

Data Security Report

On Security Frameworks, Models and Case Studies

Module Name	Data Security
Module Code	ACCA7009
Lecturer	Dr. Carlene Campbell
Student	Zhao Ning (1904564)
Date	29/01/2020
Score	

Table of Contents

List of Figures	2
List of Tables	2
Part 1. InfoSec Basics: Objectives and Controls	3
1.1 The Three Objectives of Security	3
Confidentiality, Integrity, and Availability	3
1.2 Security Controls	3
Part 2. Security Frameworks and Models	3
2.1 Security Management Models.....	3
The ISO 27000 Series.....	3
NIST Security Framework	4
PCI Security Standards (Industry-Specific).....	4
Mapping PCI DSS to the NIST Framework.....	4
CIS Secure Suite	5
Summary	5
2.2 Access Control Models	6
Part 3. Case Study	6
3.1 Case Scenario Analysis.....	6
3.2 Improve Security and Privacy in Cloud Computing.....	7
3.3 Improve WLAN Security	8
3.4 Establish Rules of Behaviour.....	9
3.5 Ensure Transmission Confidentiality and Integrity	9
3.6 Protect Intellectual Properties.....	9
Part 4. Conclusion	10
Appendix. References	10

List of Figures

FIGURE 1. NIST SECURITY FRAMEWORK.....	4
--	---

List of Tables

TABLE 1. MAPPING PCI DSS V3.2.1 TO THE NIST CYBERSECURITY FRAMEWORK.....	5
TABLE 2. SECURITY AND PRIVACY ISSUES AND RECOMMENDATIONS	7

Part 1. InfoSec Basics: Objectives and Controls

1.1 The Three Objectives of Security

CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

Maintaining confidentiality, integrity and availability is how classic information security models define their three objectives, each of which addresses a distinct aspect of information protection:¹

1. **Confidentiality:** protecting information assets from any unauthorized access. A breach of confidentiality means that unauthorized parties should not but somehow gain access to sensitive information.
2. **Integrity:** ensuring the authenticity of information. The source of the information is accurate and reliable, without being altered in any way.
3. **Availability:** ensuring the accessibility of information to its authorized users. InfoSec might be compromised by DDoS attacks which would crash the servers and render services unavailable.

1.2 Security Controls

Also known as protection measures, security controls aim to protect a system from potential risks of loss of confidentiality, integrity or availability by limiting functionality (least privilege) and removing/mitigating security vulnerabilities². There are three types of security controls as follows:

1. **Management controls:** management of risk and information system security.
2. **Operational controls:** primarily implemented and executed by people.
3. **Technical controls:** primarily implemented and executed by system hardware, software or firmware.

Part 2. Security Frameworks and Models

2.1 Security Management Models

THE ISO 27000 SERIES

This is one of the most widely known and used information security standards.

Developed by the International Standards Organisation (ISO), it is broad in scope and can be applied across businesses of varying types and sizes.

Having been tried and tested by many countries, it can be used as a good building block to customize security policies, and as a guideline for security practices. An example is the New Zealand Information Security Manual (NZISM)³.

However, for many smaller organizations it can be as discouraging as many of the ISO standards because the effort required to gain accreditation and to implement the plans

¹ https://developer.mozilla.org/en-US/docs/Web/Security/Information_Security_Basics/Confidentiality,_Integrity,_and_Availability

² https://developer.mozilla.org/en-US/docs/Web/Security/Information_Security_Basics/Security_Controls

³ <https://originit.co.nz/the-strongroom/five-most-common-security-frameworks-explained/>

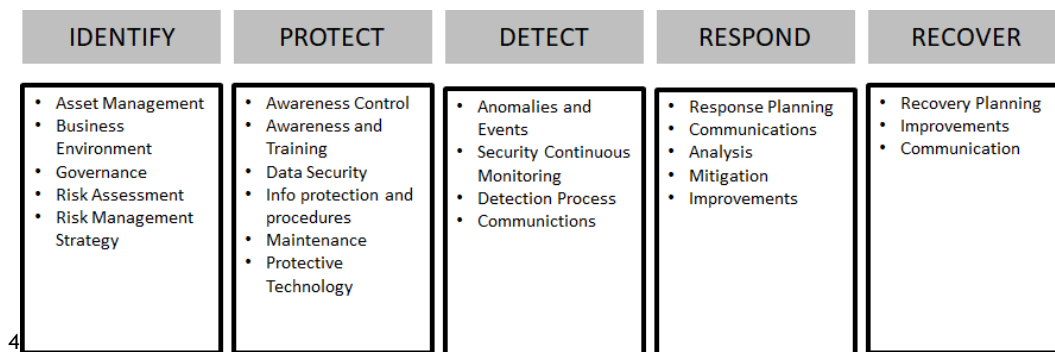
are not often within their budget (often there is a limited period of time or a limited amount of money).

NIST SECURITY FRAMEWORK

The NIST framework, developed by the US National Institute of Standards and Technology, has evolved into a mature and comprehensive framework that contains a wide range of security standards and best practices. Consisting of many practical guidance, it can also be adapted relatively easily to smaller and non-US organisations. There are two notable advantages that the NIST security standards possess over many other security frameworks:

- (1) They are publicly available free of charge.
 - (2) They have been available for over 20 years. Therefore, they have been broadly reviewed by industry professionals and governments[1][2].
- Some of the simplest yet most frequently used models are listed below in Figure 1.

Figure 1. NIST Security Framework



PCI SECURITY STANDARDS (INDUSTRY-SPECIFIC)

Developed by the PCI Security Standards Council (PCI SSC) - a global forum that brings together stakeholders in the payments industry to develop InfoSec standards and drive the adoption of secure payment resources, the PCI Security Standards are specifically catered for payment account data protection throughout the payment lifecycle. Solutions are also provided to devalue account data in order to eliminate criminal incentives⁵. They include standards on security practices for service providers and businesses, and standards for developers and technology solution vendors of secure payment products.

MAPPING PCI DSS TO THE NIST FRAMEWORK

PCI DSS and the NIST Cybersecurity Framework share the common goal of enhancing information security. Mapping PCI DSS to the NIST Framework allows stakeholders to understand how to align security efforts to meet objectives in both PCI DSS and the

⁴ <https://security-and-privacy-reference-architecture.readthedocs.io/en/latest/06-secmodels.html>

⁵ https://www.pcisecuritystandards.org/pci_security/standards_overview

NIST Cybersecurity Framework⁶. By evaluating each outcome of the NIST Framework against the requirements of PCI DSS, the relevant part for each outcome can be identified. The resultant mapping shows where they contribute to the same security outcomes, part of which is shown in Table 1.

Table 1. Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework

Category (Sub-category-1)	Mapping
Risk Management Strategy (ID.RM)	• PCI DSS v3.2.1 12.2 • NIST SP 800-53 Rev. 4 PM-9
Response Planning (RS.RP)	• PCI DSS v3.2.1 12.10 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
Recovery Planning (RC.RP)	• PCI DSS v3.2.1 12.10.6 • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8

CIS SECURE SUITE

Unlike NIST, ISO or PCI, the CIS (Centre for Internet Security) Secure Suite is developed to provide organizations with a concise and prioritized version of security controls to yield results in a quick fashion. Instead of implementing dozens of controls, this suite puts its emphasis on helping organizations focus on what the top priority is when they establish baselines for cyberspace protection and defense. It automates and combines the CIS Controls, CIS Benchmarks, and CIS-CAT Pro into a powerful and efficient cybersecurity toolkit for commercial, non-profits, and governmental entities alike⁷.

SUMMARY

All of the material covered above is designed for different motives, geographic regions or industries. In the rest of this report, we will base our design on the following InfoSec publications (with some slight modifications):

1. NIST Special Publication 800-53 (Revision 5): *Security and Privacy Controls for Information Systems and Organizations*

This update makes available a comprehensive collection of safety measures for various types of computing platforms, including cloud platforms, mobile systems, and Internet of Things (IoT) devices. Both security and privacy controls are presented in these measures to protect the critical operations and assets of organizations and the personal privacy of individuals⁸.

⁶ <https://www.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework.pdf?agreement=true&time=1580378762631>

⁷ <https://www.cisecurity.org/>

⁸ <https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf>

2. NIST Special Publication 800-144: *Guidelines on Security and Privacy in Public Cloud Computing*⁹
3. NIST Special Publication 800-153: *Guidelines for Securing Wireless Local Area Networks (WLANs)*¹⁰

2.2 Access Control Models

Access controls regulate the admission of users into trusted areas of the organization - both logical access to information systems and physical access to the organization's facilities[2].

1. The Bell-LaPadula Confidentiality Model (BLP)

- BLP is a confidentiality model or "state machine reference model" that ensures the confidentiality of the modelled system by using MACs (mandatory access control), data classification, and security clearances. Access modes can fall into two categories: (1) simple security and (2) the * (star) property.
- Simple security (also called the "read property") prohibits a subject (users or processes) of lower clearance from reading an object (files or peripherals) of higher clearance but allows a subject with a higher clearance level to read an object at a lower level. This rule is also known as "No Read-up".
- In contrast, the * property (also called the "write property") prohibits a subject of a higher clearance level from sending messages to a lower-level object. This rule is also known as "No Write-down".

2. The Biba Integrity Model

- Biba is an access control model that is similar to BLP and is based on the premise that higher levels of integrity are worthier of trust than lower levels. Biba is often referred to as 'Bell-LaPadula upside down'. Its key observation is that confidentiality is a constraint on who can read a message, while integrity is a constraint on who can write or alter it. Therefore, it may be formulated in terms of a "No Read-down" and a "No Write-up" property.

3. The Clark-Wilson Model

- The *CW model* was designed for commercial environments. It originated from double-entry bookkeeping in financial systems¹¹. The main goal is to ensure the integrity of a bank's accounting system and prevent insider fraud. It operates upon principles of change control which are listed as follows:
 - No changes are allowed to be made by unauthorized subjects.
 - No unauthorized changes are allowed to be made by authorized subjects.
 - The maintenance of internal and external consistency should be ensured.

Part 3. Case Study

3.1 Case Scenario Analysis

⁹ <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>

¹⁰ <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf>

¹¹ <https://www.cl.cam.ac.uk/~rja14/Papers/security-policies.pdf>

The Caribbean Coffee corporation uses **cloud platforms** to deliver IT services to its staff members and clients.

- (In section 3.2 we will look at several common issues that we face in cloud computing and provide solutions accordingly.)

It is estimated that almost 95% of the company's network is **wireless** based.

- (In section 3.3 we will discuss ways to improve security in a typical wireless network environment.)

The company also has a massive online presence and **social media** presence for promotion.

- (In section 3.4 we will identify responsibilities of organizational personnel who use social networking platforms for official duties or business tasks)

Owing to its large staff and international customer base, the company has recently come under immense pressure to allow both its staff and customers to use their **personal devices** to access the company's network/resources.

- (In section 3.5 we will present measures to ensure confidentiality and integrity of data transmitted through the untrusted network.)

Security of personal staff's data and client's data is the company's major concern. The company is also concerned about protecting its valuable **intellectual properties**.

- (In section 3.6 we will briefly talk about how to protect intellectual properties.)

3.2 Improve Security and Privacy in Cloud Computing

According to NIST-SP-800-144, some of the common issues facing cloud computing and their corresponding solutions with regard to our Caribbean Coffee case are listed below in Table 2.

Table 2. Security and Privacy Issues and Recommendations

Issues	Recommendations
Compliance	Understand the various types of laws and regulations that could impose security and privacy obligations on the organization and thus have a potential impact on cloud computing practices, including in particular those involving data geography, security controls and privacy, personal records (of staff members or customers) management. (For example, the Federal Information Security Management Act (FISMA) which was signed into law in 2002, requires US federal agencies to conduct annual reviews of InfoSec programs in order to keep security risks to or below specified acceptable levels.¹²) Ensure that the cloud provider's e-discovery features do not in any way compromise the security or privacy of user data. (For example, Amazon Zapproved helps customers streamline electronic discovery processes while maintaining defensible practices. It automates a continuous

¹² <https://www.tripwire.com/state-of-security/regulatory-compliance/regulatory-compliance-cloud/>

	monitoring security solution on AWS, using AWS Lambda for firewall rules management. ¹³⁾
Architecture	Understand the underlying technologies that the cloud provider uses to provision services over the full system lifecycle and across all system components. (For example, Amazon's technology stack encompasses things like Cloud-Search, Launch-Kit, EC2, Nginx, DynamoDB and many more.)
Identity and Access Management	Ensure that adequate safety measures are in place to secure authentication, authorization, and other identity and access management functions. (For example, there should be two separate identity and access management systems for staff and customers.)
Data Protection	Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider. (For example, AWS Key Management Service (KMS) enables organizations to create and manage cryptographic keys and control their use across a wide range of AWS services. It uses hardware security modules that have been validated or are in the process of being validated under FIPS 140-2 (NIST Special Specification on Security Requirements for Cryptographic Modules) for key protection and compliance needs.)

Besides, according to NIST-SP-800-53, service-level agreements (SLA) can be used to identify response requirements for incidents of non-compliance and thus enhance security controls:

- (1) IDENTIFICATION OF FUNCTIONS, PROTOCOLS, AND SERVICES
 - Require cloud providers to identify the functions, protocols, and extra services required.
- (2) ESTABLISH, DOCUMENT AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS
 - Establish, document, and maintain trust relationships with cloud providers based on organization-defined requirements or conditions.
- (3) CHECK CONSISTENCY BETWEEN INTERESTS OF CONSUMERS AND PROVIDERS
 - Verify that the interests of cloud providers reflect and are consistent with organizational interests.
- (4) PROCESSING / SERVICE LOCATION
 - Confine the location of data processing and system services based on organization-defined requirements or conditions.
- (5) ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS
 - Maintain an exclusive control of cryptographic keys.
- (6) ORGANIZATION-CONTROLLED INTEGRITY CHECKING
 - Check the integrity of data that reside in the cloud.

3.3 Improve WLAN Security

¹³ <https://aws.amazon.com/solutions/case-studies/zapproved/>

According to NIST-SP-800-153, organizations should implement the following guidelines to improve the security of their WLANs. Corresponding recommendations with regard to our Caribbean Coffee case are also presented.

- Provide standardized security configurations for common WLAN components, such as client devices and access points (Aps).
- Establish policies that clearly state the forms of connections allowed or forbidden among WLAN client devices.
- Ensure that configurations of the organization's WLAN client devices and APs are compliant with the organization's WLAN policies at all times.
- Perform both vulnerability monitoring and attack monitoring in order to improve WLAN security.
- Conduct regular WLAN security assessments.

3.4 Establish Rules of Behaviour

According to NIST-SP-800-53, rules of behaviour should be included, so do explicit restrictions on the use of social media and networking sites or the posting of organizational information on public websites.

Organizations should also address specific rules that prevent unauthorized entities from obtaining non-public organizational information (examples of which include system account information and personally-identifiable information) from social media and networking sites.

3.5 Ensure Transmission Confidentiality and Integrity

According to NIST-SP-800-53, security controls should be applied to any components that can transmit information, including distributed desktop computers and mobile devices so as to protect the confidentiality and integrity of sensitive information. This can be accomplished by physical means or by logical means:

- Physical protection can be achieved by employing protected distribution systems.
- Logical protection can be achieved by employing encryption techniques.

Organizations that rely on cloud providers to offer transmission services should determine what types of confidentiality or integrity services are available in cloud service packages. If it is not viable to obtain the assurances of an effective control through contracts, then appropriate compensating security controls should be implemented. Otherwise the organization have to accept the additional risk explicitly.

3.6 Protect Intellectual Properties

According to NIST-SP-800-53, security controls related to corporations' intellectual properties should be implemented:

- Use software and its associated documentation in accordance with contract agreements and copyright laws;
- Track the use of software and its associated documentation protected by proprietary licenses to control copying and distribution;
- Record and control peer-to-peer (P2P) file sharing practices to ensure they are not used for unauthorized distribution or reproduction of copyrighted resources.

3.7 Apply Access Control Models

- Apply the Bell-LaPadula model to ensure confidentiality based on user roles;
- Apply the Biba model to ensure integrity based on user roles;
- Apply the Clark-Wilson model to prevent insider fraud.

Part 4. Conclusion

Information security management recognises the importance of both system implementation and personnel practices. Identifying human factors is a key issue to be addressed by managers, so is assessing potential system vulnerabilities and security risks. Therefore, when we analyse InfoSec systems, it is essential to take a look at not only the technological configurations but also their social contexts.

Appendix. References

- 1 Whitman, M., and Mattord, H.: 'Principles of Information Security' (2005. 2005)
- 2 Whitman, M., and Mattord, H.: 'Management of Information Security, 4th Edition', 2014