Governing IT and Managing Risk   
COBIT5, NIST CSF, and ISO/IEC 27000 Frameworks

# Abraham Cain

# June 30, 2021

Contents

[Title Page 1](#_Toc75975180)

[Introduction 3](#_Toc75975183)

[Analysis 4](#_Toc75975184)

[ISO/IEC 27000/1/2 Overview 4](#_Toc75975185)

[COBIT 5 Overview 4](#_Toc75975186)

[NIST CSF Overview 4](#_Toc75975187)

[Application to E-Commerce 4](#_Toc75975188)

[Recommendations 4](#_Toc75975189)

[Summary and Conclusions 4](#_Toc75975190)

[References 5](#_Toc75975191)

# Introduction

In this paper, we will examine issues in IT Management/Governance, and Risk Management along with frameworks that address these issues. We will go over COBIT5, NIST CSF, and the applicability of these frameworks in relation to the three problems mentioned previously in the e-commerce industry. We will also discuss ISO/IEC 27000, 27001, and 27002 as a reference for building an information security management system (ISMS). An information security management system is defined by Technopedia (N.D.) as “a set of frameworks that contain policies and procedures for tackling security risks in an organization.” An ISMS helps an organization develop their own and integrate existing IT management frameworks into a strategy for securing information and technology resources. One such framework is the ISO/IEC 27000 series of standards.

# Analysis

## ISO/IEC 27001/27002 Overview

The ISO/IEC 27000 series has two standards that we will focus on. These are ISO/IEC 27001 and 27002. ISO/IEC 27001 paves the foundation for creating an ISMS. It is broad and does not include specific security activities and controls. The specifics are ironed out more in the 27002 standard which according to Compliance Forge (2017) was made to support ISO/IEC 27001 and together are easier to implement than other standards like NIST SP800-53. An example of this is seen when one looks at ISO/IEC 27001 8.3 which says “Implement information security risk treatment plans” (Praxiom, 2021). This is a broad statement and ISO/IEC 27002 8.3.2 goes into specifics such as “Apply storage media disposal procedures” (Praxiom, 2021) and in even more detail recommending consideration of “developing secure incineration processes for storage mediums” (Praxiom, 2021). Together, these standards form a place for an organization to start building their ISMS.

## COBIT 5 Overview

COBIT 5 is a framework that can be seen implemented hand-in-hand with ISO/IEC the 27000 series framework. According to Mark Wolden, Raul Valverde, and Malleswara Talla (2015), COBIT focuses more on business objectives than ISO/IEC 27000 which allows the two to fit well together and allows for better coverage than just one by itself. One of the big benefits of COBIT 5 according to Ingrid Horvath (2020), with Invensis Learning, is that it can help organizations maintain compliance with laws and regulations. This alongside being business-centric with objectives around cost-benefit analysis of IT investment (Orbus Software, 2014) makes it a great choice for any business looking to stay competitive while maintaining compliance and acceptable levels of risk.

## NIST CSF Overview

Being brought to fruition due to the need for a more cyber-resilient critical infrastructure in the United States of America, Executive Order 13636 in February 2013 and then becoming a government mandate for all government agencies in May 2017 with Executive Order 13800 (Calder, 2018), the NIST Cybersecurity Framework has become a requirement for any federal agencies in the US and has become a go-to framework for many other private companies looking to do business with the federal government. The CSF consists of five main functions: identify, protect, detect, respond, and recover. These are subsequently broken down into their own categories and more specific sub-categories. The cybersecurity framework is a great addition to any business or organization that may need to protect data or information systems.

## Application to E-Commerce

E-commerce companies are not too different from other businesses when it comes to applying risk management and security management frameworks. All businesses can benefit from adopting security frameworks even if they just pick and choose bits and pieces from public frameworks and construct their own. ISO/IEC 27001 and ISO/IEC 27002 can be used in conjunction with COBIT5 to help an e-commerce company develop an information security management system of policies, processes, people, and technologies. This gives them a foundation on which to implement NIST CSF security controls. The NIST CSF controls help e-commerce companies mitigate risk by first having them identify assets. One must know that a system exists before risks to it may be addressed. The next step in CSF enables businesses to build up proper defenses and policies pertaining to the identified assets and other assets that interact with them. Then the company must develop monitoring and metrics for their security program allowing them to find out when attackers have breached their defenses. However, knowing that you got breached is no help at all if you do not have policies and processes in place to deal with it. That’s where the next function comes in where businesses should create incident response plans and develop formal procedures and plans for when things go wrong. After this, it is crucial that companies plan for recovery after incidents have been stopped. A hacker’s IP address can be blacklisted on the firewalls, but it is important that the company find out how they got in and “patch the hole”.

# Recommendations

The three frameworks discussed in this paper have areas where they come together and overlap. NIST CSF DE.CM-4 mandates that “malicious code be detected”. ISO/IEC 27001:2013 A.12.2.1 overlaps with this saying that controls must be in place to detect, prevent, and recover from malware. COBIT5 DSS05.01 goes further to say that organizations should implement and maintain preventative, detective, and corrective defenses against malware (admin, 2019).

Another important area of overlap is the area of physical security which all three frameworks address. NIST CSF DE.CM-2 ensures that the monitoring is in place in the physical environment to detect cybersecurity events. ISO/IEC 27001:2013 A.11.1.1relates in that it tells companies to create “secure” areas and segment areas by the level of security. COBIT5 DSS01.04 and DSS01.5 follow up telling leaders to manage the environments and facilities.

These three frameworks have plenty of overlap and some were even created to be implemented in conjunction with others. It is because of this that I would recommend implementing them together to maximize security and business risk coverage.

# Summary and Conclusions

As with any important goal, it is vital to have a plan or strategy. Working with these security and business frameworks allows information security and risk management professionals to create a functioning information security management system. This system introduces several plans and strategies for defending information and deterring threat actors. Planning ahead for cybersecurity saves money and time because the question of a breach happening is not a question of “if”, but of “when”. It is important to plan ahead so that you aren’t doomed when there is a cyber incident and also to reduce the likelihood that an incident would happen in the first place.

# References

Admin. (2019, July 6). Security service Management–DSS05 (COBIT2019). Process-Symphony – ITSM Knowledge Orchestrators – Process Wiki. Retrieved July 4, 2021, from <https://wiki.process-symphony.com.au/uncategorized/security-service-management-dss05-cobit2019/>

Compliance Forge. (2017). Practical guide: understanding information security policies & standards. <https://examples.complianceforge.com/complianceforge-introduction-guide-to-information-security-policy-cybersecurity-program-documenation.pdf>

Horvath, I. (2020, September 8). Benefits of COBIT 5 that help achieve digital transformation. Invensis Learning Services. <https://www.invensislearning.com/blog/benefits-of-cobit-5/>

Orbus Software. (2014, March 12). What is COBIT 5? [Video]. YouTube. <https://www.youtube.com/watch?v=Y8kqh9q3Jwg>

Praxiom Research group Limited. (2014, March). ISO IEC 27002 2013 translated into plain english: details. ISO Standards and NIST Frameworks in Plain English. <https://www.praxiom.com/iso-27002-sample8.pdf>

Praxiom Research Group Limited. (2021, April 5). Outline of ISO IEC 27001 2013 information security standard. ISO Standards and NIST Frameworks in Plain English. <https://www.praxiom.com/iso-27001-outline.htm>

Praxiom Research Group Limited. (2021, April 5). ISO IEC 27002 2013 information security in plain English. ISO Standards and NIST Frameworks in Plain English. <https://www.praxiom.com/iso-27002.htm>

Techopedia. (n.d.). What is an information security management system (ISMS)? - Definition from Techopedia. Techopedia.com. <https://www.techopedia.com/definition/16515/information-security-management-system-isms>