****

**NAME: YUSSUF SEIFUDIN**

**ID: 660411**

**AUDIT FRAMEWORKS**

**COBIT FRAMEWORK**

The framework was originally developed by Information Systems Audit and Control Association (ISACA) in 1996, and focused specifically on financial auditing in IT environments. The second-most-recent version (from 2012), COBIT 5, incorporated governance activities like ISO 38500 and other ISACA frameworks while emphasizing IT governance for business success.

The COBIT framework provides a set of best-practice controls around information technology, allowing businesses to add value through IT decisions while mitigating possible risks. With COBIT, a business has a high-level roadmap for developing and managing IT governance practices.

It’s a supportive tool that bridges the gap between business and technical issues and gives stakeholders better risk management and COBIT compliance around their specific processes. With COBIT, a business gets the metrics, maturity models, and best practices that allow them to measure how objectives and processes are coordinating and succeeding.

The overall structure of COBIT:

* **Introduction and Methodology**: This section outlines the basic COBIT principles and explains the framework as a whole.
* **Governance and Management Objectives**: This section discusses the COBIT core model, including the 40 governance and management objectives.
* **Design Guide**: This section goes into depth on developing a governance strategy that suits an organization's unique needs.
* **Implementation Guide**: This section gives best practices for how a business could implement its specific strategy.

**Purpose of COBIT**

The main purpose of the COBIT framework is to ensure that IT investments are being prioritized in a way that helps businesses achieve their objectives without incurring additional IT risk. COBIT focuses on the following concepts:

* **Frameworks**: Good information should support business decisions. IT governance frameworks link IT processes to an enterprise’s requirements.
* **Process Descriptions:** Process-focused specifications are flexible for businesses. These provide a reference model in a common vernacular that all stakeholders can consider when planning, building, and monitoring.
* **Control Objectives:** COBIT encourages businesses to consider objectives around control and responsibility to ensure they can effectively negotiate IT risk.
* **Management Guidelines:** COBIT provides metrics to assess proper performance. This can be in terms of where a business needs a set of tools for assigning responsibility, as well as for self-assessing and approving IT measures
* **Maturity Models:** COBIT maturity models help businesses measure the capability of their processes in order to understand their progress and set priorities for improvement.

**The UK’s Office of Government Commerce**

The U.K. Office of Government Commerce (OGC) was established to act as a catalyst in procurement issues and to work with central civil government departments to achieve the best value for the money in their commercial activities. The Office is responsible for civil central government Procurement Policy and Best Practices including Construction, Property Management, IT, Supplier Relations, e-Procurement, etc. It is overseen by the Treasury. Responsibility for the Central Computer and Telecommunications Agency (CCTA) was transferred from the Cabinet Office to the OGC. The OGC is now part of the Efficiency and Reform Group within the Cabinet Office.

**IT INFRASTRUCTURE LIBRARY (ITIL)**

ITIL (Information Technology Infrastructure Library) is a framework designed to standardize the selection, planning, delivery, maintenance, and overall lifecycle of IT services within a business. The goal is to improve efficiency and achieve predictable service delivery.

The ITIL framework enables IT administrators to be business service partners, rather than just back-end support. ITIL guidelines and best practices align IT department actions and expenses to business needs and change them as the business grows or shifts direction.

**What is the ITIL Process Framework**

Each iteration of ITIL delivers updated documentation and certifications to prepare admins for the current infrastructure landscape and the types of services they provide. ITIL's framework is not a rigid checklist to implement best practices -- organizations evaluate and implement the aspects that are most important for their needs.

**Core Concepts of ITIL**

* **Service Strategy,** which describes business goals and customer requirements, as well as how to align objectives of both entities;
* **Service Design,** which outlines practices for the production of IT policies, architectures, and documentation;
* **Service Transition**, which advices on change management and release practices and also guides admins through environmental interruptions and changes;
* **Service Operation**, which offers ways to manage IT services on a daily, monthly, and yearly basis; and
* **Continual Service Improvement**, which covers how to introduce improvements and policy updates within the ITIL process framework.

**INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) 27000 STANDARD SERIES**

ISO 27000 series, is a series of best practices to help organizations improve their information security. Published by ISO (the International Organization for Standardization) and the IEC (International Electrotechnical Commission), the series explains how to implement best-practice information security practices.

It does this by setting out ISMS (information security management system) requirements. An ISMS is a systematic approach to risk management, containing measures that address the three pillars of information security: people, processes and technology. The series consists of 46 individual standards, including ISO 27000, which provides an introduction to the family as well as clarifies key terms and definitions. You don’t need a comprehensive understanding of ISO standards to see how the series works, and some won’t be relevant to your organization, but there are a few core ones that you should be familiar with.

**Why Use an ISO 2700 Series Standard**

Data breaches are one of the biggest information security risks that organizations face. Sensitive data is used across all areas of businesses these days, increasing its value for legitimate and illegitimate use.

ISO 27001 can be applied to organizations of any size and in any sector, and the framework’s broadness means its implementation will always be appropriate to the size of the business.

Differences between the frameworks

ISO 27000 series, is a series of best practices to help organizations improve their information security. Published by ISO (the International Organization for Standardization) and the IEC (International Electrotechnical Commission), the series explains how to implement best-practice information security practices.

The COBIT framework provides a set of best-practice controls around information technology, allowing businesses to add value through IT decisions while mitigating possible risks

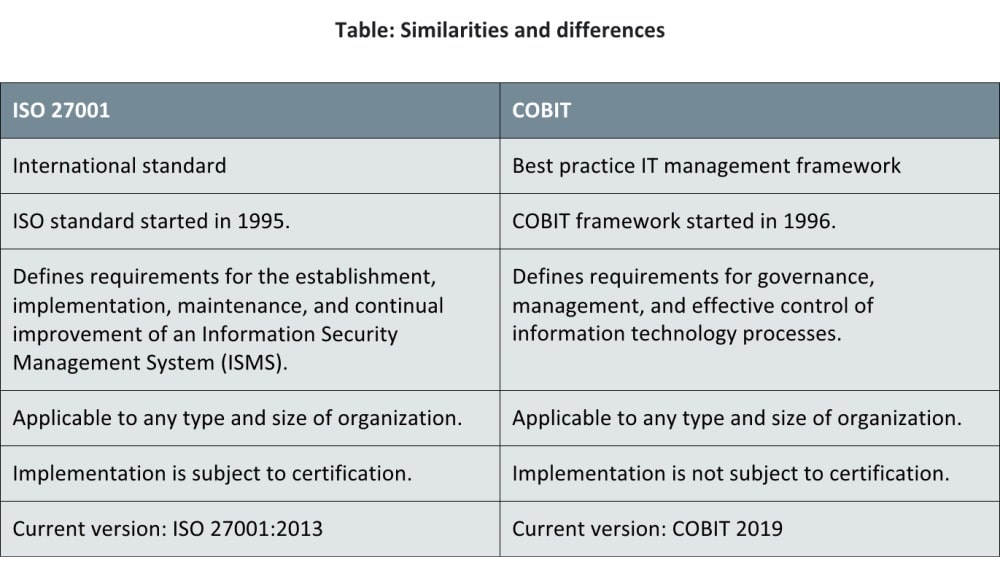


Figure 1 COBIT VS ISO

ITIL VS COBIT

|  |  |  |
| --- | --- | --- |
|  | **COBIT** | **ITIL®** |
| **Definition** | A set of guidelines for any organization to develop, implement, monitor, and improve technology governance. | A framework for best practices, planning, and selection, geared to improving IT services to better meet the company’s needs. |
| **Scope** | Focuses on ITSM, but has a broader scope than ITIL®, since it studies the entire organization. | Focuses on ITSM, and not on the whole company. It remains within the domain of IT. |
| **Approach** | A top-down approach, focusing more on IT service governance. | A bottom-up approach, focusing more on IT service management. |
| **Goals and Objectives** | 1.   Effectively manage the IT department to the company’s advantage and set it in the right direction.  2.   Align IT goals and business goals.  3.   Bring IT values to the business.  4.   Manage resources, risks, and IT efficiency. | 1.   Organize all the IT services within the company and make them run smoothly.  2.   Create opportunities for constant operational perfection.  3.   Reduce the company’s IT costs without sacrificing effectiveness.  4.   Improve the decision-making within the company. |
| **The Big Question** | **“**How do I best leverage my IT department’s resources for the benefit of the company?” | “How do I organize my IT teams and their workload in the most efficient way?” |