Ocean Graham

Abstract

[Draw your reader in with an engaging abstract. It is typically a short summary of the document.   
When you’re ready to add your content, just click here and start typing.]

402it - information security

Risk Assessment Report



Table of Contents

[Table of Figures 1](#_Toc193356116)

[Introduction 2](#_Toc193356117)

[ISo/IEC 27001 3](#_Toc193356118)

[Nist SP 800-30 4](#_Toc193356119)

[Risk identification 5](#_Toc193356120)

[Asset identification 5](#_Toc193356121)

[Risk analysis and evaluation 6](#_Toc193356122)

[References 6](#_Toc193356123)

# Table of Figures

[Figure 1 - CIA Triangle 2](#_Toc193716487)

[Figure 2 - ISO/IEC 27001 Risk Matrix 3](#_Toc193716488)

[Figure 3 - Risk Calculation 5](#_Toc193716489)

402IT – Information security

# Introduction

In this coursework the author will demonstrate a high degree of understanding of information security and the critical role in plays in guarding information from threats.

## What is information security?

Information security (InfoSec) is the protection of both physical and digital information against unauthorised access, disclosure and disruption/alteration. (IBM, 2024, What is information security?) The prevalence and rise of cyber threats (such as DoS, Malware, SQL Injections and Phishing) has created threats to the confidentiality, integrity and availability (CIA) of a person’s or organization's information. (Calder & Watkins, 2024)

## Principles of Information Security

InfoSec works under the principles of the CIA triangle (Confidentiality, Integrity & Availability), these principles are used to gauge the degree of InfoSec the information has. The three parts entail:

1. Confidentiality – preventing unauthorized access and reading of private information. (Stamp, 2011)
2. A diagram of a triangle with Great Pyramid of Giza in the background

   AI-generated content may be incorrect.Integrity – preventing/ detecting unauthorized access from altering/tampering data, making sure this data is authentic and reliable. (Stamp, 2011)

Figure 1 - CIA Triangle

1. Availability – making data available to the required personnel when needed to allow an organisation to function as it should. (Fortinet, 2023)

## ISo/IEC 27001 & 27005

The ISO/IEC 27001 and 27005 is the most used standard of certification (a credential that validates a company’s proficiency in an Information Security Management System (ISMS)) within the InfoSec field. ISO/IEC 27001 provides companies with guidance for improving an ISMS, ensuring high degree of quality to safety and security, providing a centralised framework, respond to evolving risks and reduce vulnerability to cyber-attacks. (ISO, 2022) ISO/IEC 27001 contains 5 primary steps of implementation:

1. Define Scope and Objectives
2. Conduct Risk Assessment
3. Implement Security Controls
4. Monitor and Review Performance
5. Continuous Reiteration and Improvement

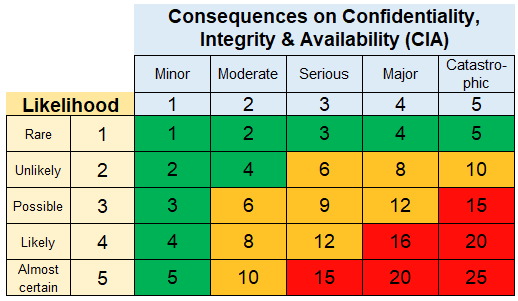
ISO/IEC 27001 also gauges risks of events through a risk assessment, calculated via Likelihood times by Impact/Consequences relating to the CIA Triangle.

Figure 2 - ISO/IEC 27001 Risk Matrix

Source - (Pope, 2023)

The reason other certifications and standards exist, compared to the seemingly primarily regarded ISO/IEC 27001, is due to the problem that comes to ISO/IEC 27001. ISO/IEC 27001 standard is a very difficult and lengthy pursuit of the certification. The standard requires significant time and financial resources into achieving the relevant certification, that whilst large companies can afford, smaller companies may not hold the capabilities to perform the demands ISO/IEC 27001 requires. It also holds the risk of companies focusing on complying with requirements over actual security needs.

## Nist SP 800-30

The NIST SP 800-30 is an alternative to ISO/IEC 27001, developed by the US National Institute of Standards and Technology. NIST SP 800-30 is a risk assessment guideline for conducting risk assessments and managements of systems and organisations. (NIST, 2012) The process of NIST SP 800-30 risk assessment preparation according to the (NIST, 2012) documentation follows:

1. Identify Purpose – Identify the purpose via the information that is assessed and the expected outcome.
2. Identify Scope – Identify the scope of the assessment in scale to the organisation’s capabilities.
3. Identify Assumptions and Constraints – Make clear the restrictions and limits of the assessment, what is acceptable.
4. Identify Information Sources – Identify the threats, vulnerabilities and impacts and what is the source of these.
5. Identify Risk Model and Analytic Approach – Identify the risk model and approach to be used in the assessment.

NIST SP 800-30 documentation (NIST, 2012) also elaborates the 6 steps “tasks” to conducting a risk assessment following NIST SP 800-30 guidelines:

1. Identify Threat Sources
2. Identify Threat Events
3. Identify Vulnerabilities
4. Determine Likelihood of Threat Event
5. Determine the Negative Impact of Threat Sources
6. A table with text on it

   AI-generated content may be incorrect.Determine Risks via the calculation (Likelihood x Impact)

Figure 3 - Risk Calculation

Source- (NIST, 2012)

Just as with ISO/IEC 27001, the NIST SP 800 series (therefore NIST SP 800-30) can be resource intensive, however due to the lack of financial demand, it allows smaller companies to have better chances to implement this standard.

# Methodology of Report

This report will be conducted via online research on vulnerabilities within the labelled systems and services within the brief of the New England Hospital. The primary source of information being the Common Vulnerabilities and Exposures (CVE) website which publicly displays and elaborates on computer system’s security faults/flaws. The CVE site will allow the author to find potential threats and gaps within the New England Hospital’s in-use systems to find threats and create a risk assessment.

An array of Virtual Machines (Via OracleVM) have also been used to simulate the hospitals systems. Allowing the Simulator to penetrate the systems to help identify the vulnerabilities and provide evidence to threats of the systems that are in use. Kali Linux was utilised in accordance with the system environments due to its modularity and variety in tools that can be utilised.

## Asset identification

Asset register

Software, hardware, data,

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Asset | Location | Vulnerability |
|  | Windows Server 2016 |  |  |
|  | Windows Server 2019 |  |  |
|  | Windows Workstation 8 |  |  |
|  | Windows Workstation 10 |  |  |
|  | Legacy Windows XP |  |  |
|  | Linux based SQL database servers |  |  |
|  | J2EE Glass Fish application servers |  |  |
|  | Online Web Services via the Internet |  |  |
|  | Web application server |  |  |
|  | Building-wide Local Area Network (LAN) |  |  |
|  | Java Resource Adapter Architecture |  |  |
|  |  |  |  |

# Risk identification

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threat | Vulnerability | Impact | Likelihood | Risk |
| Windows Server 2016 |  |  |  |  |  |
| Windows Server 2019 |  |  |  |  |  |
| Windows Workstation 8 |  |  |  |  |  |
| Windows Workstation 10 |  |  |  |  |  |
| Legacy Windows XP |  |  |  |  |  |
|  |  |  |  |  |  |

# Risk analysis and evaluation

## Mitigation

# References