та стандарти	2.5, 4.7
4.4 Компетенція	2.5, 4.7
4.5 Планування	2.5, 4.7
4.6 Проведення аудиторських перевірок	2.5, 4.7
4.7 Звітність	2.5, 4.7
4.8 Подальша діяльність	2.5, 4.7

Перехресні посилання документу CobiT® 4.1 на CobiT®, 3-тє видання

CobiT® 4.1	CobiT® 3-тє видання
PO1 розробляти стратегічний план розвитку IT	
1.1 Управління цінністю IT	5.3
1.2 Узгодження питань бізнесу та IT	Нова
1.3 Оцінка поточних потужностей та результатів (продуктивності)	1.7, 1.8
1.4 Стратегічний план IT	1.1, 1.2, 1.3,
1.4, 1.6, AI1.2, AI1.3	
1.5 Тактичні IT плани	1.5
1.6 Управління портфелем IT	Нова
PO2 формувати архітектуру інформації.	
2.1 Модель інформаційної архітектури підприємства	2.1
2.2 Словник бази даних підприємства та правила синтаксису	2.2
2.3 Схема класифікації даних	2.3, 2.4, DS5.8
2.4 Управління цілісністю	Нова
PO3 визначати технологічний напрямок.	
3.1 Планування технологічного напрямку	3.1, 3.3, 3.4
3.2 План технологічної інфраструктури	Нова
3.3 Моніторинг подальших перспектив і нормативних вимог	3.2
3.4 Технологічні стандарти standards	3.5
3.5Рада з питань IT архітектури	3.5
PO4 формувати процеси, організацію та взаємозв'язки для IT	
4.1 Структура IT процесу	Нова
4.2 Комітет з питань IT стратегії	Нова
4.3 Координаційний IT комітет	4.1
4.4 Місце IT служби в організаційній структурі	
placement of the IT function	4.2
4.5 Організаційна структура IT	4.3
4.6 Розподіл ролей та обов'язків	4.4, 4.12
4.7Забезпечення гарантії якості IT	4.5
4.8 Відповідальність за контроль ризиків, безпеку та дотримання вимог	4.6
4.9 Права власності на дані та системи	4.7, 4.8
4.10 Нагляд	4.9
4.11 Розділення обов'язків	4.10
4.12 Комплектація IT персоналом	4.11
4.13 Ключовий IT персонал	4.13
4.14 Політики та процедури щодо працівників за контрактом	4.14
4.15 Взаємозв'язки	4.15
PO5 управляти інвестиціями в IT	
5.1 Схема управління фінансами	Нова
5.2 Встановлення пріоритетів в межах бюджету IT	Нова
5.3 Формування IT бюджету	5.1, 5.3
5.4 Управління витратами	5.2, 5.3
5.5 Управління вигодою	5.3
PO6 інформувати про стратегічні цілі керівництва та напрямки розвитку	
6.1 IT політики та контрольне середовище	6.1
6.2 Внутрішній IT ризик та контрольне середовище	6.8
6.3 Управління політиками в сфері IT	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.4 Введення в дію політик, стандартів та процедур	6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.5 Інформування про IT цілі та напрямок розвитку	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
PO7 управляти персоналом IT.	
7.1 Набір кадрів та їх збереження	7.1
7.2 Компетенція персоналу	7.2
7.3 Розподіл ролей серед персоналу	Нова
7.4 Навчання персоналу	7.3, DS7.3
7.5 Залежність від конкретних фізичних осіб	7.4
7.6 Процедури перевірки благонадійності персоналу	7.5
7.7 Оцінка продуктивності роботи працівника	7.6
7.8 Зміна посади та звільнення з посади	7.7, 7.8
PO8 управляти якістю	
8.1 Система управління якістю	11.2, 11.3, 11.4
8.2 IT стандарти та практики забезпечення якості	11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.16, 11.17, 11.19
8.3 Стандарти розробки та закупівель	11.5, 11.6, 11.7
8.4 Орієнтація на замовника	New
8.5 Постійне вдосконалення	New
8.6 Вимірювання якості, моніторинг та аналіз	11.18
PO9 оцінювати та управляти IT-ризиками .	
9.1 Схема управління IT ризиками	9.1, 9.4, 9.8
9.2 Визначення середовища оцінки ризиків	9.1, 9.4
9.3 Встановлення події	9.3, 9.4
9.4 Оцінка ризику	9.1, 9.2, 9.4
9.5 Реагування на ризик	9.5, 9.6, 9.7
9.6 Підтримка та моніторинг здійснення плану заходів з реагування на ризик	Нова
PO10 управляти проектами	
10.1 Схема управління програмою	Нова
10.2 Схема управління проектами	10.1
10.3 Підхід до управління проектами	Нова
10.4 Активність зацікавлених сторін	10.2
10.5 Викладення обсягу проекту	10.4
10.6 Початок виконання етапу проекту	10.5, 10.6
10.7 Інтегрований план проекту	10.7
10.8 Ресурси проекту	10.3
10.9 Управління ризиками проекту	10.10
10.10 Планування якості проекту	10.8
10.11 Контроль за змінами до проекту	Нова
10.12 Планування методів забезпечення якості в межах проекту	10.9
10.13 Вимірювання, надання даних та моніторинг показників, досягнутих в межах проекту performance measurement, reporting and monitoring	Нова
10.14 Закриття проекту	10.13 (частина)

CobiT® 4.1	CobiT® 3-тє видання
AI1 визначати рішення з автоматизації	
1.1 Визначення та дотримання функціональних та технічних вимог з боку бізнесу	1.1, 1.9, 1.10,
1.11, 1.12	
1.2 Звіт щодо аналізу ризиків analysis report	1.8, 1.9, 1.10
1.3 Техніко-економічне обґрунтування та альтернативні програми дій	1.3, 1.7, 1.12
1.4 Прийняття рішення та схвалення вимог та техніко-економічного обґрунтування	Нова
AI2 забезпечувати придбання та підтримку прикладного програмного забезпечення	
2.1 Проектування високого рівня	2.1, 2.2
2.2 Робочий проект	2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.13, 2.17
2.3 Контроль та контрольованість прикладного ПЗ	2.12, 2.14
2.4 Захист та придатність прикладного ПЗ	2.12
2.5 Конфігурація та введення в дію придбаного прикладного ПЗ	Нова
2.6 Суттєва модернізація існуючих систем upgrades to existing systems	2.2
2.7 Розробка прикладного програмного забезпечення	Нова
2.8 Гарантія якості програмного забезпечення	2.15

CobiT® 4.1	CobiT® 3-тє видання
2.9 Управління вимогами до прикладного ПЗ	Нова
2.10 Супровід прикладного програмного забезпечення	Нова
AI3 забезпечувати придбання та підтримку технологічної інфраструктури	
3.1 План комплектації технологічної інфраструктури	PO3.4, 1.18, 3.1, 3.3, 3.4
3.2 Захист та доступність ресурсів інфраструктури	1.18, 3.1, 3.3, 3.4, 3.7
3.3 Підтримка інфраструктури	1.18, 3.1, 3.3, 3.4, 3.5, 3.7
3.4 Умови для перевірки технічної можливості	Нова
AI4 забезпечувати експлуатацію та використання	
4.1 Планування діяльності з експлуатації рішень	4.1
4.2 Передача знань керівництву бізнес-підрозділів	PO11.11, 4.2
4.3 Передача знань кінцевим користувачам	PO11.11, 2.16, 4.4
4.4 Передача знань персоналу служби підтримки та експлуатаційному персоналу	PO11.11, 2.16, 4.3, 4.4
AI5 закуповувати IT-ресурси.	
5.1 Контроль закупівель	1.2, 1.3, 1.4, 1.13, 1.14
5.2 Управління контрактами з постачальниками	DS2.3, DS2.5
5.3 Вибір постачальників	1.4, DS2.4
5.4 Придбання IT ресурсів	1.15, 1.16, 1.17, 1.18

CobiT® 4.1	CobiT® 3-тє видання
AI6 управляти змінами.	
6.1 Вносити зміни до стандартів та процедур	3.6, 6.1
6.2 Оцінка наслідків внесення змін, встановлення пріоритетів та санкціонування змін	6.2
6.3 Аварійні зміни	DS10.4, 6.4
6.4 Контроль статусу змін та звітність	6.1
6.5 Завершення процесу внесення змін та документація	6.5
AI7 впроваджувати в експлуатацію та проводити акредитацію IT-рішень та змін	
7.1 Навчання	PO10.11, PO10.12, 5.1
7.2 План тестування	PO10.11, PO11.12, PO11.13, PO11.14, PO11.15, 5.3, 5.6
7.3 План введення в дію	3.6, 5.3
7.4 Середовище тестування	PO11.12, PO11.13, PO11.14, PO11.15, 2.15, 5.7
7.5 Конверсія систем та даних	5.4, 5.5
7.6 Тестування змін	5.2, 5.7, 5.8, 5.10, 5.11
7.7 Остаточні випробування з прийомки	5.9
7.8 Введення в експлуатацію	5.12
7.9 Аналіз функціонування системи після інсталяції	5.13, 5.14

CobiT® 4.1	CobiT® 3-тє видання
DS1 визначати та управляти рівнями надання послуг	
1.1Управляти продуктивністю та потужностями послуг	1.1, 1.3
1.2 Визначення послуг	Нова
1.3 Угоди про рівень надання послуг (SLA)	1.2, 1.6
1.4 Угоди про надання послуг на операційному рівні (OLA)	Нова
1.5 Моніторинг та звітність щодо досягнення рівнів надання послуг	1.4
1.6 Перегляд угод про рівень надання послуг та контрактів	1.5, 1.7

CobiT® 4.1	CobiT® 3-тє видання
DS2 управляти послугами третіх сторін	
2.1 Встановлення взаємовідносин з усіма постачальниками	2.1
2.2 Управління взаємовідносинами з постачальниками	2.2
2.3 Управління ризиками постачальників	PO11.10, 2.6, 2.7
2.4 Моніторинг якості роботи постачальників послуг	2.8
DS3 управляти ефективністю та потужностями	
3.1 Планування продуктивності та потужностей	AI5.2, 3.1, 3.4
3.2 Поточні показники продуктивності та потужностей	3.7

CobiT® 4.1	CobiT® 3-тє видання
3.3 Перспективні показники продуктивності та потужностей	3.5, 3.6
3.4 Придатність IT ресурсів	3.2, 3.8, 3.9
3.5 Моніторинг та звітність	3.3
DS4 забезпечувати безперервність надання послуг	
4.1 Концепція безперервності IT послуг	4.1, 4.2
4.2 Плани безперервності IT послуг	4.3
4.3 Критичні IT ресурси resources	4.4, 4.10
4.4 Підтримка плану забезпечення безперервності IT послуг на належному рівні	4.5

CobiT® 4.1	CobiT® 3-тє видання
4.5 Тестування плану забезпечення безперервності IT послуг	4.6
4.6 Навчання з питань плану безперервності IT послуг	4.7
4.7 Розповсюдження плану забезпечення безперервності надання IT послуг	4.8
4.8 Відновлення процесу надання IT послуг services recovery and resumption	4.9, 4.11
4.9 Резервні засоби зберігання даних поза об'єктом backup storage	4.12, 11.25
4.10 Аналіз функціонування системи після відновлення	4.13
DS5 забезпечувати безпеку систем.	
5.1 Управління безпекою IT	5.1, 5.12
5.2 План забезпечення безпеки IT	Нова
5.3 Управління ідентифікаційною інформацією	5.2, 5.3, 5.9, 5.14, AI6.6
5.4 Управління обліковими записами користувача	5.4, 5.5, 5.6, 5.13, 10.4
5.5 Тестування системи безпеки, нагляд та моніторинг її функціонування	5.6, 5.7, 5.10
5.6 Визначення поняття інциденту в системі безпеки incident definition	5.11
5.7 Захист технології забезпечення безпеки	5.17
5.8 Управління криптографічними ключами	5.18
5.9 Попередження проникнення шкідливого ПЗ, виявлення його та вжиття коригувальних заходів	5.19
5.10 Безпека мережі	5.20
5.11 Обмін конфіденційними даними	5.15, 5.16 11.29, 13.8
DS6 визначати та розподіляти витрати.	
6.1 Визначення послуг	6.1
6.2 Ведення обліку та звітності IT	6.3
6.3 Створення моделі витрат та нарахування витрат	6.2
6.4 Підтримка моделі витрат	6.3
DS7 навчати користувачів .	
7.1 Визначення потреб у навчанні та проведенні інструктажу	7.1
7.2 Проведення навчання та інструктажу	7.2
7.3 Оцінка результатів проведеного навчання	Нова
DS8 управляти службою підтримки та інцидентами	
8.1 Служба технічної підтримки	8.1
8.2 Реєстрація запитів замовників	8.2, 10.3
8.3 Ескалація інцидентів	8.2, 8.3, 10.5
8.4 Закриття інциденту	8.2
DS9 управляти конфігураціями.	
9.1 Репозиторій даних конфігурації та базова конфігурація	9.1, 9.2, 9.8
9.2 Визначення елементів конфігурації та підтримка їх в робочому стані	9.7, 9.8
9.3 Аналіз цілісності конфігурації	9.3, 9.4, 9.5
DS9 управляти конфігураціями.	
9.1 Репозиторій даних конфігурації та базова конфігурація	9.1, 9.2, 9.8
9.2 Визначення елементів конфігурації та підтримка їх в робочому стані	9.7, 9.8
9.3 Аналіз цілісності конфігурації	9.3, 9.4, 9.5
DS10 Управляти проблемами	
10.1 Ідентифікація та класифікація проблем	8.5, 10.1, 10.5
10.2 Відстеження та врегулювання проблем	Нова
10.3 Закриття проблеми	8.4, 10.1
10.4 Інтеграція процесів управління конфігурацією, інцидентами та проблемами	Нова, 10.1
DS11 Управляти даними.	
11.1 Бізнес-вимоги до управління даними	Нова
11.2 Механізми зберігання та запам'ятовування інформації	11.12, 11.19, 11.20, 11.26, 11.30
11.3 Система управління бібліотекою носіїв інформації	11.21, 11.22, 11.25
11.4 Утилізація	11.18, 11.24
11.5 Резервування та відновлення and restoration	AI2.14, 11.23
11.6 Вимоги до безпеки при управлінні даними	11.16, 11.17, 11.27
DS12 Управляти фізичним середовищем.	
12.1 Вибір місця розташування та схема	12.1, 12.2, 12.4
12.2 Заходи фізичного захисту	12.1, 12.2
12.3 Фізичний доступ	10.4, 12.3
12.4 Захист від чинників зовнішнього середовища	12.5
12.5 Управління фізичними засобами	12.4, 12.6, 12.9
DS13 управляти операційною діяльністю	
13.1 Процедури та інструкції, що стосуються операцій	13.1, 13.2, 13.5, 13.6
13.2 Календарне планування робіт	13.3, 13.4
13.3 Моніторинг IT інфраструктури	Нова
13.4 Документи, які потребують захисту, та пристрої виводу даних	5.21, 13.7
13.5 Профілактичне техобслуговування апаратного забезпечення	AI3.2

CobiT® 4.1	CobiT® 3-тє видання
ME1 відстежувати та оцінювати ефективність IT	
1.1 Концепція моніторингу	1.0*
1.2 Визначення та накопичення даних моніторингу	1.1, 1.3
1.3 Метод моніторингу	Нова
1.4 Оцінка продуктивності	1.2
1.5 Звітність для Ради директорів та виконавчого керівництва	1.4
1.6 Коригувальні заходи	Нова
ME2 відстежувати та оцінювати ефективність внутрішнього контролю	
2.1 Моніторинг системи внутрішнього контролю	2.0*, 2.2
2.2 Перевірка в порядку нагляду	2.1, 2.3
2.3 Виключні ситуації в системі контролю	Нова
2.4 Самооцінка контролю	2.4

CobiT® 4.1	CobiT® 3-тє видання
2.5 Гарантія адекватності внутрішнього контролю	Нова
2.6 Система внутрішнього контролю у третіх осіб	3.6
2.7 Коригувальні заходи	Нова
ME3 забезпечувати відповідність зовнішнім нормативним вимогам	
3.1 Визначення законодавчих, регулятивних та договірних вимог, яких необхідно дотримуватись	PO8.1, PO8.3, PO8.4, PO8.5, PO8.6, DS12.4
3.2 Оптимізація реагування на зовнішні вимоги	PO8.2
3.3 Оцінка відповідності зовнішнім вимогам	Нова
ME3 забезпечувати відповідність зовнішнім нормативним вимогам	
3.1 Визначення законодавчих, регулятивних та договірних вимог, яких необхідно дотримуватись	PO8.1, PO8.3, PO8.4, PO8.5, PO8.6, DS12.4

CobiT® 4.1	CobiT® 3-тє видання
3.2 Оптимізація реагування на зовнішні вимоги	PO8.2
3.3 Оцінка відповідності зовнішнім вимогам	Нова
3.4 Позитивне підтвердження відповідності вимогам	Нова
3.5 Інтегрована система звітності	Нова
ME4 запровадити систему IT-управління	
4.1 Впровадження системи управління IT	Нова
4.2 Відповідність на стратегічному рівні	Нова
4.3 Забезпечення цінності	Нова
4.4 Управління ресурсами	Нова
4.5 Управління ризиками	Нова
4.6 Оцінка продуктивності	Нова
4.7 Незалежне підтвердження	Нова

Додаток VI

Стратегія наукових досліджень та розробки

Додаток VI—Стратегія наукових досліджень та розробки

Розробка змісту концептуального ядра (методології) стандарту CobiT® здійснюється під керівництвом Координаційного комітету CobiT® (CobiT® Steering Committee), інтернаціональної команди, до складу якої увійшли співробітники державних установ та комерційних підприємств, учбових закладів та фірм, які спеціалізуються у сфері корпоративного управління IT, гарантії якості, контролю та забезпечення безпеки. Були створені інтернаціональні робочі групи, які мають забезпечувати гарантію якості та давати експертну оцінку проміжним дослідженням в межах даного проекту та визначати результати. Глобальне керівництво проектом здійснює Інститут управління IT (ITGI).

ПОПЕРЕДНІ ВИДАННЯ СТАНДАРТУ CobiT®

У першій версії методології CobiT®, що викладена у першому виданні, в результаті застосування міжнародних стандартів, основоположних принципів та вивчення найкращих практик, було розроблено цілі контролю. Після цього було розроблене керівництво з аудиту, яке дозволяло оцінити чи були належним чином реалізовані цілі (завдання) контролю. Збір матеріалу для першого та другого видань передбачав підбір та аналіз певних інтернаціональних джерел, він був проведений робочими групами в Європі (Амстердамський вільний університет, Free University of Amsterdam), Сполучених Штатах Америки (Політехнічний університет штату Каліфорнія, California Polytechnic University) та в Австралії (Університет Нового Південного Уельсу, University of New South Wales). Дослідникам було доручено здійснити технічну компіляцію, аналіз, оцінку та відповідне включення міжнародних стандартів, кодексів поведінки, стандартів якості, професійних стандартів з аудиту, а також галузевих практик та вимог в частині, що стосується методології та окремих цілей контролю. Після накопичення матеріалу та його аналізу дослідники мали глибоко вивчити кожний домен і процес та запропонувати нові або модифіковані цілі контролю, застосовні до даного конкретного IT процесу. Узагальнення отриманих результатів здійснював Координаційний комітет CobiT® (CobiT® Steering Committee).

Проект зі створення 3-го видання стандарту CobiT® передбачав розробку основоположних принципів корпоративного управління та оновлення 2-го видання стандарту CobiT® з урахуванням нових та переглянутих міжнародних стандартів. Крім того, було переглянуто та вдосконалено методологію (концептуальне ядро) стандарту CobiT з метою сприяння підвищенню контролю з боку керівництва, введення управління продуктивністю та подальшого розвитку корпоративного управління IT. Для того, щоб керівництво могло застосовувати цю методологію для оцінки та впровадження заходів контролю та посилення управління інформаційними та суміжними технологіями, а також вимірювати продуктивність, основоположні принципи управління містять моделі зрілості, критичні чинники успіху, ключові індикатори цілей (KGI) та ключові індикатори продуктивності (KPI), пов'язані з цілями контролю.

Основоположні принципи управління розроблялись за участі міжнародної команди із 40 експертів – працівників учбових закладів, державних установ, спеціалістів з управління IT, гарантії якості, контролю та забезпечення безпеки. Вказані спеціалісти взяли участь у місцевому семінарі, керованому професійними координаторами, при цьому вони користувались принципами розробки, визначеними Координаційним комітетом CobiT. Вказаний семінар отримав суттєву підтримку з боку компаній Gartner Group та PricewaterhouseCoopers, які не тільки забезпечили інтелектуальне лідерство, а й надіслали кілька своїх експертів з питань контролю, управління продуктивністю та інформаційної безпеки. Результатом цього семінару стала розробка проектів моделей зрілості, критичних чинників успіху (CSF), ключових індикаторів цілей (KGI) та ключових індикаторів продуктивності (KPI) для кожного з 34 процесів стандарту CobiT®. Гарантія якості початкових і кінцевих результатів здійснювалась Координаційним комітетом CobiT (CobiT® Steering Committee), а результати були розміщені на сайті ISACA. В документі з основоположними принципами управління було запропоновано новий набір інструментів, орієнтованих на управління, з одночасною їх інтеграцією та узгодженням з методологією стандарту CobiT®.

Уточнення цілей контролю у 3-му виданні стандарту CobiT® на основі нових та переглянутих міжнародних стандартів здійснювалось членами відділень організації ISACA під керівництвом членів Координаційного комітету CobiT (CobiT® Steering Committee). Ми не мали наміру здійснити глобальний аналіз всього матеріалу або переробки цілей контролю, метою було здійснення поетапного процесу оновлення. Результати розробки основоположних принципів управління надалі були використані для перегляду методології стандарту CobiT®, зокрема, в частині принципів, цілей та формулювань опису процесів. 3-тє видання стандарту CobiT® було опубліковане в липні 2000 року.

НАЙНОВІШІ ОНОВЛЕННЯ В МЕЖАХ ПРОЕКТУ

Намагаючись постійно оновлювати основний обсяг знань, що міститься в стандарті CobiT®, Координаційний комітет CobiT (CobiT® Steering Committee) протягом останніх двох років проводив дослідження у декількох конкретних напрямках стандарту CobiT®. Вказані цілеспрямовані дослідницькі проекти передбачали розгляд елементів цілей контролю та основоположних принципів управління. Нижче наведені деякі конкретні напрямки дослідження.

Дослідження цілей контролю

• Стандарт СовіТ®— управління ІТ, розміщення за принципом «знизу – наверх»
• Стандарт СовіТ®—управління ІТ, розміщення за принципом «зверху – донизу»
• Стандарт СовіТ® та інші детальні стандарти—Детальна відповідність між стандартом СовіТ® та ITIL, CMM, COSO, PMBOK, ISF's *«Стандартом найкращих практик у сфері інформаційної безпеки»* (Standard of Good Practice for Information Security) організації ISF та стандартом ISO 27000 з метою забезпечення гармонізації з вказаними стандартами з точки зору мови, визначень та концепцій.

Дослідження основоположних принципів управління

- Аналіз причинних взаємозв'язків ключових індикаторів цілей (KGI) та ключових індикаторів продуктивності (KPI) (KGI-KPI).
- Аналіз якості показників KGI/KPI/CSF— На основі результатів аналізу причинних взаємозв'язків ключових індикаторів цілей (KGI) та ключових індикаторів продуктивності (KPI), розділення критичних чинників успіху (CSF) на категорії «що вам потрібно від інших» та «що вам необхідно зробити самостійно».
- Детальний аналіз концепцій метрик — Детальна розробка експертів з питань метрик з метою поглиблення концепцій метрик, побудови каскаду метрик «процес – ІТ – бізнес» та визначення критеріїв оцінки якості метрик.
- Встановлення зв'язку між бізнес-цілями, ІТ цілями та ІТ процесами – Детальне дослідження, проведене у восьми різних галузях, результатом якого стало поглиблене розуміння того, як процеси стандарту СовіТ® сприяють досягненню конкретних ІТ цілей, а також, відповідно, реалізації бізнес-цілей; надалі результати були узагальнені.
- Аналіз змісту моделей зрілості — Гарантована якість та узгодженість рівнів зрілості між процесами та в їх межах, в тому числі вдосконалені визначення ознак, за якими будуються моделі зрілості.

Всі вказані проекти були ініційовані та контролювались Координаційним комітетом СовіТ® (СовіТ® Steering Committee), хоча поточне керівництво та нагляд здійснювала мало чисельна група ключових спеціалістів розробки стандарту СовіТ®. Реалізація більшості вищезазначених дослідницьких проектів здійснювалась в основному на базі досвіду та зусиль групи добровольців з організації ISACA, користувачів стандарту СовіТ®, компетентних консультантів та працівників учбових закладів. Місцеві групи розробників були створені в Брюсселі (Бельгія), Лондоні (Англія), Чікаго (штат Іллінойс, США), Канберрі (Територія федеральної столиці), Кейптауні (Південна Африка), Вашингтоні (округ Колумбія США) та Копенгагені (Данія), у складі яких від п'яти до десяти користувачів стандарту СовіТ® збирались у середньому два-три рази на рік, щоб попрацювати над конкретними дослідженнями або аналізом завдань, поставлених основною групою розробників стандарту СовіТ. Крім цього деякі конкретні дослідницькі проекти були завданням таких шкіл бізнесу, як Школа менеджменту Університету Антверпена (University of Antwerp Management School (UAMS)) та Університету Гавайїв (University of Hawaii.)

Результати цієї дослідницької роботи та зворотного зв'язку з користувачами стандарту СовіТ®, а також питання, що постали при розробці нових продуктів, таких як практики контролю, були використані як вхідні дані при реалізації основного проекту розробки СовіТ для оновлення та вдосконалення цілей контролю СовіТ®, основоположних принципів управління та методології стандарту. Було засновано дві головні лабораторії з розробки, в кожній з яких працювало більш як 40 спеціалістів з питань корпоративного управління ІТ, менеджменту та контролю (менеджери, консультанти, працівники учбових закладів та аудитори) з усього світу, з метою перегляду та ретельного вдосконалення цілей контролю та змісту основоположних принципів управління. Додаткові невеликі групи спеціалістів працювали над вдосконаленням або завершенням основних кінцевих результатів, отриманих від вказаних основних закладів.

Остаточний проект пройшов процедуру розгляду за участю більш як 100 спеціалістів. Отримані в результаті цього, коментарі та зауваження було проаналізовано в ході робочого засідання з остаточного розгляду проекту Координаційним комітетом СовіТ (СовіТ® Steering Committee).

Результати роботи вказаних робочих засідань були оброблені Координаційним комітетом проекту СовіТ, основною групою розробників стандарту та Інститутом управління ІТ з метою створення нового наповнення стандарту СовіТ, представленого в даному документі. Наявність СовіТ® Online означає, що тепер існує технологія, яка дає змогу полегшити оновлення основного змісту стандарту СовіТ®, цей ресурс буде використовуватись як головний репозиторій контенту стандарту СовіТ®. Він буде підтримуватись завдяки зворотному зв'язку з базою користувачів, а також періодичному перегляду конкретних частин контенту. Будуть здійснюватись періодичні публікації (в паперовому та електронному вигляді) на підтримку звернень до контенту стандарту СовіТ в режимі офлайн.

Додаток VII

Глосарій

Додаток VII—Глосарій

Контроль доступу (access control) — процес, який обмежує та контролює доступ до ресурсів комп'ютерної системи; логічний або фізичний контроль, створений для захисту проти несанкціонованого входу до комп'ютерної системи, або її використання.

Особа, котрій звітують (accountable) — на RACI-матриці означає особу, або групу осіб, які володіють повноваженнями затверджувати до виконання або приймати результати здійсненних заходів.

Дії (activity) — основні заходи, вжиті для здійснення того чи іншого процесу CobiT®.

Прикладна програма (Application program) — Програма, що здійснює обробку бізнес-даних, а саме введення даних, оновлення або запит. Вона відрізняється від системних програм, таких як операційна система або програма по забезпеченню контролю мережі, та від програм-утілітів, таких як, програми для копіювання або сортування файлів.. . . . . .

Статут аудиту (Audit charter) — Документ, затверджений Радою директорів, у якому визначено ціль, повноваження та обов'язки щодо здійснення заходів в області внутрішнього аудиту.

Аутентифікація (Authentication) — процедура перевірки ідентичності суб'єкта комп'ютерної системи (наприклад, користувача, системи, вузла мережі) та правомірності його доступу до комп'ютерної інформації. Незважаючи на те, що аутентифікація призначена для захисту від несанкціонованого входу до системи, вона також може використовуватись для перевірки коректності певного набору даних.

Автоматизовані контролі на рівні прикладних програм — сукупність засобів контролю, інтегрованих в автоматизовані рішення (програмні продукти).

Система збалансованих показників (Balanced scorecard) — узгоджений набір показників ефективності, згрупованих в 4 категорії. Система включає як традиційні фінансові показники, так і показники, які стосуються клієнтів, внутрішніх бізнес-процесів, навчання та перспектив росту. Система була розроблена Робертом С. Капланом та Девідом П. Нортоном у 1992 році.

Порівняльний аналіз (Benchmarking) — Систематизований підхід до порівняння результатів діяльності організації з результатами діяльності схожих організацій та конкурентів, з метою вдосконалення діяльності організації (наприклад, бенчмаркінг якості, ефективності роботи логістичної функції та ін.).

Найкраща практика (Best practice) — Загальновизнана дія або процес, що успішно використовується багатьма організаціями.

Бізнес-процес (Business process) — Дивись визначення терміну «Процес».

Здатність/здібність (Capability) — наявність необхідних атрибутів для виконання тих чи інших заходів

Модель зрілості процесів CMM (Capability Maturity Model (CMM)) — Модель зрілості процесів розробки програмного забезпечення, створена Інститутом програмної інженерії (Software Engineering Institute (SEI). Модель, яка використовується багатьма організаціями для ідентифікації найкращих практик, що допомагають оцінити та підвищити рівень зрілості процесів розробки програмного забезпечення

CEO — Вища посадова особа в організації (Chief executive officer).

CFO — Фінансовий директор (Chief financial officer); посадова особа, яка несе відповідальність за управління фінансами в організації.

CIO — Директор з інформаційних технологій (Chief information officer); посадова особа, яка несе відповідальність за роботу IT служби в організації. В деяких випадках обов'язки CIO можуть бути розширені до рівня Директора з управління знаннями (Chief knowledge officer (CKO)), який має справу із сукупністю знань, а не тільки з інформацією. Дивись також визначення терміну "CTO" (Chief technology officer).

CTO — Директор з технологій/Технічний директор (Chief technology officer); посадова особа, яка визначає технічну/технологічну політику.

Конфігураційна одиниця (Configuration item (CI)) — компонент інфраструктури або елемент (наприклад, запит на

впровадження, зміни, пов'язані з інфраструктурою), що знаходиться (або має знаходитись) під контролем процеса управління конфігурацією. Конфігураційні одиниці можуть суттєво відрізнятися за складністю, розміром та типом, починаючи від цілої системи (включаючи все програмне та апаратне забезпечення, а також документацію), і закінчуючи окремим модулем або незначним апаратним

Управління конфігурацією (Configuration management) — контроль за змінами, що вносяться у сукупності конфігураційних одиниць впродовж життєвого циклу системи

Особа, з якою необхідно консультуватись (Consulted) — на RACI – матриці означає тих осіб, до яких звертаються за порадою при виконанні тих чи інших дій (двостороння комунікація)

Безперервність (Continuity)—запобігання, зменшення наслідків та відновлення після збоїв. В цьому контексті також можна використовувати терміни «план відновлення діяльності» (business resumption planning'), «план відновлення після аварій/ стихійного лиха» ('disaster recovery planning') та «план на випадок непередбачуваних обставин» ('contingency planning'), оскільки всі вони стосуються аспектів відновлення діяльності.

Система контролю (Control framework) — сукупність базових засобів контролю, що допомагають власнику бізнес-процесу попередити фінансові втрати або витік інформації в організації.

Ціль контролю (Control objective) — визначення бажаного результату або мети, якої необхідно досягти в результаті виконання процедур контролю в рамках того чи іншого процесу..

Практика контролю (Control practice) — ключовий механізм контролю, який сприяє досягненню цілей контролю шляхом відповідального використання ресурсів, належного управління ризиками та узгодження роботи служби IT з потребами бізнесу

COSO — Комітет спонсорських організацій Комісії Тредуея (Committee of Sponsoring Organisations of the Treadway Commission). Його звіт 1992 року «Внутрішній контроль – Інтегрована сиситема» (Internal Control—Integrated Framework) є міжнародно-прийнятим стандартом корпоративного управління. Дивись також сайт www.coso.org

CSF — критичний фактор успіху (Critical success factor); найбільш важливі завдання або дії керівництва, які воно має виконати для забезпечення контролю над та в межах IT процесів

Інструментальна панель (Dashboard) — інструмент для встановлення очікувань від організації на кожному рівні відповідальності та постійного моніторингу результатів її діяльності у порівнянні з встановленими цільовими показниками

Схема класифікації даних (Data classification scheme) — схема, що застосовується в масштабах всієї організації для класифікації даних за такими ознаками, як критичність, чутливість та приналежність до власника.

Словник даних (Data dictionary) — база даних, яка містить інформацію про ім'я, тип, діапазон значень, джерело та критерії доступу до кожного елементу даних, що міститься в ній

Власники даних (Data owners) — Посадові особи, як правило, менеджери або директори, які несуть відповідальність за цілісність, точну звітність та використання цифрових даних

Контроль виявлення (Detective control) — засіб контролю, який застосовується для виявлення подій (небажаних або бажаних), помилок та інших випадків, які, з точки зору організації, суттєво впливають на процес або кінцевий продукт

Домен (Domain) — В стандарті CobiT® означає об'єднання цілей контролю в групи, які відповідають логічним етапам життєвого циклу IT в рамках здійснення інвестицій в IT («Планування та організація», « Придбання та впровадження», «Експлуатація та супроводження», «Моніторинг та оцінка»).

Підприємство (Enterprise) — Група фізичних осіб, які працюють разом над досягненням спільної мети в рамках єдиної організації (корпорації, державної установи, благодійної організації або трастового фонду)

Архітектура підприємства (Enterprise architecture) — опис базової структури компонентів бізнес-системи або одного з її елементів (наприклад, технології), взаємозв'язків між ними та способу, у який вони сприяють реалізації цілей організації.

IT архітектура підприємства (Enterprise architecture for IT) — опис базової структури IT компонентів бізнесу, взаємозв'язків між ними та способу, у який вони сприяють реалізації цілей організації

Корпоративне управління (Enterprise governance) — набір повноважень, обов'язків та комплекс заходів, що виконуються Радою директорів та керівництвом з метою забезпечення реалізації стратегічних планів розвитку, реалізації цілей, належного управління ризиками та відповідального використання ресурсів.

Система (Framework) — Дивись визначення терміну «Система контролю» (Control framework).

Загальні засоби контролю комп'ютерних систем (General computer controls) — засоби контролю (відмінні від автоматизованих контролів на рівні прикладних програм), які відносяться до середовища, в якому розробляються, обслуговуються та експлуатуються комп'ютерні прикладні системи. Таким чином, ці засоби контролю застосовуються до всіх прикладних програмах. Призначення загальних засобів контролю полягає у забезпеченні належної розробки та впровадження прикладних програм, цілісності даних та комп'ютерних операцій. Подібно до автоматизованих контролів на рівні прикладних програм, загальні засоби контролю можуть бути або ручними, або автоматизованими. Приклади загальних засобів контролю включають розробку та впровадження стратегії і політики безпеки інформаційних систем (IS), організацію роботи персоналу, що працює з інформаційними системами, яка передбачає розділення несумісних обов'язків, а також планування заходів з попередження збоїв та відновлення роботи систем.

Посібник (guideline) — опис конкретного способу виконання того чи іншого завдання, який носить менш директивний характер, аніж процедура.

Інформаційна архітектура (information architecture) — один із компонентів IT архітектури (разом з прикладними програмами та технологіями). Дивись визначення терміну «IT архітектура».

Особа, яку необхідно інформувати (informed) — на RACI-матриці означає тих осіб, яких потрібно своєчасно інформувати про прогрес у виконанні тих чи інших завдань (одностороння комунікація).

Внутрішній контроль (internal control) — політики, плани та процедури, а також організаційні структури, призначені для забезпечення прийнятного рівня впевненості у досягненні бізнес-цілей, а також для попередження, або виявлення та коригування наслідків небажаних подій

Стандарт ISO 17799 (information technology - security techniques - code of practice for information security management) — міжнародний стандарт, в якому визначені заходи контролю конфіденційності, цілісності та доступності інформації.

Стандарт ISO 27001 (information technology -- security techniques -- information security management systems – requirements) — *«Управління інформаційною безпекою – Вимоги»*; заміняє собою стандарт BS7799-2. Стандарт ISO 27001 використовується для формування методологічної основи для проведення зовнішнього аудиту, приведений у відповідність з іншими стандартами управління, такими як ISO/IEC 9001 та 14001.

Стандарт ISO 9001:2000 – звід практик по управлінню якістю, створений міжнародною організацією з питань стандартизації (International Organisation for Standardisation (ISO)). Стандарт, у якому визначені вимоги до системи управління якістю в організації, яка повинна демонструвати свою здатність до створення продуктів або надання послуг, що відповідають конкретним показникам якості.

IT (information technology) — інформаційні технології; апаратне забезпечення, програмне забезпечення, комунікаційні та інші засоби, що використовуються для вводу, збереження, обробки, передачі та виводу інформації у будь-якій формі.. .

IT архітектура (IT architecture) — базова опис структури IT компонентів в рамках організації, взаємозв'язків між ними та способу, у який вони сприяють реалізації цілей організації.

ITIL (IT Infrastructure Library) — бібліотека IT інфраструктури, створена Державним Агенством торгівлі Великобританії (The UK Office of Government Commerce (OGC); набір методик управління та надання IT послуг

IT інцидент (IT incident) — будь-яка подія, що не є частиною звичайного процесу надання послуги, яка спричиняє або може спричинити перерву у наданні послуги або зниження якості її надання (відповідно до ITIL).

Інструментальна панель інвестицій в IT (IT investment dashboard) — інструмент для формування очікувань від організації на кожному рівні та постійного моніторингу результатів діяльності у порівнянні з встановленими плановими показниками щодо витрат та віддачі від реалізації інвестиційних проектів в IT з точки зору їх цінності для бізнесу.

Стратегічний план розвитку IT (IT strategic plan) — довгостроковий план, терміном на 3 - 5 років, у якому керівництво бізнес-підрозділів та IT служби спільно визначають, у який спосіб інформаційні технології сприятимуть реалізації стратегічних цілей організації.

Комітет з питань IT стратегії (IT strategy committee) — комітет, що діє на рівні Ради директорів та забезпечує залучення Ради директорів до розгляду та прийняття рішень стосовно основних питань у сфері IT. Цей комітет несе відповідальність за управління портфелями інвестицій в IT, управління IT послугами та ресурсами і є власником портфелю інвестицій в IT.

Тактичний план розвитку IT (IT tactical plan) — середньостроковий план, терміном 6 - 18 місяців, в якому стратегічний план розвитку IT представлено у вигляді необхідних ініціатив, ресурсів, засобів моніторингу їх використання та управління вигодами.

Користувач IT (IT user) — Особа, яка використовує IT для досягнення тієї чи іншої бізнес-цілі.

Ключові практики управління (Key management practices) — практики, необхідні для успішного управління та виконання бізнес-процесів.

KGI—ключовий індикатор досягнення цілі (Key goal indicator); показник, призначений для керівництва, який свідчить про те, чи реалізував IT процес поставлені перед ним бізнес-вимоги; як правило, виражається у термінах інформаційних критеріїв.

KPI—ключовий індикатор ефективності (Key performance indicator); показник, який визначає наскільки виконується процес для реалізації цілі. Ці показники є основними індикаторами того, чи буде досягнута ціль. Вони оцінюють ті дії, що має виконати власник процесу для забезпечення ефективного виконання процесу.

Рівень зрілості (Maturity)— вказує на рівень надійності або залежності організації щодо можливість бізнес-процесу досягти
бажаних цілей

Показник вимірювань (Measure) — критерій, який використовується для проведення оцінки та інформування щодо досягнення очікуваних результатів діяльності. Показники вимірювань, як правило, є кількісними за характером, вони виражаються у цифрах, грошових одиницях, відсотках тощо, але можуть також мати якісний характер, наприклад, ступінь задоволення користувача. відслідковування та звітування цих показників допомагає організації успішно та ефективно реалізовувати свою стратегію

Метрики (Metrics) — конкретні описи того, як саме потрібно здійснювати кількісну та періодичну оцінку результатів діяльності. Повноцінна метрика включає одиницю та частоту вимірювання, плановий показник, процедури проведення вимірювань та інтерпретації результатів оцінювання

OLA — угода про надання послуг на операційному рівні (Operational level agreement); внутрішня угода, яка регламентує надання послуг, спрямованих на підтримку IT організації у наданні послуг.

Організація (Organisation) — посіб, у який побудована організаційна структура організації; може також означати «підприємство».

Показники вимірювань кінцевих результатів (Outcome measures) — Критерії, які відображають наслідки раніше вжитих заходів, які часто називають індикаторами відставання (lag indicators), оскільки їх можна вимірювати тільки лише після завершення діяльності,тому їх називають індикаторами відставання. Вони часто орієнтовані на результати, отримані наприкінці звітного періоду та характеризують ефективність в рамках попередніх періодів. Їх також називають Ключовими індикаторами досягнення цілі (KGI) та використовують для демонстрації того, чи були досягнуті цілі.

Ефективність (Performance) — в сфері IT це фактичне впровадження або виконання процесу.

Чинники ефективності (Performance drivers) — показники, які вважаються «чинниками ефективності» індикаторів відставання. Їх можна вимірювати до моменту отримання кінцевого результату, тому їх називають «індикаторами випередження». Існує певний взаємозв'язок між цими двома індикаторами, який полягає у припущенні того, що підвищена ефективність, зафіксована індикатором випередження, позитивно впливатиме на показник індикатора відставання. Їх також називають ключовими індикаторами ефективності (KPI), які застосовуються для демонстрації того, чи будуть реалізовані цілі.

Управління ефективністю (Performance management) — в у сфері IT це здатність до управління будь-якими показниками, в тому числі й тими, що стосуються працівників, підрозділів, процесів, операційної та фінансової діяльності.

PMBOK—посібник знань з питань управління проектами (Project Management Body of Knowledge); стандарт управління проектами, розроблений Інститутом по управлінню проектами (Project Management Institute (PMI)).

PMO — відповідальний за управління проектами (Project management officer); окрема служба, яка несе відповідальність за підтримку процесу управління проектами, та посилення дисципліни в області управління проектами.

Політика (Policy) — В загальному випадку це документ, в якому затверджені високорівневі принципи діяльності в тій чи іншій сфері. Метою політики є регламентація процесу узгодження та прийняття тактичний і стратегічних рішень та забезпечення їх відповідності філософії, цілям та стратегічним планам, визначеним керівництвом організації. Окрім змісту, як такого, політики мають описувати відповідальність за їх недотримання, шляхи подолання виключних ситуацій та спосіб, у який буде здійснюватись оцінка ступеня відповідності політиці та відповідна оцінка.

Портфель (Portfolio) — групування програм, проектів, послуг або ресурсів, відбір, керування та моніторинг яких здійснюються з метою оптимізації результатів бізнес-діяльності.

Превентивний контроль (Preventive control) — внутрішній контроль, метою якого є попередження небажаних подій, помилок та інших інцидентів, які за визначенням організації могли б спричинити суттєвий негативний вплив на процес або кінцевий продукт.

PRINCE2 — «Проекти в контрольованому середовищі» (Projects in a Controlled Environment), розроблений Агентством державної торгівлі Великобританії (OGC); метод управління проектами, який охоплює управління, контроль та організацію проекту.

Проблема (Problem) — у сфері IT, це невідома причина одного або кількох інцидентів.

Процедура (Procedure) — документ, який містить опис кроків, які необхідно виконати для досягнення результату. Процедури за визначенням є частиною процесу.

Процес (Process) — в загальному випадку, це сукупність дій, що керуються політиками та процедурами, прийнятими в організації, отримують вхідні дані з низки джерел, в тому числі від інших процесів, певним чином оброблюють ці дані та створюють вихідні дані, в тому числі генерують інші процеси. Процеси повинні мати чітко обумовлені бізнесом причини для існування, власників, передбачати чіткий розподіл ролей та обов'язків в ході виконання, а також засоби для вимірювання ефективності

Програма (Programme) — структурована група взаємозалежних проектів, які охоплюють різні сфери бізнесу, процеси, людей, технології та організаційні заходи, необхідні і достатні для досягнення чітко визначених бізнес-цілей.

Проект (Project) — сукупність дій, структурована згідно з узгодженим графіком та в межах бюджету, що здійснюються з метою забезпечення організації певною здатністю.

Система управління якістю (Quality management system, QMS) — система, яка визначає політики та процедури, необхідні для вдосконалення та контролю різних процесів, що, в результаті призводить до підвищення ефективності організації.

RACI-матриця (RACI–chart) — показує, хто є відповідальним (Responsible), перед ким потрібно звітувати (Accountable), з ким консультуватись (Consulted) та кого інформувати (Informed) в межах організації.

Стійкість (Resilience) — в сфері бізнесу це здатність системи або мережі до автоматичного відновлення функціонування після будь-якої відмови, як правило, з мінімальними негативними наслідками.

Відповідальний (Responsible) — в RACI-матриці означає особу, яка зобов'язана забезпечити успішне завершення виконання дії

Ризик (Risk) — у сфері бізнесу це потенціал певної загрози до використання вразливостей ресурсів або групи ресурсів, що призводить до втрати та/або завдання шкоди ресурсам; зазвичай оцінюється за наслідками та ймовірністю настання.

Аналіз першопричин (Root cause analysis) — процес діагностування з метою встановлення причин настання подій, який можна використати для набуття досвіду щодо типових помилок та проблем.

Життєвий цикл розробки систем (System development life cycle, SDLC) — етапи розробки або придбання програмного забезпечення або інформаційних систем. Стандартні етапи передбачають здійснення техніко-економічного обґрунтування, вивчення потреб, визначення вимог, детальний дизайн систем, програмування, тестування, інсталяцію

та аналіз функціонування систем після інсталяції та введення в дію, але не передбачає надання послуг або здійснення діяльності з реалізації вигод.

Розподіл обов'язків (Segregation/separation of duties) — Основний внутрішній контроль, який перешкоджає появі або сприяє виявленню помилок та невідповідностей шляхом покладання на ізних осіб функцій ініціації та виконання операцій, а також функцій управління повноваженнями в системах та процесах. Зазвичай застосовується у великих IT організаціях, завдяки чому окрема особа не має змоги ввести шахрайський або зловмисний програмний код, який би не був виявлений.

Служба підтримки (Service desk) — точка контакту користувачів IT послуг з IT організацією.

Постачальник послуг (Service provider) — Стороння організація, яка надає послуги певній організації.

Угода про рівень надання послуг (Service level agreement, SLA) — угода, переважно документально оформлена, між постачальником послуг та замовником(ами)/користувачем(ами), яка визначає мінімальні цілі щодо надання послуг та способи оцінки їх ефективності.

Стандарт (Standard) — обов'язкова для дотримання вимога. Прикладами стандартів можуть бути стандарт ISO/IEC 20000 (міжнародний стандарт), стандарт внутрішньої безпеки для конфігурації UNIX або державний стандарт ведення фінансової звітності. Термін «стандарт» також використовується для позначення набору практик або специфікацій, опублікованих такими організаціями з розробки стандартів, як ISO або BSI.

Сукупна вартість володіння (Total cost of ownership, TCO) — у сфері IT включає:
- Початкову вартість апаратного та програмного забезпечення
- Вартість оновлення апаратного та програмного забезпечення
- Вартість обслуговування
- Вартість технічної підтримки
- Вартість навчання
- Витрати на здійснення конкретних видів діяльності користувачів.

План технологічної інфраструктури (Technology infrastructure plan) — План розвитку технологій, персоналу, обладнання та приміщень, який дозволяє здійснювати поточну і майбутню обробку інформації, та використовувати прикладні програми.

Додаток VIII

СовіТ і похідні роботи

Додаток VIII—СовіТ® і пов'язані продукти

Методологія СовіТ® у версіях 4.0 та вище включає:
- Методологія (структура)—пояснює, як стандарт СовіТ® забезпечує організацію корпоративного управління ІТ, а також цілей контролю та найкращих практик в ІТ домени та процеси і пов'язує їх з бізнес-вимогами.
- Описи процесів—включають 34 ІТ процеси, які охоплюють сфери ІТ відповідальності від початку і до кінця.
- Цілі контролю—визначають цілі управління для ІТ процесів на основі стандартних найкращих практик.
- Керівні принципи управління—Пропонують інструменти, які допомагають розподілити обов'язки, виміряти результативність, здійснити порівняльний аналіз (бенчмаркінг) та вивчити невідповідності потужностей.
- Моделі зрілості—надають профілі ІТ процесів, які описують можливі поточні та майбутні стани.

Вже багато років поспіль після впровадження стандарту ключовий зміст СовіТ® поповнюється, а кількість пов'язаних з ним продуктів значно зросла. Нижче подані публікації, які на сьогоднішній день є пов'язаними із стандартом СовіТ®:
- *«Брифінг Ради з питань управління ІТ»* (Board Briefing on IT Governance), 2-ге видання—Розроблений з метою допомоги виконавчому керівництву у розумінні того, чому управління ІТ є таким важливим, в чому полягають його завдання та якими є обов'язки Ради з управління ІТ.
- *СовіТ® Online*— Дозволяє користувачам адаптувати версію стандарту СовіТ® до потреб власного підприємства, а потім зберегти та використовувати цю версію за бажанням. Цей продукт пропонує огляди в режимі он-лайн в реальному масштабі часу, запитання, що часто задаються, бенчмаркінг та засіб для обговорення питань та обміну знаннями та досвідом.
- *«Практики контролю СовіТ – Настанови щодо досягнення цілей контролю з метою успішного ІТ управління»* (СовіТ® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance), 2-ге видання—Забезпечує настановами щодо уникнення ризиків та цінності, які необхідно отримати в результаті впровадження цілей контролю, а також інструкцією щодо того, як впровадити цю ціль. Практики контролю наполегливо рекомендується використовувати разом з «Настановами щодо впровадження управління ІТ: Використання продуктів СовіТ та Val IT», 2-ге видання (IT Governance Implementation Guide: Using СовіТ® and Val IT, 2nd Edition).
- *«Посібник з безпеки ІТ: Використання CobiT»* (IT Assurance Guide: Using СовіТ®— забезпечує настановами щодо того, як можна використовувати СовіТ® на підтримку різноманітних заходів із забезпечення безпеки та пропонує тестові плани для всіх ІТ процесів і цілей контролю СовіТ®. Вона заміняє інформацію у «Настанові з аудиту» (Audit Guidelines) щодо здійснення аудиту та самооцінки у порівнянні з цілями контролю, викладеними у версії СовіТ® 4.1.
- *«Цілі контролю ІТ згідно із законом Сарбейнса-Оксслі: Роль ІТ у проектуванні та впровадженні систем внутрішнього контролю за фінансовою звітністю, 2-ге видання»* (IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition)— Забезпечує настановами щодо того, як гарантувати відповідність ІТ середовища, виходячи з цілей контролю СовіТ®.
- *«Настанова щодо впровадження управління ІТ: Використання СовіТ та Val IT, 2-ге видання»* (IT Governance Implementation Guide: Using СовіТ® and Val IT, 2nd Edition)— забезпечує загальною дорожньою картою для впровадження управління ІТ з використанням ресурсів СовіТ® та Val IT та супутнім набором інструментів.
- Довідник *«СовіТ Швидкий старт»* (СовіТ® Quickstart)— забезпечує основними елементами контролю невеликі організації та принципами здійснення першого кроку до розширення підприємства.
- *Стандарт управління безпекою СовіТ® Security Baseline*— зосереджений на основних кроках на шляху впровадження інформаційної безпеки на підприємстві. Друге видання знаходиться в стадії розробки на момент написання цього розділу.
- *«Взаємозв'язки СовіТ з іншими міжнародними стандартами»* (СовіТ® Mappings)—розміщений на веб-сайті www.isaca.org/downloads:
  - *Aligning СовіТ®, ITIL and ISO 17799 for Business Benefit*
  - *СовіТ® Mapping: Overview of International IT Guidance, 2nd Edition*
  - *СовіТ® Mapping: Mapping of ISO/IEC 17799:2000 With СовіТ®, 2nd Edition*
  - *СовіТ® Mapping: Mapping of PMBOK With СовіТ® 4.0*
  - *СовіТ® Mapping: Mapping of SEI's CMM for Software With СовіТ® 4.0*
  - *СовіТ® Mapping: Mapping of ITIL With СовіТ® 4.0*
  - *СовіТ® Mapping: Mapping of PRINCE2 WithСовіТ® 4.0*
- *«Управління інформаційною безпекою: настанова для Рад директорів та виконавчого керівництва, 2-ге видання»* (Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition)—презентує інформаційну безпеку з точки зору бізнесу та містить інструменти та методики виявлення проблем, пов'язаних з безпекою.

Val IT – це загальний термін, який використовується для опису публікацій та майбутніх додаткових робіт і заходів, які стосуються структури Val IT.

На сьогодні опубліковані такі роботи, пов'язані з Val IT:
- *«Вартість підприємства: управління інвестиціями в ІТ – структура Val IT»* (Enterprise Value: Governance of IT Invest-

ments—The Val IT Framework), в якій пояснюється, як підприємство може отримати оптимальну цінність від інвестицій в IT і грунтується на методології CobiT®. Вона організована у:
  – Три процеси – управління цінністю, управління портфелями та управління інвестиціями.
  – ключові практики управління IT – основні практики управління, які позитивно впливають на досягнення бажаного результату або мети конкретної діяльності. Вони підтримують процеси Val IT і відіграють майже таку саму роль, що й цілі контролю CobiT®.
- *«Вартість (цінність) підприємства: Управління інвестиціями в IT – Бізнес-Кейс»* (Enterprise Value: Governance of IT Investments—The Business Case), яка зосереджена на розгляді одного ключового елементу процесу управління інвестиціями.
- *«Вартість підприємства: Управління інвестиціями в IT на прикладі ING»* (Enterprise Value: Governance of IT Investments—The ING Case Study), яка описує, як глобальна компанія з надання фінансових послуг здійснює управління портфелем інвестицій в IT у контексті структури Val IT.

Максимально повну та оновлену інформацію щодо CobiT®, Val IT та пов'язаних продуктів, конкретних прикладів, тренінгів, інформаційних бюлетенів та інших інформаційних матеріалів, що стосуються методології, можна знайти на веб-сайтах *www.isaca.org/cobit та www.isaca.org/valit*.

Leading the IT Governance Community

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*