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

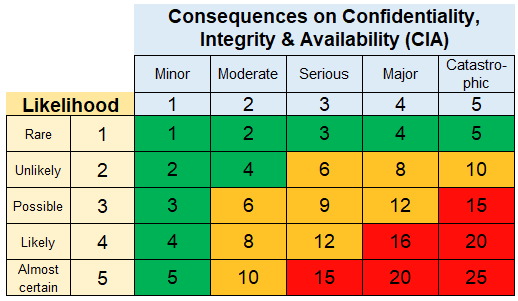
ISO/IEC 27001 also gauges risks of events through a risk assessment, calculated via Likelihood times by Impact/Consequences relating to the CIA Triangle.

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. Determine Risks via the calculation (Likelihood x Impact)

A table with text on it

AI-generated content may be incorrect.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

|  |  |  |
| --- | --- | --- |
| Category | Asset | Vulnerability |
| Software | -Windows Server 2016  -Windows Server 2019  -Windows 8  - Windows 10  -Legacy Windows XP  - Linux based SQL database servers  -J2EE Glass Fish application servers  -Web Application Server  -Online Web Services via the Internet  -Building-wide Local Area Network (LAN) | -Risk of system vulnerabilities allowing malicious attacks (malware, spoofing, reconnaissance, scanning, SQL Injections)  -Exploit poorly configured /unauthorised information systems exposed to the internet  -Disruptions via Network, Hardware or other errors  -Loss of sensitive information  -Lack of Support due to outdated older systems |
| Hardware | -Java Resource Adapter Architecture  -Workstations (Working on Windows 8 & 10)  -Removable Media (e.g. USB’s)  -Laptops and Mobile devices | -Insert malware into organisational hardware  -Environmental threats (Fire, Flooding, Hurricanes)  -Loss of devices via theft or damage  -Malfunctions due to deliberate actions or other causes |
| Data | -Patients Databases  -Communication Databases  -Financial Databases  -Staff Databases  -Communications Databases | -Threat to CIA Triangle due to security breaches of Hardware or Software  -Unauthorised access  -Spoofing (tampering with data) |
| Structural | -Staff  -Facilities | -Gossip sharing private information  -Poor security logins due to staff  -Risk of leaving systems unlocked and unsupervised  -Unauthorised access into Private locations |

## Specific Assset Vulnerabilities

The graph below presents more in-detail vulnerabilities (according to the CVE) for many of the software assets displayed.

|  |  |  |
| --- | --- | --- |
| Category | Asset | Vulnerability |
| Software | Windows Server 2016 | -End of Life (No more support)  -Remote desktop client allows attackers to execute code over a network. (**CVE-2025-26645**)  -External control of file names & paths via New Technology LAN Manager (NTLM) allowing spoofing (fraud via forgery) over network. (**CVE-2025-24996**)  - Windows Kernal memory info disclosure Vulnerability. (**CVE-2025-21323**) |
| Software | Windows Server 2019 | -End of Life (No more support)  -Remote desktop client allows attackers to execute code over a network. (**CVE-2025-26645**)  -External control of file names & paths via New Technology LAN Manager (NTLM) allowing spoofing (fraud via forgery) over network. (**CVE-2025-24996**)  -Windows Kernal memory info disclosure Vulnerability. (**CVE-2025-21323**) |
| Software | Windows Workstation 8  (Workstation working on Windows 8) | -End of Life (No more support)  -Microsoft Surface Security feature bypass vulnerability. (**CVE-2025-21194**)  **-**A kernel-mode driver in Windows 8 allows an Elevation of Privilege Vulnerability when it fails to properly handle objects in memory. (**CVE-2017-8552**) |
| Software | Windows Workstation 10  (Workstation working on Windows 10) | -Relative path traversal in Remote Desktop Client allows unauthorised attacker to execute code over network. (**CVE-2025-26645**)  **-**Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorised attacker to execute code over a network. (**CVE-2025-24051**) |
| Software | Legacy Windows XP | -End of Life (No more support)  -SQL injection in View User Profile in MicroWorld eScan Management Console allows remote attacker to dump entire database and gain windows XP command shell to perform code execution on database. (**CVE-2023-31702**) |
| Software | Linux based SQL database servers | -IBM Db2 for Linux is vulnerable to a Denial of Service (DoS), under specified non default configurations as the server may crash when using a specially crafted SQL statement by authenticated user.  (**CVE-2024-31882**) |
| Software | J2EE Glass Fish application servers | -SQL injection vulnerability in the UDDI Server allows remote attackers to execute Structured Query Language (SQL) commands. (**CVE-2016-2386**)  -Vulnerability in the Oracle Containers allows remote attackers to affect integrity. (**CVE-2010-0070**) |
| Software | Building-wide Local Area Network (LAN) | -Cross Site Scripting vulnerability allows a remote attacker to escalate privileges via the menu interface of the member center of the background administrator. (**CVE-2025-25960**) |
| Hardware | Java Resource Adapter Architecture | -JNDI injection into JDBC driver, leading to remote code execution. (**CVE-2024-54660**) |

# Risk identification

The graph below follows the NIST SP 800-30 Scale (Figure 3) for Impact, Likelihood and Risk

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threat Event | Vulnerability | Impact | Likelihood | Risk |
| Windows Server 2016 | Threat of spoofing via NTLM | Puts the Integrity of data within the server at risk due to the potential tampering of sensitive data, this is amplified due to this assets service being End of Life. | Very High | Very High | Very High |
| Windows Server 2019 | Threat of spoofing via NTLM | Puts the Integrity of data within the server at risk due to the potential tampering of sensitive data, this is amplified due to this assets service being End of Life. | Very High | Very High | Very High |
| Windows Workstation 8 | Threat of Unauthorised/Untrusted access of sensitive data due to kernel issue | Threatens Confidentiality of data as there is a threat of personnel with lake of Privilege seeing data, they don’t have clearance for.  Risk of Malicious insider exploiting fault, resulting in potential breach and spread of sensitive data. | Very High | High | High |
| Windows Workstation 10 | Threat of Heap-based buffer overflow attack in RRAS risking unauthorised access | Threatens Integrity and Confidentiality of data, this attack corrupting stored data in a way to allow attacker to overwrite structure, allowing access to read and/or alter sensitive data. | Very High | High | High |
| Legacy Windows XP | Threat of SQL injection allowing attacker to acquire database and access XP command shell | Threatens Confidentiality and Integrity, attacker gaining access to private information such as addresses, Identification, or billing accounts of patients and staff. Also potentially being able to alter information of system data through command shell. | Very High | Very High | Very High |
| Linux based SQL database servers | Threat of DoS due to attack or high traffic | Threatens Accessibility due to temporary loss of important data due to disruption caused by overwhelming of system (DoS). | Moderate | Moderate | Moderate |
| J2EE Glass Fish application server | Threat of SQL injection allowing attacker to execute SQL commands | Threatens Confidentiality, SQL commands allowing attacker to access private information such as addresses, Identification, or billing accounts of patients and staff. | Very High | Very High | Very High |
| Web application server | Threat of SQL injections | Threatens Confidentiality, SQL injections risking the sensitive data being breached and accessed by unauthorised personnel. |  |  |  |
| Online Web Services via the Internet | Threat of Phishing and Malware | Threatens systems, services and privacy due to malware damaging and disrupting systems. Phishing may also occur online by clicking an unsafe link, resulting in breaching of data security. | High | Very High | High |
| Building-wide Local Area Network | Threat of escalation of privileges | Threatens Confidentiality, attacker may escalate privileges of themselves or someone else to access priorly restricted data they lack the authorisation to access. | High | High | High |
| Java Resource Adapter Architecture | Threat of JNDI injection | Threatens Integrity, JNDI injections allowing attackers to add to/ alter text log messages and search for resources. | Very High | High | High |
| Workstation | Threat of:  -Out of Date Hardware.  -Easy to crack Passwords.  -Unsupervised open computers | Risks to Confidentiality and Integrity, the privacy of patient and staff information affected with varying degrees depending on whether the password was breached, or the computer was left open. This means personal private information can be accessed, altered and/or shared. | High | Very High | High |
| Removeable Media (e.g. USB’s) | Threat of installation of malicious software, or exportation of private information. | Threatens Confidentiality and Integrity: Access to USB ports may allow for the installation of malware which can be result in data loss, scanning or sharing. Alternatively, sensitive data may be taken from a computer via the USB ports resulting similarly in damage to Confidentiality | Very High | Moderate | Moderate |
| Staff | Threat of:  -Weak Passwords.  -Passwords or other sensitive data places in unsafe areas (easily at risk).  -Gossiping of sensitive information | Threatens Confidentiality,  Weak passwords or passwords written down result it threats to hardware breaching from unauthorised personnel. Gossiping of sensitive information may result in unauthorised malicious personnel acquiring sensitive important data. | High | Very High | High |

# Risk analysis and evaluation

## Mitigation

# References