



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Data Security

Name : Haoyi Sun

Student Number : 1904101

Module : Data Security

29/01/2020

Contents

1. Task 1

- 1.1 Information Technology Infrastructure Library (ITIL)
- 1.2 National Institute of Standards and Technology (NIST)
- 1.3 International Organization for Standardization 27000(ISO 27000)
- 1.4 Control Objectives for Information and related Technology (COBIT)
- 1.5 Comparing ITIL 4 and COBIT 2019

2. Task 2

3. References

1. Task 1

Research three or more security framework example, Information Technology Infrastructure Library (ITIL) and Security model example, International Organization for Standardization; ISO 27000. Based on your knowledge and understanding gain, critique, analyse and compare them. [1]

1.1 Information Technology Infrastructure Library (ITIL)The Information Technology Infrastructure Library (ITIL) is a library of volumes describing a framework of best practices for delivering IT services. ITIL has gone through several revisions in its history and currently comprises five books, each covering various processes and stages of the IT service lifecycle. ITIL's systematic approach to IT service management can help businesses manage risk, strengthen customer relations, establish cost-effective practices, and build a stable IT environment that allows for growth, scale and change. [2]

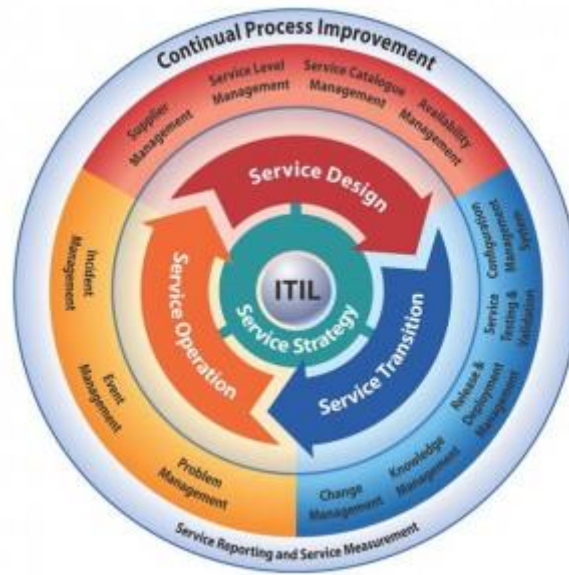


Figure 1 ITIL Structure

ITIL provides an objective, strict, and quantifiable standard and specification for IT Service Management (ITSM) practices in enterprises. It is a set of frameworks for standardizing information technology service management. It can optimize the existing resources by using processes to improve the level of information technology services, so that IT personnel no longer only think in terms of technical aspects, but also have a business purpose. The combination proves the value of IT organization to the enterprise. In order to cope with the fast-growing IT service management market, the British Department of Commerce (OGC) responsible for the development of ITIL launched the latest ITIL Version 3.0 (hereinafter referred to as ITIL V3) in 2007 to meet the actual needs of the market. In July 2011, OGC launched the ITIL V3 2011 version, which further improved the original ITIL V3, and added two processes of business relationship management and design coordination, and a solution on how CIS can be implemented. It can be said that the new version ITIL V3 is closer to reality.

1.2 National Institute of Standards and Technology (NIST)

Cybersecurity Framework

The U.S. Commerce Department's National Institute of Standards and Technology (NIST) has released version 1.1 of its popular Framework for

Improving Critical Infrastructure Cybersecurity, more widely known as the Cybersecurity Framework. [3]

The Framework integrates industry standards and best practices to help organizations manage their cybersecurity risks. It provides a common language that allows staff at all levels within an organization—and at all points in a supply chain—to develop a shared understanding of their cybersecurity risks. NIST worked with private-sector and government experts to create the Framework, which was released in early 2014. The effort went so well that Congress ratified it as a NIST responsibility in the Cybersecurity Enhancement Act of 2014.

The Framework not only helps organizations understand their cybersecurity risks (threats, vulnerabilities and impacts), but how to reduce these risks with customized measures. The Framework also helps them respond to and recover from cybersecurity incidents, prompting them to analyse root causes and consider how they can make improvements. Companies from around the world have embraced the use of the Framework, including JP Morgan Chase, Microsoft, Boeing, Intel, Bank of England, Nippon Telegraph and Telephone Corporation, and the Ontario Energy Board.

NIST continues to promote awareness of the Framework and its implementation in domestic and international markets. NIST also continues to work with industry and other stakeholders to ensure that updates to the Framework maintain its relevance and utility for a broad range of organizations.

The NIST Framework has proved itself through broad use by the business community. Among the sectoral associations that have incorporated the framework into cybersecurity recommendations are auto manufacturers, the chemical industry, the gas industry, hotels, water works, communications, electrical distribution, financial services, mutual funds, restaurants, manufacturing, retail sales, transportation, and corporate directors.

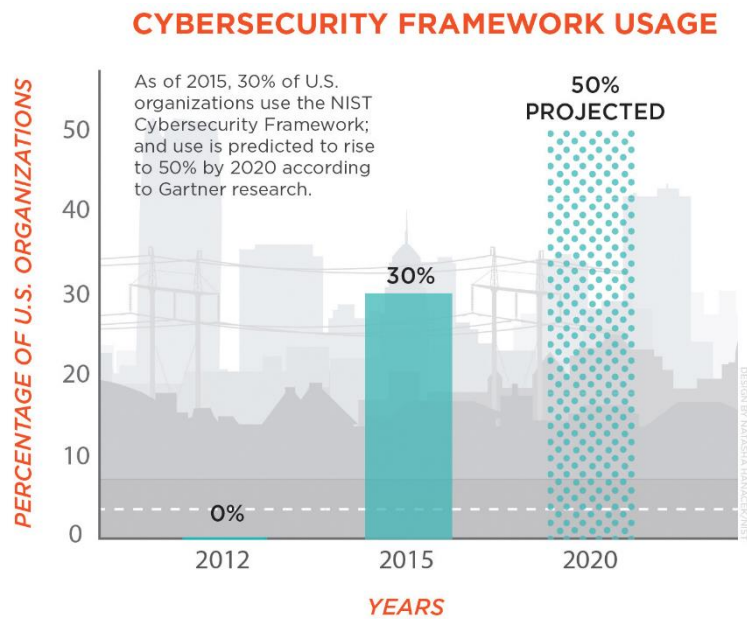


Figure 2 Framework Forecast Histogram

1.3 International Organization for Standardization 27000(ISO 27000)

The ISO / IEC 27000 standard is a general term for a series of related standards established by the International Organization for Standardization for information security management systems. It has changed a total of 60 standard numbers from ISO / IEC 27000 to ISO / IEC 27059. So far, it has officially released information security management. There are eight ISMS standards, two of which have been converted into national standards. [4]

All standards from ISO / IEC27000 to ISO / IEC 27037, as well as ISO 27799 and others, can be basically divided into the following four parts.

The first part is the requirements and supporting guidance, including ISO / IEC 27000 to ISO / IEC 27005, which are the foundation and basic requirements of the information security management system.

The second part is the guidance on certification accreditation and audit, including ISO / IEC 27006 to ISO / IEC 27008, for certification agencies and auditors.

Part III is information security management requirements for specialized

industries, such as the financial industry, telecommunications industry, or specifically for certain specific security domains, such as digital evidence and business continuity.

The fourth part is formulated by the ISO technical committee TC215 separately (instead of co-developed with the IEC). It should adopt the health industry standard ISO 27799, and some are in the research stage and gradually reflect their achievements with new projects, supply chain security, storage security, etc.

ISO / IEC 27000 is an overview and terminology of information security management, and is one of the most basic standards. It provides the common terms and basic principles involved in the ISMS standard family. Because each ISMS standard has its own terms and definitions, as well as the differences in the use environment and industry, there are often slight differences between the terms of different standards. As a result, there is a relative lack of coordination during use, and ISO / IEC 27000 is used to achieve this consistency.

1.4 Control Objectives for Information and related Technology (COBIT)

COBIT stands for Control Objectives for Information and Related Technology. It is a framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management. [5]

For anyone who wants to build governance on top of IT service creation and delivery, COBIT has been the most popular choice. COBIT has also created creativity through IT investments. Similar ones are ISO 38500, OECD principles, and Cadbury reports, but they are not as popular as COBIT, and they have not developed large knowledge bases like COBIT.

COBIT 2019 has just been released, facilitating simpler and more intuitive implementation. This will strengthen COBIT's continued role as an important driver of innovation and business transformation.

COBIT 2019 defines six principles of governance system as: providing

stakeholder value; holistic approach; dynamic governance system; separation of governance and management; tailor-made according to corporate needs; end-to-end governance system. COBIT 2019 product architecture consists of major components.

For information and technology that promotes the achievement of corporate goals, several governance and management goals should be achieved. COBIT 2019 divides 40 governance and management goals into five areas:

EDM: Assess, direct and monitor

APO: Collaboration, Planning and Organization

BAI: Build, Acquire, and Implement

DSS: Provision, Service, and Support

MEA: Monitoring, evaluation and evaluation.

To meet governance goals, every business needs to establish and maintain a system of seven components: processes; organizational structure; principles, policies, and frameworks; information; culture, ethics and behaviour; people, skills, and capabilities; services, Infrastructure and applications.

A focus area describes a series of governance topics, domains, or issues that can be addressed through a set of governance goals and their components. For example: SMEs; information security; risk; DevOps.

Organizations need to adjust the following design factors to meet their requirements: corporate strategy; corporate goals; risk profile; information and technology-related issues; threat landscape; compliance requirements; the role of IT; IT procurement models; IT implementation methods; technology adoption strategies; Enterprise size.

1.5 Comparing ITIL 4 and COBIT 2019

Both COBIT and ITIL are frameworks that senior managers in information

technology, such as CIOs, must learn. Together, they can provide comprehensive implementation guidance for effective management informationization. The latest versions of ITIL 4 and COBIT 2019 were just released around the first half of 2019, reflecting the general trend of the development of global information management. It is worthy of reference for each CIO to learn and can take a lot of detours. [6][7]

Both the new ITIL 4 and COBIT 2019 updates focus on connecting best practices to the new worlds of DevOps, Agile, and Lean.

There may be conflicts between Do Right Things and Do Things Right. If COBIT is an antibiotic, then ITIL is aspirin. Both are important and have clear but complementary goals. In the IT environment, doing the right thing can be summarized as the content of the IT team's decision to focus on achieving business goals, helping to create maximum added value for the business while reducing risk and optimizing resources. This is enterprise IT governance (EGIT). After determining the right thing, the IT team will focus on doing the right thing, that is, translate it into how the IT team will perform this task, organize the IT service (especially the work of the IT department), and provide opportunities for continuous operational improvement. This is IT Service Management (ITSM).

In terms of IT governance and IT management, COBIT's perspective is top-down. Separating governance and management is a set of practices that senior managers should understand how they should approach corporate IT. ITIL's perspective is flat-headed, talking about service management, and a roadmap for determining how to organize IT employees' work practices and processes.

Over the years, the focus of ITIL has been steadily evolving. Currently, ITIL 4 aims to provide customers with value in the form of services. The key goal is to understand the parameters and requirements involved in good service delivery, and to look at the customer or business from the service provider's perspective. The focus of COBIT is also evolving. The main

goal of COBIT 2019 is to ensure the provision of stakeholder value and service delivery engines from a business perspective.

2. Task 2

Based on the scenario on Caribbean Coffee above. Design your own approach to meet the need of the company utilising the research information on frameworks and models in task 1. Tables and diagrams may be used in your approach.

Some factors to consider in aiding appropriate solution(s):

- Security Policies
- Risk Management
- Security Management Models and Practices
- Contingencies Planning
- Protection Mechanisms
- Service Level Agreement

An information security framework, when done properly, will allow any security leader to more intelligently manage their organizations cyber risk. The framework consists of several documents that clearly define the adopted policies, procedures, and processes by which your organisation abides. [1]

It effectively explains to all parties (internal, tangential and external) how information, systems and services are managed within your organisation.

1—Choose Enterprise Information Security Policy (EISP) The high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts. An EISP is also known as a security program policy, general security policy, IT security policy, high-level InfoSec policy, or simply an InfoSec policy.

2—Risk management is the process of discovering and assessing the risks to an organization's operations and determining how those risks can be

controlled or mitigated

In Caribbean Coffee company's risk management, we need to fully consider the stability and security of our online services, the security of our employee and customer data, and the security of our intellectual property.

3—Security Management Models and Practices

In information security, a specification of a model to be followed during the design, selection, and initial and ongoing implementation of all subsequent security controls, including InfoSec policies, security education and training programs, and technological controls.

The ISO 27000 Series — One of the most widely referenced InfoSec management models is the Information Technology- Code of Practice for Information Security Management.

4—The overall process of preparing for unexpected adverse events is called contingency planning (CP). During CP, the IT and InfoSec communities of interest position their respective organizational units to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets, including human, information, and capital. The main goal of CP is to restore normal modes of operation with minimal cost and disruption to normal business activities after an adverse event.

5—In Security Maintenance, we need wireless vulnerability assessment. An assessment approach designed to find and document vulnerabilities that may be present in the organization's wireless local area networks.

6—Service Level Agreement (SLA) A document or part of a document that specifies the expected level of service from a service provider. An SLA usually contains provisions for minimum acceptable availability and penalties or remediation procedures for downtime.

3. References

- [1] Management of Information Security, 3rd Edition. ME Whitman, HJ Mattord-2010
- [2] Wu M Y, Chang S F, Li W C. Protection Management of Enterprise Endpoint Based on the ITIL Management Framework[M]// Information Technology Convergence. 2013.
- [3] Kerner S M. 'Cybersecurity Framework' From NIST Outlines Security Risks[J]. 2014.
- [4] Biggerstaff C. Adapting the ISO 27000-Series Security Framework to Space Missions[J]. 2013.
- [5] Mccollum T. ISACA UPDATES COBIT FRAMEWORK[J]. 2012.
- [6] Steuperaert, Dirk. COBIT 2019: A SIGNIFICANT UPDATE[J]. EDPACS:1-5.
- [7] Ribeiro J, Alves V, Vicente H, et al. Planning, Managing and Monitoring Technological Security Infrastructures[C]// 2019.