COBIT 2019 FRAMEWORK

24.04.2023 www.patreon.com/AndreyProkorov

Intro

- Publications
  - COBIT® 2019 Framework: Introduction and Methodology — 64 pages
  - COBIT® 2019 Framework: Governance and Management Objectives — 302 pages
  - COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution — 150 pages
  - COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution — 78 pages
- Other
  - COBIT for DevOps Audit Program
  - IT Control Objectives for Sarbanes-Oxley, 4th Edition
  - COBIT 2019 for Small and Medium Enterprises
  - COBIT Focus Area: DevOps Using COBIT 2019
  - COBIT Focus Area: Information and Technology Risk
  - COBIT Focus Area: Information Security
  - Implementing the NIST cybersecurity framework using COBIT 2019
- Cobit-2019-toolkit
  - COBIT 2019 Executive Summary_v1.1
  - COBIT 2019 Major Differences with COBIT 5_v1.1
  - COBIT 2019 Overview_v1.1
  - COBIT 2019_Governance-Management-Objectives-Practices-Activities_Nov2018, xlsx
  - COBIT 2019_Management-Awareness-Diagnostic_v1.0, xlsx
  - COBIT-2019_RACI-by-role_April 2020_v2, xlsx
  - COBITlaminate_online_R03
  - GENERAL_COBIT_2019_FAQ_v1.1 110718
- Certification
  - 1. COBIT 2019 Foundation
    - 75 Multiple-choice questions, 65% to pass
    - $175
    - 2 hours
    - Topics
  - 2. COBIT 2019 Design and Implementation
    - 60 Multiple-choice questions, 60% to pass
    - COBIT 2019 Foundation Certificate needed
    - $275
    - 3 hours
    - Topics
  - 3. Implementing the NIST Cybersecurity Framework Using COBIT 2019
    - 50 Multiple-choice questions, 65% to pass
    - COBIT 2019 Foundation Certificate needed
    - $275
    - 1.5 hours
    - Topics
- Acronyms
  - EGIT - Enterprise Governance of Information and Technology
  - I&T - Information and Technology

COBIT 5 (2012) -> COBIT 2019 What's new?

- Design Factor concept — new Design Guide
- Focus Area concept
- Performance Management and Capability Assessment
- Enablers -> Components of a Governance System
- IT-related goals -> Alignment goals
- other

What Is COBIT

COBIT is a framework for the governance and management of enterprise information and technology, aimed at the whole enterprise

COBIT defines the components to build and sustain a governance system: processes, organizational structures, policies and procedures, information flows, culture and behaviors, skills, and infrastructure

- COBIT is
  - A framework for the governance and management of enterprise I&T
  - COBIT defines the components to build and sustain a governance system
  - COBIT defines the design factors that should be considered by the enterprise to build a best fit governance system
  - COBIT is flexible and allows guidance on new topics to be added
- COBIT is not
  - A full description of the whole IT environment of an enterprise
  - A framework to organize business processes
  - An (IT-) technical framework to manage all technology
  - COBIT does not make or prescribe any IT-related decisions
- Benefits of I&T Governance
  - 1. Benefits realization
  - 2. Risk optimization
  - 3. Resource optimization
- Key concepts
  - Principles
  - Governance and Management Objectives
  - Goals Cascade
  - Components of a Governance System
  - Focus Areas
  - Design Factors

COBIT Stakeholders

- Internal
  - Boards — Provides insights on how to get value from the use of I&T and explains relevant board responsibilities
  - Executive Management — Provides guidance on how to organize and monitor performance of I&T across the enterprise
  - Business Managers — Helps to understand how to obtain the I&T solutions enterprises require and how best to exploit new technology for strategic opportunities
  - IT Managers — Provides guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, align IT strategy to business priorities, etc.
  - Assurance Providers — Helps manage dependencies on external service providers, provides assurance over IT, and ensures the existence of an effective and efficient system of internal controls
  - Risk Management — Helps to ensure the identification and management of all IT-related risk
- External
  - Regulators — Determines whether the enterprise is compliant with applicable rules and regulations and advises that the enterprise has the right governance system in place to manage and sustain compliance
  - Business Partners — Confirm that a business partner's operations are secure, reliable and compliant with applicable rules and regulations
  - IT Vendors — IT vendor's operations must establish that they are secure, reliable and compliant with applicable rules and regulations

Governance and Management

The COBIT framework makes a clear distinction between Governance and Management

- Governance ensures that: (Board Level)
  - Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives
  - Direction is set through prioritization and decision making
  - Performance and compliance are monitored against agreed-on direction and objectives
- Management plans, builds, runs and monitors activities, in alignment with the direction set by the governance body, to achieve the enterprise objectives (Executive Level)

COBIT Principles

The core requirements for a governance system for enterprise information and technology

- Governance System Principles
  - **1. Provide Stakeholder Value** — Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of I&T
  - **2. Holistic Approach** — A governance system for enterprise I&T is built from a number of components that can be of different types and that work together in a holistic way
  - **3. Dynamic Governance System** — A governance system should be dynamic. This means that each time one or more of the design factors are changed the impact of these changes on the EGIT system must be considered
  - **4. Governance Distinct From Management** — A governance system should clearly distinguish between governance and management activities and structures
  - **5. Tailored to Enterprise Needs** — A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components
  - **6. End-to-End Governance System** — A governance system should cover the enterprise end to end, focusing not only on the IT function but on all technology and information processing the enterprise puts in place to achieve its goals
- Principles for a Governance Framework
  - **1. Based on Conceptual Model** — A governance framework should be based on a conceptual model, identifying the key components and relationships among components, to maximize consistency and allow automation
  - **2. Open and Flexible** — A governance framework should be open and flexible. It should allow the addition of new content and the ability to address new issues in the most flexible way, while maintaining integrity and consistency
  - **3. Aligned to Major Standards** — A governance framework should align to relevant major related standards, frameworks and regulations

Performance Management

COBIT Performance Management (CPM) refers to how well the governance and management system and all the components of an enterprise work, and how they can be improved up to the required level

It includes concepts and methods such as Capability Levels and Maturity Levels

- Principles
  - 1. Simple to understand and use
  - 2. Consistent with, and support the COBIT conceptual model
  - 3. Provide reliable, repeatable and relevant results
  - 4. Must be flexible
  - 5. Should support different types of assessments

The capability level is a measure for how well a process is implemented and performing

Each process activity is associated with a capability level

- Process Capability Levels
  - 5 — The process achieves its purpose, is well defined, its performance is measured to improve performance and continuous improvement is pursued.
  - 4 — The process achieves its purpose, is well defined, and its performance is (quantitatively) measured.
  - 3 — The process achieves its purpose in a much more organized way using organizational assets Processes typically are well defined
  - 2 — The process achieves its purpose through the application of a basic, yet complete, set of activities that can be characterized as performed
  - 1 — The process more or less achieves its purpose through the application of an incomplete set of activities that can be characterized as initial or intuitive-not were organized
  - 0 — Lack of any basic capability; Incomplete approach to address governance and management ourDose; May or may not be meeting the intent of any process practices

Sometimes a more high-level for expressing performance is required, less granular than individual process capability ratings: Maturity Levels

- Focus Area Maturity Levels
  - ***5. Optimizing***
  - ***4. Quantitative***
  - ***3. Defined***
  - ***2. Managed***
  - ***1. Initial***
  - ***0. Incomplete***

COBIT Implementation Approach

- Initiate program — ***1. What are the drivers?***
- Define problems and opportunities — ***2. Where are we now?***
- Define road map — ***3. Where do we want to be?***
- Plan program — ***4. What needs to be done?***
- Execute plan — ***5. How do we get there?***
- Realize the benefits — ***6. Did we get there?***
- Review effectiveness — ***7. How do we keep the momentum going?***

Context

- The community's ethics and culture
- Governing laws, regulations and policies
- International standards
- Industry practices
- The economic and competitive environment
- Technology advancements and evolution
- The threat landscape
- The enterprise's:
  - Reason for existence, mission, vision, goals and values
  - Governance policies and practices
  - Culture and management style
  - Models for roles and responsibilities
  - Business plans and strategic intentions
  - Operating model and level of maturity

Design factors

Context and Design factors

Design factors are factors that Influence the design of an enterprise's governance system

- 1. Enterprise Strategy
- 2. Enterprise Goals (13)
- 3. Risk Profile (19)
- 4. I&T-Related Issues (A-T)
- 5. Threat Landscape
- 6. Compliance Requirements
- 7. Role of IT
- 8. Sourcing Model for IT
- 9. IT Implementation Methods
- 10. Technology Adoption Strategy
- 11. Enterprise Size

from... context

Focus Areas

A Focus Area describes a certain governance topic, domain or issue that can be addressed by a collection of governance and management objectives and their components

- Examples
  - Small and medium enterprises
  - Information Security
  - Risk
  - DevOps
- The number of focus areas is virtually unlimited

Components of a Governance System

Each enterprise's governance system is built from a number of components

- Components
  - Generic (described in the COBIT core model)
  - Variants
    - 1. Processes
    - 2. Organizational Structures
    - 3. Principles, Policies, Procedures
    - 4. Information
    - 5. Culture, Ethics and Behaviour
    - 6. People, Skills and Competencies
    - 7. Services, Infrastructure and Applications

Ex.enablers (COBITs)

Goals Cascade

Stakeholder needs have to be transformed into an enterprise's actionable strategy

- Enterprise goals have been consolidated, reduced, updated and clarified
- Cascade
  - Stakeholders drivers and needs
  - Enterprise goals (13)
  - Alignment goals (13)
  - Governance and Management objectives

Governance and Management Objectives

For information and technology to contribute to enterprise goals, a number of governance and management objectives should be achieved

A governance or management objective always relates to one process and a series of related components of other types to help achieve the objective

A governance objective relates to a governance process, while a management objective relates to a management process

- Governance
  - ***Evaluate, Direct and Monitor (EDM)***
- Management
  - ***Align, Plan and Organize (APO)***
  - ***Build, Acquire and Implement (BAI)***
  - ***Deliver, Service and Support (DSS)***
  - ***Monitor, Evaluate and Assess (MEA)***