# SR - DSCG Assignment v50 - FINAL

*by* Simon Rees

**Submission date:** 15-Feb-2025 01:24PM (UTC+0000)
**Submission ID:** 250642348
**File name:** 51211_Simon_Rees_SR_-_DSCG_Assignment_v50_-_FINAL_634839_1420182718.docx (12.01M)
**Word count:** 12397
**Character count:** 79716

# SECURITY FRAMEWORK EVALUATION AND APPLICATION

Simon Rees

*University of Wales Trinity St David, Swansea, Wales*

0151968@student.uwtsd.ac.uk

*Abstract*—Organisations have become ever more reliant on computer systems to function. This makes the data collected from sources such as customers, suppliers and partners, extremely valuable to the organisation and needs to be carefully managed and protected. It is crucial that devices, systems and data remain secure. Maintaining Confidentiality, Integrity and Availability, which is the cornerstone of Data Security, Governance and Compliance is crucial for organisations.

The aims of this paper are two-fold. Task 1 to research security frameworks and models to gain knowledge of frameworks and undertake an analysis of what they are, how they are implemented and the benefits they can provide. In addition, any shortfalls will also be identified. Task 2 of this paper will design an information security system for an organisation outlining how to apply these frameworks and also provide recommendations to secure their devices, systems and data. Task 2 will also analyse and critique the need to maintain and regularly update regulations and standards.

A literature review was conducted utilising credible sources such as peer reviewed papers, textbooks, governmental and industrial resources. The framework developer's websites, and information management consultancy firms were also used. Three of the most respected and widely used frameworks within the United Kingdom were selected. These were namely ISO/IEC 2700, ITIL and COBIT. Additional frameworks and standards were researched during the design and recommendation stage of this paper.

Several security frameworks have been developed, each with their own merits. Once implemented, these frameworks benefit an organisation by improving their cybersecurity posture, securing data by implementing data governance principles, ensuring that systems are properly configured and maintained to a high standard. Frameworks can also identify and manage risks, whilst others can foster an environment of continual improvement.

Some shortfalls were identified. Implementing frameworks can be costly due to factors such as recertification requirements and potential consultancy fees. They can also be complex requiring staff to embrace the framework potentially with the need for training.

For an organisation to achieve Confidentiality, Integrity and Availability of their data several recommendations were identified. These include a multi-framework environment which provides an overarching cybersecurity solution resulting in a defence-in-depth approach. The implementation of policies that meet the NIST standards is crucial to safeguard devices, systems and data. Ensuring that staff utilise devices appropriately, and systems are configured and maintained correctly will be paramount in securing data. It is crucial that an organisation complies with regulations, wherever they operate globally and that they keep abreast of any changes in regulations as and when laws are reviewed and updated. Failure to do so will result in fines incurring costs to the company and potentially court proceedings.

## I Introduction

Nature Garden (NG) is a multinational company, where data security and the protection of Intellectual Property (IP) is of paramount importance. However, there are currently no security policies in place leaving them susceptible to cybersecurity threats such as data breach/loss and system compromise.

Task 1 of this assignment will research security frameworks and models to identify their approach, scope, processes, and outline the advantages/disadvantages of each.

Task 2 will utilise the knowledge gained from research conducted in task 1 to design an InfoSec programme for NG that will meet and exceed the requirements of the organisation. A set of recommendations will also be made with the aim of drastically improving the cybersecurity posture by implementing data governance securing data and assets.

The report will also critically evaluate why it is good practice to have new or updated regulations and standards.

Task 1 Research into Security Frameworks

## T1-1: International Standards Organisation (ISO) / International Electrotechnical Commission (IEC) 27000 Series

The ISO/IEC is a non-governmental, independent, standards development organisation established in 1946. They provide standards that [1]:

- Are recognised globally
- Set benchmarks
- Provide practical solutions

The ISO/IEC 27000 is a framework of standards relating specifically to Information Security (InfoSec) Management Systems (ISMS) (See Appendix A1.1). It provides guidance on InfoSec management ensuring data confidentiality, integrity and availability, (known as the CIA triad, see Appendix A1.2), is maintained. [2] [3].

The ISO/IEC 27000 series evolved from the British Standard (BS) 7799-1:1995 [4] [5]. The BS7799 later published as the ISO/IEC 17799:2005 was one of the first standards in the ISO27000 series [4].

The BS7799 was originally in three parts, which have now been incorporated into the ISO/IEC 27000 family, see Table 1.

Table 1: BS7799 Incorporation into the ISO/IEC 27000 series *[3] [4] [3] [6] [7] [8] [9] [10] [11]*

| BS Number | ISO Number | Title | Subject Area |
|---|---|---|---|
| BS7799 - Part 1 | ISO/IEC 27002 | Information security, cybersecurity and privacy protection - **Information Security Controls** | Best practices and **Security Control objectives.** Key areas covered<br>Access Control, Cryptography, Human Resource Security, Incident Response.<br><br>Can serve as a practical **blueprint** to secure Information assets. |
| BS7799 - Part 2 | ISO/IEC 27001 | Information Security, Cybersecurity and privacy protection<br>Information Security management systems - **Requirements** | Standard for Information Management Systems (ISMS), defining **requirements** ISMS must attain. |
| BS7799 - Part 3 | ISO/IEC 27005 | Information security, cybersecurity and privacy protection - **Guidance on managing information security risks** | Used to address security risks.<br>Guidance on **performing Security Risk assessment**, **treatment and management**.<br>Fulfills requirements of ISO/IEC27001 |

This framework now incorporates over fifty distinct standards encompassing a wide range of InfoSec areas.

The framework covers many security areas; however, it is impossible to evaluate every standard.

This report will focus mainly on ISO/IEC 27001 that provides a set of requirements for ISMS and comprises of 14 categories see Figure 1 (Fig.1) and Table 2 [12] [13]:




*Figure 1 : 14 categories of ISO/IEC 27001 [14]*

*Table 2: ISO/IEC 27001 Categories [3] [6] [9]*

| # | Category | Purpose |
|---|---|---|
| 1 | Information Security Policies | Clarifies InfoSec objectives - Should include metrics for ensuring Confidentiality, Integrity and Availability. Should also include ongoing continual improvement. |
| 2 | Organisation of information security | Outlines how InfoSec should be implemented within an organisation to ensure data should be managed and secured internally. This can include: Mobile device policy (Including Bring Your Own Device (BYOD)), Teleworking - Working from Home (WFH), |
| 3 | Human resource security | This would include Non Disclosure Agreements (NDA) so that information remains confidential. Background checks, Onboarding/Offboarding. Job rotation, separation of duties and mandatory vacations. |
| 4 | Asset Management | Identification, and management of assets is crucial. So that they are maintained properly, and are disposed of securely at the end of their use. |
| 5 | Access control | This ensures that only authorised users have access to data and services that they are authorised to access. This maintains the confidentiality and integrity of the data. |
| 6 | Cryptography | Cryptography can be used to maintain information confidentiality so that data is stored or transported in an encrypted form. Also this cryptography can be used for non-repudiation in the form of digital signatures. |
| 7 | Physical and environmental security | This would include Physical locks on Network Room / Server Room doors, CCTV, Security Personnel, Secure destruction of data. Also Environmental aspects such as ensuring a safe and stable power supply for servers. Implementing devices such as Uninterruptible Power Supplies (UPS) or generators. |
| 8 | Operations security | Provides guidance on day to day InfoSec tasks, and can include: Documenting operating procedures so that a standard approach is used across the organisation. Change management implementation, Malware controls, Backup regimes, Clock synchronisation, Log management, software installation and restrictions on who can install software |
| 9 | Communications Security | Focuses on Network security management, Firewalls, Intrusion Detection/Prevention Systems (IDPS), Network segmentation, Demilitarised Zone (DMZ). |
| 10 | System Acquisition, development, and maintenance | This ensures security requirements and security controls are part of any new system acquisition. Also ensures that if an organisation is developing their own software that a secure development policy is implemented. This category also ensures that system acceptance testing is undertaken. |
| 11 | Supplier Relationships | Supplier relationships are crucial as an organisation must source their equipment from a reputable company to avoid supply chain attacks. Also maintaining a good working relationship with the supplier will help with resolving technical issues or replacing devices. |
| 12 | Information Security incident management | This category focuses on Incident Response Planning (IRP), defining roles, responsibilities and procedures. Also processes for reporting security events, isolation/containment, service restoration and after action reports to learn from incident. How incident occurred, what improvements can be made. |
| 13 | Information security aspects of business continuity management | Outlines how an organisation can continue to function during a disaster (be it natural i.e. flooding or man made i.e. data breach or ransomware attack) or a crisis. |
| 14 | Compliance | Ensures Organisation complies with Internal Policies, and Laws where the business operates. |

Annex A of the ISO/IEC 27001 standard, provides an **overview** of security controls [15]. However, ISO/IEC 27002, provides guidance on **implementing** security controls [16].

Fig.2 Shows the major process steps of ISO/IEC 27001:

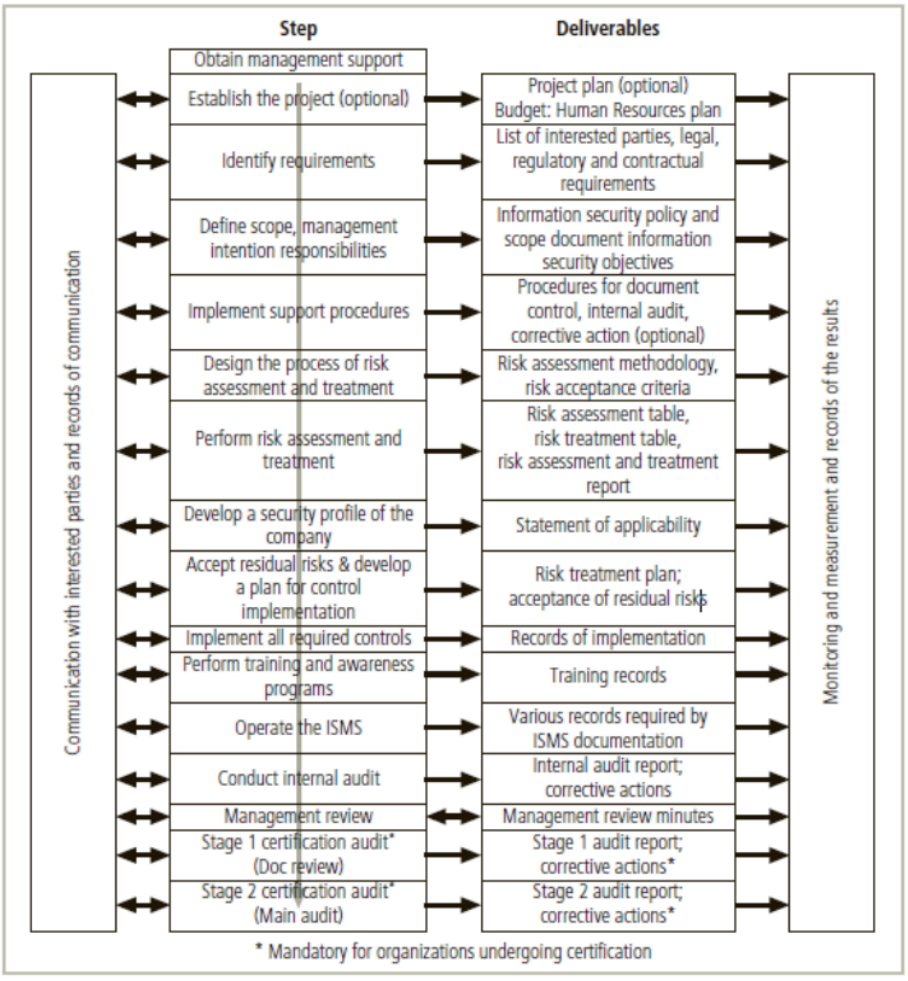



*Figure 2: ISO/IEC 27001 major process steps [12]*

Annex A has 93 security controls split into four domains see Table 3: [16] [17] [18] [19]:

*Table 3: ISO/IEC 27001 Annex A [19]*

| Domain | Subject area |
|---|---|
| Organisational Controlls | Policies, Rules, Processes, p classification of informatior |
| People Control | Human Resources, Pre-Emp Agreements (NDA), Reportin Awareness programs and tr |
| Physical Controls | Physical locks, Security Peri protocols, clear desk policy, disposal. |
| Technological Controls | Authentication, Malware prc (Segreagation, Firewall rules |

The standards of the ISO/IEC 27000 framework can be used in unison to further enhance the cybersecurity posture of an organisation [6] [7] [8] [20] [21]. Fig.3 show an illustration of this:

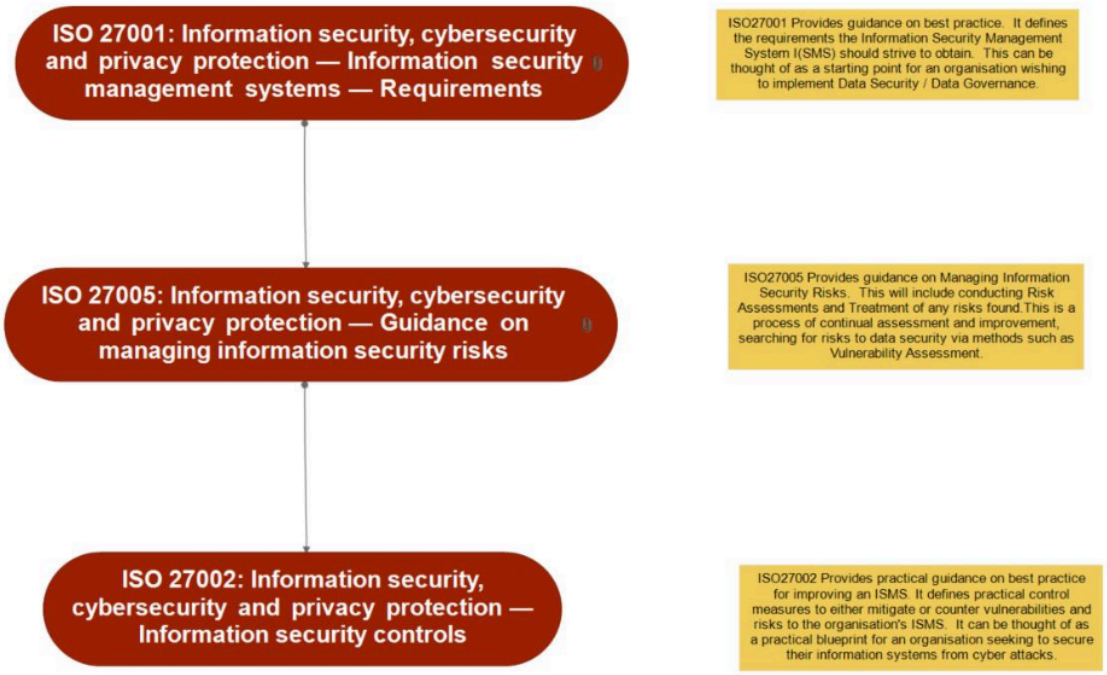



*Figure 3: ISO/IEC 27000 Standards working in unison*

The process outlined in Fig.3 enables an organisation to continually monitor its cybersecurity posture. It proactively detects and resolves vulnerabilities rather than reacting to cybersecurity incidents.

This approach allows an organisation to selectively implement some, or all standards of the framework.

This framework is a golden standard used by organisations seeking guidance on how best to secure their IT systems. The ISO/IEC conduct an annual survey showing the number of certifications attained by organisations. The latest statistics are in Table 4.

*Table 4: ISO/IEC 27001 certifications 2022-2023 [22] [23]*

| ISO/IEC 27001 Standard | | |
|---|---|---|
| Year | Number of Certificates | Number of Sites |
| 2022 | 37,766 | 66,101 |
| 2023 | 47,291 | 79,213 |

Table 4 shows an increasing trend in the adoption of the ISO/IEC 27001 standard [24]. This certification provides a benchmark for organisations demonstrating the highest security standards have been implemented for their ISMS. [25]. According to the BSI, certification can reduce business risks by 75% [17].

This gives customers, suppliers and other organisations confidence that their data is secure and gains trust which is crucial when large financial transactions are in play. The benefits and drawbacks of implementing ISO/IEC 27000 are outlined in Table 5:

*Table 5: Analysis of ISO/IEC 27000 [3] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35]*

| Advantage | Disadvantage |
|---|---|
| ISO/IEC 27000 is a mature framework, well respected and globally renowned. A tried and tested framework currently in use by many organisations today. | ISO/IEC 27001 can be costly to implement compared to other frameworks. For example NIST CSF is free and without time limits. |
| Auditing / preparing for certification can uncover potential InfoSec/Cybersecurity issues. | Potential third party consultancy costs - Daily fee of approximately £1,250 |
| Following the ISO/IEC 27000 framework guidance will improve the cybersecurity posture of the organisation. Providing guidance on a whole slew of areas. | Costs include auditing required for ISO/IEC 27001 certification, surveillance auditing to ensure that standard has been implemented properly. |
| ISO/IEC 27000 can be used selectively - organisations are able to implement only some of the standards within the framework. | Costs increase depending on the size of the business. Can range from £6,000 to well over £30,000. |
| ISO/IEC 27000 can be used selectively - organisations are able to implement only some of the standards within the framework. | Time required by staff to prepare for certification / recertification. Prepare for security audits. |
| ISO/IEC 27000 Demonstrates a commitment to ensure data security. Providing confidence in the organisation for customers and suppliers - maintaining the CIA triad. | Leading to ISO/IEC 27001 Standard has recently seen a slight decline with some organisations that are not highly regulated. |
| Organisations can obtain ISO/IEC 27001 certification a globally recognised golden standard in InfoSec and Data Governance. | ISO/IEC 27001 requires recertification required every three years. |
| ISO/IEC 27000 standards can be used together:<br>ISO/IEC 27001 to set out the requirements of the organisation,<br>ISO/IEC 27005 to implement Risk management,<br>ISO/IEC 27002 to implement controls to mitigate/eliminate risks. | |
| Companies that implement ISO 27000 framework are able to identify risks early and put measures in place to resolve them. | |
| Allows for better integration of systems as ISO 27000 standardises systems. | |
| It is possible to integrate ISO/IEC 27000 with other frameworks. It is commonplace for organisations to implement parts of the ISO/IEC 27000 framework alongside other frameworks | |
| Implementing ISO/IEC 27000 and gaining ISO certification could improve the chance of winning government and other lucrative contracts. | |
| The ISO/IEC 27000 framework is continually improving, with new standards being added as required to keep pace with changing threats, and business needs. | |
| A few potential benefits of following ISO/IEC 27000 guidance: *Placing preventative measures in place, to stop a cybersecurity attack.<br>*Risk Management to assess any potential threats so that they can be mitigated or eradicated.<br>*Security controls to improve the security of Network, Server infrastructure, applications and end user equipment.<br>*Incident response, guidance on Indicators of Compromise (IOC)<br>*Digital Forensic analysis, Electronic Discovery (e-Discovery) process | |

In summary, ISO 27000 is a globally recognised and respected set of standards. Implementation of this framework improves cybersecurity, follows industry recognised practices, identifies potential risks, puts security controls in place to mitigate risks. Although it can be costly to implement, and recertification required, some organisations see this as a worthwhile investment. It can help to avoid financial penalties [36], also the additional security accreditation may allow for more lucrative contracts.

## T1-2: Information Technology Information Library (ITIL)

ITIL is a service management framework of best practices for Information Technology (IT) service delivery. ITIL was first developed in the 1980s by the Central Computer and Telecommunications Agency part of the UK Government. ITIL was acquired by Axelos in 2013 [37]. The original aim was to standardise and incorporate manufacturers best practices from around the globe.

The driving force behind the creation of ITIL was the UK Government realising its increasing reliance on IT. The lack of standardised IT service delivery procedures resulted in increasing costs. [38].

The current version, ITIL4 is available as a series of books comprising of 34 best practices spread across three categories [39]:

- General Management Practices
- Service Management Practices
- Technical Management Practices

Fig.5 Shows an illustration of ITIL4:

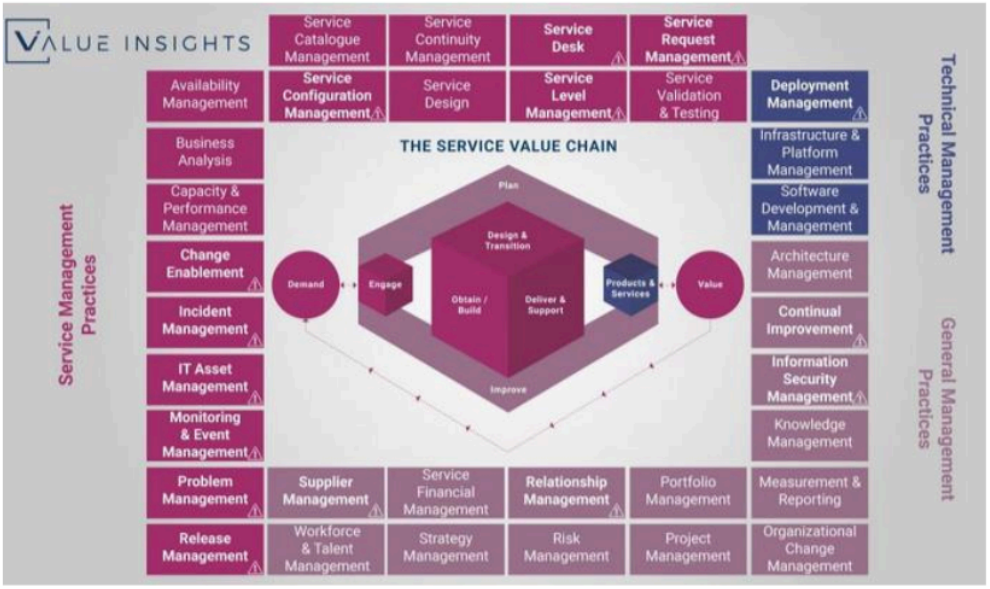



*Figure 4: 34 ITIL best practices [40]*

ITIL applies a holistic approach and provides guidance on service management across the whole organisation aligning the objectives of both the organisation with IT.

Risk management is central to ITIL, and an integral part of the organisation's activities as financial resources are not wasted by having to resolve issues [41].

See Tables 6-8 analyses ITIL principles [37] [40] [42] [43].

*Table 6: Principles 1-14 of ITIL*

| General Management Practices | | | |
|---|---|---|---|
| # | Principle | Purpose | Advantage |
| 1 | Architecture management | Provides principles to help manage the organisation's structure. | Assists with managing organisation structure. Can also manage changes. |
| 2 | Continual improvement | Continually improve processes to align with changing needs of the business. | Assists organisation to identify opportunities for improvement. |
| 3 | Information security management | Ensuring Confidentiality, Integrity and Availability (CIA) of digital information. Ensuring Authentication and Authorisation processes are in place and Preventing data breaches. | Protects the organisation's data by maintaining the CIA triad of ISMS. |
| 4 | Knowledge management | Effective and efficient use of knowledge and data. | Improves the way organisations use data |
| 5 | Measurement and reporting | To assist with good decision making, continual measuring and reporting of systems. **Risk Assessments** are a key part of this process. | Continual monitoring and Risk Assessments can identify potential issues early, allowing implementation of mitigations/ resolutions. |
| 6 | Organisational change management | Guidance on change management processes. So that changes are documented and roll back procedures are in place if required. | Smooth management of change, and roll back processes in the event of an issue. Improves the end user experience. |
| 7 | Portfolio management | Ensures that the organisation has the correct services in place to achieve the organisations goals. | Goals are achieved within the organisation's funding and resource budgets. |
| 8 | Project management | Guidance on project management, to ensure that projects are delivered successfully, on time and within budget. ITIL4 can integrate with PRINCE2 to enhance project delivery. | Ensures successful delivery of projects. Includes stakeholder involvement ensuring they are informed of progress. |
| 9 | Relationship management | Provides guidance on identifying, analyse, monitor and continually improve relationships with stakeholders. | Ensures project success by maintaining good relationships with stakeholders. |
| 10 | Risk management | Guidance on identifying and addressing risks. This approach ensures that risks are identified early to reduce financial consequences. | Identifies risks at an early stage avoiding downtime of services, and financial loss. |
| 11 | Service financial management | Guidance on efficient use of financial resources. | Reduces costs and avoids financial mismanagement. |
| 12 | Strategy management | Guidance on defining goals and strategies of achieving them. Resource allocation to achieve goals. Priority management of the organisation. | Provides clear indication of direction of travel and allocating resources to achieve goals. |
| 13 | Supplier management | Managing supplier relationships, to ensure supplier products and services are delivered smoothly. | Nurtures good relationships providing opportunity for collaborative working. |
| 14 | Workforce talent management | Onboarding procedures, guidance on recruitment, training and performance improvement of employees. Succession planning. | Ensures the right staff are in the correct roles. Also ensures that when staff leave the organisation others can continue with that role. |

*Table 7: Principles 15-31 of ITIL*

| Service Management Practices | | | |
|---|---|---|---|
| # | Principle | Purpose | Advantage |
| 15 | Availability management | Guidance on ensuring the availability of services to clients. | Ensures that customer's requirements are fulfilled. |
| 16 | Business analysis | Analysis of business processes to identify and resolve potential issues. | Promotes value creation. |
| 17 | Capacity and performance management | Provides guidance on ensuring that services meet performance levels expected by the customer. How to address current and future demands. Service Level Agreement (SLA) used to define service levels. | Service delivery performance levels agreed in the SLA are maintained. Identifies changes to demand so capacity can be increased if required. |
| 18 | Change enablement | Advises that Risk assessments are conducted prior to changes being implemented. Ensures that changes are managed efficiently. | Changes are properly authorised, and risks related to change are identified and mitigated. |
| 19 | Incident management | Incident management to ensure that minimal disruption is caused to the organisation and normal service is resumed as soon as possible. | Reduces impact of incident on customers, downtime reduced. |
| 20 | IT asset management | Management of IT Assets during the lifecycle of the asset. From purchase to disposal. Focuses on decision making, cost control and risk management. | Reduces costs of purchasing assets, ensures they are maintained properly and disposed of properly so that data is erased securely. |
| 21 | Monitoring and event management | Monitoring of Information Security Events and infrastructure services. | Ensures a quick response to security events. Identifying cyber attacks early. |
| 22 | Problem management | Focuses on cause of incidents and methods of resolving them. Assists in reducing the probability and impact of incidents. | Identifies root cause generating incidents. Resolving the root cause could resolve several incidents simultaneously. |
| 23 | Release management | Manages how services are implemented, and updated. Software upgrades, or changes to services. | Ensures that new services are rolled out smoothly, minimising impact to end users. |
| 24 | Service catalogue management | The service catalogue outlines all of the services provided. Ensures the availability of this information to authorised users. | Standardisation of services across the organisation, useful for distributed organisations. |
| 25 | Service configuration management | Service configuration is documented and available to authorised staff to assist with support. | Outlines the configuration requirement of devices, so they are configured according to best practices. Ensures that devices are configured securely. |
| 26 | Service continuity management | Guidance on how to protect services in the event of a severe incident so that the organisation remain resilient. | Ensures the organisation can continue to function and provide services during a disruptive incident. |
| 27 | Service design | Focuses on service planning, and design so that they may be successfully delivered. | Ensures that service is fit for intended purpose. Also ensures that service can be successfully delivered by organisation. |
| 28 | Service desk | Single Point of Contact for users, focused on incident resolution. | Ensures customer requests are fulfilled, providing incident resolution. |
| 29 | Service level management | Sets targets for service delivery response times. Creating a metric that can be used to identify issues and highlight required improvements. | Continual improvement of service delivery, by monitoring performance and identifying areas that require improvement. |
| 30 | Service request management | Provides guidance on supporting user service requests effectively. | Ensures customer satisfaction. |
| 31 | Service validation and testing | Ensures that any changes to services still meets the original requirements. Done by checking regulatory requirements, the objectives of the business and customer feedback. | Ensures that new or modified services meet the customer's requirements. |

*Table 8: Principles 32-34 of ITIL*

| Technical Management Principles | | | |
|---|---|---|---|
| # | Principle | Purpose | Advantage |
| 32 | Deployment management | Guidance on implementing or updating the hardware, software, process or document. Going from the initial test or staging into the live environment. | Management of service deployment from initial testing through to end user deployment. |
| 33 | Infrastructure and platform management | Monitoring infrastructure / platforms deployed within the organisation and by service providers. | Monitoring infrastructure services allows for quick identification of issues so they can be resolved quickly. |
| 34 | Software development and management | Ensures that software developed by the organisation meets the requirements of stakeholders. | Positive stakeholder engagement, ensures software meets intended requirement and is reliable. |

The Service Value Chain (SVC) is central to the ITIL framework and governs how the components interact [42], see Fig.6:

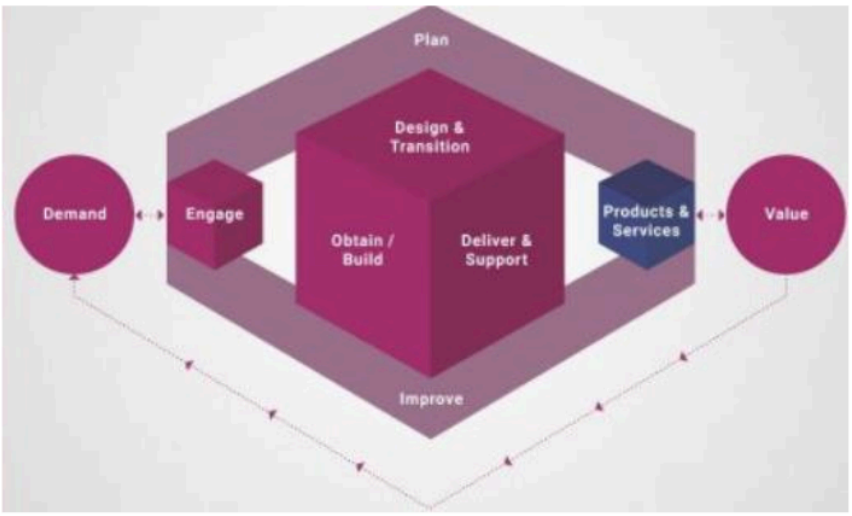



*Figure 5: ITIL4 Service Value Chain [44]*

Table 9 details the ITIL4 SVC:

*Table 9: ITIL4 SVC Activities [41] [44]*

| # | SVC Activities | Description |
|---|---|---|
| 1 | Plan | Objectives are clearly laid out and shared with all participants. |
| 2 | Engage | Engage with stakeholders to confirm requirements. Continual stakeholder engagement throughout. |
| 3 | Design & Transition | Design service to meet stakeholder's requirements. Taking into account any current services that need to migrated over to the new service. |
| 4 | Obtain/Build | Process of acquiring or developing service components. |
| 5 | Deliver & Support | The service goes live meeting stakeholder's requirements. Service is delivered and supported by Service Desk. |
| 6 | Improve | Continual improvement of service. |

ITIL is the most popular service management framework in the UK. In 2005, ITIL aligned with the ISO/IEC 20000 Service Management Standard and has gained a higher standing globally [38]. Large corporations such as NASA, Microsoft and Spotify utilise ITIL practices [43] and as of March 2024, 82% of Fortune 500 companies have also implemented the ITIL framework [45] [46].

Table 10 provides an analysis of the advantages and disadvantages of ITIL. Many of the benefits have been derived from case studies detailing the impact ITIL has had on their organisation [43] [45] [47] [48] [49] [50] [51] [52] [53] [54] [55]:

*Table 10: Analysis of ITIL*

| Advantages | Disadvantages |
|---|---|
| ITIL processes can integrate seamlessly with other Axelos products such as Agile and DevOps which are very popular software development methodologies, and PRINCE2 used in project management. | ITIL has a steep learning curve, staff that are unfamiliar with ITIL principles will need to receive training which requires time. |
| Improves efficiency and therefore saving costs. | Adopting ITIL4 can be costly, implementing changes to follow ITIL processes and training staff. |
| Allowed Spotify to maximize resource utilisation. | Implementing ITIL4 can be resource intensive. This can be an issue especially for smaller organisations. |
| Allowed Spotify to deliver services faster than their competitors. | Implementing ITIL4 can be complex and challenging to implement. |
| Allowed Spotify to improve their services faster than the competition. | Potential consultancy costs to implement ITIL4 due to complexity. |
| Allowed Spotify to visualise the overall workload, and then manage the workload to meet the needs of their customers in an efficient and | Staff may resist adoption of ITIL, some may prefering to sitck to their usual working methodology over embracing ITIL4 practices. |
| Allowed Wipro to adopt ITSM best practices. | ITIL4 is flexible, but cannot adapt to rapidly changing ciricumstances well. |
| Wipro reduced their Mean Time To Recovery (MTTR), resolving issues | |
| Wipro implemented Change control, improving change success rates. | |
| Wipro reported cost and time saving using ITIL4 principles. | |
| Wipro also noted an improvement of customer satisfaction. | |
| Wipro reported a 10-15% year-on-year reduction in service disruption since implementing ITIL4. | |
| Vodafone implimented ITIL4 leading to standardisation - this provided repeatable standard service for all new products. | |
| Vodafone reported that costs and risks were reduced by standardising products and implementing a blueprint. | |
| Vodafone also implemented the principle of continual improvement, monitoring services and reacting accordingly. | |
| Oxford University (OU) implemented ITIL4 and by re-designing their service catalogue allowed them to clarify the support structures required for each service as some had become outdated. | |
| OU simplified their IT systems to promote better support. Standardisation allowed more staff to better understand their systems. | |
| Using ITIL 4 principles OU were able to reduce the number of annual major incidents (down from eight the previous year to two). | |
| OU reported that continual improvement was key, especially following | |
| OU could easily integrate the ITIL framework with Agile methodology (already in use by the software development team). | |
| OU reported that ITIL and Agile complimented each other well:<br>*Agile focuses on the software development process<br>*ITIL can give a good overview of the entire picture. | |

ITIL principles provides many benefits to an organisation such as improved customer service, reduction of service interruptions, and improved efficiency. However, implementing ITIL can be costly, complex and requires staff to embrace ITIL, which can be challenging.

## T1-3: Control Objectives for Information and related Technology (COBIT)

The Information Systems Audit and Control Association (ISACA) was founded in 1969. ISACA are a non-governmental organisation, whose mission is the pursuit of digital trust by providing guidance on information security, privacy and governance. [56] [57]. ISACA advocate a Digital Trust Ecosystem Framework, this ensures that every digital interaction and transaction is trusted, legitimate, reflecting the CIA triad [58] [59].

In 1996, ISACA developed COBIT which provides a comprehensive IT management and governance framework. It was originally developed to assist financial auditors to ensure the security of digital data. Subsequent iterations expanded the remit of COBIT to include IT Management and Information Governance [60] [61] [62]. The current version is COBIT 2019 which has six key components, see Fig.7:

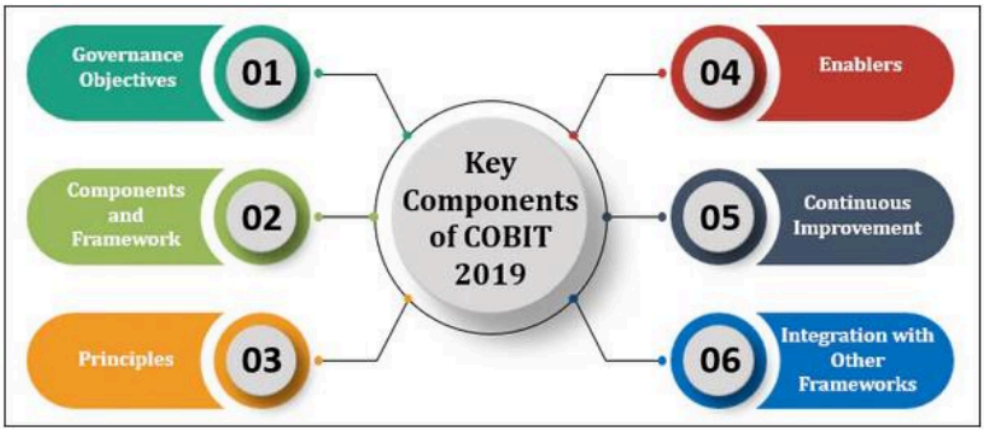



*Figure 6: Key Components of COBIT 2019 [63]*

Table 11 shows an analysis of the key components of COBIT:

*Table 11: Analysis of key components of COBIT 2019 [63]*

| # | Key Concepts | Description |
|---|---|---|
| 1 | Governance Objectives | These involve: Strategic alignment, risk assessment, value discovery, resource management, performance measurement. |
| 2 | Components and Framework | These include: Governance and Management Objectives. These provide a structured approach to IT governance and management. |
| 3 | Principles | Guidance for implementing COBIT 2019. Discussed in detail within this report. |
| 4 | Enablers | Facilitate the governance and management objectives. They are separated into seven categories:<br>Principles, Policies, Frameworks, Processes, Organisational Structures, Culture, Information. |
| 5 | Continual Improvement | This is done by regular assessment, and refining practices accordingly. Adapting the business to changes in technology and business requirements. |
| 6 | Integration with Other Frameworks | Active promotion of integrated frameworks. Allows for integration with ITIL, ISO/IEC 27001 and NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF) |

Key component number 3 of COBIT 2019 is based on six principles, illustrated in Fig.8:

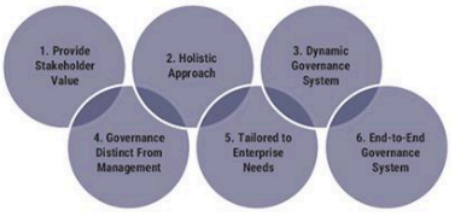



*Figure 7: COBIT 2019 Principles [64]*

Table 12 provides further analysis on the six principles of COBIT:

*Table 12: COBIT 2019 - Six Principles [65]*

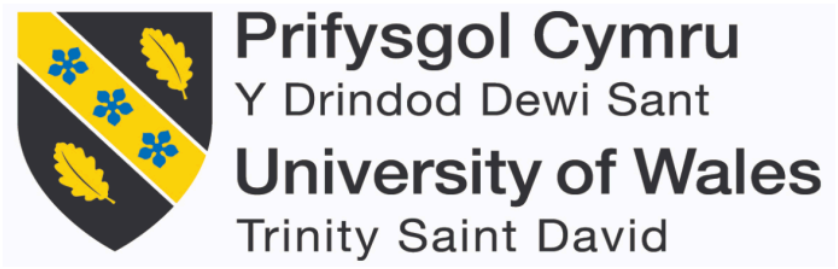
| # | Principle | Description |
|---|---|---|
| 1 | Provide Stakeholder Value | Ensures that IT decisions meet stakeholders needs. |
| 2 | Holistic Approach | IT governance comprises of many components - ensures that all components are integrated effectively |
| 3 | Dynamic Governance System | Crucial that system is dynamic to take factors such as a change in technology or strategy can be accommodated. |
| 4 | Governance Distinct from Management | Governance and Management require different supporting strategies.<br><br>Governance: Evaluates stakeholder needs and prioritises objectives.<br><br>Management: Monitoring organisation's activities and ensure that they align with stakeholder's needs. |
| 5 | Tailored to Enterprise Needs | Adapt the framework to meet the needs of the organisation. |
| 6 | End-to-End Governance System | Single integrated system aligning governance and management activities. |

Table 13 gives analysis of the advantages and disadvantages of the COBIT framework.

*Table 13: Analysis of COBIT [66] [67] [68] [69] [70] [71] [72] [73] [74] [75] [76]*

| Advantages | Disadvantages |
|---|---|
| Aligns IT and organisational goals and objectives . | COBIT is a comprehensive framework making it complex. |
| Improves IT Governance as it defines roles and responsibilities defining accountability. | It can be difficult to implement due to complexity requiring consultancy support, which can be costly. |
| Defining roles and responsibility improves the decision making process. | The implementation of the COBIT framework requires expertise, therefore there could be a steep learning curve, training required for staff to adopt the framework. |
| Enhances risk management, conducting vulnerability assessments to find and eliminate threats. | |
| Flexible, can be customised to meet organisational requirements. | |
| Continuous improvement of InfoSec systems. | |
| Holistic approach - Single integrated framework that incorporates all departments of an organisation. | |
| Designed to integrate with other frameworks, such as ISO/IEC 27000 and ITIL. Integrated frameworks can provide enhanced InfoSec benefits. For example, while COBIT focuses on IT Governance and management, ITIL focuses on Service Delivery. There are some areas that crossover such as risk management but in general COBIT can be thought of providing guidance on the strategic direction of travel, and ITIL providing practical guidance on how to get there | |
| Ensures organisations comply with policies and regulations. | |

COBIT provides a comprehensive IT governance framework which is designed to enhance security by integrating with other InfoSec frameworks (See Appendix A1.3). It provides a mechanism for risk management and continuous improvement whilst complying with policies and regulations. However, COBIT is a complex framework, which makes implementation challenging and costly as expertise from consultants or specially trained in-house staff is required.




University of Wales Trinity Saint David

Welsh Institute of Sciences and Art (WISA)

*Simon Rees (0151968)*

*MSc Cybersecurity and Digital Forensics*

*Data Security, Governance and Compliance (ACCA7028)*

V50

I confirm that I have not used any AI tools in the research and creation of this assignment. I confirm that I have not presented any AI generated materials as my own work. I confirm I have copies of my drafts, notes, and other resources I used, which I may be asked to provide in evidence.

## Table of Contents


T1-1: International Standards Organisation (ISO) / International Electrotechnical Commission (IEC) 27000 Series ..... 2

T1-2: Information Technology Information Library (ITIL) ..... 8

T1-3: Control Objectives for Information and related Technology (COBIT) ..... 13

Task 2 Applying Security Frameworks ..... 19

Task 2a Proposed Design for NG ..... 19

T2a-1 Organisational structure ..... 20

T2a-2 Information Security Design for NG ..... 22

Recommendations ..... 28

Task 2b Reasoning for updated regulations and standards ..... 30

Conclusion ..... 34

References ..... 35

Appendices ..... 52

Appendix 1 ..... 52

A1.1 ISO/IEC 27000 Family of Standards ..... 52

A1.2 Confidentiality, Integrity, Availability (CIA) and Denial, Alteration, Disclosure (DAD) Triads ..... 53

A1.3 Visual overview of InfoSec frameworks ..... 53

Appendix 2 ..... 54

A2.1 Compliance (Laws and Ethics) ..... 54

A2.2 Governance and Strategic Planning for Security ..... 56

A2.3 Security Policies ..... 60

A2.4 Risk Management ..... 63

A2.5 Security Management Models and Practices ..... 70

A2.6 Contingency Planning (CP) ..... 74

A2.7 Protection Mechanisms ..... 83

A2.8 Service Level Agreement (SLA) ..... 100

A2.9 Threat, Vulnerability Asset Worksheet ..... 101

A2.10 Service Organisation Controls (SOC) Audits ..... 102

A2.11 Continuity of Operation Planning (COOP) ..... 102

# Task 2 Applying Security Frameworks

## Task 2a Proposed Design for NG

Using the knowledge gained from task 1, the following is the proposed InfoSec design for NG that will meet and exceed the requirements of the organisation. A set of recommendations will also be made with the aim of drastically improving the cybersecurity posture by implementing data governance securing data and assets.

Table 14 Provides the company profile of NG.

*Table 14: Company Profile*

| **Company Profile:** | |
|---|---|
| Name | Nature Garden (NG) |
| Headquarters | Llanelli, Carmarthenshire, Wales, UK. |
| Business Sector | Healthy Living Produce |
| Location of Business | Global (Mainly US, Europe, Oceana) |
| Size of Business | Large (1050) |
| Promotion of activities | Massive online presence, social media presence |
| Customer base | International |
| **Technical Considerations:** | |
| Server Infrastructure | Cloud Based |
| Network Infrastructure | 95% Wireless based |
| **Requirements:** | Company under immense pressure for staff to use personal devices to access corporate network & resources |
| | Customers to use personal devices to access corporate network & resources |
| | Security of Client's data (Confidentiality, Integrity, Availability) |
| | Security of Staff data (Confidentiality, Integrity, Availability) |
| | Protection of Intellectual Properties (IP) |
| | IP is worth Billions to the company |
| | Information Security Policy - None in place currently |

## T2a-1 Organisational structure

The starting point of the design process is to assess NG's organisational structure. The location of the InfoSec team is crucial as it will have a bearing on managerial decisions which will filter down the hierarchy. It is recommended that the InfoSec team should sit within the IT department.

See Fig.9 and Table 15 Reasoning of InfoSec location [3] [4]:

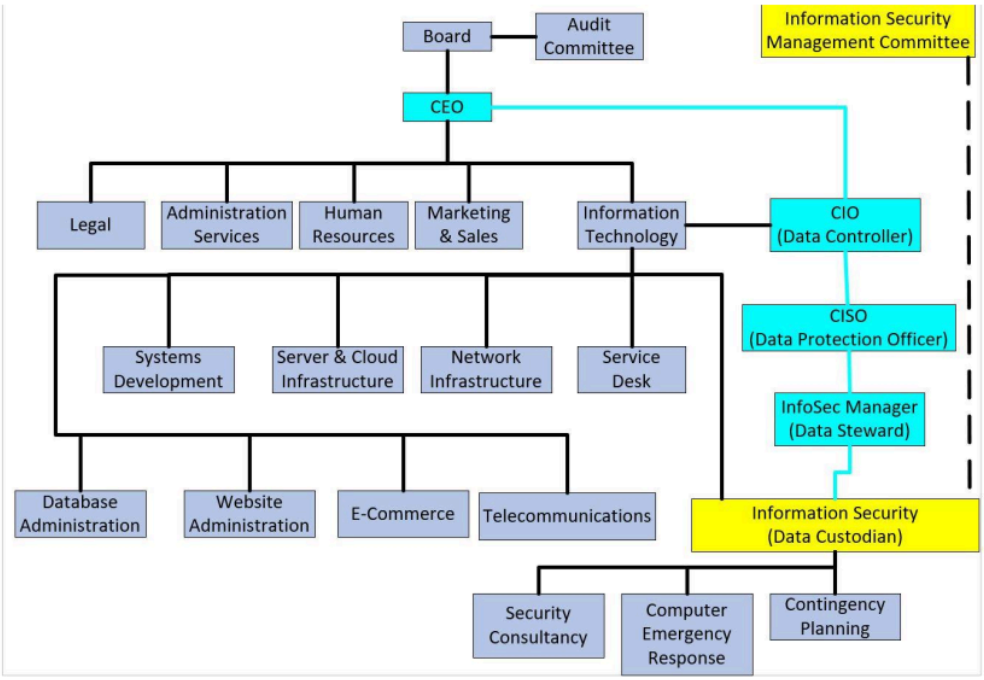



*Figure 8: Wood's Option 1: InfoSec reporting to IT department [4]*

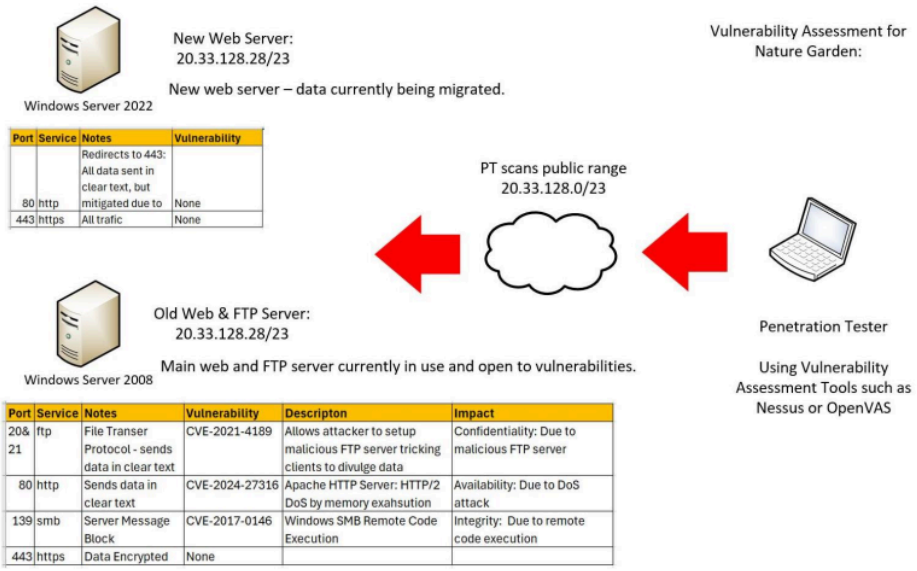
*Table 15: Analysis of placing the InfoSec team within the IT Department*

| Advantages | Disadvantages |
|---|---|
| Embedding the InfoSec team within the IT department enables close engagement. Changing the philosophy of the other IT departments so that InfoSec is at the forefront of their minds. Ensuring they build InfoSec into their projects at the early planning and development stages of their projects. | In this model the Chief Information Security Officer (CISO) reports to the Chief Information Officer (CIO) [Not shown]. This can work well if both are of the same mind. There could be a conflict of interest between security and ease of use. |
| With close working relationships between InfoSec and other IT teams, vulnerabilities can be identified and rectified quickly. | * There can be occasions where other IT teams and InfoSec team within the IT department will have opposing views on many areas including accessibility and ease of use for the end user.<br>* These challenges can be overcome by discussing the benefits of preventing unauthorised access to data with the other IT teams. |
| The InfoSec team can work with the other IT teams to document the resolutions so they can be carried out by all of the IT teams therefore reducing the overall number of vulnerabilities. | Resource allocation issues: There is a risk the CIO may favour projects that will introduce goods or services quickly to market, or enhance usability of services. Sacrificing resources for InfoSec projects, which could be seen as costly. |
| Close working relationships within the IT department will benefit contingency planning, such as Incident Response, Disaster Planning, Business Continuity, Crisis Management. | |
| During an incident close links between all IT teams will benefit the organisation as they will be able to feedback the current status of their systems, and what impact they are facing. Resolutions can be quickly fed back to these teams. Quick feedback on status of systems as they are implementing resolutions. | |
| Clearly defined roles linking to General Data Protection Regulation (GDPR) reponsibiities. | |

## T2a-2 Information Security Design for NG

### *T2a-2-1 Outlining NG's Current Security Posture*

Prior to the InfoSec design phase for NG a VA was conducted to establish the current security posture of NG. This highlighted several vulnerabilities with NG's current infrastructure. It is crucial that these vulnerabilities are mitigated prior to implementing the InfoSec design for NG, see Fig.10:




| Port | Service | Notes | Vulnerability |
|---|---|---|---|
| 80 | http | Redirects to 443: All data sent in clear text, but mitigated due to | None |
| 443 | https | All trafic | None |

| Port | Service | Notes | Vulnerability | Descripton | Impact |
|---|---|---|---|---|---|
| 20& 21 | ftp | File Transer Protocol - sends data in clear text | CVE-2021-4189 | Allows attacker to setup malicious FTP server tricking clients to divulge data | Confidentiality: Due to malicious FTP server |
| 80 | http | Sends data in clear text | CVE-2024-27316 | Apache HTTP Server: HTTP/2 DoS by memory exahsution | Availability: Due to DoS attack |
| 139 | smb | Server Message Block | CVE-2017-0146 | Windows SMB Remote Code Execution | Integrity: Due to remote code execution |
| 443 | https | Data Encrypted | None | | |

*Figure 9: VA process*

Several vulnerabilities were identified during the VA process, see Appendix A2.4 for more details. These were prioritised using a risk matrix see Table 16:

*Table 16: Risk rating worksheet*

| Asset | Vulnerability | Likelihood | Impact | Risk-Rating Factor | Details |
|---|---|---|---|---|---|
| Existing Web server | HTTP DoS Vulnerability | 8 | 9 | 72 | This is a critical vulnerability of NG, as this will impact online sales, and needs to be resolved first. |
| Existing Web server | SMB Remote Code execution | 7 | 9 | 63 | The consultants have advises NG that the likelihood of the SMB attack is slightly less, this is also a critical vulnerability but the http has higher priority. Both vulnerabilities need addressing as soon as possible. |
| Existing FTP server | Malicious FTP Server vulnerability | 6 | 6 | 36 | The FTP server is in the process of being decommissioned, impact is less severe. |

It was discovered that the Web server had a critical vulnerability that would have a major impact to NG.

A Cost Benefit Analysis to mitigate this vulnerability can be found in Table 17:

*Table 17: Calculation of ALE and CBA for NG [77] [78]*

| Item | Value | Details |
|---|---|---|
| Asset Value (AV) | £10,000 per hour | During DDoS (Distributed Dinal of Attack) attack, server undamaged, but service degraded and unable to meet demand. |
| | 2 Hours | After discussions with Cybersecurity consultants, it is anticipated that a single DoS attack could last for two hours. |
| AV | £ **20,000.00** | |
| Annualised Rate of Occurrence (ARO) | 4 Attacks | It is anticipated that 4 attacks will take place annually. |
| Exposure Factor (EF) | 90% | It is expected that system capacity will be reduced by 90% during a DoS attack. |
| | | |
| Single Loss Expectancy (SLE) | £ 18,000.00 | SLE = AV x EF (£20,000 x 90%) |
| | | |
| Annualised Loss Expectancy (ALE) | £ 72,000.00 | ALE = SLE x ARO (£18,000 x 4) |

| Item | Value | Details |
|---|---|---|
| Annual Cost of Safeguard (ACS) | £ 3,000.00 | Cloud Service Provider DDoS protection: Amazon Web Services Shield (DDoS protection service) |
| | | |
| ALE (Precontrol) | £ 72,000.00 | |
| ALE (Postcontrol) | £ 8,000.00 | AWS Shield in place for one year. (EF now 10%) |
| | | |
| Cost Benefit Analysis (CBA) | £ 61,000.00 | CBA = ALE (Pre) - ALE(Post) - ACS (£72,000 - £8,000) - £3,000 |

### *T2a-2-2 InfoSec Design for NG*

Based on the research conducted in task 1, the best InfoSec design approach for NG is a multi-framework environment which includes ISO/IEC 27000, ITIL and COBIT.

The design considerations in Table 18 need to be incorporated to meet the requirements of NG. In addition, further supporting evidence can be found in the appendices listed in Table 18:

*Table 18: NG InfoSec Design*

| NG Requirement | Design Considerations | For Supporting Research See Appendix: |
|---|---|---|
| Compliance (Ethics) | The **Virtue** approach is the most suitable ethical approach for NG as the nature of the business embracing virtues such as compassion for their customers and the environment being key. Along with honesty and integrity so that good relationships can be build with both their customers and suppliers alike. | A2.1 |
| Compliance (Law) | For NG to meet legal compliance it is crucial that **jurisdiction** in the geographic areas of operations is considered. Following the restructure of NG, clearly defined roles now map directly to the General Data Protection Regulation (**GDPR**) roles. | |
| Governance and Strategic Planning for Security. | NG requires guidance on its long term direction and plan for protecting information assets. Implementation of **COBIT 2019** and **ISO/IEC 27014** frameworks. | A2.2 |
| Security Policies | Currently NG does not have any security policies in place. Implementation of recommended Security Policies as outlined by the National Institute of Standards and Technology **(NIST) 800-14,** including **Social Media**. See Fig.10 | A2.3 |
| Risk Management | A number or risks have been identified at NG with no formal procedure of reporting or resolution.<br>See Fig.9 for an example of risk discovered by a Vulnerability Assessment (**VA**), the Risk Rating and Cost Benefit Analysis in Tables 17-18. | A2.4 & A2.9 |
| Security Management Models and Practices | Several Security Management Frameworks have been recommended which includes: **ISO/IEC 27000** to provide guidance on Security system implementation, **ITIL4** to provide guidance on Service Delivery, Cloud Security Alliance (**CSA**) - Cloud Control Matrix (**CCM**), to provide guidance on securing cloud infrastructure.<br>Complying with these frameworks satisfies requirements of cybersecurity audits such as the Service Operational Controls (**SOC**) audits. | A2.5 & A2.10 |
| Contingency Planning (CP) | It is critical that the relevant CP teams are created along with the policies, plans in order to support the organisation in the event of an Incident, Disaster, or Crisis. Having the ability to support Business Continuity from an alternate site allows the organisation to mitigate the impact of a disaster. | A2.6 & A2.11 |
| Protection Mechanisms | Several detailed recommendations have been made to improve NG's infrastructure which includes Authentication, Firewalling, Wireless, Device Management Systems, implementing a new network design. Staff **personal devices** being used to access sensitive IP data is also addressed. | A2.7 |
| Service Level Agreement | Currently NG does not have any formal SLAs in place when providing customer support. This has resulted in poor response times and poor customer satisfaction. | A2.8 |

NG currently do not have any InfoSec policies in place which is a major security risk. From the research conducted for task 1, it is essential that as part of the InfoSec design that appropriate InfoSec policies are implemented according to NIST guidelines, see Fig.11:

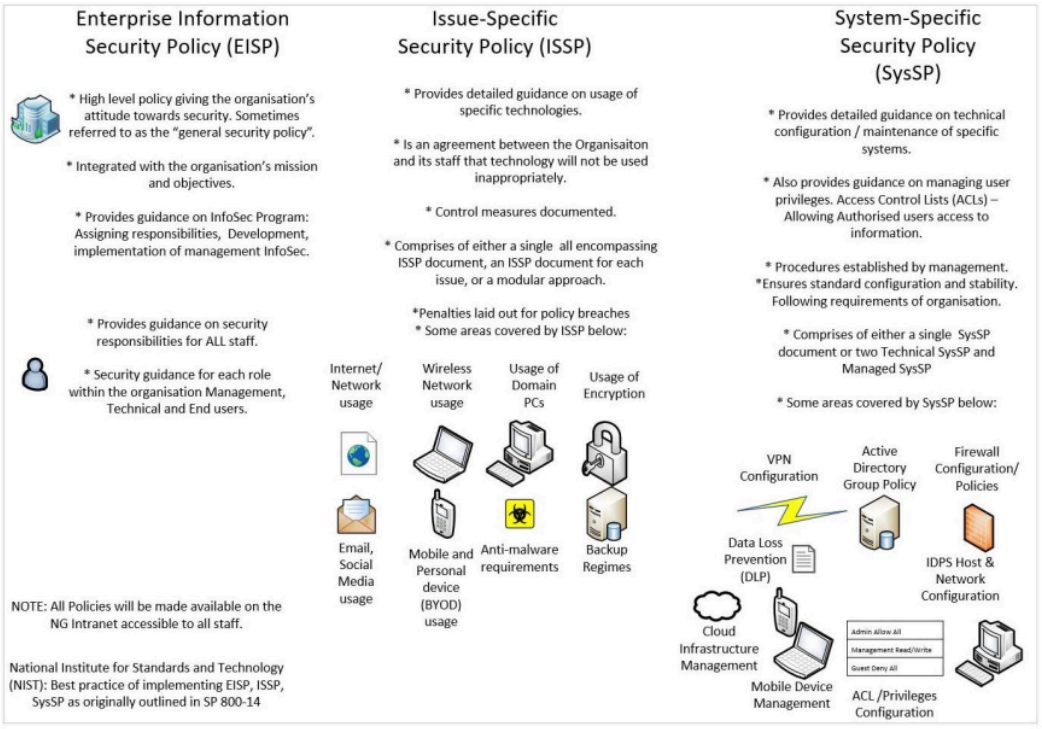



*Figure 10: Illustration of InfoSec policies*

After considering NGs requirements and the knowledge gained from task 1, the proposed InfoSec design for NG outlining recommended frameworks can be found in Table 19 along with a new network design in Fig.12.

*Table 19: Proposed InfoSec design utilising Security Frameworks for NG [3] [4]*

| Recommended Frameworks | Specific principles/ standards implemented | Benefits of framework for NG |
|---|---|---|
| ISO/IEC 27000 | ISO/IEC 27001: System Requirements | Sets out best practices for a range of InfoSec areas including InfoSec policies, Access Control (**Securing Intellectual Property**), Physical security, HR Security, Asset Management. |
| | ISO/IEC 27002: Security Controls | Provides guidance on implementing security controls to secure areas outlined in ISO/IEC 27001. |
| | ISO/IEC 27005: Risk Assessment | Continual risk assessment, to identify and control risks. Utilising Vulnerability Assessments (VA) to highlight potential risks, categorising them according to Likelihood and Impact. Risk Management will controls put in place prioritised using cost benefit analysis (CBA). |
| | ISO/IEC 27014: Governance of Information Security | Sets InfoSec standard for the organisation, ensures risks are taken into account during decision making, provides direction of investment decision making. Ensures the organisation complies with both policies and laws, promotes a positive mindset towards security and performance reviews related to business output |
| ITIL4 | Continual Improvement, InfoSec Management, Availability management, Incident management, Asset Management, Service Continuity Management, Service Delivery. | Improved data security, service delivery, efficiency, reduction of costs, continual improvements, reduced downtime, risk assessments (crossover with ISO 27005). |
| Control Objectives for Information and related Technology (COBIT 2019) | Continuous improvement, Integrations with other frameworks, Governance Objectives, Enablers (To facilitate data governance) | * Provides guidance on the strategic direction of organisation.<br>* Provides Strategic alignment with organisation's mission objectives.<br>* Emphasis on continual improvement<br>* Flexibility, COBIT strategy can change with needs of business, technological advancements or resource constraints.<br>* Single end-to-end governance system.<br>* Integration with other frameworks actively promoted. (ISO/IEC 27000, ITIL, NIST, CSA) |
| Cloud Security Alliance (CSA) | Cloud Controls Matrix (CCM) v4 | *Secures Cloud Infrastructure<br>* Implementation of Cloud Security Brokers (CASB) to monitor user activity and enforce policy.<br>* Resource policies are in place, to place limits on usage and prevent excessive costs.<br>*Maps to ISO/IEC 27000 (Specifically ISO 27001 and ISO 27002) |
| National Institute of Standards and Technology (NIST) | SP 800-14:<br>*Enterprise Information Security Policy (EISP) (General Security Policy)<br>*Issue-Specific Security Policy (ISSP)<br>*System-Specific Security Policy (SysSP) | Implementation of Security Policies.<br>*EISP provides direction for all staff on Data security.<br>*ISSP regulates the usage of specific technology at NG, such as Wired and Wireless devices, BYOD & COBO, Internet and Social Media usage.<br>*SysSP provides technical staff direction from management on system configuration, and group policy - ACLs, and privilege settings. |
| National Institute of Standards and Technology (NIST) | Cybersecurity Framework (CSF) 2.0 | Provides a mechanism to assist with Incident Response (IR) via 5 core functions:<br>1. Identify: Identifies Assets<br>2. Protect: Control measures from ISO27002 are in place.<br>3. Detect: Next Gen Firewall with IDPS is in place to detect IoCs<br>4. Respond: IR plan is enacted, IR team are notified.<br>5. Recover: Ensure that services are recovered appropriately so that re-infection does not occur. |

Fig.12 New network design for NG.

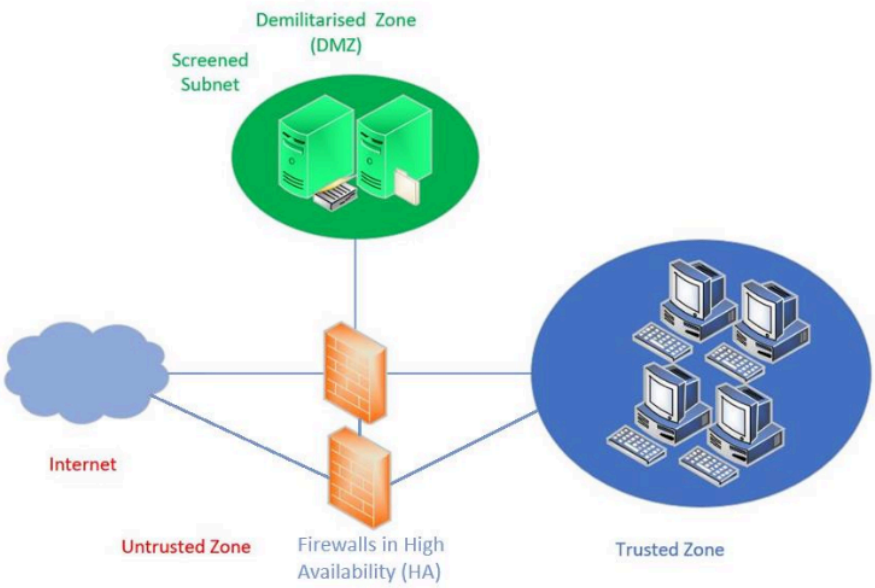



*Figure 11: Screened-Subnet with FWs in HA.*

## Recommendations

Tables 20-21 outline the recommended frameworks for NG to improve the security posture of the organisation, it is recommended that a **defence in depth** approach is implemented.

*Table 20: Summary of recommendations-1*

| Area | Risk Identified | Description | Recommendation | Framework | Standard |
|---|---|---|---|---|---|
| Wireless Infrastructure | Over reliance on wireless network - over 95% deployment | Wireless is a shared medium, network traffic could be intercepted using sniffing techniques. Evil Twin WAP attack, War driving, War Flying | **Geofencing** to ensure devices only have access to IP data within the NG | ISO 27000 | ISO 27001 |
| | | | **Geotagging** devices to ensure it is known where devices are at all | | |
| | | | Implement **VPN** (IPSec) to encrypt data in transit. | | |
| | | | * Upgrade Wireless infrastructure to Enterprise Level **WPA3** standard in **Enterprise** mode.<br>* **Disable** support for **802.11 a,b,g devices**. This will stop legacy, vulnerable devices from connecting to the wireless network. | | |
| | | | Implementation of centralised RADIUS authentication utilising **IEEE 802.1X** standard. | | |
| | | | **MAC based Authentication** to ensure that only trusted devices can access NG systems, utilising **IEEE 802.1X** | | |
| | | | New **WAPs** to have **NAC** functionality to support **IEEE 802.1X** | | |
| Device Deployment | BYOD | Staff utilising their personal devices on the corporate network is a risk. The device may be infected, or poorly managed and vulnerable to exploitation.<br><br>With billions in IP at stake, this is a risk the CISO is not willing to accept for corporate data. | **BYOD** devices will be placed on a separate guest VLAN allowing internet access only via IEEE 802.1X.<br>**BYODs** will NOT access NG systems or connect to other BYODs.<br>**COBO** deployment recommended for all staff.<br>**UEM** implementation to manage all COBO devices.<br>**EDR** implementation to detect compromise.<br>**FDE** implementation to ensure data is encrypted and secure while at rest to maintain confidentiality and integrity. | ISO 27000 | ISO 27001 |
| Wired Infrastructure | Under utilisation | Wired infrastructure is currently not in place as NG are over-reliant on wireless networking. | Wired infrastructure deployment, **new switching** to have **NAC** functionality to support **IEEE 802.1X / RADIUS Auth.** | ISO 27000 | ISO 27001 |
| | | | Wired PCs to be deployed. Managed by **AD** and Group Policy (**GP**), utilising **Kerberos**. This ensures that sensitive data is retained within the NG systems. **EDR** to be implemented. | | |
| | Improvements required. | Wired network infrastructure recommendations. | Replace current packet filtering firewall with a Next-Generation | | |
| | | | Creation of a Screened-Subnet (Demilitarised Zone (**DMZ**)) to house **SFTP** server required by suppliers. | | |
| Cloud Infrastructure | Potential Misconfigurations. | A review of cloud server configurations to take place. | Implementation of **CCM** recommendations, including Cloud Access Security Brokers (**CASB**), resource monitoring. | CSA | CCM |
| | Potential data breach | | Cloud infrastructure to be encrypted with NG InfoSec team to retain encryption keys, thus insuring confidentiality and integrity of data. | | |
| | Data Centre location | Consultation with the CSP required to ensure that data centres are located within | Data centres in the UK should preferably be utilised from a legal point of view as local jurisdiction. | | |
| Governance | IP data at risk | Currently no security programme is in place, therefore IP is at risk or data breach, data | Data Categorisation, **DLP** implementation. | ISO 27000/ COBIT | ISO 27014 |
| | | Organisation and InfoSec strategies need to be aligned. | Strategic alignment to ensure that | COBIT | |
| Risk Management/Treatment | Currently not being undertaken | Continual risk assessment procedure to be implemented assessing control measures. | Asset Identification, regular Vulnerability Assessments (**VA**), risk treatment, control measures, patching regimes. | ISO 27000 | ISO 27005<br>ISO 27002 |
| Compliance | NG's global presence. | NG's global presence will need to comply with legislations. | Implementation of real time compliance monitor (Such as Checkpoint Compliance monitor). | COBIT | |

*Table 21: Recommendations-2*

| Area | Risk Identified | Description | Recommendation | Framework | Standard |
|---|---|---|---|---|---|
| Contingency Planning | Currently no CP in place. | CP is crucial for the survival of an organisation, IR/DR management and recovery. In the event of a severe disaster, BC can allow the organisation to function, mitigating the impact. | Formation of **CP** teams (**CPMT**, **IR**,**DR**,**BC**, and **CM** teams). | | |
| | | | **CP** strategies, policies and plans to be developed, managed and updated periodically. | | |
| | | | **CP** Plans to be rigorously tested, with training for relevant teams. | | |
| | | | * Purchase of alienate site for **BC**.<br>* Initially this will be a COLD site,<br>* As infrastructure upgraded, legacy systems installed at Cold site, transferring it to a WARM site with an **IPSec VPN** Link between. Eventually becoming a HOT site as resources allow. | | |
| | | | * **Backup Regime implementation**: Full Backup carried out on Friday night, with incremental backups to be taken throughout the week.<br>* **3-2-1** Backup methodology to be implemented.<br>* Once WARM site operational, backup replication to warm site.<br>* **Immutable** backups to be implemented, so that once backup has completed, it is not possible to write or modify that backup data. | | |
| Protection Mechanisms | Current systems have not been updated to match current requirements. | * The protection systems in place have not been updated since the company has grown.<br>* Over-reliance on wireless infrastructure<br>* Investment is required to maintain data security. | Centralised **RADIUS** authentication for Wired and Wireless networks. **PEAP** used for general staff access, **EAP-TLS** used for enhanced security for staff requiring access to IP data assets. | ISO 27000 | ISO 27001<br>ISO 27002 |
| | | | Upgrade FWs to **NGWF** features: IDPS, DPI, UTM, AV, DLP, URLF, AC, SSLI. | | |
| | | | Centralised **NGFW** implementation so that multiple FWs can be managed from one location. | | |
| | | | NGFW configured in **HA** utilising a **Screened-Subnet** architecture. Creating three zones (**Trusted**,**Untrusted, DMZ AND Immutable backup zone**). | | |
| | | | **IPSec VPN** infrastructure to be implemented for site to site communications and for remote workers. | | |
| | | | **MFA** to be implemented utilising **biometric authentication**. | | |
| | | | Implementation of Role Based Access Control (**RBAC**) | | |
| | | | **SIEM / SOAR** implementation | | |
| | | | Regular VAs, network scans to identify devices, ports open. | | |
| | | | Configuration Hardening of all devices -Ensure **TLS 1.2/1.3** used. | | |
| | | | Secure encryption to be implemented. **AES** and **RSA**. | | |
| | | | Implementation of **Digital Certificates / PKI**. Configure **OCSP**. | | |
| | | | Email Client Security provided by **S/MIME, IMAPS, POPS** to Encrypt and add Digital Signature to email ensuring Confidentiality, Integrity, and Nonrepudiation. | | |
| | | | Email Server Security provided by **SPF**, **DKIM** and **DMARC**. To identify malicious email servers, spam/phishing emails, and to apply policies to quarantine or block malicious emails. | | |
| InfoSec Policy | Currently no InfoSec policies in place. | InfoSec Policies provides direction on the organisations attitude to cybersecurity. Gives staff guidance on expected behaviour. | Should be made available to all staff, with acknowledgement mechanism that key policies have been read and understood. | | |
| | | | Policies to be reviewed annually. | | |
| | | | **EISP**: Provides general overview of organisational attitude security . | | |
| | | Potential for staff to become victim to hackers using social engineering techniques. | **ISSP**:**SETA** programme to raise awareness of social engineering techniques used by hackers. | | |
| | | Inappropriate communications via staff. Electronic Communication/Social Media | **ISSP**: **Social Media Policy** to ensure that all communications are appropriate. | | |
| | | Provides guidance from Senior management on expected user behaviour. | **ISSP**: Acceptable Usage Policy (**AUP**) and Password Policy (**PP**) to be implemented. | | |
| | | Provides guidance from Senior management on infrastructure configuration requirements. | **SysSP**: Provides guidance for implementation of **NGFW**, Wired and Wireless network systems. | | |
| | | | **SysSP**: **VPN** implementation ensure data is secured via encrypted transit. | | |
| Organisational Structure | Current structure does not provide clear defined roles. | There is currently no dedicated InfoSec team, with IT staff carrying out this role along with other duties. | Re-organise structure to place an InfoSec team under IT department. This will prove clear definitions of roles and responsibilities, | | |
| | | | Will promote cybersecurity practices throughout the IT department. | | |

In addition to the recommendations outlined above, NG will also need to consider the challenges in Table 22:

*Table 22: Additional Design Considerations*

| Challenges | Solutions |
|---|---|
| From knowledge gained in task 1 it is clear implementing frameworks is costly and time consuming. | Implement these recommendations on a prioritised basis, utilising project management so that systems are implemented properly and within budget. |
| Steep learning curve for staff to become familiar with the new framework processes. | Implement a training programme to familiarise staff with the new systems. |
| Staff may resist implementation of the framework or subvert the newly implemented security processes. | Implement a SETA programme to maintain cybersecurity awareness at NG. |
| Complexity of implementing frameworks. | Consultancy may be required, incurring additional cost. |

## Task 2b Reasoning for updated regulations and standards

The research in task 1 shows that following best practices and standards are crucial to providing a clear strategic InfoSec plan.

InfoSec frameworks are continually being revised, ensuring a good cybersecurity posture is maintained, the organisation's data is secure and improves customer service.

The threat landscape is constantly changing therefore standards and regulations also need to evolve to ensure that data remains secure.

Fig. 13 shows data compromises in the US between 2005-2023, there is a clear upward trend of data breaches from 157 in 2005 to 3,205 in 2023.

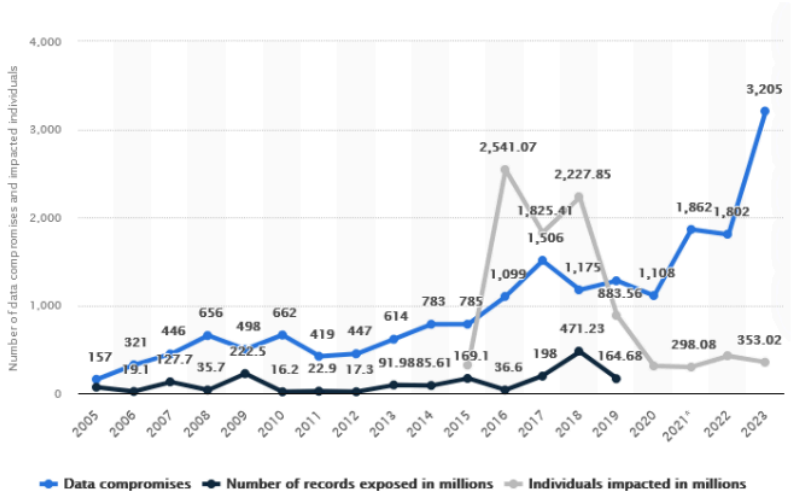



*Figure 12: Data compromises in US 2005-2023 [79]*

This upward trend includes more sophisticated attack methods, ageing technologies with exploitable vulnerabilities and higher frequency of attacks such as malware. Fig.14 shows the projected forecast of malware attacks [80].

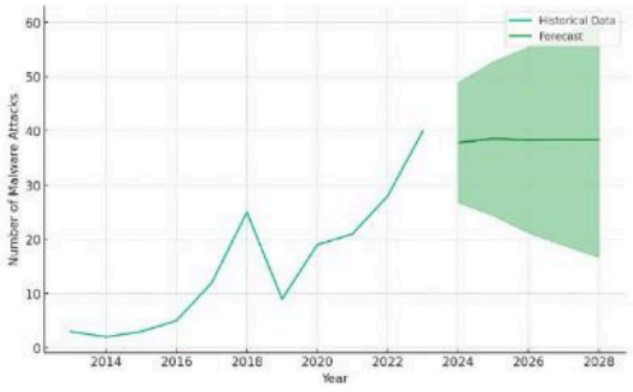



*Figure 13: Malware attacks between 2014-2024 and projection onto 2028 [80]*

The data breach and malware attack statistics show that organisations need to be proactive in implementing updated InfoSec frameworks. This ensures InfoSec security standards are met, risk and vulnerability assessments are carried out and that InfoSec control measures are put in place to resolve any issues uncovered. Proactively implementing up-to-date control measures helps safeguard organisations and their data from such attacks.

New technologies are continually being developed providing customers with new services and features; however, they can also bring new threats.

Two recent technologies that have had a global impact are:

- **Internet of Things (IoT)**, also known as "smart devices". (E.g. Smart speakers, TVs and doorbells).
- **Artificial Intelligence (AI)** enabled devices.

Fig.15 gives an indication of the pace of adoption of IoT technologies which is forecast to increase within the next decade.

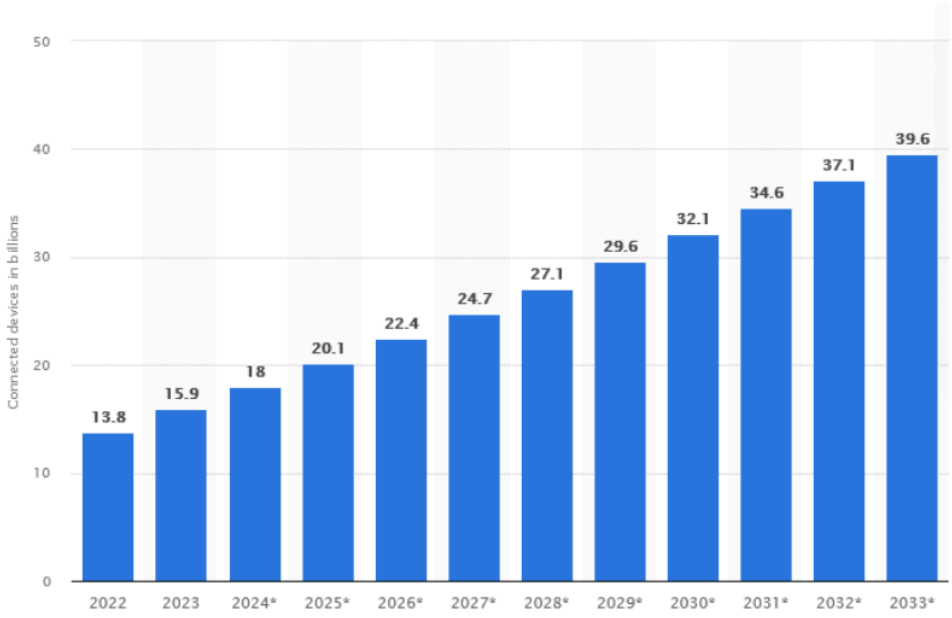



*Figure 14: The Global Number of Internet of Things (IoT) connected devices 2022-2023, forecasted to rise between 2024-2033 [81]*

IoT devices are developed and released quickly, making it challenging to regulate as the adoption of these technologies can outpace legislation. Legislation and standards are crucial as they keep users from harm and maintain the CIA triad [82].

Manufacturers/developers release new goods/services to market quickly for financial gain. However, this results in legislation lagging technical advancements due to the time required to enact legislation as it must go through a formal process, see Fig.16 [83]

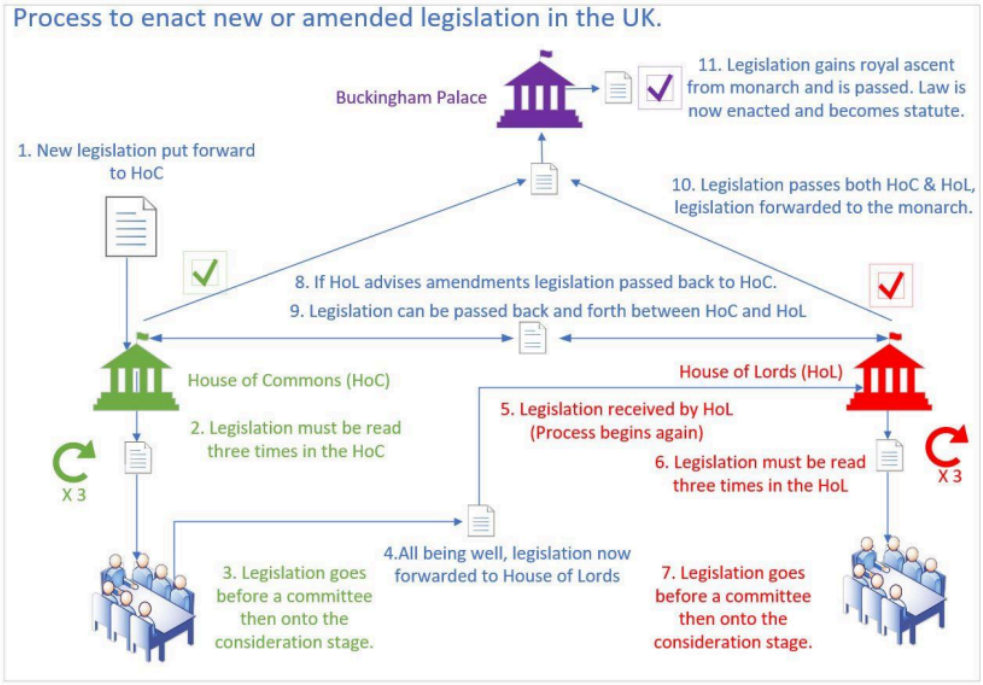



*Figure 15: Enacting UK legislation*

According to the National Cyber Security Centre (NCSC) new UK legislation was introduced on the 29th of April 2024 to safeguard users of IoT devices by implementing a "**secure by design**" strategy [84] [85] [86]. This law provides protection for users of IoT devices. When this legislation was enacted, there were already 18 billion connected IoT devices globally [81] [86]. This shows that legislation and standards are not being kept updated to keep pace with emerging technologies.

The rise of AI has been meteoric with the introduction of services such as Chat Generative Pre-Trained Transformer (ChatGPT), Microsoft CoPilot, and Google Gemini [82].

AI is now commonly embedded within other technologies such as smartphones and smart speakers giving rise to AI of Things (AIoT) [87] [88]. The AIoT platform provides users with many benefits such as bandwidth and energy efficiency, as computations will be carried out on the device [87].

It is forecast by Maximise Market Research for AI embedded technology to increase annually by 5.4%. By 2029 the market value will be over $45 billion (USD) [87]. The UK government expect the AI sector to grow to over $1 Trillion (USD) by 2035 [89].

According to the UK Government, the Automated Vehicles (AV) sector with embedded AI, will have driverless cars on UK roads by 2026 [90]. The UK government quickly introduced a new legislation to safeguard UK citizens [91]. This law has been enacted prior to the introduction of AVs, but there are serious concerns that have not been addressed in this legislation.

Having examined this legislation there are some provisions for InfoSec, such as the sections on "Protection, collection and sharing of Information". One glaring oversight is the act pays no mention to cybersecurity or cyberthreats, highlighting the risk of quickly forcing legislation through without proper scrutiny. According to the UK Parliament it is anticipated the AV sector will benefit the UK

economy by creating 38,000 jobs by 2035 and providing an annual economic benefit of £66 Billion by 2040. These are the main driving factors behind this legislation [92]. Policymakers should place the safety of end users at the forefront of legislation [93].

Even though legislation has been enacted, these points show that there are blatant omissions from a perspective of InfoSec which will need to be addressed in future. It is therefore urgently required for parliamentarians to conduct post-legislative scrutiny of this act so that cybersecurity threats can be considered [83].

Many global leaders recognise the benefits that AI can provide but also have concerns over the risks of AI. In November 2023, the very first AI safety summit was held at Bletchley Park, UK with many government and industry representatives attending [82] [94] [95].

During the summit many risks were discussed including:

- Global security from AI misuse
- Unpredictable advances in AI capability
- Loss of control over AI
- Developer responsibility
- Policies to manage frontier AI

[94] [96] [97]

The major outcomes of this AI summit were:

- **The Bletchley Declaration** – Signed by all participants, recognises the opportunities and threats of AI.
- **Formation of the AI Safety Institute** (AISI) – Institute for Advanced AI governance.

[89] [95] [98] [99] [100] [101]

As of October 2024, the UK still does not have a general statutory regulation of AI, a whitepaper was published in March 2023 which is the first step towards this process. According to former prime minister Rishi Sunak "it is difficult to regulate AI if you do not fully understand it". This once again illustrates that technology outpaces regulation [89] [102].

As a safeguard measure, formal legislation of AI is required. Collaborative working between Government, industry and the AISI, is crucial so that experts in the field can work alongside legislators to provide guidance. By working alongside AI developers, the government can ensure that legislation is expedited to regulate the latest advancements.

## Conclusion

The purpose of security frameworks is to minimise threats to an organisation and maintain the CIA triad. There are many security frameworks available. Although there are some commonalities between the frameworks e.g. risk management/treatment, each has a slightly different focus with varying complexities.

The research from task 1 showed that ISO/IEC 27000 was predominantly focused on security, containing standards for providing recommendations for ISMS and control measures. ITIL focuses on Service Delivery, from the case studies researched in task 1 ITIL can improve efficiency and save costs. ITIL also has InfoSec elements such as Incident Response. COBIT mainly centres on data governance and continual improvement.

It was found that different security frameworks integrated well with each other. A multi-framework environment is extremely beneficial to an organisation improving their cybersecurity posture and providing a comprehensive InfoSec programme.

Task 2 showed that legislation often lags advancements in technology or is rushed through parliament without proper scrutiny. Politicians find legislating complex technology challenging as they do not understand the functionality or the capabilities of systems. Closer collaboration with trusted technological organisations such as the NCSC and AISI is key.

NG is currently vulnerable to cyberthreats; to improve their cybersecurity posture several recommendations have been made based on a multi-framework design, these are outlined in Tables 20-21.

To immediately ensure NG safeguards their data, assets and crucially their IP against cyberthreats it is imperative that they implement the frameworks and recommendations outlined in this report.

It will be vital that NG stays compliant with any changes in legislation and standards. Policies need to be reviewed periodically to ensure their InfoSec systems are robust and remain fit for purpose.

# References


[1] Internaitonal Standards Organisation (ISO), “About ISO - Practical solutions for real-world problems,” Invernaitonal Standards Organisation (ISO), n.d. [Online]. Available: https://www.iso.org/about. [Accessed 9 November 2024].

[2] The ISO 27000 Directory, “ISO 27000 - ISO 27001 and ISO 27002 Standards,” 27000.org, 2019. [Online]. Available: https://27000.org. [Accessed 7 November 2024].

[3] M. Chapple and D. Seidl, CompTIA Security+ Study Guide EXAM SA0-601, Hoboken: Sybex, 2021, pp. 2-4.

[4] M. E. Whitman and H. J. Mattord, Management of Information Security, Boston, Wales: Cenage, 2016.

[5] British Standards Institute (BSI), “BS 7799-1:1995,” British Standards Institute (BSI), 2024. [Online]. Available: https://knowledge.bsigroup.com/products/information-security-management-code-of-practice-for-information-security-management-systems?version=standard. [Accessed 7 November 2024].

[6] International Standards Organisation (ISO), “ISO/IEC 27001:2022 - Information Security, cybersecurity and privacy protection - Information security management systems - Requirements,” International Standards Organisation (ISO), n.d. [Online]. Available: https://www.iso.org/standard/27001. [Accessed 8 November 2024].

[7] International Standards Organisation (ISO), “ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection - Information security controls,” International Standards Organisation (ISO), n.d. [Online]. Available: https://www.iso.org/standard/75652.html. [Accessed 8 November 2024].

[8] Information Standards Organisation (ISO), “ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection - Guidance on managing information security risks,” Information Standards Organisation (ISO), n.d. [Online]. Available: https://www.iso.org/standard/80585.html. [Accessed 8 November 2024].

[9] M. Edwards, “The Ultimate Guide to ISO 27001,” Information Security Management Systems Online, 2024. [Online]. Available: https://www.isms.online/iso-27001/. [Accessed 9 November 2024].

[10] A. Harvey, “The Ultimate Guide to ISO 27002,” Information Security Management Systems Online, 2024. [Online]. Available: https://www.isms.online/iso-27002/. [Accessed 9 November 2024].

[11] Information Security Management Systems Online, “ISO/IEC 27005 InfoSec Risk Management,” Information Security Management Systems Online, 2024. [Online]. Available: https://www.isms.online/iso-27005/. [Accessed 9 November 2024].

[12] M. E. Whitman and M. J. Herbert, “Principles of Information Security,” in *Principles of Information Security*, Boston, Cengage, 2022, p. 8.

[13] M. Malachi, “Management of enterprise cyber security: A review of ISO/IEC 27001:2022,” *International Conference On Cyber Management And Engineering (CyMaEn),* vol. 10, no. 10051114, pp. 117-122, 2023.

[14] OMNEX, “ISO/IEC 27001:2022 Cybersecurity - Consulting, Implementation, & Coaching,” OMNEX , 2024. [Online]. Available: https://www.omnex.com/aerospace/consulting-implementation-coaching-aerospace-iso-27001-cybersecurity. [Accessed 14 November 2024].

[15] C. Rajak, J. Bharti, A. Mateen, N. Mehndiratta, J. Chauhan and R. Marndi, “A Roadmap to ISMS ISO 27001 Implementation Process,” *3rd International Conference on Range Technology (ICORT),* vol. 10.1109, no. ICORT56052.2023.10249115, pp. 1-5, 2023.

[16] V. Monev, “Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002,” *International Conference on Information Technologies (InfoTech),* vol. 10.1109, no. InfoTech49733.2020.9211066, pp. 1-5, 2020.

[17] British Standards Institute (BSI), “ISO/IEC 27001 - Information Security Management System,” British Standards Institute (BSI), 2024. [Online]. Available: https://www.bsigroup.com/en-ID/ISO-IEC-27001/. [Accessed 9 November 2024].

[18] British Standards Institute (BSI), “What is the ISO/IEC 27002,” British Standards Institute (BSI), 2024. [Online]. Available: https://www.bsigroup.com/en-ID/iso-27002-information-security-controls/. [Accessed 9 November 2024].

[19] M. Edwards, “ISO 27001:2022 Annex A Explained,” Information Security Management Systems Online, 2024. [Online]. Available: https://www.isms.online/iso-27001/annex-a/. [Accessed 8 November 2024].

[20] A. Z. Mahfud, I. R. Hikmah, S. U. Sunaringtyas and T. Yulita, “Information Security Risk Management Design Based on ISO/IEC 27005:2022, ISO/IEC 27001:2022, and NIST SP 800-53 Revision 5 (A Case Study at ABC Agency),” *4th International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS),* vol. 10.1109, no. ICE3IS62977.2024.10775428, pp. 181-186, 2024.

[21] S. Jaya Putra, M. Nur Gunawan, A. Falach Sobri, J. Muslimin, Amilin and D. Saepudin, “Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company,” *8th International Conference on Cyber and IT Service Management (CITSM),* vol. 10.1109, no. CITSM50537.2020.9268845, pp. 1-5, 2020.

[22] International Standards Organisation (ISO), “The ISO Survey,” International Standards Organisation (ISO), 31 December 2023. [Online]. Available: https://www.iso.org/the-iso-survey.html. [Accessed 7 November 2024].

[23] International Standards Organisation (ISO), “ISO Survey of certifications to management system standards - Full results,” International Standards Organisation (ISO), 31 October 2024. [Online]. Available: https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top. [Accessed 7 November 2024].

[24] H. Guo, M. Wei, P. Huang and E. G. Chekole, “Enhance Enterprise Security through Implementing ISO/IEC 27001 Standard,” *IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI),* vol. 10.1109, no. /SOLI54607.2021.9672401, pp. 1-6, 2021.

[25] International Standards Organisation (ISO), “ISO: Global Standards for trusted goods and services,” International Standards Organisation (ISO), n.d. [Online]. Available: https://www.iso.org/home.html. [Accessed 8 November 2024].

[26] British Standards Institute (BSI), “Case studies and testimonials for ISO/IEC 27001,” British Standards Institute (BSI), 2024. [Online]. Available: https://www.bsigroup.com/en-IN/ISOIEC-27001-Information-Security/Case-studies-for-ISOIEC-27001/. [Accessed 12 November 2024].

[27] British Standards Institute (BSI), “CogentHub Case Study,” British Standards Institute (BSI), n.d. [Online]. Available: https://www.bsigroup.com/globalassets/localfiles/en-in/kitemark/cogenthub_casestudy_in_2022-1.pdf. [Accessed 12 November 2024].

[28] British Standards Institute (BSI), “Befree Case Study,” British Standards Institute (BSI), n.d. [Online]. Available: https://www.bsigroup.com/globalassets/localfiles/en-in/kitemark/befree_casestudy_in_2022-1.pdf. [Accessed 12 November 2024].

[29] Romano Security Consulting, “ISO 27001 Internal Audit Case Study,” Romano Security Consulting, 2024. [Online]. Available: https://www.romanosecurityconsulting.com/case-studies/iso-27001-audit. [Accessed 12 November 2024].

[30] M. Siddiqui, “A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard,” *National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA),* vol. 10.1109, no. NCETSTEA48365.2020.9119914, pp. 1-3, 2020.

[31] IT Governance, “Estimated ISO 27001 certification costs,” IT Governance, 2024. [Online]. Available: https://www.itgovernance.co.uk/iso27001-certification-costs. [Accessed 17 November 2024].

[32] M. Malatji, “Management of enterprise cyber security: A review of ISO/IEC 27001:2022,” *International Conference On Cyber Management And Engineering (CyMaEn),* vol. 10.1109, no. CyMaEn57228.2023.10051114, pp. 117-122, 2023.

[33] K. N. Zakaria, S. H. Othman and A. Zainail, “Review of Cybersecurity Audit Management and Execution Approaches,” *IEEE - International Conference on Research and Innovation in Information Systems (ICRIIS),* vol. 1109/ICRIIS48246.2019.9073641, no. 10, pp. 1-6, 2019.

[34] A. Ziro, S. Toibayeva, S. Gnatyuk, A. Imanbayev, M. Iavich and Z. Zhaybergenova, “Research of the Information Security Audit System in Organizations,” *IEEE - International Conference on Smart Information Systems and Technologies (SIST),* vol. 1109/SIST58284.2023.10223557, no. 10, pp. 440-444, 2023.

[35] M. Goman, “How to Improve Risk Management in IT Frameworks,” *62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS),* vol. 10.1109, no. ITMS52826.2021.9615327, pp. 1-6, 2021.

[36] M. Helo and P. Suorsa, “Information Security Failures Measured and ISO/IEC 27001:2022 Controls Ranked by General Data Protection Regulation Penalty Analysis,” *11th International Conference on Cyber and IT Service Management (CITSM),* vol. 10.1109, no. CITSM60085.2023.10455413, pp. 1-5, 2023.

[37] Service Now, “What is ITIL (IT Infrastructure Library)?,” Service Now, 2024. [Online]. Available: https://www.servicenow.com/uk/products/itsm/what-is-itil.html. [Accessed 10 November 2024].

[38] S. K. White and L. Greiner, “What is ITIL? Your guide to the IT Infrastructure Library,” CIO.com, 16 May 2022. [Online]. Available: https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html. [Accessed 9 November 2024].

[39] S. Lopes, P. Leite, S. Carvalho and P. Teixeira, “Using ITIL as part of the NIST Cybersecurity Framework,” *12th International Symposium on Digital Forensics and Security (ISDFS),* vol. 10.1109, no. ISDFS60797.2024.10527256, pp. 1-6, 2024.

[40] A. Schmidt, “The ITIL 4 Practices Overview,” Value Insights, 20 July 2020. [Online]. Available: https://valueinsights.ch/the-itil-4-practices-overview/. [Accessed 10 November 2024].

[41] D. Berger, N. Shashidhar and C. Varol, “Using ITIL 4 in Security Management,” *8th International Symposium on Digital Forensics and Security (ISDFS),* vol. 10.1109, no. ISDFS49300.2020.9116257, pp. 1-6, 2020.

[42] S. Susnjara and I. Smalley, “What is ITIL?,” IBM, 2 October 2024. [Online]. Available: https://www.ibm.com/topics/it-infrastructure-library. [Accessed 10 November 2024].

[43] Axelos, “What is ITIL,” Axelos, 2024. [Online]. Available: https://www.axelos.com/certifications/itil-service-management/what-is-itil. [Accessed 10 November 2024].

[44] Y. Al-Ashmoery, H. Haider, A. Haider, N. Nasser and M. Al-Sarem, “Impact of IT Service Management and ITIL Framework on the Businesses,” *International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI),* vol. 10.1109, no. MTICTI53925.2021.9664763, pp. 1-5, 2021.

[45] L. Giannotti, “What is ITIL?,” Tech Monitor, 1 March 2024. [Online]. Available: https://www.techmonitor.ai/what-is/what-is-itil/?cf-view. [Accessed 19 November 2024].

[46] I. Aylesbury, “Using ITSM best practices to deliver quality IT support,” Rock IT Consultancy, February 2024. [Online]. Available: https://www.rock.co.uk/insights/itsm-best-practices/. [Accessed 19 November 2024].

[47] A. Peliarachchi and J. Wijayanayake, “Evaluating Business As Usual activities between Agile and Information Technology Infrastructure Library (A-ITIL): Industry practitioners’ point of view,” *International Research Conference on Smart Computing and Systems Engineering (SCSE),* vol. 10.1109, no. SCSE59836.2023.10215034, pp. 1-7, 2023.

[48] A. R. Permatasari, S. Sulistyo and P. I. Santosa, “Optimizing IT Services Quality: Implementing ITIL for Enhanced IT Service Management,” *11th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE),* vol. 10.1109, no. ICITACEE62763.2024.10762782, pp. 296-301, 2024.

[49] A. Tanović and A. Ć. Hasibović, “Implementation of Service Desk Solutions on the Example of a Company for the Production and Distribution of Electricity Energy Using the Principles of the ITIL Framework,” *47th MIPRO ICT and Electronics Convention (MIPRO),* vol. 10.1109, no. MIPRO60963.2024.10569200, pp. 1782-1787, 2024.

[50] M. Thomas, “Adopting ITSM Best Practice Approaches: The Benefits and Drawbacks,” ITSM Tools, 14 February 2019. [Online]. Available: https://itsm.tools/adopting-itsm-best-practice-approaches-the-benefits-and-drawbacks/. [Accessed 17 November 2024].

[51] Amazon Web Services (AWS), “What’s the Difference Between Agile and DevOps?,” Amazon Web Services (AWS), 2024. [Online]. Available: https://aws.amazon.com/compare/the-difference-between-agile-devops/. [Accessed 10 November 2024].

[52] Axelos, “Spotify: An ITIL Case Study,” Axelos, 3 February 2019. [Online]. Available: https://www.axelos.com/resource-hub/case-study/spotify-itil-case-study. [Accessed 11 November 2024].

[53] Axelos, “Case study: How ITIL 4 helped Wipro deliver value,” Axelos, 12 September 2023. [Online]. Available: https://www.axelos.com/resource-hub/case-study/case-study-how-itil-4-helped-wipro-deliver-value. [Accessed 11 November 2024].

[54] Axelos, “Vodafone Aligns Support Service Model to ITIL 4 Case Study,” Axelos, 20 September 2021. [Online]. Available: https://www.axelos.com/resource-hub/case-study/vodafone-aligns-support-service-model-to-itil-4. [Accessed 11 November 2024].

[55] Axelos, “The University of Oxford and ITIL Case Study,” Axelos, 7 August 2020. [Online]. Available: https://www.axelos.com/resource-hub/case-study/university-of-oxford-and-itil-case-study. [Accessed 11 November 2024].

[56] I. Cooke, “ISACA - Coincidence or History?,” Information Systems Audit and Control Association (ISACA), 1 July 2019. [Online]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/coincidence-or-history. [Accessed 12 November 2024].

[57] Information Systems Audit and Control Association (ISACA), “ISACA - About us,” Information Systems Audit and Control Association (ISACA), 2024. [Online]. Available: https://www.isaca.org/about-us. [Accessed 12 November 2024].

[58] Information Systems Audit and Control Association (ISACA), “Leading the way in the pursuit of Digital Trust,” Information Systems Audit and Control Association (ISACA), 2024. [Online]. Available: https://www.isaca.org/digital-trust. [Accessed 12 November 2024].

[59] Information Systems Audit and Control Association (ISACA), “Digital Trust - Board Briefing,” Information Systems Audit and Control Association (ISACA), 2024. [Online]. Available: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/ebooks/digital-trust-board-briefing_ebook.pdf. [Accessed 12 November 2024].

[60] Information Systems Audit and Control Association (ISACA), “Effective IT Governance at your fingertips,” Information Systems Audit and Control Association (ISACA), 2024. [Online]. Available: https://www.isaca.org/resources/cobit#1. [Accessed 12 November 2024].

[61] CIO, “What is COBIT? A framework for alignment and governance,” CIO, 12 June 2023. [Online]. Available: https://www.cio.com/article/228151/what-is-cobit-a-framework-for-alignment-and-governance.html. [Accessed 12 November 2024].

[62] W. Febriyani, M. I. Alhari and T. F. Kusumasari, “Design of IT Governance based on Cobit 2019: A Case Study of XYZ Education Foundation,” *1st International Conference on Information System & Information Technology (ICISIT),* vol. 10.1109, no. ICISIT54091.2022.9872888, pp. 289-294, 2022.

[63] R. Hurkadli, “COBIT 2019 Framework,” ITSM Docs, 28 August 2023. [Online]. Available: https://www.itsm-docs.com/en-gb/blogs/cobit/cobit-2019-framework. [Accessed 16 November 2024].

[64] G. Braga, “COBIT 2019 and the IIA 2019 Guiding Principles of Corporate Governance: Two Frameworks, Many Similarities,” Information Systems Audit and Control Association (ISACA), 13 July 2020. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-the-iia-2019-guiding-principles-of-corporate-governance. [Accessed 16 November 2024].

[65] K. Harisaiprasad, “COBIT 2019 and COBIT 5 Comparison,” Information Systems Audit and Control Association (ISACA), 27 April 2020. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison. [Accessed 12 November 2024].

[66] Axelos, “Using ITIL and COBIT 2019 for an integrated I&T framework,” Axelos, 17 July 2021. [Online]. Available: https://www.axelos.com/resource-hub/white-paper/using-itil-cobit-2019-create-integrated-environment. [Accessed 12 November 2024].

[67] C. Fares, A. Rachini, M. A. Assaf and E. A. Aad, “Universities Cyber Security Standardization,” *2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI),* vol. 10.1109, no. EICEEAI60672.2023.10590478, pp. 1-5, 2023.

[68] Information Systems Audit and Control Association (ISACA), “Synergies Between ITIL 4 and COBIT 2019,” Information Systems Audit and Control Association (ISACA), 16 June 2021. [Online]. Available: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-17/new-resource-illustrates-synergies-between-itil-4-and-cobit-2019. [Accessed 12 November 2024].

[69] A. Ishlahuddin, P. W. Handayani, K. Hammi and F. Azzahro, “Analysing IT Governance Maturity Level using COBIT 2019 Framework: A Case Study of Small Size Higher Education Institute (XYZ-edu),” *3rd International Conference on Computer and Informatics Engineering (IC2IE),* vol. 10.1109, no. IC2IE50715.2020.9274599, pp. 236-241, 2020.

[70] M. Yasin, A. Akhmad Arman, I. J. M. Edward and W. Shalannanda, “Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ),” *14th International Conference on Telecommunication Systems, Services, and Applications (TSSA),* vol. 10.1109, no. TSSA51342.2020.9310875, pp. 1-5, 2020.

[71] C. H. Heruatmadja, F. L. Gaol, S. H. Supangkat and B. Ranti, “Ensuring Success in Quick Commerce by Evaluating Its Application Development Capability Maturity Using COBIT 2019,” *International Conference on Information Management and*

*Technology (ICIMTech),* vol. 10.1109, no. ICIMTech59029.2023.10277994, pp. 265-270, 2023.

[72] B. Visitsilp and N. Bhumpenpein, "Guidelines for Information Technology Governance Based on Integrated ISO 38500 and COBIT 2019," *Research, Invention, and Innovation Congress: Innovation Electricals and Electronics (RI2C),* vol. 10.1109, no. RI2C51727.2021.9559772, pp. 14-18, 2021.

[73] K. S. Saputra, M. Isnaini, A. S. Tasya, S. Mariam and Candiwan, "Analysis of Information Technology Governance on Process Management Services and Management of Information Technology Security Using COBIT 2019 (Case Study: PT XYZ)," *IEEE 8th International Conference on Computing, Engineering and Design (ICCED),* vol. 10.1109, no. ICCED56140.2022.10009924, pp. 1-6, 2022.

[74] S. E. Hiererra, F. L. Gaol, B. Ranti and S. H. Supangkat, "Proposed IT Governance Model for Smart Tourism Destinations based on COBIT 2019 Framework," *International Conference on Information Management and Technology (ICIMTech),* vol. 10.1109, no. ICIMTech55957.2022.9915077, pp. 499-504, 2022.

[75] K. Teitler-Santullo, "Case Study: Driving Digital Transformation Through COBIT," Information Systems Audit and Control Association (ISACA) , 1 November 2022. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/case-study-driving-digital-transformation-through-cobit. [Accessed 16 November 2024].

[76] Fortinet, "What Is The COBIT Framework?," Fortinet, 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-cobit. [Accessed 19 November 2024].

[77] Amazon Web Services (AWS), "Managed DDoS protection - AWS Shield," Amazon Web Services (AWS), n.d. [Online]. Available: https://aws.amazon.com/shield/. [Accessed 5 December 2024].

[78] Amazon Web Services (AWS), "Pricing AWS Shield," Amazon Web Services (AWS), n.d. [Online]. Available: https://aws.amazon.com/shield/pricing/. [Accessed 5 December 2024].

[79] Statista, "Annual number of data compromises and individuals impacted in the United States from 2005 to 2023," Statista, 2024. [Online]. Available: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/. [Accessed 1 December 2024].

[80] O. Falowo, M. Ozer, C. Li and J. Abdo, "Evolving Malware and DDoS Attacks: Decadal Longitudinal Study," *IEEE Articlea,* vol. 12, no. 10.1109/ACCESS.2024.3376682, pp. 39221-39237, 2024.

[81] Statista, "Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033," Statista, 2024. [Online]. Available:

https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. [Accessed 20 November 2024].

[82] UK Parliament, “AI offers significant opportunities but twelve governance challenges must be addressed says Science, Innovation and Technology Committee,” UK Parliament, 31 August 2023. [Online]. Available: https://committees.parliament.uk/committee/135/science-innovation-and-technology-committee/news/197236/ai-offers-significant-opportunities-but-twelve-governance-challenges-must-be-addressed-says-science-innovation-and-technology-committee/. [Accessed 20 November 2024].

[83] Institute for Government, “The legislative process in parliament,” Institute for Government, 13 September 2022. [Online]. Available: https://www.instituteforgovernment.org.uk/explainer/legislative-process-parliament. [Accessed 28 November 2024].

[84] National Cyber Security Centre (NSCS), “Smart devices: new law helps citizens to choose secure products,” National Cyber Security Centre (NSCS), 29 April 2024. [Online]. Available: https://www.ncsc.gov.uk/blog-post/smart-devices-law. [Accessed 20 November 2024].

[85] UK Government, “Secure by design,” UK Government, 2 May 2024. [Online]. Available: https://www.gov.uk/government/collections/secure-by-design. [Accessed 20 November 2024].

[86] UK Government, “Policy paper: The UK Product Security and Telecommunications Infrastructure (Product Security) regime,” UK Government, 2 May 2024. [Online]. Available: https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime. [Accessed 20 November 2024].

[87] H. Lin, “Embedded Artificial Intelligence: Intelligence on Devices,” *IEEE: Computer ,* vol. 56, no. 10.1109/MC.2023.3280397, pp. 90-93, 2023.

[88] K. S. Awaisi, Q. Ye and S. Sampalli, “A Survey of Industrial AIoT: Opportunities, Challenges, and Directions,” *IEEE Access,* vol. 10.1109, no. ACCESS.2024.3426279, pp. 96946-96996, 2024.

[89] UK Government: Department for Science, Innovation and Technology, “A pro-innovation approach to AI regulation: government response,” UK Government: Department for Science, Innovation and Technology, 6 February 2024. [Online]. Available: https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response#fn:1. [Accessed 20 November 2024].

[90] M. Harper (Transport Secretary), “Self-driving vehicles set to be on roads by 2026 as Automated Vehicles Act becomes law,” UK Government, 20 May 2024. [Online]. Available: https://www.gov.uk/government/news/self-driving-vehicles-set-to-be-on-

roads-by-2026-as-automated-vehicles-act-becomes-law. [Accessed 28 November 2024].

[91] UK Government, “Automated Vehicles Act 2024,” UK Government, 20 May 2024. [Online]. Available: https://www.legislation.gov.uk/ukpga/2024/10/contents/enacted. [Accessed 28 November 2024].

[92] UK Parliament, “Autonomous transport,” UK Parliament, 7 October 2024. [Online]. Available: https://post.parliament.uk/autonomous-transport/. [Accessed 28 November 2024].

[93] H. Cooreman and Q. Zhu, “Critical Reflections on the Ethical Regulation of AI: Challenges with Existing Frameworks and Alternative Regulation Approaches,” *IEEE International Symposium on Technology and Society (ISTAS),* vol. 10.1109, no. ISTAS55053.2022.10227116, pp. 1-5, 2022.

[94] UK Government, “AI Safety Summit 2023,” UK Government, 2023. [Online]. Available: https://www.gov.uk/government/topical-events/ai-safety-summit-2023. [Accessed 20 November 2024].

[95] UK Government, “Chair’s Summary of the AI Safety Summit 2023, Bletchley Park,” UK Government, 2 November 2023. [Online]. Available: https://www.gov.uk/government/publications/ai-safety-summit-2023-chairs-statement-2-november/b4ce6e54-47f0-4fa5-b159-71f7eef1788c. [Accessed 28 November 2024].

[96] UK Government, “AI Safety Summit: day 1 and 2 programme,” UK Government, 16 October 2023. [Online]. Available: https://www.gov.uk/government/publications/ai-safety-summit-programme/ai-safety-summit-day-1-and-2-programme. [Accessed 20 November 2024].

[97] UK Government, “Frontier AI: capabilities and risks – discussion paper,” UK Government, 25 October 2023. [Online]. Available: https://www.gov.uk/government/publications/frontier-ai-capabilities-and-risks-discussion-paper. [Accessed 20 November 2024].

[98] UK Government, “The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023,” UK Government, 1 November 2023. [Online]. Available: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023. [Accessed 28 November 2024].

[99] UK Government, “Introducing the AI Safety Institute,” UK Government, 17 January 2024. [Online]. Available: https://www.gov.uk/government/publications/ai-safety-institute-overview/introducing-the-ai-safety-institute. [Accessed 28 November 2024].

[100] UK Government, “AI Safery Institute (AISI) - (UK Department for Science, Innovation, and Technology),” UK Government, 2024. [Online]. Available: https://www.aisi.gov.uk/. [Accessed 28 November 2024].

[101] P. Masters, M. Buns, J. Griga, R. Iniesta and S. H. Jaiwei, “King's researchers comment on the outcomes of the UK AI Safety Summit,” King's College London, 23 November 2023. [Online]. Available: https://www.kcl.ac.uk/news/kings-researchers-comment-on-the-outcomes-of-the-uk-ai-safety-summit. [Accessed 28 November 2024].

[102] UK Parliament, “Artificial intelligence: ethics, governance and regulation,” UK Parliament, 7 October 2024. [Online]. Available: https://post.parliament.uk/artificial-intelligence-ethics-governance-and-regulation/. [Accessed 7 November 2024].

[103] Information Security Management System Online , “ISO/IEC 27000 Overview & Recommended Reading,” Information Security Management System Online , 2024. [Online]. Available: https://www.isms.online/iso-27000/. [Accessed 7 November 2024].

[104] International Standards Organisation (ISO), “ISO/IEC 27000 Family - Information Security Management,” International Standards Organisation (ISO), n.d. [Online]. Available: https://www.iso.org/standard/iso-iec-27000-family. [Accessed 7 November 2024].

[105] S. Mehta, “A Beginner’s Guide to Information Security Frameworks,” 24 March 2019. [Online]. Available: https://grcmusings.com/a-beginners-guide-to-information-security-frameworks/. [Accessed 8 November 2024].

[106] His Majesty’s Stationery Office, “Intellectual Property Act 2014,” His Majesty’s Stationery Office, 2014. [Online]. Available: https://www.legislation.gov.uk/ukpga/2014/18/contents. [Accessed 11 December 2024].

[107] EUR-lex, “Regulation - 2016/679 - EN - GDPR,” EUR-lex, 27 April 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed 11 December 2024].

[108] Cabinet Office, “Procurement Policy Note – Updated Guidance,” Cabinet Office, December 2022. [Online]. Available: https://assets.publishing.service.gov.uk/media/63876b508fa8f5370b118363/Procurement-Policy-Note-03_22-Updated-Guidance-on-Data-Protection-Legislation.docx.pdf. [Accessed 11 December 2024].

[109] UK Government, “Data Protection,” UK Government, 2018. [Online]. Available: https://www.gov.uk/data-protection. [Accessed 11 December 2024].

[110] His Majesty’s Stationery Office (HMSO) , “Data Protection Act 2018,” His Majesty’s Stationery Office (HMSO) , 2018. [Online]. Available:

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. [Accessed 11 December 2024].

[111] US Congress, "H.R.8152 - American Data Privacy and Protection Act," US Congress, 6 June 2022. [Online]. Available: https://www.congress.gov/bill/117th-congress/house-bill/8152. [Accessed 11 December 2024].

[112] Office of the Australian Information Commissioner, "The Privacy Act," Office of the Australian Information Commissioner, 1988. [Online]. Available: https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act. [Accessed 11 December 2024].

[113] Office of the Australian Information Commissioner, "Australian Privacy Principles," Office of the Australian Information Commissioner, 1988. [Online]. Available: https://www.oaic.gov.au/privacy/australian-privacy-principles. [Accessed 11 December 2024].

[114] P. Dewitte and J. Ausloos, "Chronicling GDPR Transparency Rights in Practice: The Good, the Bad and the Challenges Ahead," *International Data Privacy Law,* vol. 14, no. 2 (doi.org/10.1093/idpl/ipad026), p. 106–133, 2024.

[115] D. Erdos, "he UK and the EU personal data framework after Brexit: A new trade and cooperation partnership grounded in Council of Europe Convention 108+?," *Computer Law & Security Review,* vol. 44, no. doi.org/10.1016/j.clsr.2021.105639, pp. 1-17, 2022.

[116] C. Fischer, "Re-thinking the allocation of roles under the GDPR in the context of cloud computing," *International Data Privacy Law,* vol. 14, no. 1 (doi.org/10.1093/idpl/ipad023), p. 53–65, 2024.

[117] L. B. Rózenfeldová, P. Sokol, R. Hučková and M. Mesarčík, "Personal data protection enforcement under GDPR—the Slovak experience," *International Data Privacy Law,* vol. 14, no. 3 (doi.org/10.1093/idpl/ipae008), p. 278–297, 2024.

[118] R. Becker, D. Chokoshvili and E. S. Dove, "Legal bases for effective secondary use of health and genetic data in the EU: time for new legislative solutions to better harmonize data for cross-border sharing?," *International Data Privacy,* vol. 14, no. 3 (doi.org/10.1093/idpl/ipae014), p. 223–246, 2024.

[119] A. Calvi, "Data Protection Impact Assessment under the EU General Data Protection Regulation: A feminist reflection," *Computer Law & Security Review,* Vols. 1-20, no. doi.org/10.1016/j.clsr.2024.105950, p. 53, 2024.

[120] UK Government: Central Digital & Data Office, "Data Ownership in Government (HTML)," UK Government: Central Digital & Data Office, 26 April 2024. [Online]. Available: https://www.gov.uk/government/publications/essential-shared-data-assets-and-data-ownership-in-government/data-ownership-in-government-html. [Accessed 13 December 2024].

[121] Check Point, “Security Compliance Monitor,” Check Point, 2024. [Online]. Available: https://www.checkpoint.com/quantum/security-compliance/. [Accessed 15 December 2024].

[122] I. Mahendra, P. H. Meyliana and A. N. Hidayanto, “Information Technology Challenges for Integrated Governance, Risk and Compliance (GRC),” *1st International Conference on Smart Technology, Applied Informatics, and Engineering (APICS),* vol. 10.1109, no. APICS56469.2022.9918797, pp. 79-84, 2022.

[123] M. N.-E. Saulaiman, M. Kozlovszky and Á. Csilling, “Side Benefits of Cybersecurity Measures an Empirical Study,” *IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics (SISY),* vol. 10.1109, no. SISY60376.2023.10417952, pp. 581-588, 2023.

[124] Toyeer-E-Ferdoush, B. K. Ghosh and K. A. and Taher, “Security Policy Based Network Infrastructure for Effective Digital Service,” *International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD),* vol. 10.1109, no. ICICT4SD50815.2021.9396907, pp. 136-140, 2021.

[125] W. B. Ismail, S. Widyarto, K. Syafrullah and M. Tajuddin, “An Information Security Policy Development Process in Higher Education Institution: A Case Study Approach,” *9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI),* vol. 10.23919, no. EECSI56542.2022.9946593, pp. 147-152, 2022.

[126] B. Clark, RTFM: Red Team Field Manual, London: Amazon, 2017.

[127] G. D. Sign, The Ultimate Kali Linux Book, Birmingham - Mumbai: Packt, 2022.

[128] H. Sharma, Kali Linux - An Ethical Hacker's Cookbook, Birmingham - Mumbai: Packt, 2019.

[129] E. S. Mandrakov, D. A. Dudina, V. A. Vasiliev and M. N. Aleksandrov, “Risk Management Process in the Digital Environment,” *International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS),* vol. 10.1109, no. ITQMIS56172.2022.9976622, pp. 108-111, 2022.

[130] A. White and B. Clark, BTFM: Blue Team Field Manual, London: Amazon, 2017.

[131] National Institute of Standards and Technology (NIST), “National Vulnerability Database (NVD): CVE-2021-4189,” National Institute of Standards and Technology (NIST), 11 November 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-4189. [Accessed 5 December 2024].

[132] The Mitre Corporation, “CVE-2017-0146,” The Mitre Corporation, 2024. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0146. [Accessed 5 December 2024].

[133] National Institute of Standards and Technology (NIST), “National Vulnerability Database (NVD): CVE-2024-27316,” National Institute of Standards and Technology (NIST), 21 November 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2024-27316. [Accessed 5 December 2024].

[134] Cloud Security Alliance, “Cloud Controls Matrix (CCM) Version 4,” Cloud Security Alliance, 2024. [Online]. Available: https://cloudsecurityalliance.org/research/cloud-controls-matrix. [Accessed 14 December 2024].

[135] National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), “Publications,” National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), n.d. [Online]. Available: https://csrc.nist.gov/publications. [Accessed 14 December 2024].

[136] National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), “NIST SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View,” National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), 3 March 2011. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/39/final. [Accessed 14 December 2024].

[137] National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), “NIST SP 800-53A Rev. 5: NIST SP 800-53A Rev. 5,” National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), 7 November 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/53/a/r5/final. [Accessed 14 December 2024].

[138] National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), “NIST SP 800-55 Vol. 1: Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures,” National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), 4 December 2024. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/55/v1/final. [Accessed 14 December 2024].

[139] National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), “NIST SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), 20 December 2018. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/37/r2/final. [Accessed 14 December 2024].

[140] National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), “Compliance FAQs: Federal Information Processing Standards (FIPS),” National Institute of Standards and Technology (NIST): Computer Security Resource Centre (CSRC), 3 July 2024. [Online]. Available: https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips. [Accessed 14 December 2024].

[141] E. B. Blancaflor, M. M. T. Cortez, D. M. Geneta, M. N. T. D and C. B. G. Alegre, "Comparative Analysis of Cybersecurity Frameworks Utilized by Industries in the Philippines," *3rd International Conference on Computer Systems (ICCS),* vol. 10.1109, no. ICCS59700.2023.10335521, pp. 158-162, 2023.

[142] W. Wong, Z. Alomari, Y. Shao and M. I. Satti, "Knowledge Graph to Facilitate Cloud Security Compliance with NIST Cybersecurity Framework," *2nd International Conference on Computer, Vision and Intelligent Technology (ICCVIT),* vol. 10.1109, no. ICCVIT63928.2024.10872451, pp. 1-6, 2024.

[143] M. Haidar, Y. G. Sucahyo, T. Sukardi and A. Gandhi, "Analysis of Csirt Services in Facing Cyber Security Challenges in Indonesia," *4th International Conference on Information and Communications Technology (ICOIACT),* vol. 10.1109, no. ICOIACT53268.2021.9563925, pp. 154-159, 2021.

[144] A. Setyawan, G. Y. Sucahyo and A. Gandhi, "Design of Disaster Recovery Plan: State University in Indonesia," *Fifth International Conference on Informatics and Computing (ICIC),* vol. 10.1109, no. ICIC50835.2020.9288543, pp. 1-5, 2020.

[145] S. Nikolovski and P. Mitrevski, "On the Requirements for Successful Business Continuity in the Context of Disaster Recovery," *57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST),* vol. 10.1109, no. ICEST55168.2022.9828701, pp. 1-4, 2022.

[146] C. Bansal and S. Tanwar, "The Role of Cloud Computing in Ensuring Business Continuity During Disasters," *6th International Conference on Contemporary Computing and Informatics (IC3I),* vol. 10.1109, no. IC3I59117.2023.10397987, pp. 782-787, 2023.

[147] V. S. Gnesdilov and Y. B. Mironov, "User Authentication and Authorization While Accessing a Virtual Laboratory," *Systems of Signals Generating and Processing in the Field of on Board Communications,* vol. 10.1109, no. IEEECONF60226.2024.10496805, pp. 1-5, 2024.

[148] G.-C. Cristescu and V. Croitoru, "Volumetric Distributed Denial-of-Service and Session Replay Attacks-Resistant AAA-RADIUS Solution Based on EAP and LDAP," *International Symposium on Electronics and Telecommunications (ISETC),* vol. 10.1109, no. ISETC50328.2020.9301119, pp. 1-4, 2020.

[149] G.-C. Cristescu and V. Croitoru, "Spoofed Packet Injection Attack-Resistant AAA-RADIUS Solution Based on LDAP and EAP," *International Symposium on Signals, Circuits and Systems (ISSCS),* vol. 10.1109, no. ISSCS52333.2021.9497398, pp. 1-4, 2021.

[150] N. Ikhsan, A. A. Sukmandhani, J. Ohliati and Y. D. Prabowo, "Design and Build AAA Server using Free Radius Study Case Network Security Management at PT. XYZ," *IEEE 9th International Conference on Computing, Engineering and Design (ICCED),* vol. 10.1109, no. ICCED60214.2023.10425645, pp. 1-6, 2023.

[151] Institute of Electrical and Electronic Engineers (IEEE), "IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control," *IEEE Std 802.1X-2020 (Revision of IEEE Std 802.1X-2010,* vol. 10.1109, no. IEEESTD.2020.9018454, pp. 1-298, 2020.

[152] S. Kumar, A. Kumar, S. Kumar and P. K. Chaurasia, "Comprehensive Analysis of Cloud Security: Issues & Challenges," *6th International Conference on Contemporary Computing and Informatics (IC3I),* vol. 10.1109, no. IC3I59117.2023.10398097, pp. 622-627, 2023.

[153] S. Aparajit, R. Shah, R. Chopdekar and R. Patil, "Data Protection: The Cloud Security Perspective," *3rd International Conference for Emerging Technology (INCET),* vol. 10.1109, no. INCET54531.2022.9825151., pp. 1-5, 2022.

[154] A. R. Reddy, K. L. Flower, J. Anitha and A. K. Kandru, "Detecting and Preventing Unauthorized User Access to Cloud Services by CASBs," *Second International Conference on Electronics and Renewable Systems (ICEARS),* vol. 10.1109, no. ICEARS56392.2023.10085406, pp. 868-873, 2023.

[155] Y. Qian, Y. C. Feng and Hsiao-Hwa, "WLAN Security," *IEEE - Security in Wireless Communication Networks,* vol. 10.1002, no. 9781119244400.ch7, pp. 129-152, 2022.

[156] A. Chaudhary and K. Kumar, "Vulnerability Analysis of WPA Security Protocols," *15th International Conference on Computing Communication and Networking Technologies (ICCCNT),* vol. 10.1109, no. ICCCNT61001.2024.10725681, pp. 1-7, 2024.

[157] G. Sagers, "WPA3: The Greatest Security Protocol That May Never Be," *International Conference on Computational Science and Computational Intelligence (CSCI),* vol. 10.1109, no. CSCI54926.2021.00273, pp. 1360-1364, 2021.

[158] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," *IEEE Symposium on Security and Privacy (SP),* vol. 10.1109, no. SP40000.2020.00031, pp. 517-533, 2020.

[159] S. D. Sanap and V. More, "Analysis of Encryption Techniques for Secure Communication," *International Conference on Emerging Smart Computing and Informatics (ESCI),* vol. 10.1109, no. ESCI50559.2021.9396926, pp. 290-294, 2021.

[160] Q. Zhang, "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption," *2nd International Conference on Computing and Data Science (CDS),* vol. 10.1109, no. CDS52072.2021.00111, pp. 616-622, 2021.

[161] G. A. Cordis, F. M. Costea, G. Pecherle, R. Győrödi and C. Győrödi, "Considerations in Mitigating Kerberos Vulnerabilities for Active Directory," *17th International Conference on Engineering of Modern Electric Systems (EMES),* vol. 10.1109, no. EMES58375.2023.10171623, pp. 1-6, 2023.

[162] S. H. Qatinah and I. A. Al-Baltah, “Kerberos Protocol: Security Attacks and Solution,” *1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI),* vol. 10.1109, no. ICETI63946.2024.10777133, pp. 1-7, 2024.

[163] J. R. Dora and L. Hluchy, “Attacks on Active Directory - Kerberos Delegation: *Exploitation of Active Directory using Kerberos Constrained Delegation,” *6th International Symposium on Logistics and Industrial Informatics (LINDI),* vol. 10.1109, no. LINDI63813.2024.10820404, pp. 103-108, 2024.

[164] C. D. Motero, J. R. B. Higuera, J. B. Higuera, J. A. S. Montalvo and N. G. Gómez, “On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey,” *IEEE Access,* vol. 10.1109, no. ACCESS.2021.3101446, pp. 109289-109319, 2021.

[165] University of Texas, “Knowledge Base Article - Service Portal,” University of Texas, 2024. [Online]. Available: https://ut.service-now.com/sp?id=kb_article&number=KB0011708. [Accessed 25 November 2024].

# Appendices

## Appendix 1

### A1.1 ISO/IEC 27000 Family of Standards

Table 23 Lists all current standards of the ISO/IEC 27000 framework.

*Table 23:ISO/IEC 27000 Family of InfoSec Standards [103] [104]*

| # | ISO Standard | Published ISO 27000 standards |
|---|---|---|
| 1 | ISO/IEC 27000 | Information security management systems. |
| 2 | ISO/IEC 27001 | Information technology – Security Techniques – Information security management. |
| 3 | ISO/IEC 27002 | Code of practice for information security controls. |
| 4 | ISO/IEC 27003 | Information security management system implementation guidance |
| 5 | ISO/IEC 27004 | Information security management — Monitoring, measurement, analysis and evaluation. |
| 6 | ISO/IEC 27005 | Information security risk management. |
| 7 | ISO/IEC 27006 | Requirements for bodies providing audit and certification of information security management systems. |
| 8 | ISO/IEC 27007 | Guidelines for information security management systems auditing. |
| 9 | ISO/IEC TR 27008 | Guidance for auditors on ISMS controls. |
| 10 | ISO/IEC 27009 | Internal document for the committee developing sector/industry-specific versions or implementation guidelines for the ISO27K standards. |
| 11 | ISO/IEC 27010 | Information security management for inter-sector and inter-organisational communications. |
| 12 | ISO/IEC 27011 | Information security management guidelines for telecommunications organisations based on ISO/IEC 27002. |
| 13 | ISO/IEC 27013 | Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. |
| 14 | ISO/IEC 27014 | Information security governance. |
| 15 | ISO/IEC TR 27015 | Information security management guidelines for financial services. |
| 16 | ISO/IEC TR 27016 | Information security economics. |
| 17 | ISO/IEC 27017 | Code of practice for information security controls based on ISO/IEC 27002 for cloud services. |
| 18 | ISO/IEC 27018 | Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. |
| 19 | ISO/IEC 27019 | Information security for process control in the energy industry. |
| 20 | ISO/IEC 27021 | Competence requirements for information security management systems professionals. |
| 21 | ISO/IEC TS 27022 | Guidance on information security management system processes – Under development. |
| 22 | ISO/IEC TR 27023 | Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002. |
| 23 | ISO/IEC 27031 | Guidelines for information and communication technology readiness for business continuity. |
| 24 | ISO/IEC 27032 | Guideline for cybersecurity. |
| 25 | ISO/IEC 27033 | IT network security. |
| 26 | ISO/IEC 27033-1 | Network security – Part 1: Overview and concepts. |
| 27 | ISO/IEC 27033-2 | Network security – Part 2: Guidelines for the design and implementation of network security. |
| 28 | ISO/IEC 27033-3 | Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues. |
| 29 | ISO/IEC 27033-4 | Network security – Part 4: Securing communications between networks using security gateways. |
| 30 | ISO/IEC 27033-5 | Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs). |
| 31 | ISO/IEC 27033-6 | Network security – Part 6: Securing wireless IP network access. |
| 32 | ISO/IEC 27034-1 | Application security – Part 1: Guideline for application security. |
| 33 | ISO/IEC 27034-2 | Application security – Part 2: organisation normative framework. |
| 34 | ISO/IEC 27034-3 | Application security – Part 3: Application security management process. |
| 35 | ISO/IEC 27034-4 | Application security — Part 4: Validation and verification – Under development. |
| 36 | ISO/IEC 27034-5 | Application security — Part 5: Protocols and application security controls data structure. |
| 37 | ISO/IEC 27034-5- | Application security — Part 5-1: Protocols and application security controls data structure, XML schemas. |
| 38 | ISO/IEC 27034-6 | Application security – Part 6: Case studies. |
| 39 | ISO/IEC 27034-7 | Application security — Part 7: Assurance prediction framework. |
| 40 | ISO/IEC 27035-1 | Information security incident management – Part 1: Principles of incident management. |
| 41 | ISO/IEC 27035-2 | Information security incident management – Part 2: Guidelines to plan and prepare for incident response. |
| 42 | ISO/IEC 27035-3 | Information security incident management — Part 3: Guidelines for ICT incident response operations. |
| 43 | ISO/IEC 27035-4 | Information security incident management — Part 4: Coordination – Under development. |
| 44 | ISO/IEC 27036-1 | Information security for supplier relationships – Part 1: Overview and concepts. |
| 45 | ISO/IEC 27036-2 | Information security for supplier relationships – Part 2: Requirements. |
| 46 | ISO/IEC 27036-3 | Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security. |
| 47 | ISO/IEC 27036-4 | Information security for supplier relationships – Part 4: Guidelines for security of cloud services. |
| 48 | ISO/IEC 27037 | Guidelines for identification, collection, acquisition and preservation of digital evidence. |
| 49 | ISO/IEC 27038 | Specification for Digital redaction on Digital Documents. |
| 50 | ISO/IEC 27039 | Intrusion prevention. |
| 51 | ISO/IEC 27040 | Storage security. |
| 52 | ISO/IEC 27041 | Investigation assurance. |
| 53 | ISO/IEC 27042 | Analysing digital evidence. |
| 54 | ISO/IEC 27043 | Incident investigation. |
| 55 | ISO/IEC 27050-1 | Electronic discovery – Part 1: Overview and concepts. |
| 56 | ISO/IEC 27050-2 | Electronic discovery – Part 2: Guidance for governance and management of electronic discovery. |
| 57 | ISO/IEC 27050-3 | Electronic discovery – Part 3: Code of practice for electronic discovery. |
| 58 | ISO/IEC 27701 | Information technology – Security Techniques – Information security management systems — Privacy Information Management System (PIMS). |
| 59 | ISO 27799 | Information security management in health using ISO/IEC 27002 – guides health industry organisations on how to protect personal health information using ISO/IEC 27002 |

## A1.2 Confidentiality, Integrity, Availability (CIA) and Denial, Alteration, Disclosure (DAD) Triads

Fig.17 illustrates the CIA triad and the DAD Triad, which is the goal of potential attackers.

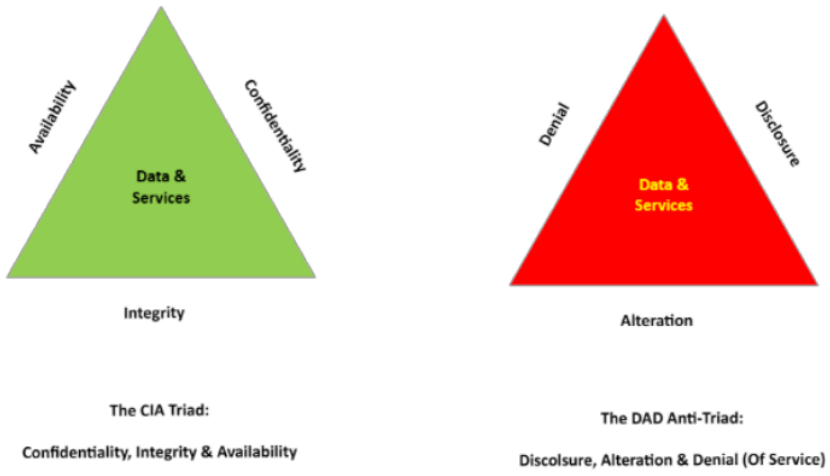



*Figure 16: Example (CIA and DAD TRIAD) [3]*

## A1.3 Visual overview of InfoSec frameworks

Fig.18 illustrates how the most popular InfoSec frameworks overlap with each other.

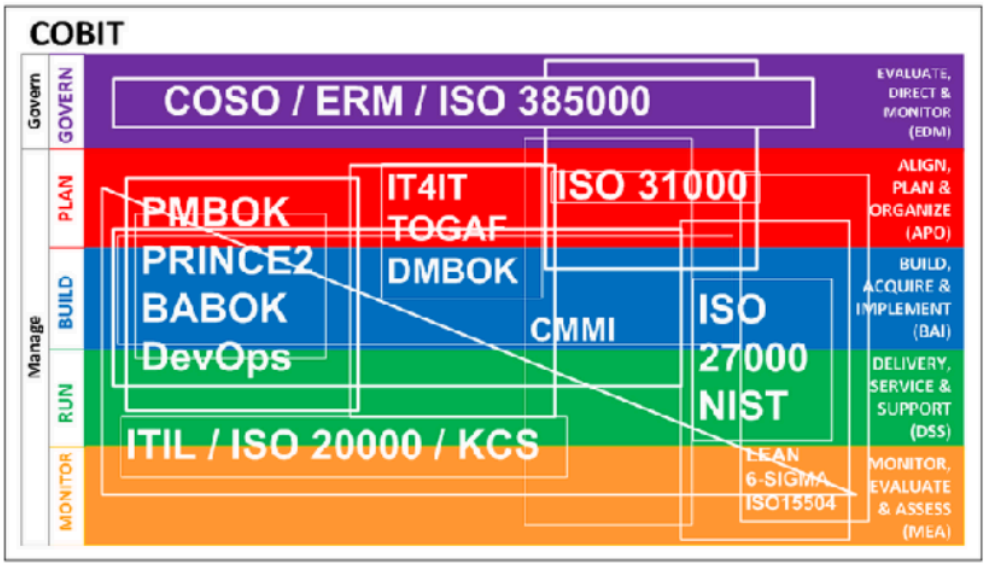



*Figure 17: Map of Information Security Frameworks [105]*

# Appendix 2

## A2.1 Compliance (Laws and Ethics)

Table 24 lists ethical approaches evaluated for NG. The virtue approach was recommended as it best suited the nature of the business as it embraces virtues such as honesty, integrity and fairness [4].

*Table 24: Review of Ethical approaches*

| Ethical Approach | Description | Selection of Ethical Approach for NG |
|---|---|---|
| Utilitarian approach | Results in most good/least harm. | This approach does not take into account relationships with customers and suppliers. It has therefore been discounted. |
| Rights approach | Protects human rights e.g. right to safety, privacy, free will to make choices. | Human rights are very important and need to be protected. However this approach does not encompass the nature of the business. |
| Fairness/Justice approach | All humans are equal and should be treated as such providing a level playing field. | It is widely recognised that all humans are equal, and should be treated with fairness.<br>This will be enforced by a discrimination at work policy, and is covered by UK law under the equalities act 2010.<br>This will ensure all are provided with a level playing field. |
| Common good approach | Focuses on common welfare, promoting compassion for all. | This only focuses in on compassion for others, whilst being highly commendable, other virtues are not embraced. |
| **Virtue approach** | **Promotes the virtues of honesty, fairness, fidelity, integrity, compassion. It also advises that consideration of outcomes to actions undertaken.** | **After careful deliberation, the Virtue approach is the most suitable ethical approach for NG.** With compassion for their customers and the environment being key. Along with honesty and integrity so that good relationships can be build with both their customers and suppliers alike. |

Table 25 Outlines legal concepts and provides recommendations for NG.

*Table 25: Key legal concepts and recommendations for NG [3] [4]*

| Concept | Description | Recommendations for NG |
|---|---|---|
| Jurisdiction | Power of court and law enforcement to make legal decisions and judgements | Laws must be adhered to wherever data is collected, stored processed and used. All laws will carry equal weight.<br><br>NG implementing cloud infrastructure means that the data could be stored anywhere on the globe.<br><br>NG needs to set out requirements with Cloud Service Provider (CSP) the location of datacentres to be used for NG and customer data. |
| Local jurisdiction | Laws that cover data collection and usage of a particular country. | |
| Long-arm jurisdiction | Ability of a court or law enforcement to extend its legal influence by connecting an entity outside of its jurisdiction to a local jurisdiction. | |
| Data Sovereignty | Data is subject to the local jurisdiction where it is collected stored and processed. | This re-inforces the requirement to ensure that data is stored in data centres in suitable locations.<br><br>In addition, all data stored on cloud infrastructure should be encrypted, with NG InfoSec team retaining encryption keys.<br>This ensures Confidentiality and Integrity of NG data. |
| Personally Identifiable Information (PII) | Data that can be used to uniquely identify a person, such as name, address, contact details. | All data should be encrypted, ensures Confidentiality and Integrity.<br>Data minimisation should be implemented, so that only necessary data is collected and retained - in accordance with GDPR. |

Table 26 predominantly outlines UK laws that NG must comply with to collect and process customer data and to protect Intellectual Property (IP) [106] [107] [108] [109] [110] [111] [112] [113].

*Table 26: Laws that NG must comply with*

| Act | Acronymn | Date | Area | Jurisdiction | Description |
|---|---|---|---|---|---|
| Intellectual Property Act | IPA | 2014 | Intellectual Property (IP) | UK | A legal framework to protect the IP of UK businesses. |
| General Data Protection Regulation | GDPR | 2016 | Protection of personal Information - Applies to EU citizens worldwide. | EU | A legal framework setting guidelines for collection and processing of EU citizens. |
| General Data Protection Regulation - UK | GDPR-UK | 2018 | Protection of personal Information - Applies to UK citizens worldwide. | UK | GDPR-UK is an adapted version of GDPR legislation for the UK. |
| Data Protection Act | DPA | 2018 | Protection of personal Information. | UK | This is the UK implementation of the GDPR legislation. Outlines Data Protection Principles, and individual's rights. |
| American Data Privacy and Protection Act | ADPPA | 2022 | Protection of personal data for US citizens. | US | Establishes how organisations must handle personal data. Outlining consumer data protections. |
| The Privacy Act | TPA | 1988 | Protection of personal data for Australian citizens. | Australia | Outlines 13 Australian Privacy Principles (APP), giving direction on the collection, use and disclosure of personal information. |

GDPR is a crucial legal framework in the UK and EU [114] [115] [116] [117] [118] [119].

Table 27 shows GDPR's main principles. Table 28 shows the roles and responsibilities in relation to NG [3] [120].

*Table 27: GDPR Principles*

| GDPR principles | Description |
|---|---|
| Lawfulness, fairness and transparency | Everything must be open and legitimate. |
| Purpose limitation | Data collected must be for the specified reason only. |
| Data minimisation | Only relevant data collected and processed according to original purpose. |
| Accuracy | Ensures data is accurate and updated. |
| Storage limitation | Data is stored for only as long as it is required for its original purpose. Personal data may be stored for longer. |
| Integrity and confidentiality (security) | Personal data must be secure, control measures must be in place to secure data from alteration, unauthorised access, or |
| Accountability | Data controller responsible to demonstrate GDPR legislation is being utilised e.g. Proving what data is being processed, and how long data has been processed for. |

*Table 28: GDPR Roles and Responsibilities*

| GDPR Roles | Description | NG |
|---|---|---|
| Data Controller | The Data Controller determines the purpose and method personal data is processed. | CIO |
| Data Steward | Members of staff that carry out the intent of data controller. Has oversight of data governance and responsible for day-to-day operational activities of data governance. | Manager of InfoSec team. |
| Data Custodian | Responsible for safeguarding data. | InfoSec team. |
| Data Processor | Usually service providers that process data on behalf of data controller. | Credit Card processing service. |
| Data Protection Officer (DPO) | Specific individual at an organisation responsible for data privacy efforts. | CISO |

NG needs to accept payments from customers using credit/debit cards. To do this NG needs to comply with the standard outlined in Table 29. By implementing the recommended frameworks of this report NG will meet these standards [3] [4].

*Table 29: Payment card standard*

| Standard | Acronym | Date | Area | Description | Jurisdiction |
|---|---|---|---|---|---|
| | | | | | |
| Payment Card Industry Data Security Standard v4.0.1 | PCI DSS | 2022 | Credit and Debit Card payments | Provides guidance on: Firewall configuration, Cardholder data protection, vulnerability management, Continual Network monitoring, InfoSec policy. | Global |

Some firewalls have a built-in functionality to continually detect and report on levels of compliance. Fig.19 Shows an example from Checkpoint [121]:




*Figure 18: Checkpoint firewall compliance monitor*

## A2.2 Governance and Strategic Planning for Security

A strategic plan outlines the long-term direction that an organisation will take. It is imperative that this is aligned with the strategic security plan of the InfoSec department, to ensure that both are working together.

The aim of governance is to provide a strategic plan for protecting the organisation's data including all information assets. This is achieved by implementing practices and assigning corporate responsibilities. This can be accomplished by using an industry approach known as Governance, Risk Management and Compliance (GRC) [122].

Table 30 shows a selection of COBIT 2019 principles that satisfies the GRC requirements and outlines advantages it provides to NG.

*Table 30: Selection of COBIT 2019 principles*

| Feature of COBIT 2019 | Advantages for NG |
|---|---|
| Strategic alignment | Ensures that Organisational and Security strategic plan work in unison. |
| **Governance** | InfoSec governance refers to the management and protection of sensitive data/information data assets. |
| **Risk Assessment** | As discussed Risk Assessment and Treatment is a key component to identifying vulnerabilities and implementing control measures. |
| **Compliance** | Ensures that the organisation complies with regularity requirements. |
| Performance Measurement | Measuring security outcomes of an organisational can ne a key indicator, and can be used to improve the organisational security. |
| Continual Improvement | This ensures that security sytesms are continually evolving to meet new cyber threats and the implementation of new technology and systems. |
| Flexibility | COBIT is designed to be flexible in order to react to changing organisational needs. |
| Integration with other Frameworks | This is crucial as multi-framework organisations can |

To implement an InfoSec programme, the Security System Development Life Cycle (SDLC) methodology can be adopted, see Fig.20 and Table 31 [4] [123].

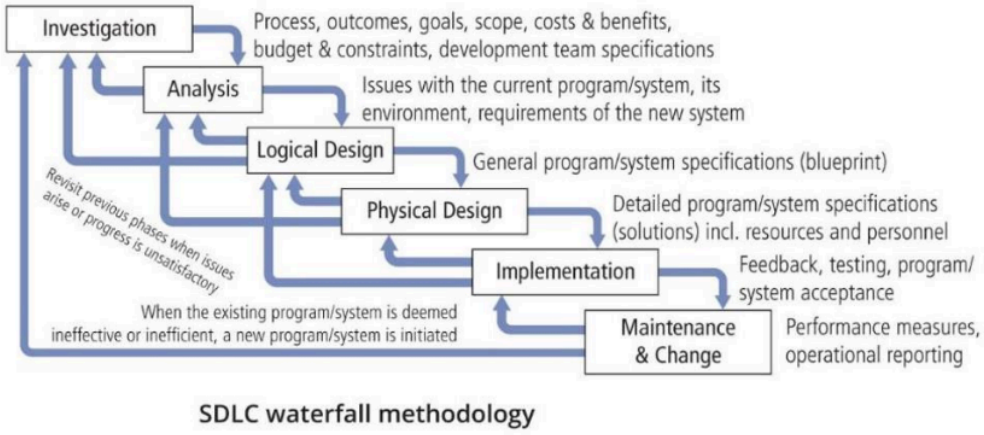



*Figure 19: SecSDLC Waterfall*

*Table 31: SecSDLC Analysis*

| SecSDLC Phase | Description |
|---|---|
| Investigation | 1.Directive from Senior Management Team (SMT) Specifying budget, outcomes, process and goals of project.<br>2.Current policies and new policies evaluated.<br>3.Development team is assembles of managers, employees and consultants to discuss the following :<br>* Define the scope<br>* Investigate potential issues<br>* Identify Goals and Objectives<br>* Identify any further constraints not covered by the EISP<br>4.Feasibility analysis: Ensures the organisation has sufficient resource and commitment for the Analysis and Design phases. |
| Analysis | 1.The Analysis team studies the documentation from the investigation phase.<br>2.The Development team from phase 1 now carries out initial analysis on current security policies, known threats and controls.<br>3.Risk Management is undertaken (discussed in detail later in this assignment). |
| Logical Design | 1.Blueprint for security created, key policies implemented that can influence decision making.<br>2.Feasibility analysis: Confirms if project should continue in-house or by 3rd party consultancy. |
| Physical Design | 1.Technology evaluation to support blueprint.<br>2.Blueprint evaluated to ascertain if any changes are required in the physical design phase.<br>3.Blueprint finalised and final design agreed upon.<br>4.Feasibility analysis: confirms status of organisation to accept proposed project. User consultation takes place.<br>5.User feedback assessed<br>6.Formal approval required for project to go ahead.<br>7.Assessment of Security Controls -discussed in detail later in this assignment. These include:<br>* Three categories: Managerial, Operational, Technical Controls.<br>8.Contingency Planning (CP) is addressed at the design phase. CP is discussed in detail later in this assignment. |
| Implementation | 1.The Security solution has now been either purchased or developed, tested, implemented and re-tested.<br>2.User issues are evaluated - Security Education and Training Awareness (SETA) programme conducted.<br>3.Security Package put forward to the SMT for final approval. If approval granted, continue with implementation.<br>4.Project plan management which contains three steps:<br>* Project planning<br>* Supervision of project action points<br>* Finalising project plan<br>5.With the project plan finalised, the next step is to continue with Project management utilising a framework such as PRINCE2<br>6.Project team is assembled which includes:<br>*Champion: A senior executive to ensure resources are available and promote project.<br>*Team Leader: Project Manager that understands InfoTech requirements.<br>*Security Policy developer: Staff that are familiar with current policy and can develop/implement new policies.<br>*Risk Assessor: Expert in Financial risk assessment techniques/assets, familiar with security methods.<br>* Security Professionals: Security experts with experience of InfoSec ISMS<br>*System Administrators: Responsible for safeguarding data and systems.<br>*End users: Staff that will use the new security system most frequently. Their feedback is critical to the success of the new project to ensure that it is adopted.<br>7.IT Staffing to ensure that the Project is implemented smoothly and to evaluate any knock on effects with other IT systems. |
| Maintenance & Change | 1.Continual monitoring/testing of new system and maintenance (updating firmware, modifying config)<br>2.If new system becomes ineffective or is superseded the process begins again. Either amending the current system or developing/purchasing a new replacement system. |

The ISO/IEC 27014 provides guidance specifically on governance of InfoSec it is best used as an assessment tool to test whether its InfoSec programme meets the standard requirements for ISO certification.

Table 32 shows the ISO/IEC 27014 principles.

*Table 32: ISO/IEC 27014 Principles*

| # | Principle |
|---|---|
| 1 | Establish organisation-wide InfoSec |
| 2 | Adopt risk-based approach |
| 3 | Set direction of resource decisions |
| 4 | Ensure compliance of policy and regulationary requirements |
| 5 | Promote a security-positive environment within the organisation. |
| 6 | Continual performance monitoring related to business outcomes. |

There are correlations between ISO/IEC 27014 and COBIT.

Fig.21 Shows the ISO/IEC 27014 process and Table 33 gives further detail [4].

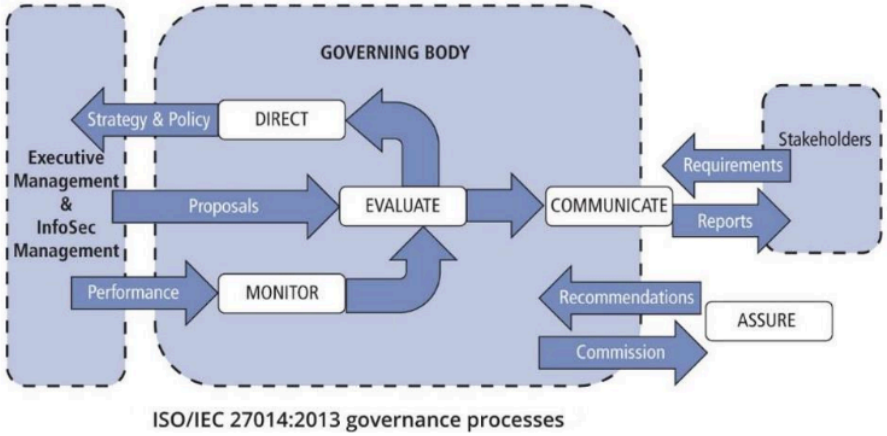



*Figure 20: ISO/IEC 27014 Governance Process*

*Table 33: ISO/IEC 27014 Process*

| # | Principle | Desription |
|---|---|---|
| 1 | Evaluate | An evaluation is carried out to ensure InfoSec objectives meet strategic goals. Determining whether modifications are required to the InfoSec programme. |
| 2 | Direct | Evaluation is forwarded to board of directors which provides direction on any modifications to the InfoSec programme. Modificaions can include:<br>*Alteration to organisational risk appetite<br>* Modifications to the risk management<br>* Re-allocation of resources<br>* Re-prioritiseation of efforts<br>* Adoption of new policy |
| 3 | Monitor | InfoSec performance measurement utilised to assess whether goals and objectives, set by the governing body, are being met.<br>**(COBIT 2019 implementation will provide performance measurements)** |
| 4 | Communicate | Communication between Governing body and stakeholders exchanging reports and requirements:<br>Governing Body: Reports detailing recommendations and organisation's efforts.<br>Stakeholders: Requirements |
| 5 | Assure | This allows the organisation to demonstrate to external entities such as customers, suppliers, stakeholders that InfoSec governance program meets best practice standards. This is done by:<br>* Certification e.g. ISO/IEC 27001, ISO/IEC 27014 certification<br>* InfoSec Audits e.g. Service Organisation Controls (SOC) - SOC2 Type I & II or SOC3 |

See Appendix 2.10 for further details for SOC Audits.

## A2.3 Security Policies

Security Policies are crucial to implementing an InfoSec programme; they provide rules and guidance that all staff within an organisation must follow. Fig.22 Illustrates the sphere of security that represents the control measures and the areas they secure.

A defence in depth approach is utilised whereby multiple controls are used to secure data. Most measures apply to the network as this is the ingress point for many attacks.

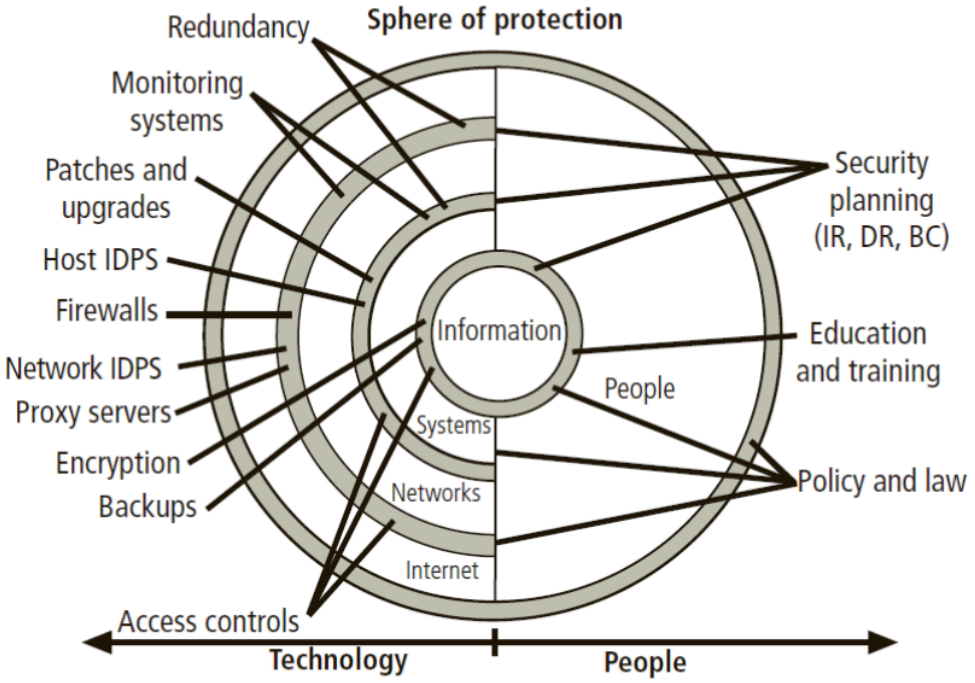



*Figure 21: Sphere of security/protection [4] [12]*

According to the National Institute of Standards of Technology (NIST) three types of InfoSec policies should be implemented to secure data, see Table 34 [4]:

*Table 34: InfoSec policies to be implemented by NG*

| Policy | Acronym | Purpose | Audience |
|---|---|---|---|
| Enterprise Information Security Policy | EISP | High-level policy outlining the InfoSec ethos of the organisation | All |
| Issue-Specific Security Policy | ISSP | Provides guidance to staff on the usage of specific technologies | All |
| System-Specific Security Policy | SysSP | Provides guidance on configuration of systems and implementation of access policies according to managerial direction. | Technical Staff |

Fig.23 shows an illustration of these three policies:

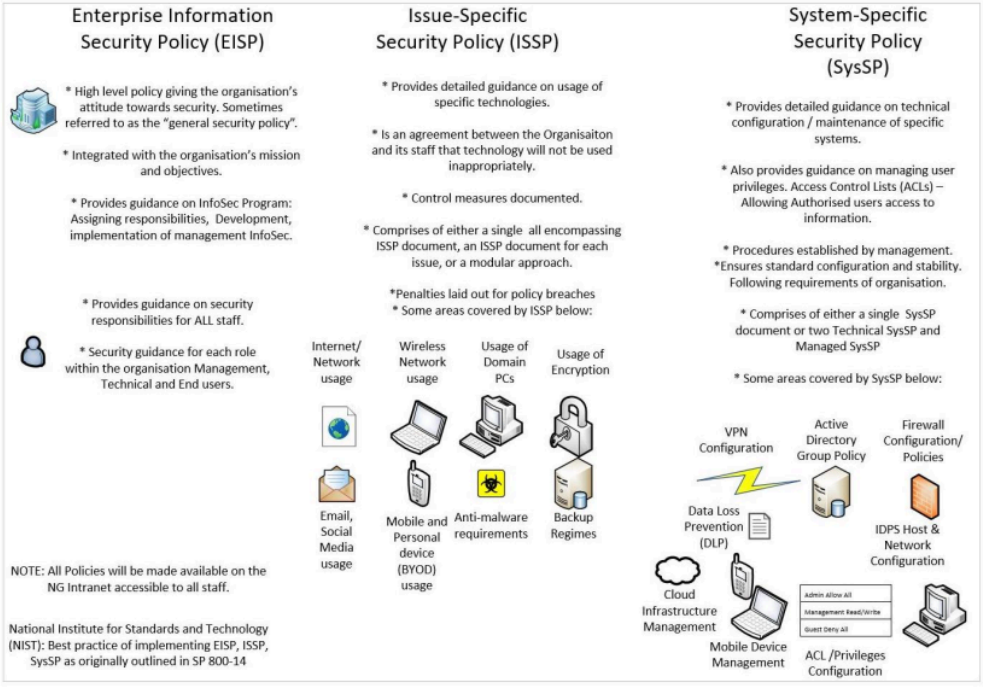



*Figure 22: Illustration of EISP, ISSP and SysSP*

The recommendations for each of these policies can be found in Tables 35-37 [3] [4] [12] [124] [125].

*Table 35: EISP Recommendations*

| # | EISP Recommendations | Detail | Reasoning |
|---|---|---|---|
| 1 | Publication of EISP available to all staff | This will outline the organisation's position on Information Security. | To inform all staff of InfoSec philosophy at the organisation and highlight its importance. |
| 2 | Information should be safeguarded to maintain the Confidentiality, Integrity, Availability, which is the CIA triad. | Information should be kept secure to guard against unauthorised access, alteration or denial of access. | Information Security is CRITICAL to the success of the organisation. Without it competitors will have an edge, projects could be undeliverable, the organisation could suffer financial loss or fines. |
| 3 | Inform staff of their responsibilities regarding InfoSec. | Provides general guidance of InfoSec to all staff. | Will raise awareness of data security, the responsibilities of staff members. |

*Table 36: ISSP Recommendations*

| # | ISSP Recommendations | Detail | Reasoning |
|---|---|---|---|
| 1 | Internet / network usage. | Definition of expected usage of network resources. | To ensure appropriate use of resources. |
| 2 | Electronic communications: Email, Instant Messaging and **Social Media.** | Defines the usage of electronic communications. So that only appropriate content is used.<br><br>Particularly for **social media** usage to ensure a professional communications at all times. | To provide guidance on what is expected of staff when using social media, to ensure that content is appropriate and aligns with the ethos of NG. |
| 3 | Company Owned Business Only (COBO) Deployment of Smartphones. | After deliberations it was decided that with the risk to IP was too great to allow **BYOD** deployment.<br><br>A **COBO** deployment is advised instead for all staff. | It would be possible to implement BYOD with VPN connectivity to corporate network, along with storage segmentation.<br><br>**However, it is recommended that a COBO deployment is implement** due to the value of IP to the organisation<br><br>With COBO all devices will be fully managed and secured. |
| 4 | Wireless Communications. | Reduction of reliance on Wireless connectivity. | NGs reliance on Wireless communications is a risk to the business as wireless networks are a shared medium. The potential for data breach is increased.<br><br>Advise Wired domain PCs are used for **Intellectual Property (IP) data**. |
| 5 | Wired Domain PC Usage. | Deployment of wired domain PCs. | Wired domain PCs are more secure as the data will be contained within the infrastructure of the building. Also, the PC will be fully managed by NGs IT Security team. |
| 6 | IT Usage Policies | Acceptable Usage Policy (**AUP**)<br><br>Password Policy (**PP**): Ensures that passwords have complexity and length standards. Also changed every 6 months. | Ensures that IT equipment is used appropriately.<br><br>Ensures passwords are difficult to crack, and are changed periodically. |

*Table 37: SysSP Recommendations*

| # | SysSP Recommendations | Detail | Reasoning |
|---|---|---|---|
| 1 | Next Generation Firewall implementation | Provides additional features to secure data. | Integrated IDPS, Unified Threat Management, **Data Loss Prevention (DLP)** |
| 2 | Data Classification | Data is classified based on sensitivity. Levels used are: Public, Private, Sensitive, Confidential. | Using classification will identify IP data, to ensure that it can be tracked and remains secure. |
| 3 | Data Loss Prevention implementation. | DLP can safeguard IP data from data breaches. Keeping NG data secure from competitors. | Data classification is used in conjunction with **DLP** to identify and safeguard **IP data**. |
| 4 | Implementation of Enterprise level Wireless. | **WPA3** (Wi-Fi Protected Access version 3) to be implemented with all wireless devices. **Enterprise level authentication** using **RADIUS** (Remote Authentication Dial-in User Service) servers. | This will provide the highest level of security as the latest wireless authentication protocol will be used. Authenticated via Active Directory. |
| 5 | IDPS configuration | Ensures that systems are continually monitored for Indications of Compromise (**IoC**). | Any suspicious activity can be detected and resolved quickly. |
| 6 | Virtual Private Network (VPN) implementation. | Safeguards NG staff that work from home, remote working. | Ensuring data is encrypted and secure while traversing the internet. |
| 7 | Cloud server configuration. | Ensuring that cloud services are configured securely according to the Cloud Security Alliance (**CSA**) Framework. Utilising the Cloud Controls Matrix (**CCM**). | Allowing access to services for NGs customers and staff, while maintaining maintaining data security and the CIA triad. |
| 8 | Geotagging implementation. | Geolocation configuration on all mobile devices to ensure that all mobile devices can be tracked. | Ensures the security of mobile devices. |
| 9 | Geofencing implementation. | It is possible for mobile devices to be blocked from accessing sensitive IP data once they leave the NG building. | To ensure NG's proprietary IP data remains secure. |

## A2.4 Risk Management

Risk Assessment is a key component of InfoSec frameworks. Firstly, it is crucial to define "Risk" see Fig.24.

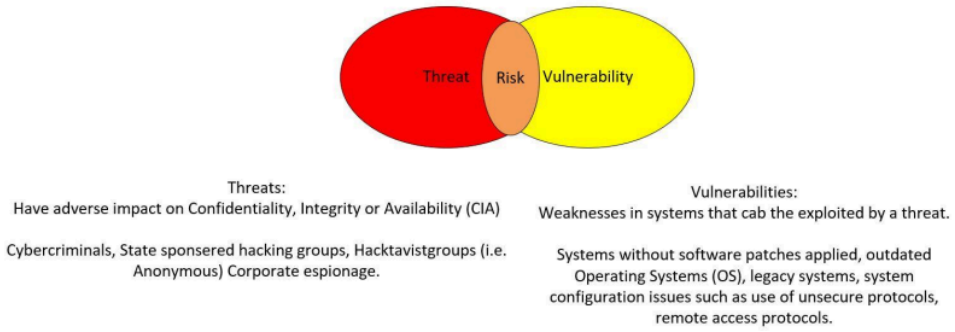



*Figure 23: Definition of "risk"*

Table 38 details how organisations deal with risk.

*Table 38: Description of risk*

| Terminology | Description | Relating to NG |
|---|---|---|
| Risk Appetite | The level of risk an organisation is willing to accept. This will depend on the organisation, the impact the risk has, the cost of implementing control measures in relation to financial loss suffered if risk is realised. | **NG's risk appetite is low.** If a data breach were to occur Intellectual Propery assets could be lost incurring financial loss of several billions. |
| Inherent Risk | Level of risk facing an organisation, without any control measures in place. | This is NG's current situation. No controls or mitigations in place. |
| Residual Risk | The level of risk remaining after control measures have been implemented. | Threats and Vulnerabilities have been identified in this report. Recommendations to mitigate, or remove these using risk treatment strategies have been made. |

Risk comprises of threats and vulnerabilities. Organisations can implement control measures to mitigate or eliminate vulnerabilities.

The main threats to NG have been identified in Tables 39-41 [3] [126] [127] [128].

*Table 39: Examples of Internal Threats*

| Internal Threats | | | | |
|---|---|---|---|---|
| **Threat** | **Description / Example** | **Recommendations for NG** | **Recommended Framework** | **Recommended Policy** |
| Human Error | Human error can be very commen, a typical example bing a member of staff forwarding an email with sensitive information to the wrong person, unintentionally damaging critical infrastructure, deleting files/backups resulting in data loss. | Controls for this could be Data Categorisation, and Data Loss Prevention (**DLP**). Regular backups of data using the 3-2-1 approach as advised by NCSC. three backup copies, one two systems, one offsite. | ISO/IEC 27000 | System-Specific Security Policy (SysSP) |
| Disgruntled Employee | This is a member of staff that may have an issue with the company and may intentionally damage infrastructure or alter data to cause disruption.<br><br>This is very dangerous as the member of staff is an authenticated user and potentially has authorisation to access, modify and delete data. | This is the most difficult to regulate. An Intrusion Detection/Prevention System (**IDPS**), can take a baseline of normal activity and any activity out of the ordinary for a member of staff will be highlighted.<br>Known as **behaviour-based or Heuristic** detection. | ISO/IEC 27000 | SysSP |
| Insider Attack | Once again this is an authenticated member of staff. But on this occasion their motivation is to disclose confidential data, such as Intellectual Property. | **DLP** and **Heuristic detection** should be implemented. | ISO/IEC 27000 | SysSP |
| System Failure | This can be due to the failure of a critical device, such as a firewall, or onsite server such as a Domain Controller (DC). Or software accessibility issues, such as a software update issue or licensing issue. | System Security Policy should address this by advising redundancy should be built into system design, such as backup DCs, Pairs of Firewalls to be installed in High Availability (**HA**) mode. | ISO/IEC 27000 | SysSP |
| System Maintenance Issues | If systems are not properly maintained, critical updates and software patches are not applied. This will result in vulnerabilities which can be exploited by attackers. System misconfiguration issues. | Patching regime should be put in place, this should be carried out closely with Vulnerability Assessments to highlight required updates. | ISO/IEC 27000 | SysSP |
| Wireless Networks | NG's over reliance of wireless, 95% of network devices currently connected. Wireless is a shared medium, therefore attackers can intercept wireless traffic, using network sniffing techniques. Wireless attacks such as **'Evil twin'** can be used whereby a malicious Wireless Access Point (WAP) is installed, broadcasting NG's Wireless name. Staff could then connect to the malicious WAP and send sensitive data to the attacker. An attacker can also attempt to connect to the network using Wardriving, or recently Warflyling (using drones) techniques. | Update to enterprise level wireless infrastructure using **WPA3**.<br>WAP with Network Access Control (**NAC**) capabilities.<br>Virtual Private Network (**VPN**) technology to be implemented.<br>Wired infrastructure to be implemented. Wired PCs managed by Active Directory (AD) and Group Policy (GP)<br>Unified Endpoint Management (**UEM**) implementation for management of all endpoint wireless devices Mobile, Laptop and Tablets (Microsoft, Apple, Android/Linux). | ISO/IEC 27000 | SysSP & ISSP (Issue-Secific Security Policy) |
| Bring Your Own Device (BYOD) | BYOD are a risk as device may have become compromised and as it is not managed by NG IT Dept, then this would not be picked up. Potential data breach issue if sensitive data is stored on compromised BYOD. | Advise NG Implement a Corporate Owned Business Only (**COBO**) deployment of devices for staff so that all devices can be managed by **UEM** and **AD/GP**.<br><br>A separate guest network with dedicated guest Virtual Local Area Network (**VLAN**). This will grant BYOD devices internet access only. Access to NG server infrastructure will be **denied from BYOD devices.** | ISO/IEC 27000 | SysSP & ISSP (BYOD) |
| Shadow IT | Some members of staff may use Devices or software without the knowledge of the IT department. There is no | Network Infrastructure upgrade: Media Access Control (MAC) based authentication for all switching such as **IEEE 802.1X** to ensure only authorised devices are connected to the network. All switching to impliment Network Access Control (NAC) and dynamic **VLAN** assignemnt.<br><br>Monitoring of network traffic, so that any unauthorised software can be detected. | ISO/IEC 27000 | SysSP & ISSP |

*Table 40: Examples of External Threats*

| External Threats | | | | |
|---|---|---|---|---|
| **Threat** | **Description / Example** | **Recommendations for NG** | **Recommended Framework** | **Recommended Policy** |
| Malware | Member of staff could download malicious software such as a virus, worm or ransomware. | Security Education Training and Awareness (**SETA**) Programme. Cybersecurity and awareness training for all staff. Further cybersecurity training for technical staff.<br><br>All software and firmware to be updated regularly, Anti-Virus to be installed on all PCs.<br>Endpoint Detection and Response (**EDR**) system to be implemented.<br>Implementation of a Security Information and Event Management (**SIEM**)system.<br>Incident Response Plan (**IRP**) to be drawn up. | ISO/IEC 27000 | SysSP (Patching regime policy) |
| Email | Phishing emails are designed to entice a user to click on a link, initiating an attack. | **SETA** Programme and **EDR**. | ISO/IEC 27000 | ISSP |
| Social Media | Social media can be used by attackers to harvest information about an organisation, direct messaging users with malicious links. Inappropriate usage of social media by staff. | **SETA** Programme and **EDR**. Specific Social media policy to ensure that all communications are professional and staff are **aware of social engineering techniques used by attackers.** | ISO/IEC 27000 | ISSP (Social Media Policy) |
| Cloud | Cloud infrastructure can be targeted by attackers, improperly configure Access Controls, vulnerabilities, Application Programme Interface (API) keys | Implementation of Vulnerability Assessment (VA), and risk assessments. Configuration according to Cloud Control Matrix (CCM) principles. | ISO/IEC 27000/ CCM | SysSP |
| Environmental | Loss of Power, Flooding, Wind Damage, Lightning strikes. Severe adverse weather e.g. tornados. | Disaster Recovery (DR) and Businesses Continuity (BC) plans to be drawn up. Implementation of Uninterruptible Power Supplies (UPS) devices, diverse power supplies. | ISO/IEC 27000 | SysSP, Enterprise Information Security Policy (EISP) |

A Risk Management (RM) policy should be in place so that the RM process is formally documented, see Table 41.

*Table 41: Example of Sections within RM policy.*

| RM Policy Section | Details |
|---|---|
| Purpose and Scope | Outlines the usage constraints of RM policy |
| Intent and Objectives | Aligns with Organisations Goals and Objectives |
| Roles and Responsibilities | Lists staff (by position) and what is expected of them during the RM process. |

The ISO/IEC 27005 assists with RM to identify, evaluate and treat risks [21]. See Fig.25 showing the ISO/IEC 27005 risk management process:

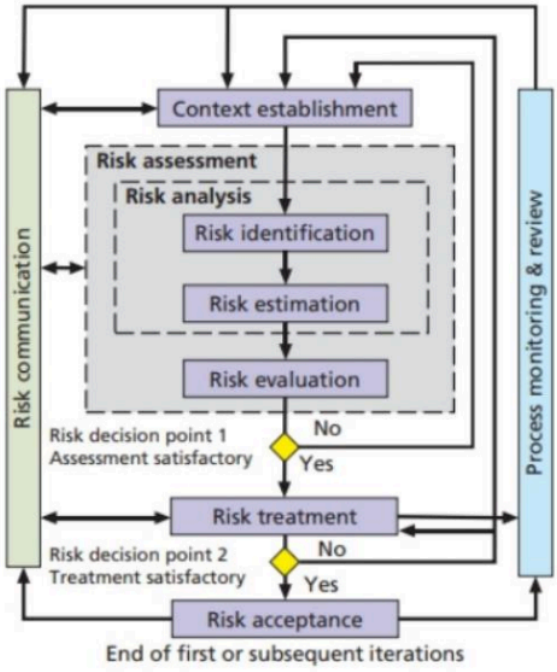



*Figure 24: Illustration of the ISO/IEC 27005 RM process [4]*

Table 42 provides more details of the RM process [129].

*Table 42: RM Process detail*

| RM Process | Detail |
|---|---|
| Context establishment | Defines objectives of RM process |
| Risk Identification | Conducting Vulnerability Assessments |
| Risk estimation | Based on Likelyhood and Impact |
| Risk Treatment | Putting control measures in place, identified in ISO/IEC 27002 |
| Risk Acceptance | The organisation's risk appetite may be higher than the residual risk. Therefore the risk would be deemed acceptable. |
| Risk Communication | Ensures that risks are communicated to key parties, |
| Process and Review | RM is a continual process, as new risks are discovered regularly. |

It is crucial to identify assets of an organisation, and the importance of the asset. This gives an indication of the severity of the risk if the asset were to become compromised. Organisations use software packages such as IRM Pro to carry out this task see Fig.26.

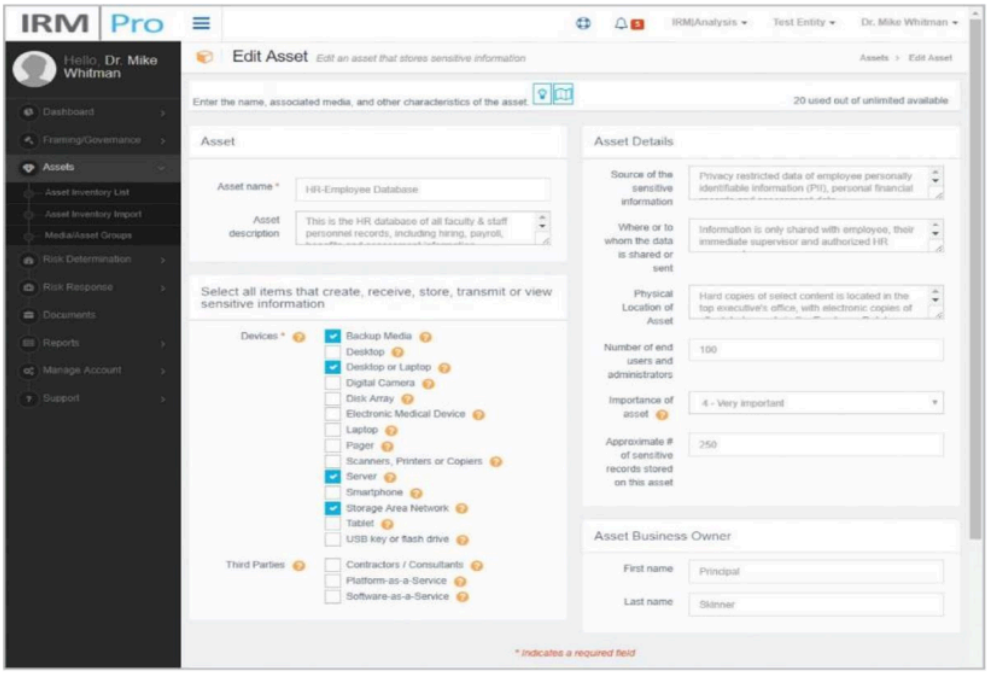



*Figure 25: IRM Pro software for RM [4]*

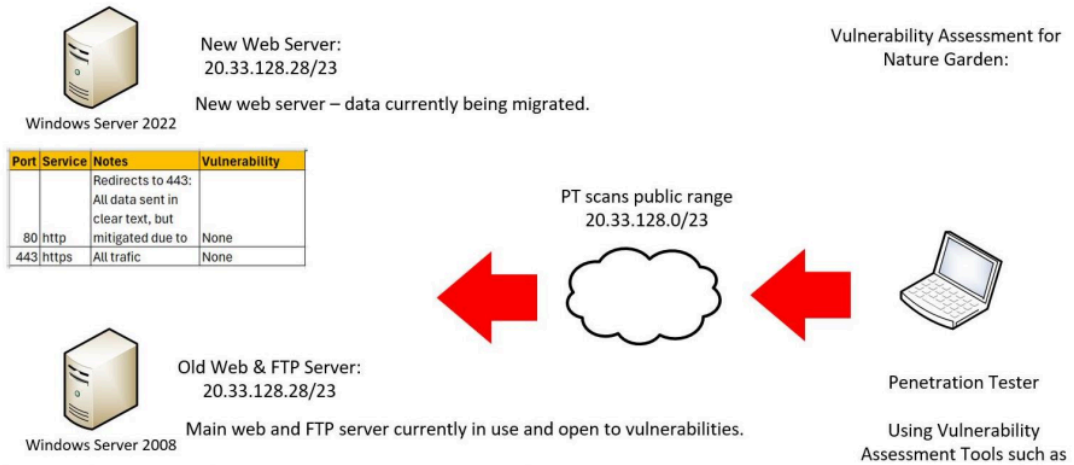
Information Assets would also be classified to give a similar rating of their importance, see Table 43:

*Table 43: Examples of Data Classification [3]*

| Private Sector | Military |
|---|---|
| Highly Sensitive | Top Secret |
| Sensitive | Secret |
| Internal | Confidential |
| Public | Unclassified |

These techniques are used to quickly identify critical assets at an organisation that need to be protected.

Once the assets are identified a Vulnerability Assessment (VA) can be conducted by the InfoSec team or an external Penetration tester, Fig.27 illustrates a VA in progress [130] [131] [132] [133].




| Port | Service | Notes | Vulnerability |
|---|---|---|---|
| 80 | http | Redirects to 443: All data sent in clear text, but mitigated due to | None |
| 443 | https | All trafic | None |

| Port | Service | Notes | Vulnerability | Descripton | Impact |
|---|---|---|---|---|---|
| 20& 21 | ftp | File Transer Protocol - sends data in clear text | CVE-2021-4189 | Allows attacker to setup malicious FTP server tricking clients to divulge data | Confidentiality: Due to malicious FTP server |
| 80 | http | Sends data in clear text | CVE-2024-27316 | Apache HTTP Server: HTTP/2 DoS by memory exahsution | Availability: Due to DoS attack |
| 139 | smb | Server Message Block | CVE-2017-0146 | Windows SMB Remote Code Execution | Integrity: Due to remote code execution |
| 443 | https | Data Encrypted | None | | |

*Figure 26: Example of VA in progress*

Once the vulnerabilities have been identified the next stage is to priorities which vulnerability to address first. This can be done by using a Risk Rating Matrix, see Table 44.

*Table 44: Risk Matrix [4]*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Impact | 5 | Severe | Low | Medium | High | High | Critical |
| | 4 | Major | Low | Medium | Medium | High | High |
| | 3 | Moderate | Low | Low | Medium | Medium | High |
| | 2 | Minor | Low | Low | Low | Medium | Medium |
| | 1 | Insignificant | Low | Low | Low | Low | Low |
| | | Rating | Rare | Unlikely | Moderate | Likely | Almost Certain |
| | | Value | 1 | 2 | 3 | 4 | 5 |
| | | | Likelihood | | | | |

Vulnerabilities are then scored according to the risk matrix. A risk rating worksheet can be created to prioritise which devices need control measures applied and their urgency. See Table 45.

*Table 45: Risk rating worksheet*

| Asset | Vulnerability | Likelihood | Impact | Risk-Rating Factor | Notes |
|---|---|---|---|---|---|
| Existing Web server | HTTP DoS Vulnerability | 8 | 9 | 72 | This is a critical vulnerability of NG, as this will impact online sales, and needs to be resolved first. |
| Existing Web server | SMB Remote Code execution | 7 | 9 | 63 | The consultants have advises NG that the likelihood of the SMB attack is slightly less, this is also a critical vulnerability but the http has higher priority. Both vulnerabilities need addressing as soon as possible. |
| Existing FTP server | Malicious FTP Server vulnerability | 6 | 6 | 36 | The FTP server is in the process of being decommissioned, impact is less severe. |

The Risk rating worksheet highlights the webserver is the priority; the other risks will be resolved in turn.

Once the vulnerabilities have been prioritised, the RM treatment strategy is implemented. Fig.28 illustrates the RM treatment cycle, which goes through the process of evaluating risk, implementing controls and crucially continual monitoring. This ensures that no new vulnerabilities are identified, and control measures remain effective.

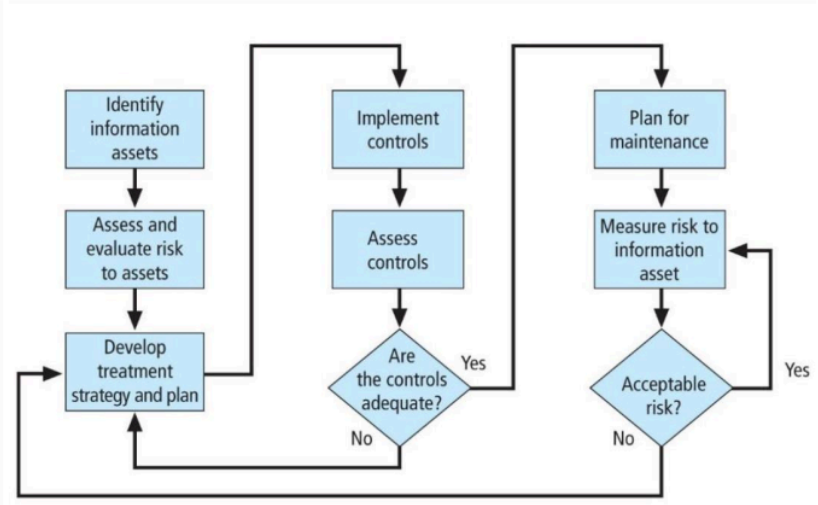



*Figure 27: RM treatment cycle [4]*

Cost of control implementation must be proportionate; Cost Benefit Analysis (CBA) must be conducted to ascertain whether implementation of control measures to the business is worth investing resources. See the CBA analysis for Distributed Denial of Service (DDoS) of NG in Table 46.

*Table 46: Calculation of ALE and CBA for NG [77] [78]*

| Item | Value | Details |
|---|---|---|
| Asset Value (AV) | £10,000 per hour | During DDoS (Distributed Dinal of Attack) attack, server undamaged, but service degraded and unable to meet demand. |
| | 2 Hours | After discussions with Cybersecurity consultants, it is anticipated that a single DoS attack could last for two hours. |
| AV | £ **20,000.00** | |
| Annualised Rate of Occurrence (ARO) | 4 Attacks | It is anticipated that 4 attacks will take place annually. |
| Exposure Factor (EF) | 90% | It is expected that system capacity will be reduced by 90% during a DoS attack. |
| | | |
| Single Loss Expectancy (SLE) | £ 18,000.00 | SLE = AV x EF (£20,000 x 90%) |
| | | |
| Annualised Loss Expectancy (ALE) | £ 72,000.00 | ALE = SLE x ARO (£18,000 x 4) |

| Item | Value | Details |
|---|---|---|
| Annual Cost of Safeguard (ACS) | £ 3,000.00 | Cloud Service Provider DDoS protection: Amazon Web Services Shield (DDoS protection service) |
| | | |
| ALE (Precontrol) | £ 72,000.00 | |
| ALE (Postcontrol) | £ 8,000.00 | AWS Shield in place for one year. (EF now 10%) |
| | | |
| Cost Benefit Analysis (CBA) | £ 61,000.00 | CBA = ALE (Pre) - ALE(Post) - ACS (£72,000 - £8,000) - £3,000 |

After the CBA has been carried out, the Chief Information Security Officer (CISO) of the organisation can now discuss potential Risk Treatment strategies with the Senior Management Team (SMT), see Table 47.

*Table 47: Risk Treatment Strategies [3]*

| Strategy | Description | Example |
|---|---|---|
| Defence | Upgrading firmware, applying patches, system configuration hardening. | Disabling publicly accessible TCP/UDP ports of server |
| Transference | Transferring the risk onto another organisation. | Cybersecurity Insurance |
| Mitigation | Control measures put in place to reduce impact of risk. | DDoS protection services from CSP |
| Acceptance | Organisation decides to accept risk, no measures are taken. Could be due to cost of control measure. | Specialised hardware required for business, but too costly to replace. (Common in Health Services due to financial constraints). |
| Termination | Ceasing service, changing supplier, or changing hardware to avoid risk. | NG disabling FTP server in favour of SFTP server. |

The CISO has decided on a defence strategy of the webserver outlined in Table 48.

*Table 48: RM Strategy for Webserver*

| Strategy | Action | Result |
|---|---|---|
| Mitigation | Implement the DDoS protection from AWS (AWS Shield) immediately. | Control measure in place and will mitigate the risk. Vulnerability still in place even after control measure, therefore a residual risk is present. |
| Defence | Migrate the website over to the new Windows 2022 Webserver as soon as possible. | This will resolve the DDoS vulnerability.<br><br>Continual VAs and Risk Assessments should be carried out to ensure there are no new vulnerabilities. |

## A2.5 Security Management Models and Practices

Maintaining the CIA triad is crucial to the success of any organisation. Designing an InfoSec programme from scratch is daunting and time-consuming process. Utilising security management models and frameworks, the process and procedures are already in place, and the organisation can begin implementing them right away. This ensures that data is secured in a standardised manner which can demonstrate that the organisation has obtained a high standard of security of their systems and allows integration with other organisations.

As discussed there are many security management models and frameworks, Table 49 outlines some additional frameworks researched for this assignment [3] [4] [134] [135] [136] [137] [138] [139] [140] [141] [142].

*Table 49: Additional Security Frameworks researched*

| Developer of Framework/Model | Framwork/Model | Description |
|---|---|---|
| Cloud Security Alliance (CSA) | Cloud Controls Matrix (CCM) v4 | * Security framework designed to promote best practices for cloud infrastructure.<br>* Defines responsibilities of Cloud Service Providers (CSP) and Customers.<br>* Mapped against other security frameworks and standards (ISO/IEC 27000, NIST SP800-53A, PCI DSS) |
| National Institute of Standards and Technology (NIST) | Special Publications (SP) | * There are currently nearly 300 NIST SPs.<br>*NIST SPs are separated into three categories:<br>**SP 500**: Information Technology<br>**SP 800**: Computer Security<br>**SP 1800**: Cybersecurity practical guides<br>* Some relevant NIST SPs identified for NG:<br>SP 800-39: Managing InfoSec Risk<br>SP 800-53A: Assessing Security and Privacy Controls<br>SP 800-55: Performance Measurement Guide for InfoSec |
| | Cybersecurity Framework (CSF) 2.0 | *CSF is designed to assist organisations in assessing their current cybersecurity posture, the target cybersecurity posture, and identifying risks that need to be addressed.<br><br>* CSF is a very useful tool to prepare for IR events.<br><br>* The Core of the CSF framework has five functions:<br>1. Identify: Asset Management (Physical and Non-Physical)<br>2. Protect: Implimenting control measures (from ISO 27002)<br>3. Detect: Intrusion Detection/Prevention System (IDPS), Security Information Event Management (**SIEM**), Security Orchestration, Aautomation and Response (**SOAR**)<br>4. Respond: Utilising an Incident Response (IR) Plan to manage an incident.<br>5. Recover: Re-enable services post an IR, potentially using a Sandbox to and Malware analysis to ensure that system re-infection does not occur. |
| | Risk Management Framework (RMF) | *The RMF is used to identify risks, assit with selecting and implementing control measures. Finally the RMS then continually monitors the control measures for any signs of compromise.<br>* RMF integrates with other NIST publications (SP and FIPS)<br>* RMF is formally documented in SP 800-37 |
| | Federal Information Processing Standards (FIPS) | FIPS have been designed by the federal government of the United States (US). They are used where there are currently no industry standards in place for a US government requirement. Currently 13 FIPS standards have been published. |

Implementation of security frameworks improves the security posture or an organisation, proactively identifying vulnerabilities and applying security measures and fixes to mitigate or remove the risk of an adverse event. In addition, providing evidence that a certain standard has been achieved, such as ISO certification, improves confidence of suppliers and partners in an organisation's security programme.

Key security practice can focus on the organisation's personnel. This will ensure the information assets remain secure, by ensuring the:

- Right people are in the right roles
- They have the correct permissions
- Adequate cybersecurity training is provided

Further details of personnel management principles can be found in Table 50:

*Table 50: Personnel management principles*

| Personnel Management Principle | |
|---|---|
| **Principle** | **Description** |
| **Hiring** | Onboarding: Standardised process for when a new member of staff joins the organisation.<br>Actions: **Background checks**, configuring the **correct AC permissions** for their role, deployment of equipment, PC, Laptop, mobile.<br>Signing of an **NDA - This is crucial for NG as they need to protect their Intellectual Property.** |
| **Firing** | Offboarding: Standardised procedure for staff terminations or resignations.<br>Actions: AC Privelege revocation, deactivation of AD user account, return of equipment. Remind the former employee of their responsibility to abide by the **NDA** which is STILL legally enforceable, even through they have left the organisation.<br><br>This procedure needs to take into account the circumstances of dismissal.<br>**Friendly departure**: Normal procedure to be followed<br>**Hostile departure**: Immediate dismissal (Either by breach of policy or due to criminal action):<br>Immediate deactivation of AD user account, collection of organisation's equipment.<br>This ensures that a potentially disgruntled former employee cannot cause damage to data. |
| **Least Privilege** | Only the required privileges in order for member of staff to **carry out their daily role**. **PAM** to be used when privileges need to escalated temporarily. |
| **Separation of Duties** | Recommended for extremely sensitive roles. E.g. A single member of staff should **NOT** be able to create a new vendor account **AND** send payments to vendor accounts. |
| **Two person control** | Requires two members of staff to carry out a single sensitive tasks. This ensures that two people are present and must be in agreement to carry out the task. E.g. The military use this method when firing missiles. |
| **Job rotation** | Employees with sensitive roles have more opportunity to carry out fraudulent activity. Moving staff to different roles in the organisation can uncover potential fraudulent activity. Where continual concealment is required to hide wrongdoing. |
| **Mandatory holidays** | Similar to job rotation, this ensures that staff are away from the organisation for a week or more so that any potential wrong doing can be detected. |
| **Nondisclosure Agreement (NDA)** | NDAs are signed by new employees to protect any confidential information/data at the organisation. NDAs apply even after the employee leaves an organisation, which should be discussed during an exit interview. |
| **Social Media** | It is advised for NG to write an ISSP Social Media policy. This outlines the behaviour expected of staff when using social media. Periodic social media analysis may be part of the policy to assess the impact to the organisation. |
| **Security Education and Training Awareness (SETA)** | SETA should take into account the audience, therefore role-based training is advisable. This ensures that users receive the most appropriate training. Awareness of Cyberthreats such as Social Engineering techniques, Phishing, and ransomware training. Techniques that staff are most likely to encounter.<br><br>Programms such as phishing simulation campaigns to identify staff that need further training.<br><br>More technical Cybersecurity training for IT departmental staff. So they are aware of hacking methods, Red, Blue and Purple teaming events. |

Most security frameworks have an element continual monitoring, reporting and improvement, this considers any new systems, services or structure changes implemented by the organisation. This also ensures that any new vulnerabilities are identified and resolved.

One method of providing a starting point or measuring performance is benchmarking which is comparison metric of an organisation's effectiveness against an established measure, see Table 51:

*Table 51: Benchmarking and Gap Analysis*

| Benchmark Type | Description |
|---|---|
| External Benchmarking | A process of anaylsing the practices of another organisation, to replicate the same results, in this instance relating to InfoSec processes. |
| Internal Benchmarking (Baselinking) | This process compares a metric for differences between past and current performances. |
| Gap Analysis | If benchmarking results in a shortfall, gap analysis can be used to identify issues and create a plan to ascertain the required level of performance. |

NIST SP 800-55 provides guidance on performance measurement implementation, see Table 52 and Fig.29:

*Table 52: Performance measurement implementation*

| Phase | Task | Description |
|---|---|---|
| 1 | Prepare for data collection. | Seletion of InfoSec metrics, identification of data to focus on specific issue. |
| 2 | Collect data and analyse results. | Collect data from various sources ( e.g. Service Desk Ticketing system, Firewall logs, InfoSec team).<br><br>Analyse data: comparing current and target metrics conduct gap analysis. |
| 3 | Identify corrective actions. | A set of corrective actions to mitigate security issues identified in phase 2. Provides guidance on closing the gap between the current and target position. |
| 4 | Develop business | Justificatication of cost for applying corrective actions. |
| 5 | Obtain resources. | Budgeting for acquiring and implementing security actions. |
| 6 | Apply corrective actions. | Security actions implementated. Gap closed on target solution. |
| | | Return to Phase 2 to re-gather data to determine if additional measures are required. |




*Figure 28: Performance measurement implementation [4]*

Table 53 shows a list of typical metrics used to determine the performance of security program and measures, and the outcomes. This is useful to establish where additional resource is required to improve the security posture at an organisation.

*Table 53: Typical Security Metrics*

| Metric | Description | Outcome |
|---|---|---|
| Number of blocked inbound network | This is the number of attempted internal network connections to an organisation and the country of | This can yield useful information on the origin of the attackers and attempted connection types. |
| Security Costs | The security costs over a specified period of time. | This can be used for Cost Benefit Analysis (CBA). |
| Policy violations | This indicates the device usage by staff, and if any inappropriate behaviour was detected. | This can then indicate whether additional training or disciplinary measures are required. |
| Number of spam emails received | This is a useful metric to determine the performance of spam protection. | This is one of the key initiators for data breaches or malware. |
| Results of phishing exercises | As part of the Security awareness training, an IT department can send staff test phishing emails. | Determine how staff react and whether additional security training is required. |
| Number of Incidents | This is a good overall metric of InfoSec performance. It would be useful to collect data via the Service Desk ticketing system to allow managers to "drill down" to find specific details of the incident. | Determines the quantity of incidents. The nature of the incidents, their cause, impact and resolution. This may point to a trend where additional security measures, policies, or training are required. |

Some organisations may be required by law to adopt a stipulated minimum level of security. This is termed as “Due Care” and ensuring they are implemented is termed as “Due Diligence”, see Table 54.

*Table 54: Due Care/Diligence*

| | Description | Legal standpoint |
|---|---|---|
| **Due Care** | Adopting a minimum standard of security to protect the interests of the organisation. | Establishes a potential future legal defense that the organisation has put standards in place that any other prudent organisation would do in similar circumstances. |
| **Due Diligence** | Requires an organisation to ensure that these standards are implemented. | Adds further credence to a legal case that the organisation has done everything possible to ensure safety. |

## A2.6 Contingency Planning (CP)

CP is the overall planning for unexpected adverse events and consists of four major components, see Table 55 below:

*Table 55: Major components of CP.*

| Acronymn | Component | Description |
|---|---|---|
| BIA | Business Impact Analysis | Identification and Analysis of:<br>* Vulnerabilities, and Threats facing the organisation<br>* Organisation's Processes and the resources required for it to function<br>* Determine the priority of each process, how critical it is to the organisation<br>* Creates a prioritised list of system recovery, so the most critical systems are restored first. |
| IR | Incident Response Plan | The purpose of an IR plan is the immediate response to an adverse event. |
| DR | Disaster Recovery Plan | The purpose of a DR plan is reestablishing the oganisation's functions at the **Primary Site** |
| BC | Business Continuity Plan | The purpose of a BC plan is reestablishing the oganisation's functions at an **Alternate Site** |
| CM | Crisis Management Plan (Sometimes part of the DR Plan) | The focus of CM Plan is to establish a control centre following a disaster. Going on to provide guidance on setting clear lines of communication with emergency services, to account for personnel, inform the wider public and safeguard the organisation's image. |

Fig.30 Below illustrates the CP lifecycle [4]

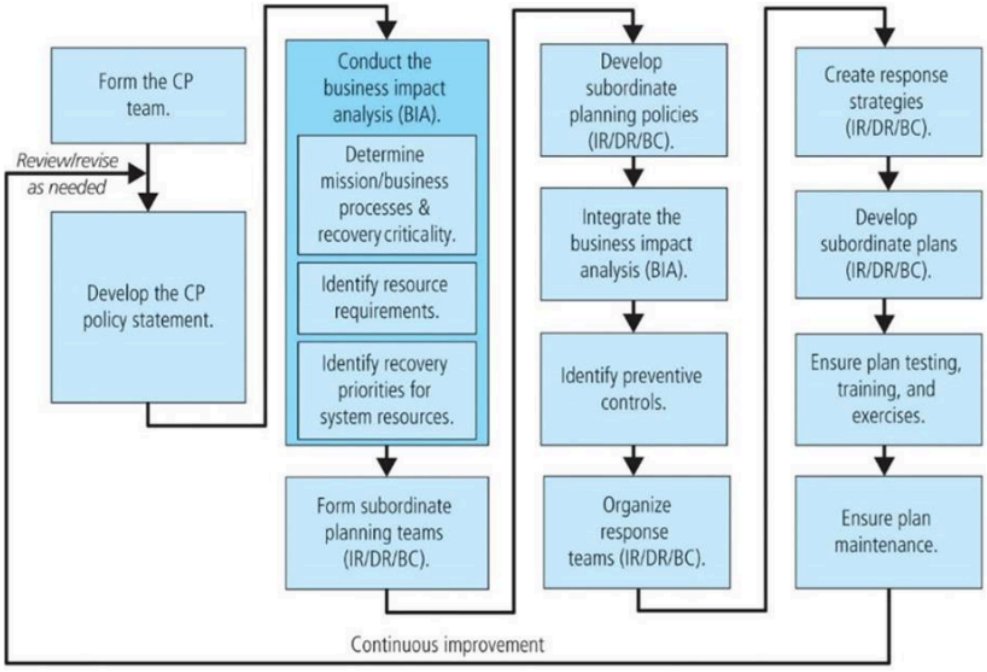



*Figure 29: CP Lifecycle*

Table 56 provides a list of all the teams involved in CP and their roles [4] [143] [144] [145] [146].

*Table 56: CP Teams and roles*

| Acronymn | Team | Role |
|---|---|---|
| CPMT | Contingency Planning Management Team | Develops CP Policy Statement |
| | | Develops Policy Environment |
| | | Conducts Businsess Impact Analysis |
| | | Forms the Planning Teams (IRPT,DRPT,BCPT, CMPT) |
| | | Leads on ALL CP efforts |
| | | Collects information about organisation and threats faced |
| **Incident Response Team** | | |
| IRPT | Incident Response Planning Team | Develops the IR Policy |
| | | Manages the IR Plan |
| | | Planning and Preparing for IR Event |
| | | Forms the CSIRT |
| CSIRT | Computer Security Incident Response Team | Executes the IR Plan |
| | | Detecting, Evaluating, Reacting to and Recovering from Incidents |
| | | Conduct an After-Action Review (AAR) |
| **Disaster Recovery Team** | | |
| DRPT | Disaster Recovery Planning Team | Develops the DR Policy |
| | | Manages the DR Plan |
| | | Planning and Preparing for DR |
| | | Forms the DRRT |
| DRRT | Disaster Recovery Resonse Team | Executes the DR Plan |
| | | Detecting, Evaluating, Reacting to Disasters. |
| | | Reestablishes operations at the primary site. |
| **Business Continuity Team** | | |
| BCPT | Business Continuity Planning Team | Develop the BC policy |
| | | Manages the BC Plan |
| | | Planning and preparing for Business Continuity |
| BCRT | Business Continuity Response Team | Executes the BC Plan |
| | | Establishes alternate site operations Hot,Warm,Cold Sites so that business can still finction during a Disaster. |
| **Crisis Management Team** | | |
| CMPT | Crisis Management Planning Team | Establishes a command centre near the site of the disaster |
| | | Verify Personnel Status |
| | | Activate Alert Roster |
| | | Coordinate with Emergency Services |
| CMRT | Crisis Management Response Team | Support personnel and loved ones during crisis |
| | | Keeping public informed |
| | | Communicating with customers, suppliers, partners, media |

Fig.31 shows the CP Hierarchy, where IR Planning is separated from DR, BC and CM planning which together are termed as Business Resumption Planning (BRP).

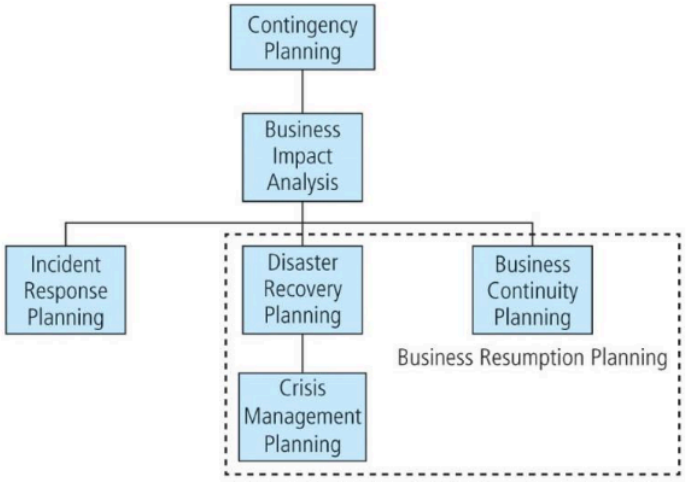



*Figure 30: Contingency Planning Hierarchy*

Table 57 shows the process used during the CP process.

*Table 57: The NIST Seven-Step Process of CP*

| # | Step | Detail |
|---|---|---|
| 1 | Develop the CP policy statement | Provides the authority and guidance to develop an effectual contingency plan. |
| 2 | Conduct BIA | Analysis of:<br>Vulnerabilities, and Threats facing the organisation<br>Mission/Business processes, resource requirements, and recovery criticality |
| 3 | Identify preventative controls | Security measures implemented to mitigate, or stop potential adverse events from taking place. |
| 4 | Create the contingency strategies | The creation of rigorous recovery strategies, providing long-term direction, purpose and allocation of resources to ensure that systems can be restored in an effectual and timely manner following a disruption. |
| 5 | Develop contingency plan | Provides guidance and procedures for recovering an organisation's services, functions and facilities following a disruption. |
| 6 | Ensure plan testing, training and exercise | Testing: Substantiates that an organisation's restoration capabilities are effective.<br><br>Training: Allows the recovery teams to become familiar with contingency guidance and procedures.<br><br>Exercise: This can identify any gaps in the contingency plans. |
| 7 | Ensure plan maintenance | The plan should be revised regularly to take into account any new systems, or system changes any organisational changes. Or any new threats that have been identified.<br><br>The plan should be considered a living document, and should also be revised after Testing, Training and Exercises reflect any weaknesses or gaps identified in the plan. |

Business Impact Analysis (BIA)

The National Institute for Standards and Technology (NIST) have released a Special Publication (SP) providing guidance on how to conduct the BIA in SP 800-34 which states three stages:

- Determine the mission/business processes and their recovery criticality
- Identify resources required
- Identify recovery priority of system processes

Fig.32 and Table 58 outlines the metrics used to determine the time taken to recover systems following an adverse event.

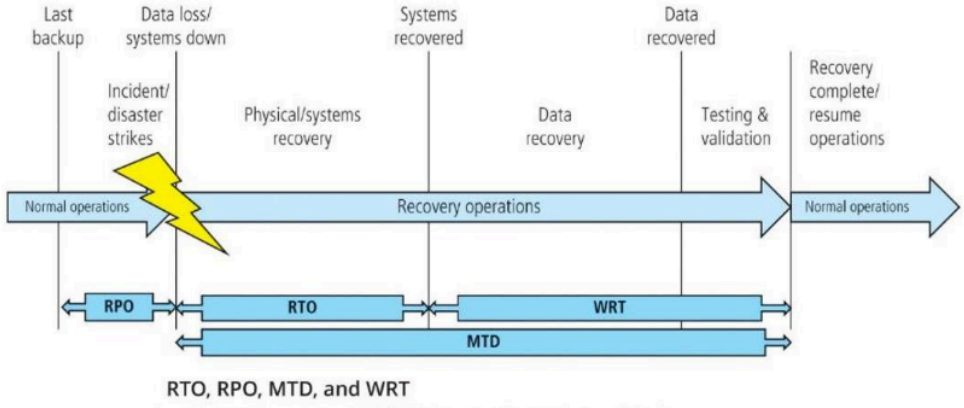



*Figure 31: Recovery Metrics [4]*

*Table 58: Recovery Metrics*

| Acronym | Recovery Metrics | Description |
|---|---|---|
| RPO | Recovery Point Objective | The Point in time where last backup was taken. All work from this point onwards will be lost. It would appear that the organisation will be going back to this point in time. |
| RTO | Recovery Time Objective | Time taken to physically restore systems. |
| WRT | Work Recovery Time | Time taken to resore data, includes testing and validation times. |
| MTD | Maximum Tolerable Downtime | Total time to recover systems (RTO + WRT) |

Once the MTD is established, an appropriate backup regime can be put in place. Backup systems with reduced recovery times are more expensive, so a Cost Balance Point can be established.

Once an adverse event occurs, it needs to be categorised to determine whether it is an actual incident, this is illustrated in Fig.33.



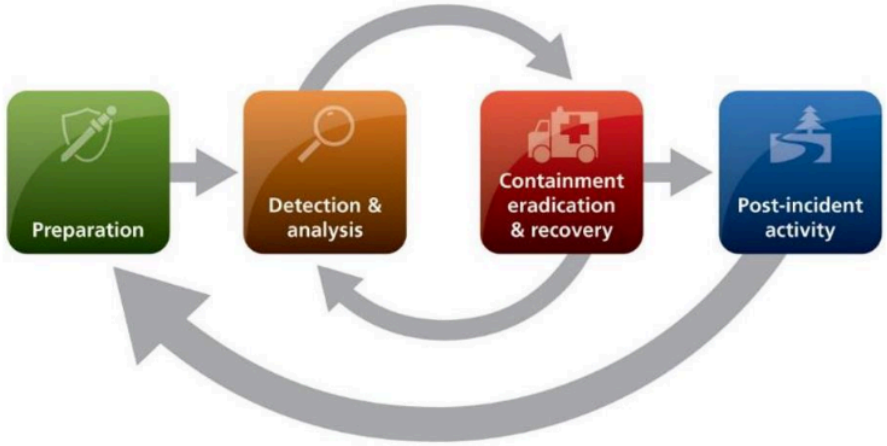

*Figure 32: Incident Classification Process*

Incident identifiers can be found in Table 59 [4]:

*Table 59: Incident Identifiers*

| Possible Indicators | Probable Indicators | Definite Indicators | Potential Incident Results |
|---|---|---|---|
| Presence of unfamiliar files | Activity at unexpected times | Use of dormant accounts | Loss of availability |
| Presence or execution of unknown programs or processes | Presence of new accounts | Changes to logs | Loss of Integrity |
| Unusual consumption of computing resources | Reported attacks | Presence of hacker tools | Loss of Confidentiality |
| Unusual system crashes | Notifications from IDS | Notifications by partner or peer | Violation of Policy |
| | | Notification by hacker | Violation of Law |

Once an incident has been identified, the CSIRT can now begin the IR process as outlined in Fig.34. Initial reactions are described in Table 60:




NIST incident response life cycle

Source: NIST Special Publication 800-61, Rev. 2: The Computer Security Incident Handling Guide.

*Figure 33: IR Lifecycle [4]*

*Table 60: Actions reactions following an incident*

| Action | Action Detail | Description |
|---|---|---|
| Notify | Notification of Key Personnel | Notification of Key personnel utilising an **Alert Roster** (A document containing contact details of key personnel) **Alert Messaging** (Automated/Scripted messaging to alert key personnel of incident. |
| Document | Document Incident | The incident should be documented to provide a chronological timeline of events so that this can be reviewed at a later stage during an After Action Review (**AAR**). This can be used to improve future Incident Responses. |
| Contain | Incident Containment Strategies | Mitigating the impact of an incident, and regaining control of systems. |
| Escalate | Incident Escalation | If the CSIRT is unable to handle the incident, then it may need to be escalated to a disaster or to a third party. |

Table 61 outlines detection methods:

*Table 61: Detection Methods*

| Detection Methods | Description |
|---|---|
| End user report | End user reporting is key to IR, ensuring a mechanism is in place to allow efficient reporting is crucial. End users can detect, or sometimes trigger, an incident e.g. by clicking on a link in an email. Quick reporting and reaction times are critical to mitigating damage caused. |
| Intrusion Detection System (IDS) | This can be either host or network based systems. It provides notification of any suspicious activity. |
| Security Information and Event Management (SIEM) | A SIEM system can receive inputs from many sources and can provide advanced services such as **log aggregation and analysis, event correlation** to detect potential incidents. |
| Anti-Virus (AV) Software Alerts | Alerts are sent from AV software to alert of potential infection. |
| Endpoint Detection Response (EDR) | Real-time continuous monitoring of endoints, provides alerts of suspicious activity. |
| Network Monitoring Tools | These tools can monitor traffic usage and the status of network devices. Can be configured to send alerts if certain thresholds are breached. |
| System Administrators | System Administrators are likely to detect incidents as part of their role, by monitoring systems, receiving reports from peers and partners. |

Table 62 outlines containment strategies:

*Table 62: Containment Strategies*

| Containment Strategy | Description |
|---|---|
| Disabling compromised accounts. | Ensures that an attacker cannot access data or systems as that particular user. |
| Reconfiguring a firewall to block problem traffic. | If a particular service is being accessed by a hacker, (e.g. Simple Network Management Protocol (SNMP), this traffic can be blocked. |
| Temporarily disabling the compromised process / service. | Disabling the service will deny the service to staff, and traffic from a potential hacker will still be able to access services. |
| Disconnecting the affected network or network segment. | This could contain an incident (e.g. a virus) from affecting other devices on a network. |
| Powering down, computers, servers or network devices. | This is the most extreme containment strategy. It may be the only option available if a serious incident were in progress. (e.g. Cryptomalware infecting files.) |

Table 63 outlines the recovery process:

*Table 63: Recovery Process*

| Recovery Process | Description |
|---|---|
| Identify the vulnerabilities and resolve them. | Reduces risk of re-infection. |
| Address the safeguards that failed. Install, replace, or upgrade them. | Addresses security issues that caused incident. |
| Evaluate monitoring capabilities. Improve detection and reporting methods . | Ensures monitoring capabilities are in place ready to determine if another incident were to occur. |
| Restore the data from backups, as needed. | Data is restored as outlined during the BIA process, restoring critical data and resources first. |
| Restore the services and processes in use. | Methodically restoring services. |
| Continuously monitor the system. | Monitoring for further incidents. |
| Restore the confidence of the members of the organisation's communities of interest. | Management to issue a short memorandum outlining the incident and assuring all that the incident was handled and the damage was controlled. |

If the CSIRT are unable to contain an incident it may need to be escalated, Table 64 provides definitions of adverse events.

*Table 64: Adverse Event Descriptions/Examples*

| Adverse Events | Description | Example |
|---|---|---|
| Incident | Any adverse event, no matter how minor can be termed an incident. The organisation is still able to function. | Accidental deletion of a file.<br>Failure of a server |
| Disaster | If the CSIRT are unable to handle the incident, or the incident is going to impact the organisation over a long period of time, then it is escalated to a disaster. | **Natural:** A storm or flood impacting the functionality of an organisation.<br>**Man-made:** Cyber attack (E.g. Ransomware).<br>**Slow Onset:** Drought, or environmental issues.<br>**Rapid Onset:** Earthquake, tornado. |
| Business Continuity | The process of mitigating the impact of a disaster by enabling business functionality from another location. | Organisation temporarily re-locates to a secondary site. |
| Crisis | A large incident that impacts on human life. | A large fire involving emergency services. |

The escalation process is outlined in Fig.35:

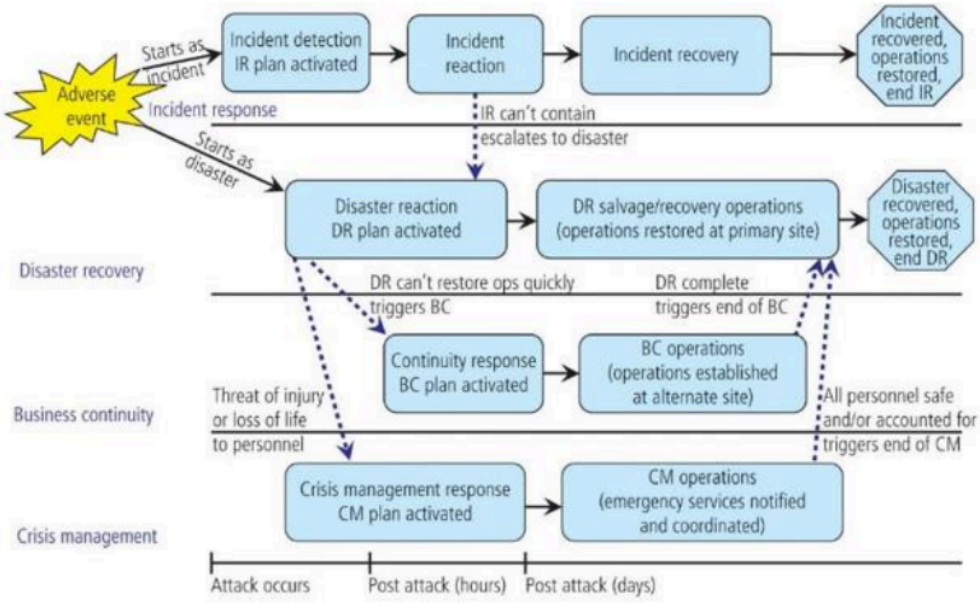



*Figure 34: CP Implementation Timeline [4]*

Table 65 outlines BC strategies:

*Table 65: BC Strategies*

| BC Strategy | Basis | Description | Advantage | Disadvantage |
|---|---|---|---|---|
| Hot Site | Exclusive Use | *An alternate site which is an identical replica to the primary site.<br>*All systems, network connectivity and live data are in place. | Allows for organisation to continue functioning immediately in the event of a disaster. | Most costly option. May be seen a waste of resources if not utilised. Could resources be better used elsewhere? |
| Warm Site | Exclusive Use | An alternate site with either all or some systems and connectivity in place.<br>Live data is not kept up to date. | Can provide with a location to resume functioning, within a matter of minutes/hours/days. | * Some work required to provide access to latest data.<br>*Systems in place, but functionality needs testing - potential issues. |
| Cold Site | Exclusive Use | An alternate site with power and connectivity, but no systems or data. | Can provide with a location to resume functioning, within a matter of days/weeks. | * Need to source systems, with potential lead time issues.<br>* Significantly longer MDT. |
| Timeshare | Shared Use | A Location that is shared with other organisations. | Reduces cost of an alternate site. | Issue if multiple organisations neat to use the alternative site at the same time. E.g a large fire that impacts all organisations at the same time. |
| Service Bureaus | Shared Use | An alternate location provided by a service agency for a fee. This is similar to renting a location for the use of DR/BC purposes. | * More cost effective than purchasing an alternate location outright.<br>* No maintenance costs when not in use. | * Contracts need to be renewed periodically, subject to rate rises.<br>* Can be expensive. Renting can be seen as dead money. |
| Mutual Agreement | Shared Use | Two organisations agree to support one another in the event of a disaster. It allows the stricken organisation to use the facilities of the other in the event of a disaster. | This is the most cost effective option of all discussed. | * Potentially time limited - organisation can wear out its welcome.<br>* Severe issue if both organisation impacted by a disaster. |

Once the CP plans have been developed, it is critical that they are tested regularly, Tables 66 outlines testing methods:

*Table 66: CP Testing methods*

| Testing Method | Description | Advantage | Disadvantage |
|---|---|---|---|
| Desk Check | * A meeting arranged for all members of the respective team can review the IR, DR, BC, or CM plan. | *Simplest form of test<br>* It gives an opportunity for the team to become familiar with the plan and raise any concerns, and for updates to be made. | * Not a true test, more of a review. |
| Structured Walkthrough | * A meeting arranged for all members of the respective team can go through the appropriate plan step-by-step.<br>* Each member of the team can discuss their actions and responsibilities at each step of the plan during the exercise. | * Simple method of checking the plan.<br>* Team become familiar with plan.<br>* Confirms the roles and actions each team member is to carry out. | |
| Simulation | * A simulation is a role play exercise.<br>* The team is provided with a scenario, and carry out the actions required by the relevant plan.<br>* All communications must have "TEST" or "SIMULATION" in the subject heading to ensure that all staff know that this is an exercise.<br>* The simulation does not require staff to perform actions such as restoring data from backup.<br>* The simulation ends with an AAR session to discuss the exercise, any areas that could be improved. | * More realistic for staff as an actual scenario is provided.<br>*Applying the relevant plan to a scenario | *Potential for a member of staff to mistake the simulation as a real event. |
| Full Interruption | * All members of the team carry out all actions of the relevant plan. These include service interruptions, data restoration from backup. | * Most rigorous testing method.<br>* Tests data restoration - provides confidence in backup & restoration system | * Most disruptive test<br>*Should be conducted out of hours, unsociable hours.<br>* Potentially too risky for some organisation to carry out. |

Contingency Planning is key to the survival of an organisation. By proactively devising IRP, DRP and BCP these can be enacted quickly if required. With pre-defined roles and responsibilities, staff are aware of what is expected of them beforehand and can act immediately. Hartford Insurance Company 40% of businesses fail for not having a DRP in place this highlights the importance of CP to an organisation [4].

## A2.7 Protection Mechanisms

Protecting an organisation's data and information assets is critical to maintaining the CIA triad. Proving a user's identity and granting them the appropriate level of access is crucial; this is carried out by Access Control (AC) which incorporates the four elements in Table 67 [3]:

*Table 67: AC Elements*

| Access Control Elements | Description | Examples |
|---|---|---|
| Identification | A subject makes a claim about their identity. Subjecs are usually people, but can also be applications, devices, services, or organisations. | Usernames, Tokens, Certificates, Secure Shell (SSH) Keys. |
| Authentication | Authentication allows the user to prove that the identity is theirs. | Password, Personal Identification Number (PIN), Biometrics, Keycards, (Fingerprint, Retina/facial/voice recognition), Multi Factor Authentication (MFA) or Two Factor Authentication (2FA). Kerberos, IEEE 802.1X. |
| Authorisation | Once the subject's identity has been authenticated, they can then be granted authorisation | AC Schemes Attribute based, Role Based AC. Access Control Lists (ACL). File |
| Accountability | Maintains a record of successful and unsuccessful log on attempts. | Authentication Logs |
| Identification, Authentication, Authorisation, Accountability (IAAA) | | |

Fig.36 illustrates the IAAA process [3]:

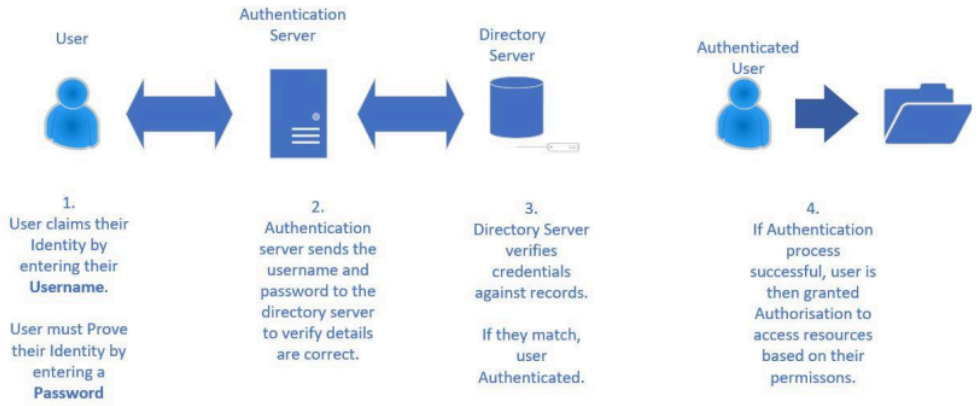



*Figure 35: IAAA Process*

Table 68 outlines authentication technologies used [147] [148] [149] [150] [151].

*Table 68: Authentication Technologies*

| Technology | Acronymn | Description | Advantage | Disadvantage |
|---|---|---|---|---|
| Remote Authentication Dial-in User Service | RADIUS | * Authentication server with a client-server architecture.<br>* Accepts authentication attempts from client and checks credentials against a cetralised directory service. | * Cetralised authentication system - allows for authentication to be granted or rescinded quickly.<br>* Commonly used throughout industry.<br>* Vendor agnostic. | * Requires additional encryption between the RADIUS and Directly servers. |
| Lightweight Directory Application Protocol | LDAP | * Protocol to allow authentications.<br>*Allows systems to start and close sessions.<br>* Allows entries to be Added or Deleted. | * Open source, vendor agnostic protocol. | * Needs to be configured correctly to maintain security. |
| Active Directory | AD | * Service supported by Microsoft Windows Server.<br>* Provides Database services to store data on both Users and Computers.<br>* Utilises Kerberos for Authentication. | * Centralised database of users and computers.<br>* Can centrally manage permissions/ access control across the network.<br>* Integrates with other Windows Server functions, such as group policy (GP). | * Proprietary to Microsoft |
| Kerberos | - | * Authentication protocol<br>* Grants tickets to allow users/devices<br>* Utilises Symmetric Key Encryption<br>* Consists of three services:<br>* Authentication Server (AS)<br>* Key Distribution Centre (KDC)<br>* Kerberos Ticket Granting Service (TGS) | * Kerberos 5 utilises strong encryption Advanced Encryption Standard (AES). | * Kerberos utilises Timestamps, therefore Time synchronisation is crucial.<br>* Weaker Data Encryption Standard (DES) utilised by legacy versions.<br>* Vulnerable to **Kerberoasting** Attacks.<br>***Gold/silver Ticket Attack** |
| Institute of Electrical and Electronic Engineers Standard 802.1X | IEEE 802.1X | * Industry standard used for authentication.<br>* Allows authentication based on:<br>*Credentials enterd during authentication.<br>* Media Access Control (MAC) address of device.<br>Known as **MAC Auth**.<br>* Can use Extensible Authentication Protocol (EAP) | * Dynamic Virtual Local Area Network (VLAN) assignment based on authentication.<br>*A Member of staff can be placed on the staff network with access to services.<br>* A visitor or guest can be placed on a separate network, with internet access only or denied access entirely. | * Complexity, may require support to configure and implement.<br>* MAC Auth susceptible to MAC spoofing attacks. |
| Network Access Control | NAC | * Accepts user authentications and forwards it onto authentication server using the IEEE 802.1X standard.<br>* Utilises IEEE 802.1X standard to place user on appropriate VLAN. | * Restricts unauthorised users from accessing a corporate network.<br>* Allows guest traffic to be segmented on a different VLAN, securing corporate network. | * Issue with unmanaged devices<br>* Some devices cannot support IEEE 802.1X. |
| Wireless Access Point | WAP | *Not strictly an authentication technology - Main function is to provides wireless services to users.<br>* Provides NAC services.<br>* Acts as an authenticator, passing authentication requests onto the RADIUS server and placing user on correct VLAN via IEEE 802.1X. | * Provides security at the edge of the network closest to the user - permitting/denying access. | * If user's device is not configured correctly, may require assistance from Service Desk. |
| Network Switch | - | As above for wired services. | As above for wired services. | As above for wired services. |
| Extensible Authentication Protocol | EAP | *A framework used for authentication. (Usually for Wireless networks).<br>* Several variants of EAP protocols | * Some EAP vairants utilise Transport Layer Security (TLS) therefore Secure.<br>* Vendor agnostic | * Can be complex to implement<br>* Some variants of EAP require certificates, require significant resources to manage certificates. |

EAP allows both wired and wireless authentication and integrates with a RADIUS server; the EAP variants can be found in Table 69 [3] [151].

*Table 69: EAP Variants*

| Wireless Authentication Protocol | Acronymn | Certificates Requirement | Description | Advantage | Disadvantage |
|---|---|---|---|---|---|
| Protected Extensible Authentication Protocol | PEAP | Servers authenticated using certificates. | * Keys are replaced regularly using Temporal Key Integrity Protocol (TKIP)<br>* Transport Layer Protocol (TLS) to secure authentication process.<br>*** Recommended to NG for general authentications.** | * Server Authenticated as well as user.<br>* Tunneling maintains confidentiality. | |
| Extensible Authentication Protocol Flexible Authentication via Secure Tunneling | EAP-FAST | Certificates not required. | Developd by Cisco, enables fast re-authentication. Utilises Symetric Pre-shared Key (PSK), or dynamic public keys. | * Quick re-authentication. | *PSK may not be the most secure. |
| Extensible Authentication Protocol Transport Layer Protocol | EAP-TLS | Certificates required. Required for both user device and servers. | * Very secure as both servers and user devices are authenticated using certificates.<br>*** Recommended to NG for authenticating users with access to IP.** | * Mutual authentication based on certificates. | Certificate Management overhead. |
| Extensible Authentication Protocol Tunneled Transport Layer Protocol | EAP-TTLS | Servers authenticated using certificates. | * User devices do not require certificates.<br>* Additional software required. | Removes certificate management overhead of EAP-TLS. | Additional software required on user device. |

Fig.37 illustrates the 802.1X authentication process [3]:

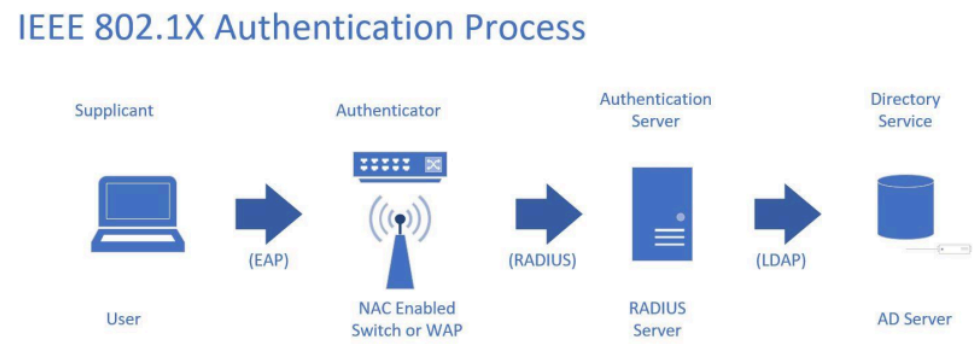



*Figure 36: IEEE 802.1X Authentication Process*

Biometric Authentication is regularly used for authentication with varying degrees of success, see Table 70, and biometric authentication metrics in Table 71:

*Table 70: Examples of biometric authentication*

| Biometric Authentication | Description | Advantage | Disadvantage |
|---|---|---|---|
| Fingerprint | Utilises the unique patterns of ridges and valleys of a users fingertips. | * Most common and widely adopted method of biometric authentication.<br>* Does not rely on user memorising password.<br>* Easy to use. | * Injury to hand or fingers |
| Facial Recognition | Measurements of facial features are used. | * Easy to use.<br>* Becoming more widely used and accepted. | * Some instances of fraudulent authentications by using photographs of user.<br>* Privacy issues as a photograph of users must be stored. |
| Voice Regoniton | Uses the sound, patterns, rhythm or a user's voice. | * Commonly accepted use as an authentication over the phone for some banks.<br>* Ease of use. | * Potential fraudulent authentication using a recording of the user.<br>* Authentication failure due to user having a medical issue such as a cold. |
| Retina Scan | Uses the unique patterns of blood vessels at the back of the eye. | * Unique method of authentication | * User must be close to the retinal scan reader for successful authentication.<br>* Not the most convenient method of biometric authentication. |

*Table 71: Metrics used in biometric authentication*

| Error Type | Metric | Acronymn | Description |
|---|---|---|---|
| I | False Reject Rate | FRR | The genuine user attempted to authenticate, but was rejected using the biometric method. |
| II | False Acceptance Rate | FAR | An authentication is attempted by a fraudulent user and is accepted. |
| | Relative Operating Charecteristric | ROC | This is the comparison of FRR against FAR. A graph is used to illustrate this. |
| | Crossover Error Rate | CER | This is the area on the ROC graph where the FRR and FAR intersect. |

Fig.38 illustrates ROC:

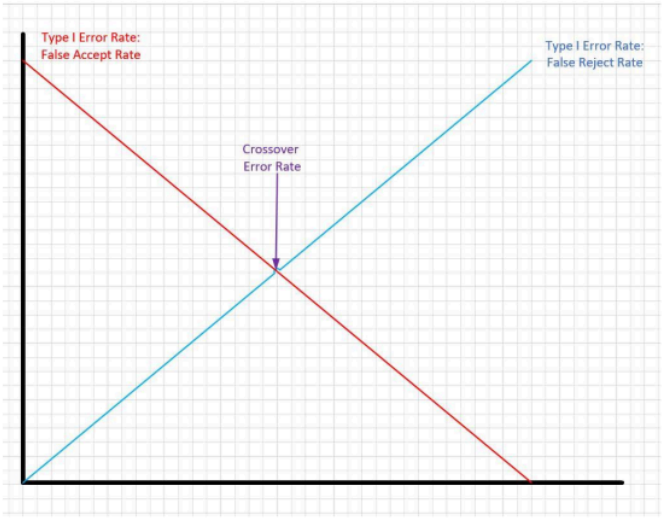



*Figure 37: Graph displaying ROC and CER*

See Table 72 for MFA techniques regularly used to confirm the authentication of a user:

*Table 72: MFA Techniques*

| Authentication Method | Examples | Advantage | Disadvantage |
|---|---|---|---|
| Something you know | Password, PIN | Most widely accepted form of authentication (Auth). Most users are familiar with this form of Auth. | Human factors: Use of simple passwords, re-use of the same password. **Solution:** A Password policy requires users to generate a password of minimum length and complexity. Also they must change their password after a set period. |
| Something you have | Mobile Phone: MFA Applications (App) | Most people have smartphones today therefore MFA Apps are very popular. | Mobile phones can be stolen or become lost. Or potentially run out of battery power. |
| | Hardware token. | Hardware tokens are still available, dedicated Auth device. | Cost implications, the provider must manufacture, and ship the hardware token to the user. The token could become lost or stolen. |
| Something you are / can produce | Biometric Auth techniques. Fingerprint, Iris/Retina scan. Voice recognition. | Some methods more successful than others, but overall easy to use and no need for user to remember anything. | Some methods not widely accepted, e.g. DNA. Medical condition can cause an issue. E.g. if the user has a cold, voice recognition may not work. |

Once authenticated, AC grants permission to services, resources and data based on their user account and permissions. This process is known as **authorisation**, which is outlined in Table 73.

*Table 73: Access Control Schemes*

| Form of Access Control | Acronymn | Description |
|---|---|---|
| Attribute Based Access Control | ABAC | ABAC is used with Active Directory (AD) where attributes can be configured for a user's accout to permit/deny access and set privileges. |
| Discretionary Access Control | DAC | DACs can be used PCs (Windows and Linux) to secure files and directories. |
| Mandatory Access Control | MAC | MAC are configured centrally and are generally used in high security environments. Utilised by Government departments such as the National Security Agency (NSA) and the military. Implemented in the Security Enhanced distribution of Linux (SELinux). |
| Role Based Access Control | RBAC | RBAC uses role defines to configure privileges and access controls. A user with an IT Administrator and Canteen Manager will have different levels of access to carry out their roles. |
| Rule Based Access Control | RuBAC | RuBAC utilises Rules such as Access Control Lists (ACLs) to grant access. An example of RuBAC are the rule sets used with simple firewalls, routers and switches. |
| Privileged Access Management | PAM | PAM is a process where least privilege permissions are configured, only allowing the user enough permissions to carry out their daily role. If required, PAM allows privilege escalation for a set period of time for an administrator to carry out a task, before removing that permission again. |

User file permissions are outlines in Table 74:

*Table 74: Description of file permissions*

| Permissions | Description |
|---|---|
| Read | Permission to read file/directory |
| Write | Permission to write to a file/directory |
| Execute | Permission to run executable files and scripts. |
| Modify | Permission to add or delete files to directory, or modify file and file properties. |

Fig.39 shows a screenshot of file permissions in a Windows OS.

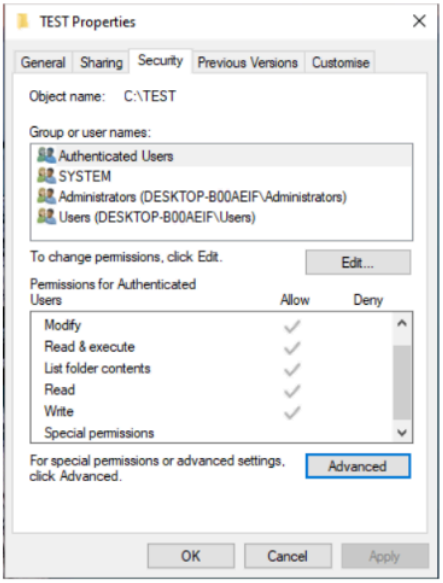



*Figure 38: Example of permission configuration in Windows*

By implementing security frameworks, organisations also implement security practices to safeguard their information assets, and systems. Security controls are a key component of an InfoSec programme, some examples are detailed in Table 75:

*Table 75: Security Control Categories*

| | Preventative | Deterrant | Physical | Detective | Corrective | Recovery | Compensating |
|---|---|---|---|---|---|---|---|
| Management | Guest/visitor registration | Policy (EISP, ISSP, SysSP) | Policy: Security clearance required for secure locations | SIEM correlation reporting | Offboarding process - User AD account deactivation | Disaster Recovery Plan (DRP) | Two person control, separation of duties |
| Operational | Gates, Locks, flood lights | Signage | Fire suppression, Gates, bollards, burglar alarm. | CCTV, Security Guards | Uninterruptible Power Supply (UPS) | Procedures in DRP followed | Defense in depth |
| Technical | Authentication Systems | Encryption, Login Banners | Electronic Locks can audit access to secure areas. | Network Monitoring tools, IDPS, SIEM, Logs | Backup restoration, file recovery | Backup restoration, file recovery | Segregated VLAN, Isolated network |

It is recognised that data can be in one of three states which needs to be considered when implementing protection mechanisms these are described in Table 76:

*Table 76: Three states of data*

| State | Description | Protection Mechanism | Recommendations |
|---|---|---|---|
| Data at rest | Data stored on a server or on backup media. | Full Disk Encryption (FDE) | FDE should be configured on all NG devices. This ensures that data is secure when the device is not in use. Also, if device is stolen, the data will remain secure. Maintaining Confidentiality. |
| Data in motion | Data being transported across a network. | Virtual Private Network (VPN) | VPN (IPSec) to be implemented. This ensures that data is encrypted whilst in transit. This is crucial especially for Wireless networks. VPNs ensure confidentiality is maintained of NG's Intellectual Property. |
| Data in use | Data loaded into active memory and being accessed/edited | Firewall rules | Ensures that only trusted devices can gain access to PCs on the NG network. |
| | | Configuration hardening of end user device. | This will make it more difficult for an attacker to gain access to the user's PC, by closing unused ports, removing applications that are not required. Recusing the attack surface of the end user's PC. |

It has already been established that the securing the network is crucial as that is the ingress point for many attacks, the protection mechanisms used to protect the network are described in Table 77 [152] [153] [154]:

*Table 77: Protection Mechanisms*

| Device/Service | Acronymn | Description | Advantage | Disadvantage |
|---|---|---|---|---|
| Firewall | FW | Standard Firewalls that permit/deny access to data or services based on Internet Protocol (IP) Address, Port, or Application Layer status. | Simple configuration. | Subject to spoofing attacks. |
| Next Generation Firewall | NGFW | Provides functionality of traditional firewall combined with many of the features below. | All in one Cybersecurity solution. | Configuration can be more challenging. |
| Intrusion Detection Service | IDP | System that monitors network traffic and sends and alert to CSIRT. | If attack is detected a message is sent to CSIRT to take action. | * Delay in action, could be a number of hours if during evening or during holiday season. |
| Intrusion Prevention Service | IPS | System that monitors network traffic and blocks traffic automatically. | Action takes place as soon as incident detected. | * If false alarm this could cause an outage.<br>* Would reduce confidence in the IPS. |
| Intrusion Detection/Prevention Service | IDPS | * Most IDS and IPS are the same device or service, therefore termed IDPS.<br>* Configuration or deployment is the only difference.<br>* Network or Host based (NIDPS or HIDPS)<br>* Signature based IDPS - Based on attack patterns<br>* Anomaly-Based IDPS - Baseline used to establish normal traffic, abnormal activity triggers IDPS. | * Some IDPS systems implement agents and report back to a central location. Protecting both the network and devices. | * Poorly configured IDPS can generate unnecessary alerts.<br>* Administrators may miss a genuine alert. |
| Deep Packet Inspsection | DPI | Inspects the contents of each packet as it passes through the FW. | * Detect and blocks malicous traffic.<br>* Detect traffic from malicious websites. | Potential privacy issues. |
| Unified Threat Management | UTM | * A UTM combines the capabilities of a Stateful Packet Inspection (SPI) firewall with the below:<br>* IDPS, DPI, Spam filter, Content Filter | Provides significant advantages over standard firewalls. | Has now been superseded by NGFW. |
| Anti-Virus | AV | * AV should be installed on end devices and servers.<br>* AV capabilities also build into NGFW so that malicious traffic can be blocked. | * Monitors and detects virus infections.<br>* Can send alerts of virus infections. | * AV must be maintained regularly by Service Desk.<br>* Ensure that only one AV installed on device. |
| Data Loss Prevetntion | DLP | * Data is categorised according to sensitivity.<br>* DLP then uses categorisation, together with group policy to identify sensitive data. | * Sensitive data can be detected<br>* If leaving a protected zone can be:<br>* Encrypted, Modified or deleted | |
| Website Filtering (Unified Resource Locator Filtering) | URLF | * Can be used to create policies to determine which URLs can be accessed from the organisation. | Blocks access to known malicious sites. | |
| Access Control | AC | Allows access to resources based on User account or device. | Allows access to resources required by staff, using Least Privilege methodology. | |
| Application Control | AC | Used to determine an application being used on the network, policies can then be applied to the traffic to permit/deny access. | Can block access to applications deemed high risk, such as data sharing applications. | |
| Threat Intelligence feeds | | Automated notifications from a variety of sources (E.g. manufactureres, governments, open source) advising of newly identified threats. | Can provide Indicators of Compromise (IoC) | |
| Sandboxing | | Isolation environment that allows potential malware to be analysed. | Analysis of code suspected of being malware. | |
| Threat Prevention | | Can conduct checks on data entering the network to determine if it is malicious before the user is even aware of the data. | Utilises a virtual sandbox to inspect email attachments to ensure they are safe. | |
| Secure Socket Layer Inspection | SSLI | Enables the NGFW to inspect encrypted data such as HTTPS traffic. | * Detect and blocks malicous traffic.<br>* Detect encrypted sensitive data leaving protected | Potential performance issues of FW or network. |
| Full Disk Encryption | FDE | Encrypts data of device when data is at rest. | Ensures data is secure if mobile device has been stolen | Additional configuration requirement |
| Security Information and Event Management | SIEM | * Collects data from several sources (Network from switching and router logs, FW, IDPS, PCs, EDR, Servers, Threat Intelligence, 3rd parties)<br>* Correlates data and alerts CSIRT. | * Collects and Analyses Security logs and data<br>* Allows for detailed Log analysis<br>* Event Correlation<br>* Centralised Cybersecurity tool<br>* Automated alerting | * Focused on data collection and analysis, does not automatically implement security measures. |
| Security Orchestration, Automation and Response | SOAR | Extends the cabalilities of SIEM by automatically implementing IR processes, E.g. blocking malicious traffic. | * Quickly and automatically reacts to IR events.<br>* Automatically acts on Threat Intelligence. | * Complexity to configure<br>* Over-reliance on automation |
| Cloud Access Security Broker | CASB | Act as an intermediaries between user and CSP.<br>* Ensures Data Security, Threat Protection, Compliance and Visibility.<br>* Can implement resource policies to limit damage. | * Ensures that CIA triad is maintained between organisation of cloud services.<br>* Can ensure budgets are maintained. | * Complexity of implementation, especially if a number of Cloud services are iimplemented.<br>* CASB solutions are costly. |
| Mobile Device Management | MDM | * Provides a platform to manage mobile devices (Android and Apple)<br>* Allows deployment of new software, Operating System (OS) updates, new configuration uploads, and remote wipe capabilities. | * Can provide remote management for all Mobile devices across the organisation in one location.<br>* Processes can be automated to run out of hours. | |
| Unified Endpoint Management | UEM | * UEMs provide the same management of mobile devices as MDM<br>* In addition can manage desktop and laptop PC and many other devices. | * As MDM, but extends the capabilities to many more devices. | |
| File Integrity Monitor | FIM | Montors and reports on any file changes. | * Can detect and alert on file changes.<br>* Can be configured to restore files to original version. | * Can be challenging to configure and maintain.<br>* Generates a lot of network traffic. |
| Endpoint Detection and Response | EDR | * Deployed on endpoints to monitor anomalies and IoCs. | * Automated reporting to CSIRT or SIEM<br>* Early detection and response mechanism. | Complexity to configure and implement. |

Table 78 Outlines the variety of firewalls that can be implemented:

*Table 78: Firewalls*

| Firewall Type | Description | Advantage | Disadvantage |
|---|---|---|---|
| Packet Filtering Firewall | * Network traffic is filtered based on:<br>* Source/Destination Internet Protocol (IP) Address<br>* Protocol (E.g. IP, Transport Control Protocol (TCP), or User Datagram Protocol (UDP)<br>* Source/Destination Port | * Simple to configure. | * Maintenance issue, need to update IPs regularly.<br>* Susceptible to IP Spoofing attacks<br>* Scalability is an issue, due to simple configuration and technology.<br>* Evaluates each packet individually, cannot permit/deny traffic based on full stream.<br>* Cannot provide the functionality of newer, more advanced firewalls. |
| Application Layer Proxy Firewall | * Situated between the server and client and filters traffic at the Application Layer.<br>* Allows Proxying by accepting requests on one port and, if traffic is permitted, forwards them on another port. Otherwise packet is dropped.<br>* Allows Network Address Translation (NAT). Translating IP Addressing between Public and Private IP Address ranges as ourlined by Request For Comment (RFC) 1918.<br>* NAT allows a 1-to-1 translations.<br>* Port Address Translations (PAT) can be used in conjunction with NAT utilising port numbers to allows firewall to translations based on port numbering.<br>* PAT allows many-to-one translations. | * More secure that Packet Filtering Firewall<br>* Obscures internal network behind single IP Address<br>* Utilising NAT/PAT allows many devices to connect and appear to be from a single IP Address.<br>* Utilising Proxy can improve throughput - e.g. if multiple users request the same webpage. | * More resource required by the Application Layer Proxy Firewall as it carries out more advanced filtering.<br><br>* Some applications will not function if they see two or more device connecting from the same public IP Address. |
| Web Application Firewall (WAF) | * Similar to Application Layer Firewall but specifically protects Web Services.<br>* Recommended for organisations that host their own web services.<br>*** NOT Rquired by NG as they utilise cloud services. It has been confirmed that the Cloud Service Provider (CSP) implement WAF as part of their infrastructure.** | * Protects against:<br>*Cross-Site Scripting (XSS)<br>*Server-Side Request Forgery (SSRF)<br>*Cross Site Request Forgery (CSRF)<br>*Structured Query Language (SQL) Injection (SQLi) | * Incorrect configuration can provide a false sense of security. |
| Stateless Firewall | * Evaluates each packet individually to ascertain whether to permit/deny traffic<br>* Does NOT store the current state of the network connection.<br>* Does NOT inspect the full stream of traffic from one device to permit/deny traffic. | * Simple configuration<br>* Lower latency due to less traffic analysis. | * Scalability is an issue, due to simple configuration and technology.<br>* Cannot provide the functionality of newer, more advanced firewalls.<br>* Evaluates each packet individually, cannot permit/deny traffic based on full stream. |
| Stateful Packet Inspection (SPI) Firewall | * Keeps track of all established network connectsions<br>* Maintains a state table which logs of all connections<br>* Monitors the full stream of traffic and makes decisions of traffic in the stream rather then individual packets.<br>* If SPI Firewall cannot match a packet based on state table information, it will resort to packet filtering. | * Filters traffic based on connection state.<br>* Hardened configuration - does not require many ports open to provide a reliable connection.<br>* SPI firewalls can log network behaviour, if under attack, these logs can be used to analyse the attack and prevent future attacks. | * Configuration more complicated than other firewall types.<br>* More resources required to anayse traffic. |
| Next-Generation (NextGen) Firewall (NGFW). | * NGFWs combine the functionality of the SPI firewall discussed above with other protection mechanisms to provide a complete security solution.<br>* Allows integration with AD for end user authentication.<br>* Depending on Make and Model, examples of additional features provided by NGFWs are:<br>* UTM, Anti-Malware, Anti-Virus (AV), IDPS, DPI, DLP, SSL Inspection, Website Filtering, Access Control, Application Control, Threat Intelligence feeds, Sandboxing, Threat Prevention, Centralised Management. | * Centralised Management allows InfoSec team to configure, maintain and manage NGFWs at multiple locations.<br>* Full Cybersecurity solution, not only a firewall.<br>* Threat prevention can stop malicious attachments from being opened by user. | * Configuration more complicated than other firewall types.<br>* More resources required to anayse traffic.<br>* Cost - of both the NGFW and ongoing costs for subscriptions. |

Table 79 Outlines the implementation of FWs:

*Table 79: Firewall Implementation methods.*

| Architecture | Description | Advantage | Disadvantage |
|---|---|---|---|
| Single Bastion Host | * Single FW device, usually with two network interfaces, known as dual homed.<br>* Interface 1: Connected to the Local Area Network (LAN) - Internal / Trusted Zone. (Private IP Addressing as outlined by RFC 1918)<br>* Interface 2: Connected to the Internet Service Provider (ISP)- External/Untrusted Zone. (Public IP Addressing)<br>* Provides Routing, Firewalling, Proxy and Translation services (via NAT/PAT).<br>*Suitable for:<br>* Domestic use / Working From Home (WFH)<br>* Small Office/Home Office (SOHO).<br>* Small/ Medium sized organisations. | Simple configuration, easy to install and maintain. | * Simple architecture, potential target for attackers.<br>* Single FW, fault or attack could render the organisation without network connectivity.<br>* Cannot securely provide access to shared resources for customers, partners, or suppliers. |
| Screened-Host | * Single Application Layer FW device, with three or more network interfaces.<br>* Interface 1: LAN - Internal / Trusted Zone. (Private IP)<br>* Interface 2: ISP- External/Untrusted Zone.<br>* Interface 3: Screened Host network. Private and Public IP Addressing.<br>* Two Domain Name Service (DNS) entries - Screened-Host (One Public the other Private).<br>* Provides Routing, Firewalling, Proxy and Translation services (via NAT/PAT) also provides controlled access by filtering requests from untrusted internet zone to the Screen-host. | * More advanced Application Layer FW used - providing enhanced filtering.<br>* Allows controlled inbound traffic to the screened-Host.<br>* Authenticated and Authorised users (Customers, partners, suppliers) can access shared resources. | * Single FW, resiliency issues.<br>* Only one device can be hosted in the Screened-Host zone. |
| Screened-Subnet | * As above, but in place of a single Screened-Host device, a new zone is created termed the Demilitarised Zone (DMZ).<br>* The DMZ can host several servers that can be accessed externally by authorised users.<br>* Additional filtering is in place to restrict access to the DMZ, ensuring that traffic cannot be routed from the Untrusted to the Trusted zone via the DMZ. | * Allows Authenticated users to access multiple servers in DMZ.<br>* Allows for load balancing incoming requests - soluton for high traffic. | * Single FW, resiliency issues. |
| High Availability (HA) | * As Screened-Host - Three Zones - Trusted, Untrusted and DMZ.<br>* Two FWs connected together in HA and appear as a single FW.<br>* Each FW can be connected to a different ISP to improve resilience.<br>*** It is recommended that NG implement a Screened-Subnet with FWs in HA.** | * Benefits of Screened-Host.<br>* Resilient Networking. | * Complexity<br>* Cost of hardware and ISP. |

Fig.40 Illustrates the recommended FW deployment for NG:

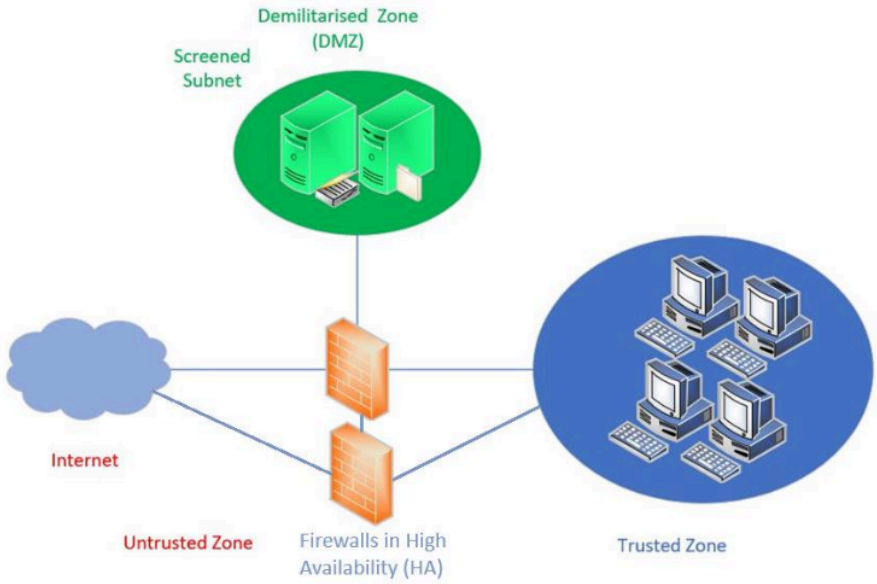



*Figure 39: Screened-Subnet with FWs in HA.*

As discovered during research, it is crucial to the success to a security programme that InfoSec teams can proactively scan and analyse the network identifying weaknesses which can be resolved. Table 80 outlines the tools used.

*Table 80: Tools used to network analysis*

| Type | Description | Examples | Advantage | Disadvantage |
|---|---|---|---|---|
| Port Scanners | * Used to scan a device or network to view open/closed ports on a device or devices. | Nmap, Zenmap | * Useful for fault finding<br>* Configuration Hardening | * Attackers can test which ports are open, and then go on to search for exploits based on open ports. |
| Vulnerability Scanners | * Used to scan a device or network to view vulnerabilities.<br>* The scanner will list any Common Vulnerabilities and Exposures (CVE).<br>* The Common Vulnerability Scoring System (CVSS) will score the vulnerability from 0-10.<br>* CVSS None(0), Low (0.1-3.9), Medium (4-6.9), High(7-8.9), Critical (9-10).<br>* Resolutions are also provided in the report. | Nessus, OpenVAS | * Pro-Active action - searching for vulnerabilities and resolving them.<br>* Once identified, control measures can be put in place.<br>*Vulnerability Scans can be scheduled to run automatically.<br>* Report produced can be shared with other departments. | * Allows attackers to search for vulnerabilities. |
| Packet Sniffers | * Used to view traffic on the wired or wireless networks.<br>* Can save network traffic to a capture file for later analysis. | Wireshark, Tshark, TCPDump | * Useful for fault finding<br>* Configuration Hardening | * Allows attackers to view sensitive data if transmitted in clear text (E.g. Passwords).<br>* Possible to re-send capture in a replay attack. |
| Trap and Trace: Honey Pot/Net/File | * A decoy system used by administrators to monitor malicious activity.<br>* Used to gather information on how attackers behave so that live systems can be better protected. | T-Pot, Glutton, SNARE. | * Distraction for attackers, takes their attention away from live systems.<br>* Provides valuable information on types of attacks possible. | * Requires resources, to configure, maintain and monitor the honeytrap.<br>* Poorly configured honeytrap could be used as a jumpbox into live systems. |

Once weaknesses have been identified, the InfoSec team can resolve them by either deploying a software/firmware update or through configuration changes, disabling weak protocols in favour of secure/encrypted equivalents, this process is known as **configuration hardening**, see Table 81:

*Table 81: Examples of Configuration Hardening*

| Unsecure Protocol | Acronymn | Port | Description | Secure Equivilent | Acronymn | Port | Description |
|---|---|---|---|---|---|---|---|
| Telnet | - | 23 | *Telnet sends all communication in clear text. This includes all passwords and commands.<br>* Allows an attacker to intercept this traffic and log into the device. | Secure Shell | SSH | 22 | * Encrypts all traffic.<br>* If attacker were to intercept traffic, all communications carried out in ciphertext. |
| Hypertext Transfer Protocol | HTTP | 80 | *HTTP sends all communication in clear text. This includes all usernames and passwords.<br>* Allows an attacker to intercept traffic and gather usernames and passwords. | Hypertext Transfer Protocol Secure | HTTPS | 443 | * Encrypts all traffic.<br>* If attacker were to intercept traffic, all communications carried out in ciphertext. |
| File Transfer Protocol | FTP | 20 & 21 | * Does not implement encryption - all traffic send in clear text including passwords.<br>* FTP not as common now, web / HTTP services are preferred. | Secure File Transfer Protocol | SFTP | 22 | * Implements SSH to provide encryption.<br>* Preferred as port 22 may already be permitted allowing SSH & SFTP. |
| | | | | File Transfer Protocol Secure | FTPS | 989 & 990 | * Implements TLS to provide encryption.<br>* Additional ports need to be opened increasing attack surface. |
| Domain Name Service | DNS | 53 | * If the DNS server does not have a DNS record, it sends a recursive DNS lookup to any DNS servers.<br>* Potential for DNS poisoning, where a malicious DNS record is fed back. | Domain Name Service Secure | DNS Sec | 53 | * Does NOT provide confidentiality, but authenticates other DNS servers via Digital Signatures.<br>* Confirms integrity of DNS records from trusted sources.<br>* Builds a chain of trusts. |
| Simple Network Management Protocol Versions 1&2 | SNMP v1/2 | 161 & 162 | * All data is sent in clear text<br>* Provides some authentication via a "community string" | Simple Network Management Protocol Versions 3 | SNMP v3 | 161 & 162 | * Provides encryption, and authenticaton<br>* Vaidates SNMP messages. |

Several different logs are generated by systems, some of the key logs are detailed in Table 82 [3]:

*Table 82: Log files*

| Log File | Description | Advantage | Disadvantage |
|---|---|---|---|
| System Logs | Tracks all actions while system is functioning. | Provides details on all system changes error messages generated by the system can also be located here. | Many log messages are generated by the system, so familiarity of log system is crucial. |
| Application Logs | Messages generated by applications are tracked here. | Application updates or error messages logged. | As above. |
| Security / Authentications Logs | Stores all successful and unsuccessful authentications. | * Malicious authentication attempts can be tracked, e.g. several incorrect login attempts.<br>* Privileged use is logged. | Some processes, such as wireless, re-authenticate every so often increasing log size. Knowledge of log filtering and searching is imperative. |
| Web Logs | Services like Microsoft Internet Information Services (IIS) and Apache will track web activity. | * Tracks what services where accessed, when and from what IP.<br>* These logs are crucial when dealing with an IR scenario where a hacker is attempting to attack web services. Such as DoS or SQLi. | Many genuine requests will be found in this log, therefore Log analysis skills are crucial in detecting malicious activity. |
| DNS Logs | All DNS queries are tracked here. | * Can indicate compromised systems based on DNS queries.<br>* Can indicate an attacker carrying out reconnaissance / footpinting. | As above. |

The IEEE introduced the 802.11 wireless standards which sets out the capabilities of wireless devices, these are outlined in Table 83:

*Table 83: IEEE 802.11 Standards*

| IEEE 802.11 standards | Speed (Mbps) | Frequency (GHz) | Analysis |
|---|---|---|---|
| A | 54 | 5 | It is recommended that 802.11A/B/G be disabled on NGs wireless network. This will stop older devices connecting to the wireless network, which are more likely to have vulnerabilities.<br><br>Also will improve performance as a Wireless Access Point (WAP) can only transmit data at the speed of the slowest connected device. Therefore if a single device using 802.11B connects, then **ALL** devices will only be able to transmit at 11 Mbps. |
| B | 11 | 2.4 | |
| G | 54 | 2.4 | |
| N | 600 | 2.4/5 | |
| AC | 1,300 | 5 | |
| AX | 9,600 | 2.4/5/6 | It is recommended that NG purchase a wireless system capable of supporting AX as a minimum specification. This ensures system the system is fit for purpose for a long period and that it does not become End of Life (EoL) soon after installation.<br><br>This is crucial from a security standpoint to ensure that security updates and maintenance contracts are available for the wireless infrastructure. |
| BE | 40,000 | 2.4/5/6 | The BE standard having only been released will be too costly at this stage. |

Protecting wireless data whilst in transit is crucial this can be done by implementing suitable Wireless security standards outlined in Table 84 [3] [155] [156] [157] [158]:

*Table 84: Wireless Security Standards*

| Wireless Security standard | Acronymn | Status | IEEE | Description | Analysis |
|---|---|---|---|---|---|
| Wired Equivalent Privacy | WEP | Compromised | | This wireless security standard has been compromised for some time now. It uses a compromised RC4 encryption algorithm. | Not suitable for use. |
| Wi-Fi Protected Access | WPA | Compromised | 802.11i | WPA uses some of the same techniques as WEP and has since been compromised. | Not suitable for use. |
| | WPA2 | In current use | 802.11i | WPA2 uses Advanced Encryption System-Counter Mode Cipher Block Chaning Message Authentication Protocol<br><br>**AES-CCMP** encryption and therefore strong.<br>Key Length: 128-256 bit<br>Two vairants of WPA2:<br><br>**WPA2-Personal:** This allows a Preshared Key (PSK). Users enter a wireless password to authenticate.<br><br>**WPA2-Enterprise:** This requires a centralised Authentication infrastructure - RADIUS server utilising IEEE 802.11x. Therefore each user has unique login credentials via AD. | This Wireless security standard is the currently accepted standard. This would be suitable for use by NG.<br><br>But it has been decided to utilise WPA3 for its enhanced security features. As they would exceed the security requirements and less likely to become compromised. |
| | WPA3 | Slowly being implemented. | 802.11i | WPA3 uses a stronger form of AES encryption and therefore very strong.<br><br>AES Using Galois-Counter Mode<br><br>**AES-GCM**<br>Key Length: 192-256 bit<br>There are also two vairants of WPA3:<br><br>**WPA3-Personal:** Utilises Simultaneous Authentication of Equals (**SAE**) process in place of Preshared . Users generate their own password to authenticate. Implements **Perfect Forward Secrecy** - This ensures data is encrypted even if password has been compromised.<br><br>**WPA3-Enterprise:** RADIUS Auth as WPA2. Additional encryption of network frames at Layer 2. | **It is recommended that NG implement:**<br><br>**WPA3 in Enterprise mode as it provides the latest security features.**<br><br>**Centralised Auth utilising 802.1x via a RADIUS server.**<br><br>**This server will also authenticate users via the Wired LAN.** |

It is crucial that data transmitted over wireless is encrypted to ensure the CIA triad. Table 85 outlines the two methods of encryption [3] [159] [160]:

*Table 85 Encryption Comparison*

| Encryption Type | Description | Advantage | Disadvantage |
|---|---|---|---|
| Symmetric | A Private Key is shared between users. Sometimes known as a shared secret. This is also sometime referred to Pre Shared Key (PSK). | * Fast Encryption.<br>* Single Shared Key to Encrypt and Decrypt<br>* Simpler configuration (On small scale)<br>* Provides Confidentiality and Integrity Only.<br>* Bulk encryption. | * Not Scalable.<br>* Sharing key is difficult - Out-of-band exchange.<br>**Solutions**: Physical key exchange or **Diffie-Hellman** (DH) key exchange.<br>* Cannot provide **Authentication** OR **Non-repudiation** (Proves Validity or the sender of data) as single key is shared. |
| Asymmetric | Each user has two keys - A Public and Private key pair.<br>Public Key: Encrypts message<br>Private Key: Decrypts message<br><br>Public Key: Decrypts Digital Signature<br>Private Key: Encrypts Digital Signature | * Scalable.<br>* In-band key exchange<br>* Provides C,I,A and Nonrepudiation. Each key is unique therefore can validate sender.<br>*Used in Public Key Infrastructure (PKI)<br>* Used for Digital Signatures<br>* Nonrepudiation of user, & Integrity of data.<br>* Digital Certificates - Endorsed copy to public key.<br>* Authenticates user, device or service<br>* Provides Data Intrgrity<br>* Ensures Confidentiality<br>* Non-repudiation of sender | * Slower Encryption.<br>* More complex configuration |

Fig.41 Illustrates the Symmetric Encryption process used to send a message.

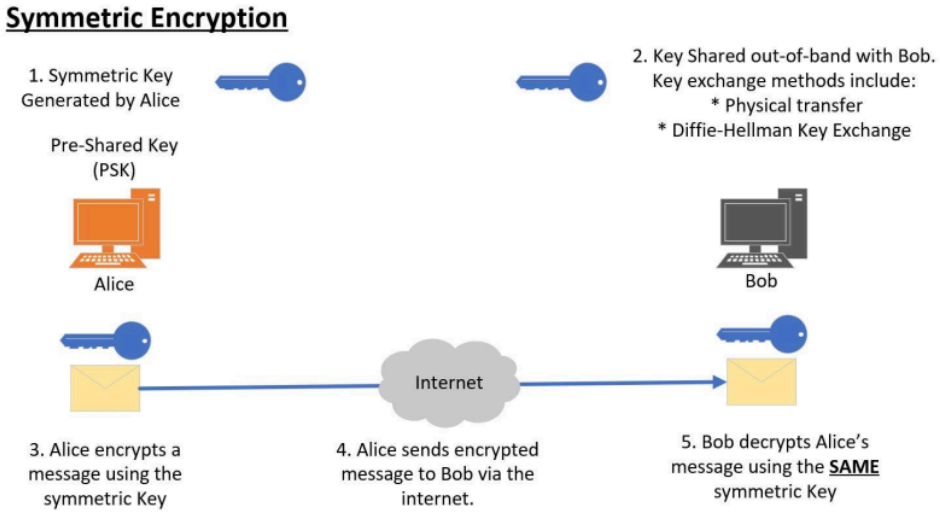



*Figure 40: Example of Symmetric Encryption*

Fig.42 Illustrates the Asymmetric Encryption process used to send a message.

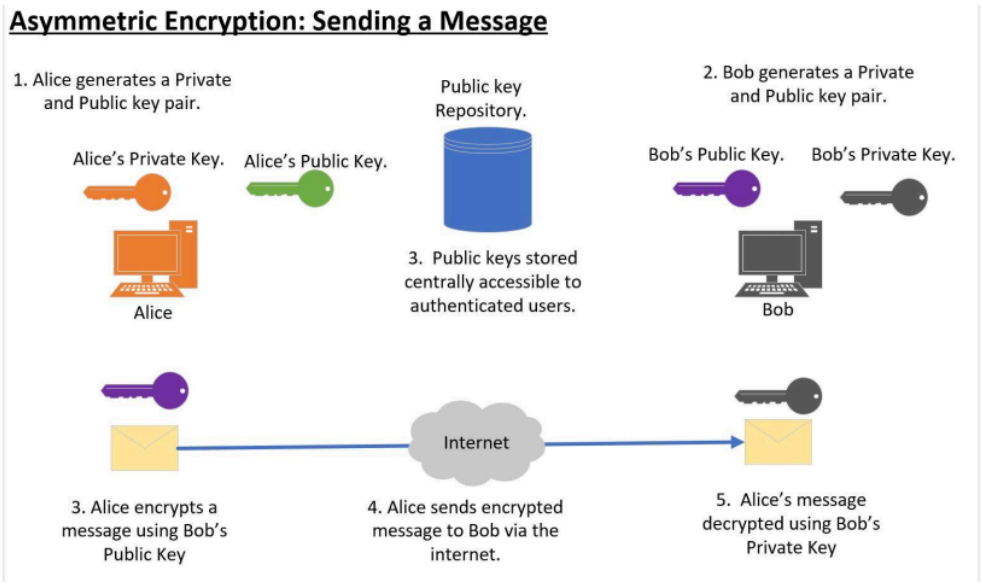



*Figure 41: Example of Asymmetric Encryption – Message*

Fig.43 Illustrates the Asymmetric Encryption process used to send a digital signature.

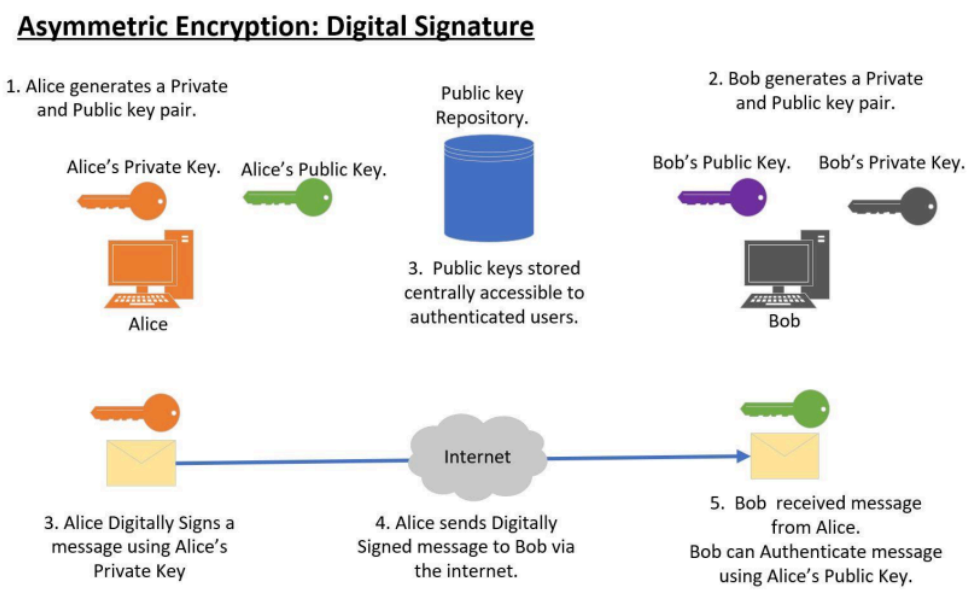



*Figure 42: Example of Asymmetric Encryption - Digital Signature*

There are different encryption standards which support different key length. A longer the key length increases the amount of time taken by an attacker to decipher the encrypted data, examples are found in Table 86 [3]:

*Table 86: Encryption Cypher Standards*

| Encryption Standard | Acronymn | Algorithm type | Key Length (bits) | Status |
|---|---|---|---|---|
| Rivest Cipher 4 | RC4 | Symmetric | 8-2048 | Unsecure |
| Data Encryption Standard | DES | Symmetric | 56 | Unsecure |
| Triple Data Encryption Standard | 3DES | Symmetric | 168 (3x56) | Unsecure |
| Advanced Encryption Standard | **AES** | Symmetric | 128, 192, 256 | **Secure** |
| Rivest Shamir Adleman | **RSA** | Asymmetric | 1024 - 4096 | **Secure** |

The two Formulae below can be used to illustrate the number of keys required based on the number of staff, the result can be found in Table 87.

*Equation 1: Symmetric Cryptography Formula [3]*

$$\frac{n(n-2)}{2} \; keys$$

*Equation 2: Asymmetric Cryptography Formula [3]*

$$2n \; keys$$

*Table 87: Comparison of Symmetric and Asymmetric Key Numbers*

| People | Symmetric | Asymmetric |
|---|---|---|
| 1 | 0 | 2 |
| 2 | 1 | 4 |
| 3 | 3 | 6 |
| 4 | 6 | 8 |
| 5 | 10 | 10 |
| 6 | 15 | 12 |
| 7 | 21 | 14 |
| 8 | 28 | 16 |
| 9 | 36 | 18 |
| 10 | 45 | 20 |
| 20 | 190 | 40 |
| 30 | 435 | 60 |
| 50 | 1,225 | 100 |
| 100 | 4,950 | 200 |
| 200 | 19,900 | 400 |
| 300 | 44,850 | 600 |
| 400 | 79,800 | 800 |
| 500 | 124,750 | 1,000 |
| 1,050 | 550,725 | 2,100 |

From Table 87 for all staff at NG to receive a key using Symmetric encryption would require over half a million keys. Using asymmetric encryption requires more processing power. The solution is a hybrid system using both encryption methods. An example of this is the Diffie-Hellman key exchange where:

- A symmetric key is encrypted using asymmetric encryption (Public key of recipient to encrypt).
- The recipient then decrypts the symmetric key using their private key.
- Now both parties swap over to use the Symmetric Key.

Using Public Key Infrastructure (PKI) utilises asymmetric encryption to allow organizations/users that were currently unknown to one another to communicate securely. This is done by using Digital Certificates which both provide the public key to the other party. Digital Certificates are also signed by a trusted Certificate Authority (CA) providing a chain of trust. Fig.44 Illustrates and Table 88 describes this process:

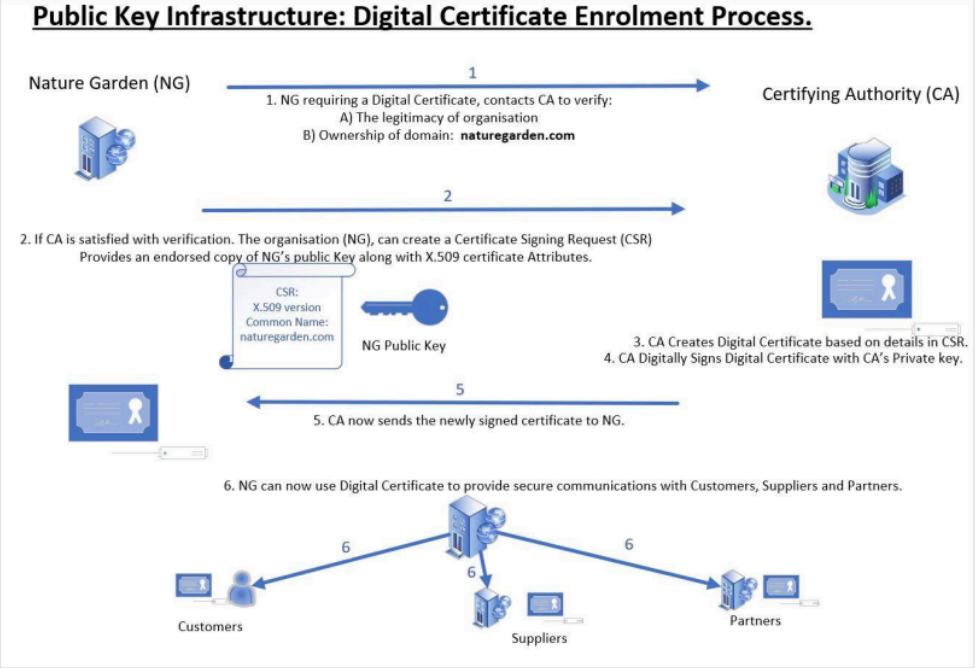



*Figure 43: PKI Certificate Enrolment*

*Table 88: Digital Certificate Enrolment*

| Step | Digital Certificate Enrolment | Description |
|---|---|---|
| 1 | Enrolment with Certifying Authority (CA). | Verification of organisation to CA, proof of ownership of domain. |
| 2 | Create a Certificate Signing Request (CSR) | Provides CA with a copy of the Public Key along with X.509 attributes. |
| 3 | CA creates Digital Certificate. | Certificate created using details in CSR. |
| 4 | CA signs newly created certificate using the CA's Private key. | This proves the authenticity of the newly created Digital Certificate. |
| 5 | CA provides organisation with a copy of their newly signed Digital Certificate. | This Digital Certificate is now authenticated by the CA and is usually valid for a set period. Typically 1-3 years. |
| 6 | Organisation can now use Digital Certificate. | Organisation can now distribute this Digital Certificate with anyone they wish to ensure secure communications. |

Table 89 outlines the verification process, steps 1-2 are automated in the browser, step 3 can be carried out by the user.

*Table 89: Digital Certificate Verification*

| Step | Digital Certificate Verification | Description |
|---|---|---|
| 1 | Certificate is checked against CA's public key. | Ensures Certificate Authenticity. |
| 2 | Check if Certificate has been revoked. | Confirmed by checking the Certificate Revocation List (CRL) or by using the Online Certificate Status Protocol (OSCP). |
| 3 | Visual inspection of Digital Certificate. | The Certificate can be checked manually to ensure it is associated with the correct trusted domains, from a trusted CA (e.g. Amazon Web Services (AWS), Comodo, Symantec). |

Table 90 provides examples of certificate revocation.

*Table 90: Digital Certificate Revocation*

| Digital Certificate Revocation Examples | Description |
|---|---|
| Compromised Certificate. | Private key has been accessed. |
| Certificate erroneously issued | CA issued certificate without correct verification. |
| Details of certificate changes. | Change to X.509 attributes, e.g. Common Name (CN). |

Table 91 Outlines the Transport Layer Security (TLS) used to encrypt traffic whilst data in transit [3].

*Table 91: Trasport Layer Security*

| Transport Layer Security Protocol | Version (s) | Status | Details |
|---|---|---|---|
| Secure Sockets Layer (SSL) | 1.0, 2.0, 3.0 | Unsecure | Earliest form of transport layer security and classed as vulnerable. |
| **Transport Layer Security (TLS)** | 1.0, 1.1 | Unsecure | An upgrade of SSLv3.0, but is still considered as vulnerable. |
| | **1.2** | **Secure** | Defined in 2008, is fairly old protocol, but is still currently considered secure. Utilises AES encryption. |
| | **1.3** | **Secure** | Utilises the latest cypher suites, highest form of encryption to date. |

Table 92 outlines email protocols used for transporting and securing messages:

*Table 92: Email Protocols*

| Email Protocol | Acronym | Description | Advantage | Disadvantage |
|---|---|---|---|---|
| Post Office Protocol. | POP | * Protocol used to facilitate transfer of emails.<br>* Downloads emails from server to a single device.<br>*Currently on version 3 (POP3) | Widely supported. | * Messages transferred in clear text.<br>* Legacy protocol. |
| Internet Message Access Protocol. | IMAP | * Protocol used by clients (such as Outlook) to retrieve emails from an email server.<br>* More advanced - can synchronise emails from server to multiple devices. | * Widely supported.<br>* Can synchronise with multiple devices. | Messages transferred in clear text. |
| Post Office Protocol. | POPS | As POP3, with the addition of TLS encryption. | Messages are encrypted. | Provides Confidentiality, but not Integrity or Non-repudiation. |
| Internet Message Access Protocol. | IMAPS | As IMAP, with the addition of TLS encryption. | Messages are encrypted. | Provides Confidentiality, but not Integrity or Non-repudiation. |
| Secure/Multipurpose Internet Message Extensions. | S/MIME | * A Protocol that uses PKI to :<br>* Encrypt emails (Providing Confidentiality and Integrity)<br>* Add digital signatures (Providing Authentication, Non-Repudiation and Integrity) | * Provides CIA and Non-repudiation.<br>* Can support TLS, but is not reliant on TLS. | * Requires Digital Certificate addend complexity.<br>* Certificate can be revoked.<br>* Email may not be viewable if receiving device configured improperly. |
| Pretty Good Privacy | PGP | * Can be used to Encrypt Emails, and Encrypting files.<br>* Does not reply on PKI and Digital Certificates.<br>* Utilises Public, Private and Session keys.<br>* PGP can be used in conjunction with Digital Signatures, to provide Authentication. | * Provides CIA and Non-repudiation.<br>* Utilises Asymmetric encryption<br>* However, does **not** rely on PKI.<br>* Renowned for its strong encryption. | * Complexity - Not user friendly.<br>* Key Management Issues.<br>* Compatibility issues, both devices must use the same version of PGP. |
| Sender Policy Framework | SPF | * Email authentication method.<br>* Provides email server authentication. | * Identifies genuine/trusted email servers<br>* Identifies malicous spam/phishing emails.<br>* Identifies fraudulent emails from a domain owned by a legitimate organisation.<br>* Domain reputation is maintained. | * System Complexity<br>* Maintaining SPF records is challenging.<br>* DNS lookup limitations of SPF records, leading to SPF authentication failures. |
| Domain Keys Identified Mail | DKIM | * Email Authentication protocol.<br>* Uses Digital Signatures<br>* Detects forged sender addresses in emails.<br>* Stops attackers from impersonating legitimate domain addresses. | * Widely supported.<br>* Provides Integrity, Authentication and Non-repudiation.<br>* Identifies emails from potential attackers. | * Adds complexity<br>* Does **not** provide encryption.<br>* Issues if DKIM configured incorrectly. |
| Domain -based Message Authentication, Reporting & Conformance. | DMARC | * Email Authentication, policy and reporting protocol.<br>* Works in conjunction with DKIM.<br>* Analyses DKIM applies a standard validation test:<br>* Checks IP Blocklist, Reputation Lists.<br>* Applies DMARC policy to determine how email should be forwarded:<br>* Passed onto the user<br>* Placed in Quarantine<br>* Blocked | * Additional security measure to catch malicious emails.<br>* Pro-actively quarantines or blocks emails spam / phishing before user receives email.<br>* Avoids risk of user interacting with spam emails, avoiding malware/ransomware being downloaded and data breaches. | * System complexity<br>* Issues with DKIM records not kept up to date.<br>* Relies on DKIM being configured correctly.<br>* DMARC configuration/policy issues. |

IPSec is a VPN technology that can be used to provide encryption for data in transit. Table 93 provides details of IPSec:

*Table 93: IPSec details*

| IPSec Authentication Protocols | Acronymn | Description | Advantage | Disadvantage |
|---|---|---|---|---|
| Authentication Header | AH | * Provides a mechanism for authentication only. | * Ensures Integrity of data.<br>* Ensures Authentication of IP Packets sent. | Does not encrypt data. |
| Encapsulating Security Payload | ESP | * Provides Encryption for<br>* Can also provide Integrity and Authentication in certain circumstances. | * Can provide Confidentiality, Integrity and Availability. | * Adds complexity.<br>* Managing Encryption keys.<br>* Encryption policies. |
| **IPSec Mode** | | **Description** | **Advantage** | **Disadvantage** |
| Transport mode | - | * IP Data payload of packet is encrypted only.<br>* Used for client-server communication.<br>* Default IPSec configuration. | * Reduced encryption requirements.<br>* Provides faster connectivity | Does not establish a fully secure connection. |
| Tunnel mode | - | * Full packet is encrypted - Header and Data.<br>*Used for site-to-site Virtual Private Networks (VPN)<br>* Full Tunnel where all data sent via IPSec tunnel.<br>* Split-Tunnel traffic destained for corporate network sent via IPSec. All other traffic sent to internet. | * All data is encrypted va ESP.<br>* ESP provides Confidentiality, Integrity and Availability.<br>*Provides a secure connection between sites. | Additional overhead required for full encryption and packet encapsulation. |

Kerberos is a system used to secure the authentication process, designed to function on an untrusted network Kerberos provides encryption for authentication data. Table 94 provides the main elements of Kerberos [3] [161] [162] [163] [164]:

*Table 94: Kerberos elements*

| Kerberos | Acronymn | Description |
|---|---|---|
| Authentication Server | AS | The service that issues Ticket Granting Tickets used for authenticating users, resources, devices or services within the domain. |
| Key Distribution Centre | KDC | Runs on a Windows Domain Controller (DC) and authenticates and verifies user identities by using AD. |
| Ticket Granting Service | TGS | Service that issues tickets to access services within the domain or |
| Ticket Granting Ticket | TGT | A Kerberos Ticket used to obtain other tickets. |

## A2.8 Service Level Agreement (SLA)

An SLA are formal contracts between a vendor and customer specifying the levels of service the customer should expect and penalties if a vendor breaches the SLA this would usually be a fine. Response times and availability of support are covered in SLAs.

Customer service is one of the key benefits of implementing ITIL, this is illustrated by best practice number 29 “Service Level Management” which provides guidance on what services a customer should expect. Table 95 below shows the typical response times to a service request as stated in an SLA:

*Table 95: ITIL SLA Response Times [165]*

| Name | Duration | Schedule |
|---|---|---|
| Priority 1 Response | 15 min | 24x7 |
| Priority 1 Resolution | 4 hours | 24x7 |
| Priority 2 Response | 1 hour | 8-5 Weekdays Excluding Holidays |
| Priority 2 Resolution | 9 hours | 8-5 Weekdays Excluding Holidays |
| Priority 3 Response | 4 hours | 8-5 Weekdays Excluding Holidays |
| Priority 3 Resolution | 18 hours | 8-5 Weekdays Excluding Holidays |
| Priority 4 Response | 9 hours | 8-5 Weekdays Excluding Holidays |
| Priority 4 Resolution | 45 hours | 8-5 Weekdays Excluding Holidays |

Utilising these practices ensures that the customer receives a timely response to their request based on urgency.

## A2.9 Threat, Vulnerability Asset Worksheet

Fig.45 shows the Threat, Vulnerability, Asset (TVA) worksheet. This is another more granular method of prioritising which vulnerabilities must be resolved first. The TVA worksheet considers each Threat (e.g. Data breach, data loss), Vulnerability (Software/firmware vulnerability, and Asset (Servers, PCs, COBO devices.

| | Asset 1 | Asset 2 | Asset 3 | ... | ... | ... | ... | ... | ... | Asset n |
|---|---|---|---|---|---|---|---|---|---|---|
| Threat 1 | T1V1A1<br>T1V2A1<br>T1V3A1<br>... | T1V1A2<br>T1V2A2<br>... | T1V1A3<br>... | T1V1A4<br>... | | | | | | |
| Threat 2 | T2V1A1<br>T2V2A1<br>... | T2V1A2<br>... | T2V1A3<br>... | | | | | | | |
| Threat 3 | T3V1A1<br>... | T3V1A2<br>... | | | | | | | | |
| Threat 4 | T4V1A1<br>... | | | | | | | | | |
| Threat 5 | | | | | | | | | | |
| Threat 6 | | | | | | | | | | |
| ... | | | | | | | | | | |
| ... | | | | | | | | | | |
| Threat n | | | | | | | | | | |
| Priority of effort | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | ... | |

*Figure 44: TVA Worksheet [4]*

## A2.10 Service Organisation Controls (SOC) Audits

Regular cybersecurity audits, known as Service Organisation Controls (SOC) audits are crucial to maintaining a good cybersecurity posture and identify any potential vulnerabilities [3]. An audit can provide advice and guidance on cybersecurity best practices and highlight any unknown flaws in security. To standardise the approach to cybersecurity and information security the ISO/IEC 27001 and 27002 were introduced to provide resilience and maintain data Confidentiality, Integrity, and Availability (CIA). The auditor will check the companies for their policies on passwords, user accounts, backup regimes, network change logging (implementation of a change advisory board). Also, the following procedures would be scrutinised:

- Incident Response
- Disaster Recovery procedures
- Business continuity plans

See Table 96 below that provides further details on SOC audits.

*Table 96: SOC Audits [3]*

| Audit Type | Details |
|---|---|
| SOC1 | Financial Audit |
| SOC2: Type 1 | Cybersecurity audit describing the security measures in place to maintain CIA and avoid Disclosure, Alteration and Denial (DAD). Offers the auditor's opinion on their suitability. |
| SOC2: Type 2 | As type 1 above, but auditor also provides the result of the effectiveness of the measures. Neither SOC2 audits would be released external to the organisation. |
| SOC3 | Cybersecurity audit, meant for publication available on request. |

## A2.11 Continuity of Operation Planning (COOP)

The Continuity of Operation Planning (COOP) is a four-phase business continuity strategy programme in the United States (US), see Fig.46. It is a federally sponsored standard, set out by the Federal Emergency Management Agency (FEMA) that all government agencies must meet to ensure continuity of operations if faced with a large disaster. It sets out the essential functions of an organisation, the delegation of authority and the order of succession so that the agency can still function in the face of a catastrophic event. The COOP strategy was introduced by President Eisenhower in the 1950s as a response to the growing threat of nuclear war. The COOP strategy was activated for the first time after the 9/11 attack in 2001.

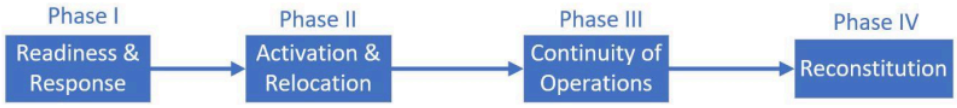



*Figure 45: Four phase COOP Strategy [3]*

# SR - DSCG Assignment v50 - FINAL

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

94/100

PAGE 1

QM

## Abstract

Abstract should be the last to be written to outline the key finding or contribution that would interest key players of what was done. This will fit perfectly in the introduction where it gives a background to the work along with some general research information of the subject areas, followed by what the rest of the report will include.

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

PAGE 32

PAGE 33

PAGE 34

PAGE 35

PAGE 36

PAGE 37

PAGE 38

PAGE 39

PAGE 40

PAGE 41

PAGE 42

PAGE 43

PAGE 44

PAGE 45

PAGE 46

PAGE 47

PAGE 48

PAGE 49

PAGE 50

PAGE 51

PAGE 52

PAGE 53

PAGE 54

PAGE 55

PAGE 56

PAGE 57

PAGE 58

PAGE 59

PAGE 60

PAGE 61

PAGE 62

PAGE 63

PAGE 64

PAGE 65

PAGE 66

PAGE 67

PAGE 68

PAGE 69

PAGE 70

PAGE 71

PAGE 72

PAGE 73

PAGE 74

PAGE 75

PAGE 76

PAGE 77

PAGE 78

PAGE 79

PAGE 80

PAGE 81

PAGE 82

PAGE 83

PAGE 84

PAGE 85

PAGE 86

PAGE 87

PAGE 88

PAGE 89

PAGE 90

PAGE 91

PAGE 92

PAGE 93

PAGE 94

PAGE 95

PAGE 96

PAGE 97

PAGE 98

PAGE 99

PAGE 100

PAGE 101

PAGE 102

GRADING FORM: L7 DSGC (ACCA7028)

| | |
|---|---|
| SIMON REES | **94** |

**ENGAGEMENT WITH LITERATURE**

*Your work must include articles published by peer reviewed journals, conference proceedings, books, and related website (e.g. IEEE, ACM, Science direct). Information from website such as ehow, wiki, forums, etc. will not be accepted (15 marks)*

Exceptional engagement with an extensive range of relevant and credible literature, informed by the latest research. High-level referencing skills consistently and professionally applied.
You are awarded marks based on:
awarded for:

- Diversity of sources and materials used
- Key concepts discussed
- Appropriate summaries of articles and level of critical appraisal of literature
- Application of appropriate referencing conventions

**14**

**KNOWLEDGE AND UNDERSTANDING**

*Your work must demonstrate understanding of concepts and underlying principles. You should explain and analysis the chosen area in a meaningful way. (15 marks)*

You have demonstrated specialised area of knowledge. Understanding of the concepts of the subject informed by current research. Critical awareness of current problems and insights.
You are awarded marks based on:

- Depth of the research
- Strength of the statements

**14**

- Structure of the paper
- Quality of the report

**COGNITIVE AND INTELLECTUAL**

*Your work must demonstrate critical analysis and evaluation of your approach for security framework and model. Your work must also justify your findings and provide evidences. (40 marks)*

Exceptional critical evaluation/ critique of current research and methodologies, Proposes new hypotheses, where appropriate.
Marks are awarded based on:
critical analysis and evaluation of your approach for security framework and model.
How you justify your findings and provide evidences.

**38**

**PRACTICAL SKILLS**

*Marks will be awarded based on the quality of and level of detail provided for the design approach; diagrams, table, charts and any other design methods utilise will enhance marks. (20 marks)*

You have provided relevant and appropriate tables. and have used other form of diagrams to aid your own approach.
Marks are awarded based on the quality of and level of detail provided for the design approach; diagrams, table, charts and any other design methods utilise will enhance marks.

**20**

**TRANSFERABLE SKILLS FOR LIFE**

*This should be presented in an academic way and therefore must include an abstract, an introduction, a conclusion and a list of references. (10 marks)*

Well presented and professional report that flow excellently. **8**