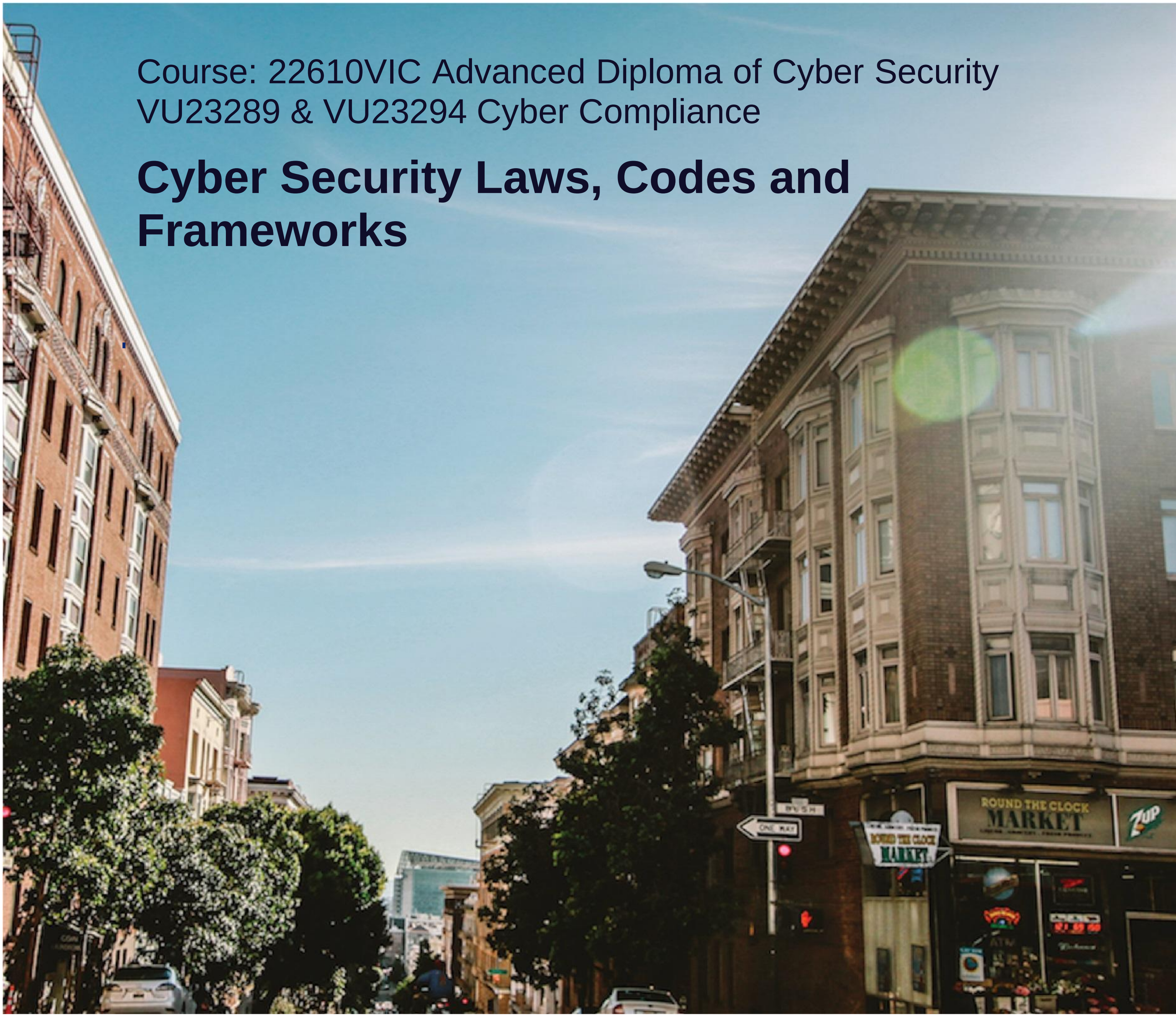
Course: 22610VIC Advanced Diploma of Cyber Security
VU23289 & VU23294 Cyber Compliance

Cyber Security Laws, Codes and Frameworks



Team: AOJC

Authorized by: Alex, Or, Jin, Carlos

Contents

Part A1 – Research and Analysis

I. Cyber Security Legislation

i. Federal Legislation

1. *Cybercrime Act 2001.*

The *Cybercrime Act 2001* covers several key areas such as

Schedule 1 - Computer Offences

- Australian Security Intelligence Organization Act 1979
- Crimes Act 1914
- Criminal Code Act 1995
- Educational Services for Overseas Students Act 2000
- Telecommunications (Interception) Act 1979

Part 10.7 - Computer Offences

- **Division 476 - Preliminary**
  - 476.1 Definitions
  - 476.2 Meaning of unauthorised access, modification or impairment
  - 476.3 Geographical Jurisdiction
  - 476.4 Saving of other laws
  - 476.5 Liability for certain acts

- **Division 477 - Serious Computer Offences**
  - 477.1 Unauthorised access, modification or impairment with intent to commit a serious offence.
  - 477.2 Unauthorised Modification of data to cause impairment
  - 477.3 Unauthorised impairment of electronic communication

- **Division 478 - Other Computer Offences**
  - 478.1 Unauthorised Access to, or modification of, restricted data
  - 478.2 Unauthorised impairment of data held on a computer disk etc
  - 478.3 Possession or control of data with intent to commit a computer offence
  - 478.4 Producing, supplying or obtaining data with intent to commit a computer offence

Schedule 2 - Law Enforcement Powers relating to electronically stored data

Crimes Act 1914

- 3LA Person with knowledge of a computer or a computer system to assist access etc
- 3LB Accessing data held on other premises-notification to occupier of that premises

Customs Act 1901

- 201A Person with knowledge of a computer or a computer system to assist access etc.
- 201B Accessing data held on other premises-notification to occupier of that premises

Active threats to the health sector: The definitions and provisions in the act related to unauthorised access, modification, and impairment of computer systems and data can help identify potential active threats in the health sector. Understanding these offences can assist in recognizing the types of cyber threats that healthcare organisations may face.

Impacts of cyber-attacks to the health sector: The serious computer offences outlined in the act, such as unauthorised access with intent to commit a serious offence and unauthorised modification of data to cause impairment, shows you the potential impacts of cyber-attacks on the health sector.

Preventative measures to attack: The provisions concerning unauthorised access, modification, and impairment of data, as well as the possession or control of data with intent to commit a computer offence, can inform you about the types of cyber threats that need to be prevented in the health sector. Implementing measures to mitigate these risks can help prevent cyber-attacks.

Appropriate management of all personal data storage (GDPR): While the act does not specifically mention GDPR, the sections related to unauthorised access to restricted data and unauthorised impairment of data held on a computer disk can be relevant to ensuring appropriate management of personal data storage. Complying with these provisions can contribute to maintaining the security and integrity of personal data in line with GDPR requirements.

2. *The Privacy Act:*

The Privacy Act is a piece of federal legislation that has a primary purpose of protecting the privacy of individuals across Australia and gives instructions about how data needs to be collected, used, handled and stored by the Australian government agencies and businesses.

The main key points of the privacy act are:

- APPs (Australian Privacy Principles): there are 13 APPs in the act which includes standards, rights and instructions of how to handle, use and manage personal information.
- Outline the individual rights to access their information upon request and edit the information as they wish if there is any mistake in the information shown.
- The organisation must get a consent directly from the relevant individual before collecting and storing the information. Furthermore, any information must be collected by fair and lawful means.
- The personal information must be used or disclosed for the specific purpose it has been collected for, unless the individual agreed to have his information used by a secondary party.
- The data should be secured by taking the right steps to avoid unauthorised access, loss, modification or disclosure to unwanted third parties.
- The organisation needs to have transparency with its users regarding the up-to-date privacy policy for the user to know how they handle and manage his personal information.

Regarding the health sector, the privacy act is critical, as organisations in the health sector handle sensitive health information which should be accessed by the individual and authorised parties only.

The health sector has threats such as:

- Ransomware attacks which can encrypt essential data and demand a payment to decrypt it.
- Malware attacks which can disrupt health organisation operations.
- Phishing and social engineering against health sector employees which could trick them and lead to stealing credentials or install malicious software on the systems.
- Insider threats could use their privileges to access sensitive information, steal it and use it for malicious purposes.
- Outdated medical devices and healthcare systems could lead to vulnerabilities in the software which can be used later by an attacker.

- Medical devices which are connected to networks which are not secured properly could be exploited by an attacker and disrupt the operations or have sensitive data leaked.

Cyber-attacks on the health sectors could impact the operations and users by:

- Emergency services could be impacted and harm the patients who need the services immediately.
- Medical services could be impacted due to downtimes caused by the cyber-attack. Patient records might not be available to the patient who needs it at this specific time.
- Financial costs for ransom payments, recovery, IT stuff or legal fees as well as loss of revenue due to downtime or reputational damage.
- The customers might lose trust due to the damage of the reputation of the healthcare provider.
- The organisation might face legal and regulatory consequences such as fines and penalties by the government for not complying with the Privacy Act 1988. Also, patients could take legal actions after their sensitive data got leaked which can increase the costs and the damage of the reputation.

The privacy act 1988 does not focus on measures which could be taken to prevent and mitigate cyberattacks, however, it is focusing on the protection and management of personal information which could help to prevent data breaches if being followed correctly.
Data security is mentioned on APP 11 for the security of personal information such as in APP 11.1, 11.2 and 11.3.

- **11.1:** require the organisation to take the right measures to ensure the security of the personal information in use and consider whether it is permitted to retain personal information.
- **11.2:** if the organisation holding the personal information, it must protect it from misuse, loss, unauthorised access, modification or disclosure.
- **11.3:** destroying any personal information which is no longer in use to prevent it from being used or disclosed.

The steps the organisation should consider for implementing strategies needs to be related to the following:

- governance, culture and training
- internal practices, procedures and systems
- ICT security
- access security
- third party providers (including cloud computing)

- data breaches
- physical security
- destruction and de-identification
- Standards.

The privacy act is not mentioned in the GDPR (General Data Protection Regulation) from the European Union; however, they have many similarities such as data handling, transparency, concert from the user etc. International health sector organisations operating and using data in Australia and Europe must follow both the GDPR of the EU and the Australian Privacy Act.

ii. State Legislation

1. *Privacy & data protection.*

In Australia most states and territories have their own state level data protection legislation alongside legislation in place to protect other privacy that is applicable to state agencies and how they handle, process and distribute data of individuals. It is important to remember that a federal act always overwrites a state act. In this document I will be focusing more on the relevant key points for the health sector.

The threat to the health sector could be:

- Ransomware, malware and phishing attacks
- Unauthorised access
- Data breaches
- Insider threats

The threats above could lead to service disruption, data loss, privacy violations and financial costs.

State privacy legislation includes:

IPA Act - Information Privacy Act 2014 (ACT): Outline the steps which personal information is handled by the public sector agencies and some private sector businesses within the ACT. The health sector information requires to be handled more carefully under the IPA due to its sensitivity. The IPA has several APPs (Territory Privacy Principles) which give guidance about how to collect, use and manage personal information. There are some TPPs which more relevant to the health sector such as:

- **TTP 1 - Collection:** The health information must be collected after getting a consent from the individual. Only the relevant information should be collected for lawful purposes.
- **TPP 2 - Use and Disclosure**: The information must be used or disclosed for the exact use it was collected for, unless the individual gave his consent for further use, or it is required for legal purposes or public health emergencies.
- **TPP 3 - Data Quality:** The health information must be accurate, complete and up to date.
- **TPP 4 - Data Security:** Protecting data from misuse, loss, unauthorised access, modification or disclosure. Encryption and data controls should be in place.
- **TPP 5 - Openness:** The ways the information is handled and protected should be available to the public.

- **TPP 6 - Access and Correction:** Individuals must be able to access and correct their information at any time as they wish.
- **TPP 7 - Identifiers:** Do not give the permission to use unique identifiers unless necessary for the organisation's activities.
- **TPP 8 - Anonymity:** Give the option for individuals to remain anonymous when interacting with the organisation.
- **TPP 9 - Transborder Data Flows:** Any health information which needs to be transferred outside ACT should be protected as required within the ACT.
- **TPP 10 - Sensitive Information:** Sensitive information such in the health sector must be handled with extra care and have extra protection.

To prevent such threats and impacts in the health sector, it is important to follow **TPP 4** for data security, **TPP 9** - transborder data flows and **TPP 10** - sensitive information, which could help to protect the information of individuals and prevent those threats.

Some areas in the IPA align with the European GDPR. **TTP 1** - collection, **TPP 6** - access and correction and **TPP 9** - transborder data flows are ensuring data minimization, data accuracy, data security, access and correction and data transfer and are **like the GDPR** data minimization, accuracy principle, data protection by design and by default, data subject rights and international data transfer.

PDP Act - Privacy and Data Protection Act (VIC): The PDP does not apply directly to health information protection. There is the Health Records Act 2001 of Victoria which gives a specific instruction to the health sector, however, in this document we will discuss the PDP and find relevant points which could help the health sector protect privacy and data.

The PDP has **10 IPPs** which can help organisations to protect data and privacy.
IPP 4 talking about Data Security Requirements and Risk Management which must be implemented to protect personal information from being misuse, lost, unauthorised access, modification or disclosure with the preparation of risk assessments to be able to deal and respond to risks and cyber-attacks which could risk the personal data.
There are similarities between the EU GDPR and the PDP of Victoria. **IPP 1** talks about data minimization, **IPP 3** about data accuracy, **IPP 6** about access and correction, **IPP 5** about transparency and **IPP 4** about data security.

PPIP Act - Privacy and Personal Information Protection Act 1988 (NSW): Is an act which is designed to protect the privacy and the data of individuals in the public sector agencies within NSW. There are several principles divided between divisions in 8 parts. In this section we will write about the PPIP and find relevant points which could help the health sector to protect privacy and data.

In Part 2, Division 1, **section 12** of the PPIP (Retention and security of personal information), they are outlining the expectation of organisations when handling personal information. It is important to destroy any data which is no longer in use, to ensure the information is protected by using security tools that can prevent loss, unauthorised access, use, modification or disclosure, and against all other misuse. The act is not outlining the tools which need to be used and it is giving a general guidance about what an organisation should follow when structuring his security measures. **Section 9** is talking about using the data for lawful purposes only and **section 18** about limiting disclosure to ensure the privacy and the integrity of the data.

IPPI Act - Information Privacy Principles Instruction (SA): It is an act in South Australia which gives guidance about how to handle personal information across the state in the public sector agencies. It is not as detailed as the federal act. There are 10 principles under this act which can help to protect the health sector data.

IPP 4 is about storage and security which can minimise the risk of loss of sensitive data or unauthorised access in the health sector. By following the steps and implementing strong security protocols, such as encryption, IDS and conducting regular security assessments, the risk of a cyber incident could be minimised. Also, staff training, access controls and incident response plans could prevent such an event. There are similarities between the IPPI act and the European GDPR, such as collecting only necessary personal information, dispose of data which no longer require, have transparency about data handling and getting a consent from the user before storing his data.

PIP Act - Personal Information Protection Act 2004 (Tasmania): It is an act in Tasmania for keeping personal information safe in the public sector. On **Schedule 1** there are 10 principles which can help organisations to keep the personal information safe.

Principles 1 and 2 are talking about collecting only the necessary data which the organisation needs for its functions and activities and its lawful use with the consent of the user. Principle 4 is about data security to ensure that the organisations are taking reasonable steps to protect data for misuse, loss, unauthorised access, modification or disclosure and dispose of any data which is no longer needed. Preventing cyber incidents could be done by using encryption, firewalls and protocols along with employee training and incident response plans in place.

PIPP 1 - Collection, **PIPP 4** - Data Security and **PIPP 6** - Access and Correction are like the European GDPR which talks about data minimization, data accuracy and data security which can protect personal information.

IP Act - Information Privacy Act 2009 (Queensland): This is the privacy act in Queensland governs the management of personal information by the public sector agencies. On **schedule 3** of the act there are 11 principles that need to be followed to minimise the risks of cyber security incidents in the health sector.

The most relevant IPPs for preventing the threats in the health sector are:

- **IPP 1:** Collecting personal information in a lawful way.
- **IPP 2:** Always have a consent from the individual before storing the information.
- **IPP 4:** The most important principle for storage and security of personal information. The agency must ensure that all personal information is protected against loss, unauthorised access, use, modification, disclosure or any other misuse.
- **IPP 10:** Limiting the use of personal information for the purpose it was collected for, unless the individual agreed to use it for different purposes.

The act is aligning with the European GDPR for the management of personal data storage. Data minimization and accuracy on **IPP 1** and **IPP 3**, security of processing on **IPP 4**, Access and Correction rights on IPP 6 and lawful processing on **IPP 2**.

The Information Act 2002 of Northern Territory: Providing a framework for protecting personal information in the public sector, including health information, within the Northern Territory. On schedule 2 of the act there are 10 principles that need to be followed to minimise the risks of cyber security incidents in the health sector.

The most relevant IPPs for preventing the threats in the health sector are:

- **IPP 1:** Collecting only necessary personal information in a lawful way.
- **IPP 4:** The most important principle for storage and security of personal information. The agency must ensure that all personal information is protected

against loss, unauthorised access, use, modification, disclosure or any other misuse. Also, any data which is no longer needed must be destroyed.

- **IPP 9:** The organisation should not transfer personal information outside the territory unless it is required by the law, or the individual gave his consent for that.

IPP 1 - Collection, **IPP 4** - Data Security, **IPP 6** - Access and Correction and **IPP 9** - Transborder Data Flows are aligning with the European GDPR for data minimization, data security, access and correction rights and data transfers to ensure the appropriate management of all personal data storage.

PRIS Act - Privacy and Responsible Information Sharing Legislation (WA): currently (06.08.2024) the WA government is still working on this act in parliament. Once the bill passes, WA will have a privacy act like every other state across Australia.

II. Australian & International Mitigation Strategies

iii. Australian Signal Directorate

The Australian Signal Directorate (ASD) is an Australian agency for signals intelligence and cyber security. It operates under the control of the Australian Government and collaborates with Australian and international intelligence and security agencies. ASD's goal is to protect the country’s national interests and provide advice and assistance to Australian business and individuals.

1. *ASD Essential 8*

ACME Consulting employs Essential 8 to mitigate the risk of network infiltration or compromise, which could lead to data or services breaches, loss, or theft of client information that we host and manage.

The Essential Eight is a security framework created by the Australia Signals Directorate to keep organisations safe and build up strong defences against cyber threats. It outlines eight vital mitigation strategies:

- Patch applications
- Patch operating systems
- Multi-factor authentication
- Restrict administrative privileges
- Application control
- Restrict Microsoft Office macros
- User application hardening
- Regular backups

The implementation of the strategies to mitigate cybersecurity incidents requires assessing the current security posture of the organisation by identifying critical assets and using the

Essential Eight Maturity Model. ASD recommends implementing the framework in three phases (Maturity Level One/Two/Three) with a minimum of Maturity Level Three for cyber threat protection as baseline.

According to the experts, **Phishing** is the most prevalent cybersecurity threat in the healthcare sector. **Ransomware** attacks are an increasing threat for healthcare providers, typically injected into a system through a phishing attack. The sector experiences an unusually high number of **Data Breaches**, and **DDoS** attacks are forcing healthcare organisations offline and will only stop when a ransom is paid.

Defensive strategies to prevent attacks regarding Essential Eight:

Patch applications:

- It involves vulnerability scans to detect missing patches and security updates. Apply updates and fixes as soon as they are available and remove applications that are no longer supported by vendors.

Application control:

- It enables organisations to block all applications (including ransomware) from running on any device by default, allowing only the applications needed.

User application hardening:

- It focuses on protecting applications that interact with the web, like web browsers, PDF software, and Microsoft Office by setting strong configurations, such as blocking ads, restricting access to specific sites. It also includes disable unnecessary features and enables strict privacy settings.

Restrict Microsoft Office macros:

- This policy setting blocks the execution of macros in MS Office files originating from the internet.

- Microsoft Office macro security settings cannot be changed by users.

Defensive strategies to limit attack impact regarding Essential Eight:

Patch Operating Systems:

- It involves regularly checking for updates and analysing data to assess system vulnerabilities. It is important to test new patches before installation to ensure they are necessary and safe.

Restrict Administrative Privileges:

- Restrict access to certain applications, files and data to strengthen the organisation's defences. It enables more control by allowing that sensitive data is only available to those who need it.

Multi-Factor authentication:

- It is a security measure that requires verification of a user's identity by presenting at least two different forms of credentials before granting access to a system, application, or service. It offers greater security by protecting sensitive data, preventing unauthorised access, and regulatory compliance.

Defensive strategies to ensure Data Availability regarding Essential Eight:

Daily Backups:

- It requires regular backups for critical data, software and configuration settings. The framework specifies guidelines for accessing, modifying and deleting backups.
- ASD recommends using a third-party backup solution, and performing regularly tests so the backup solution can effectively restore the critical data, software and configuration settings.

DLP (Data Loss Protection):

Data Loss Prevention (DLP) is a set of policies and software applications. Its goal is to monitor the information in the system and avoid the possibility of data loss or breach for various reasons. There are three types of data that require special handling: intellectual property, corporate data and customer data.

Types of DLPs:

- **Network DLP**: it monitors network activity and traffic (such as emails and file transfers), to detect security policy violations. It logs access to sensitive data (who accessed it and where it moved), and it provides full visibility into all network data.

- **Endpoint DLP**: it monitors all network endpoints (such as servers, cloud storage, computers, laptops and different devices) to prevent data leakage, loss or misuse. It supervises where data goes and what happens to it.

- **Cloud DLP**: its primary focus is to maintain the confidentiality and security of data in the data warehouse. It is a type of surveillance service with an alarm.

Benefits:

- It keeps data in use, at rest and in transit safe.

- Endpoint data movement monitoring (it tracks and analyses the transfer of data within a network to prevent unauthorised data transfers).

- Vulnerability prevention (such as disclosure of sensitive information whether intentionally or by accident).

- It helps identify the source of the internal information leak when a data breach occurs.

- It mitigates financial risk linked to data loss or leaks, particularly regarding ransomware attacks.

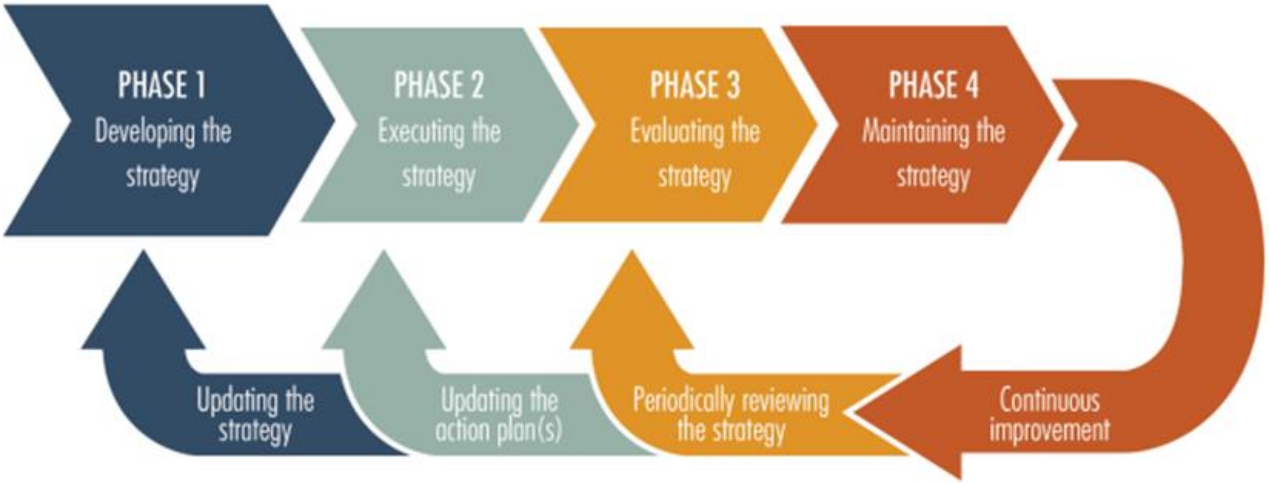
iv. International

1. ENISA (European Network and Information Security Agency)

The European Union Cyber Security Agency (ENISA) is a key entity in protecting the EU's digital infrastructure. Its main function is to promote cybersecurity, provide expert advice, develop guidelines and encourage collaboration between Member States and stakeholders on cybersecurity.

National Cyber Security Strategies (NCSS) are key documents for countries to outline strategic principles, guidelines, goals and specific actions to mitigate cybersecurity risks.

NCSS lifecycle

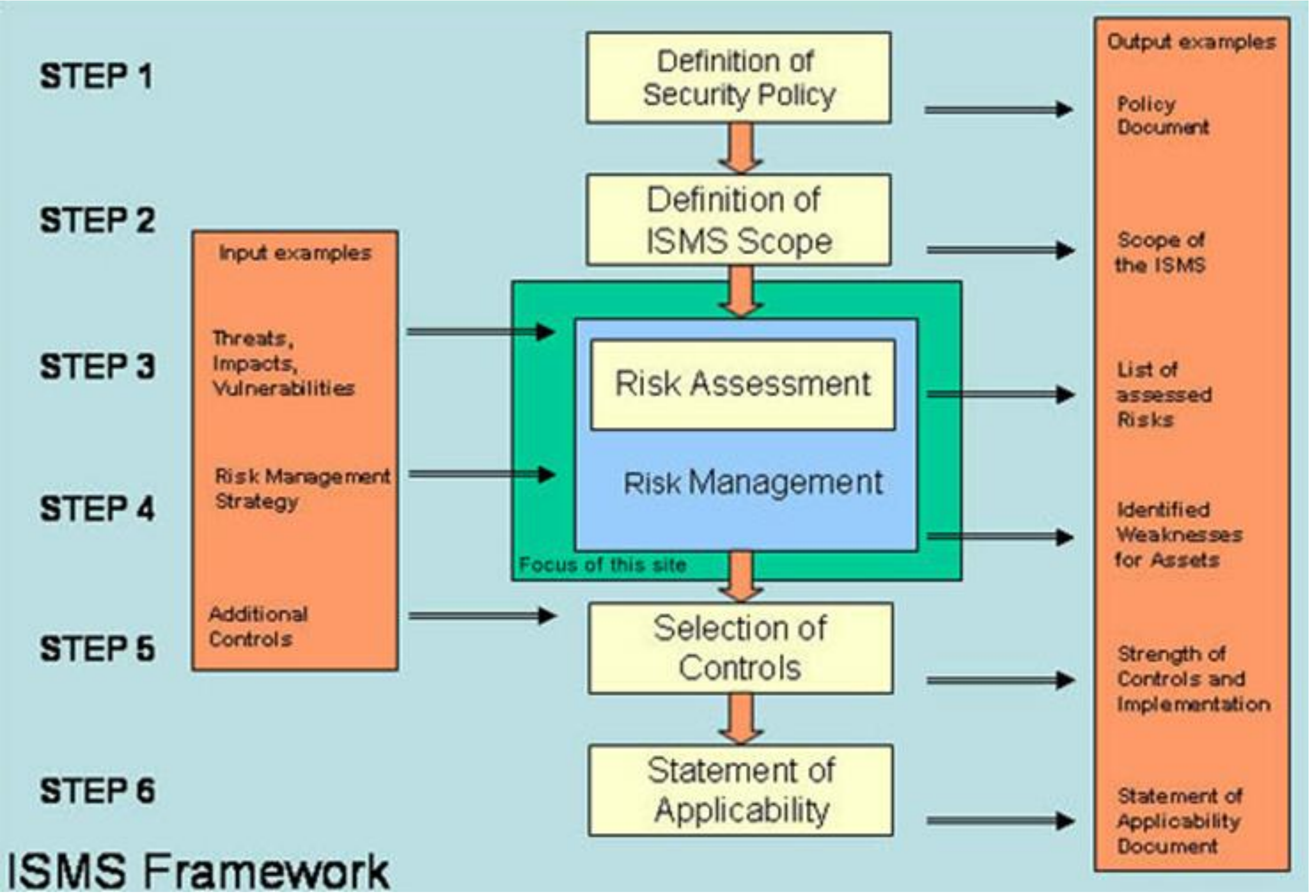


Source: ENISA

Baseline security measures establishment:

- Identify, analyse, and adopt appropriate security measures to manage the threats.
- Identify the information security threats and map these threats to the existing measures.
- Identify the gaps and derive mitigation measures from the existing technical standards (ISO 27000 family, PCI-DSS, CobiT).
- Update the baseline requirements based on reported incidents.

The Information Security Management System (ISMS) Framework:



Source: Brightspace

ENISA recommends implementing this framework to mitigate the impact of security threats and vulnerabilities that affect an organisation. To develop it, it is necessary to follow six steps:

Step 1: Definition of Security Policy (Policy Document): this document establishes the standards and procedures that an organisation must follow to protect its information systems and data (guarantee the confidentiality, integrity and availability of an organisation's critical information) and be prepared for possible cyberattacks.

Step 2: Definition of ISMS Scope: during this step it is clearly defined which systems, data and resources are covered by the policy and which are not.

Step 3-4: these steps are related to risk management. The intention of this process is to identify cybersecurity risks, their sources and how to mitigate them to an acceptable level of risk. An inventory of information assets, procedures and processes is established to understand which are the critical assets and which represent the greatest risk.

Step 5: Selection of Controls: this is a strategy used in any type of security to give greater depth to defences. Different control layers can be highlighted such as Physical security, Network security, Endpoint security, Application security and Data security.

Step 6: Statement of Applicability (SOA): it is a detailed report that identifies and describes the security controls selected to protect the organisation's information and systems and which ones have been decided to exclude along with their justification.

2. Cybersecurity Information Sharing Act of 2015 (CISA 2015)

The Cybersecurity Information Sharing Act is a U.S. federal law with the objective of enhancing cybersecurity by increasing the exchange of information about cyber threats. It enables the sharing of Internet traffic details between the U.S. government and technology and manufacturing companies. The law simplifies the process for companies to share personal data with the government in the context of cybersecurity issues. To protect privacy, the bill includes measures to ensure that personally identifiable information not related to cybersecurity is not shared.

Framework:

- CISA is applicable solely to information exchanged for cybersecurity purposes.
- CISA provides for two categories of information that may be shared:
    1- **Cyber Threat Indicators** (malicious reconnaissance, exploitation of vulnerabilities)
    2- Defensive Measures (programs to detect malicious activity, firewall rules, techniques for screening traffic for suspicious content)
- Personally Identifiable Information Must be Removed:
    1- Protected Health Information (medical records, lab reports)
    2- Human Resource Information (employee’s personal file, performance reviews)
    3- Consumer Information/History (purchases, preferences, credit)
    4- Education History (transcripts, training, certifications)
    5- Financial Information (bank statements, credit reports, insurance)
    6- Information Regarding Property Ownership
    7- Information Regarding Minor Children (under the age of 13)
- Information must be shared via a Department of Homeland Security (DHS) Sanctioned Method (Web forms, email submissions)

3. General Data Protection Regulation (GDPR)

GDPR is a law created by the European Union that guarantees the protection and privacy of user data. This law regulates the processing of data of individual EU users, which may include the collection, storage, transfer, use and even exclusion of such data. This law is applied to companies with and without physical presence in European territory. It is enough for the company's site to serve users in the Union for them to be subject to the regulations.

The regulation divides organisations into "controllers" and "processors". The first are organisations that hold the data, while the second are responsible for processing it by following the commands of the controllers.

GDPR determines seven elements that organisations must respect and follow when processing personal data (Art. 5):

- Transparency, Lawfulness and fairness (in relation to the data subject)
- Purpose limitation (specific data with specific intentions)
- Data minimization (information not related to the service offered is prohibited)
- Accuracy (keep personal data accurate and up to date)
- Storage limitation (keep data for as long as necessary and for the specified purpose)
- Integrity and confidentiality (ensure appropriate security: encryption – hashing)
- Accountability (data controller should be able to demonstrate GDPR compliance with all this principles)

Privacy rights for data subjects:

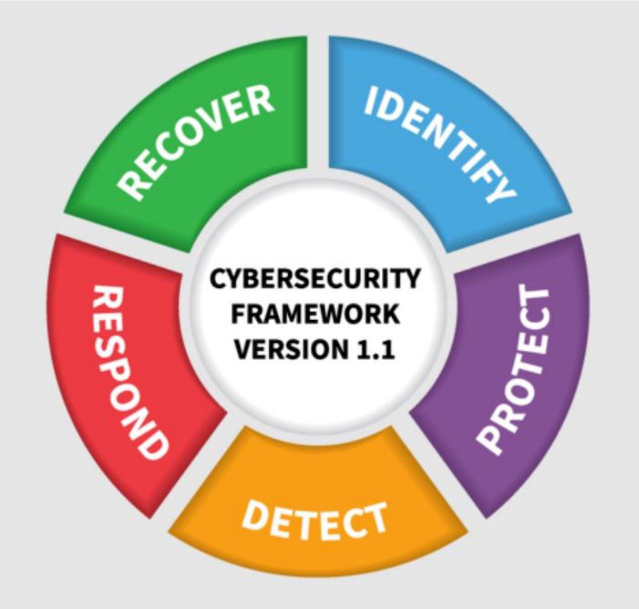
- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing

- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Data controllers and data processors must recognize and uphold these rights to ensure compliance.

III. Current Frameworks

v. NIST CSF

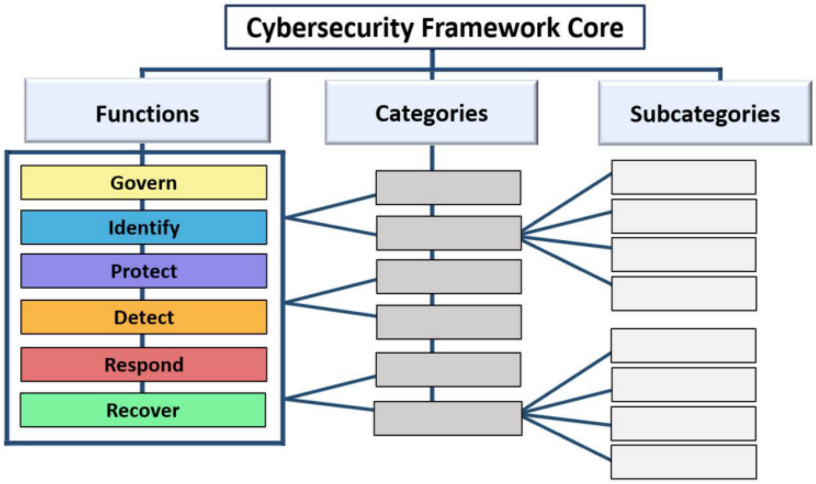


https://www.nist.gov/sites/default/files/styles/480_x_480_limit/public/images/2018/04/16/framework-01.png?itok=Ay5Aqe0J

NIST is a worldwide framework providing ways to manage and reduce cybersecurity risks. NIST CSF is relevant across various sectors, including the health sector, which handles sensitive data more than other sectors. This framework is for the use of individuals who are responsible for developing and leading cybersecurity programs, but also can be used by technology professionals, risk managers, lawyers, human resources specialists and cybersecurity and risk management auditors for instance. The CSF will address the cybersecurity risks with some other risks of the organisation, such as, financial, privacy, supply chain, reputational, technological or physical. While cybersecurity risks are expanding regularly, following this guidance will be valuable for any organisation and provide appropriate guidance over a long time.

An organisation can use the **CSF Core, Profiles and Tiers** to understand, assess, prioritise and communicate cybersecurity risks. The CSF is a flexible framework which can be used along with other frameworks, standards, guidelines and regulatory requirements.

The CSF Core is a set of cybersecurity outcomes which are arranged by function, category and finally subcategory. The outcome is not fixed, and every organisation could take its own actions to achieve its desired outcome based on its needs.



https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

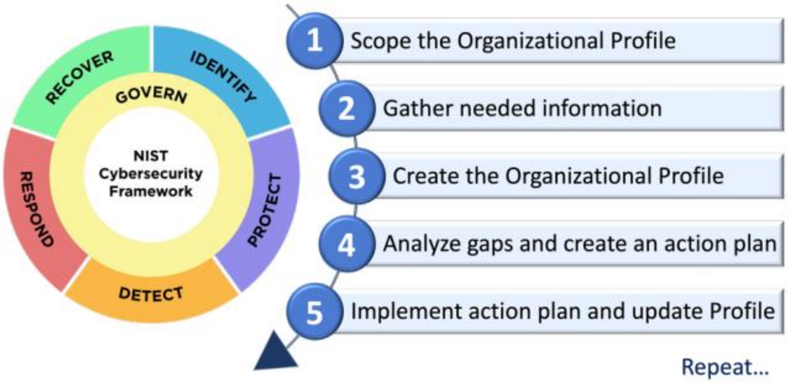
The CSF Core Functions are:

- **Govern (GV):** The organisation will decide which outcome to prioritise based on the context of its mission and the expectations of stakeholders. The Govern addresses the cyber security strategy of the organisation including its policies, roles and responsibilities.
- **Identify (ID):** Understanding the current cybersecurity risks of the organisation and its assets, such as data, hardware, software, systems, facilities, services and people. This can help to prioritise the right risk management strategies to keep the organisation safe.
- **Protect (PR):** Have appropriate safeguards in place to ensure a safe delivery of critical services and protect them from cybersecurity incidents by having access control in place, awareness and training, data security, information protection, maintenance and security technologies and platforms.
- **Detect (DE):** To monitor the systems to identify cybersecurity events so the organisation can mitigate them on time with proper incident response plans and recovery activities on the next phases.
- **Respond (RS):** After detecting a cybersecurity event it is important to have a response plan in place for every risk to be able to mitigate the incident as soon as possible.
- **Recover (RC):** After mitigating the incident, there should be a recovery plan in place to be able to restore systems which got affected by the cyber incident, to update the recovery plan for future incidents and communicate with the public to maintain trust.

All functions above have a critical role in a cybersecurity incident, and it should be ready at all times for any incident which might occur.

The CSF Profiles represents the current or the targeted (desired) cybersecurity posture of the organisation in relation to the Core's outcomes. The CSF Profiles checks the alignment of standards, guidelines and practices with the organisation's requirements, risk tolerance and resources available. It is important to view the current profile of the business and find gaps to prioritise the actions which need to be taken to improve the cybersecurity posture of the business and implement the new plan of the updated profile.

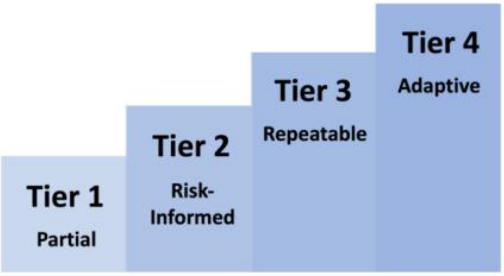
there are 5 phases that should be taken to create a profile:


RECOVER
IDENTIFY
GOVERN
NIST
Cybersecurity
Framework
RESPOND
PROTECT
DETECT
1 Scope the Organizational Profile
2 Gather needed information
3 Create the Organizational Profile
4 Analyze gaps and create an action plan
5 Implement action plan and update Profile
Repeat…

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

The CSF Tiers have 4 tiers which give an overview about the current profile of the organisation, but it can be used to define the desired tier which the organisation wishes to achieve. The tiers are based on how the organisation views its cybersecurity risks and the practices in place to avoid and mitigate them.

The tiers are:



https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Due to the sensitivity of the data the health sector handles, Tier 4 should be the desired tier for this sector. Tier 4 is showing that the organisation has a mature, adaptive approach to managing cybersecurity risk with a continuous improvement.

The NIST CSF focuses on the importance of governance to ensure that policies and procedures are in place to protect personal data like the European GDPR, also the protect (PR) function aligns with the GDPR requirement of the protection and the handling of personal data with strong access controls and preventing measurements.

vi. ISO/IEC 27001

ISO/IEC 27001 is an international standard for information security management system (ISMS) which is critical in any business in today's world including those in the health sector. Following those standards can help the organisation to establish, implement, maintain and improve the ISMS.

The ISMS is flexible to the organisational needs and gives comprehensive policies, procedures and controls to manage and mitigate risks in information security. There are few key aspects to be followed:

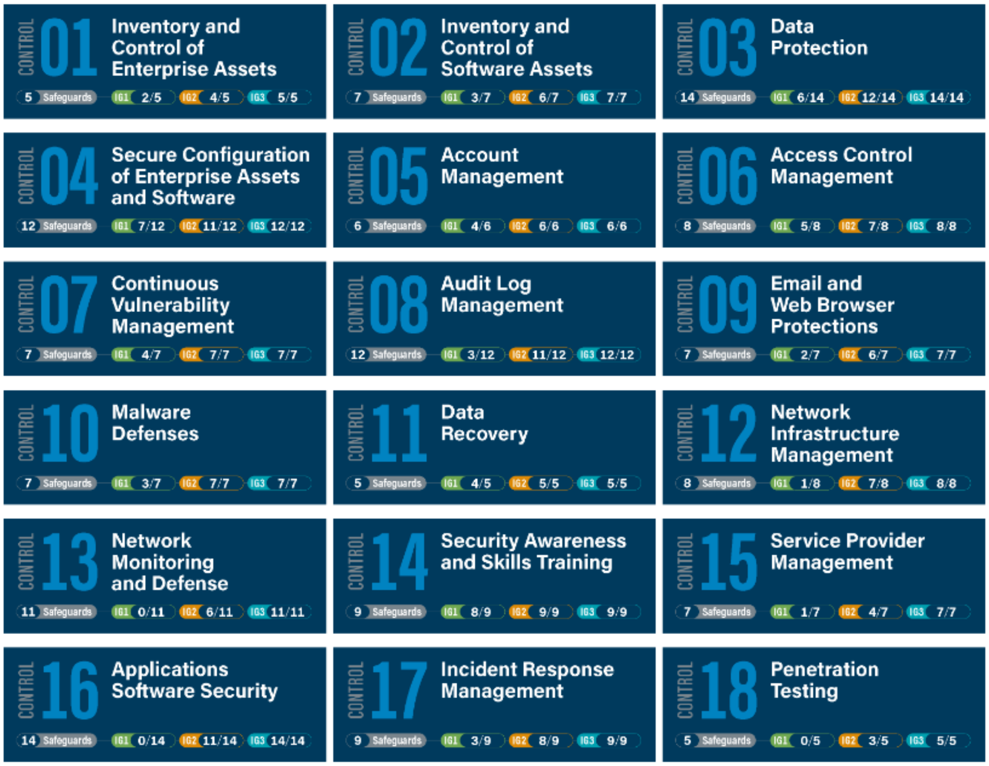
- **Risk Management:** assessing the security risks regularly to be able to identify the threats, vulnerabilities and impact of the risks by conducting a risk assessment and identify the potential risks to the confidentiality, integrity and availability of the data. Then, based on the risk assessment, the organisation will need to implement controls and have mitigation strategies in place for any risk which may occur. The controls could be selected from the standard's Annex A which gives a variety of security controls as you can view in the next section.
- **Annex A - Security Controls:** giving a list of controls to be implemented by the organisation to protect information, such as cryptography, physical security, communications security and incident management for instance.
- **Ongoing Improvement:** Following the Plan-Do-Check-Act (PDCA) for establishing policies and processes for risk management, implement it, monitor and review the performance of the ISMS regularly and take actions based on the results to ensure the ongoing protection.
- The organisation could choose to have a **certificate** to show that the business is following this standard and enhance more customer trust along with showing a strong compliance with legal and regulatory requirements.
- Following this standard can also support the implementation of **other standards such as GDPR, HIPAA or PCI-DSS** which could improve even more the compliance of the organisation with the legal and regulatory requirements.

This standard is critical for the health sector, as it can prevent cyber security incidents which are related to the health sector, such as malware, phishing attacks, unauthorised access or insider threats. It forces strong access controls, ensures improvement, minimises risks and helps with the recovery after an incident which can ensure the ongoing operation of the business along with protecting the sensitive data of it.

vii. CIS Controls

The CIS controls (Centre for Internet Security Controls) are a set of guidelines and controls which are designed to help organisations to improve their cybersecurity posture. The CIS is a nonprofit organisation, and it focuses on more practical aspects and the prioritised actions needed to be taken to defend the business against cyber threats.

As shown in the figure below, there are 18 controls to be followed with a variety of safeguards.


CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5
CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7
CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12
CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6
CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8
CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7
CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12
CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7
CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7
CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5
CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8
CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11
CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9
CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7
CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14
CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9
CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

https://www.cisecurity.org/controls/implementation-groups

In this document we will be focusing on the important controls in the health sector.

To avoid cybersecurity threats in the health sector we need to focus on the following controls:

- **Control 1 - Inventory and Control of Enterprise Assets:** Managing all assets including end-user devices, network devices, servers and IoT devices which are connected to the infrastructure in any physical, virtual or remote way, to be able to monitor them and identify unauthorised or vulnerable assets which could be targeted by threats.

- **Control 2 - Inventory and Control of Software Assets:** Making sure all softwares installed is approved and secured to reduce risks of malware infections.
- **Control 14 - Security Awareness and Skills Training:** Humans can be vulnerable to threats, such as phishing and harm the systems and the data even more than other cyber threats. The right education and awareness could reduce the risks of a cybersecurity event dramatically with the right human behaviour.

The impact of a cybersecurity event could be minimised by following the following controls:

- **Control 5 - Account Management:** Managing the accounts well with strong authentication methods to prevent unauthorised access to sensitive information.
- **Control 13 - Data Protection:** Having strong encryption and data protection to avoid data leak or minimise the impact.
- **Control 17 - Incident Response Management:** Having an incident response plan in place to allow the healthcare organisation to contain and mitigate cyber-attacks as soon as possible and to minimise its impact

Preventing such of incidents could be done by the following controls:

- **Control 7 - Continuous Vulnerability Management:** Scanning the systems regularly and trying to identify vulnerabilities before an attacker exploiting them.
- **Control 4 - Secure Configuration of Enterprise Assets and Software:** Ensuring all configurations in the systems and software are secured and following best practices to reduce the risks of an attack.
- **Control 12 - Network Infrastructure Management:** Having a proper management of network devices in place, such as firewall, routers and subnets to prevent network-based attacks.

As with most frameworks and standards there are similarities between the European GDPR and CIS controls. GDPR gives a guideline regarding data minimization, data accuracy, data security and data subject rights, while some of the CIS controls giving a guideline about how to handle and protect sensitive data in the health sector. Some of the controls with similarities to the GDPR are:

- **Control 1 - Inventory and Control of Enterprise Assets:** Managing all assets including end-user devices, network devices, servers and IoT devices which are connected to the infrastructure in any physical, virtual or remote way, to be able to monitor them and identify unauthorised or vulnerable assets which could be targeted by threats.
- **Control 2 - Inventory and Control of Software Assets:** Making sure all software installed is approved and secured to reduce risks of malware infections.

- **Control 5 - Account Management:** Managing the accounts well with strong authentication methods to prevent unauthorised access to sensitive information.
- **Control 8 - Audit Log Management:** Collect and review log events which can detect unauthorised access to sensitive data.
- **Control 13 - Data Protection:** Having strong encryption and data protection to avoid data leak or minimise the impact.

IV. Good Practice Frameworks

i. COBIT

1. What is COBIT?
   It is a framework focused on IT governance, aimed at managing and controlling IT assets to ensure alignment with business objectives. The current version of BOCIT (COBIT 2019) is a framework for developing, implementing, monitoring, and improving IT governance and management practices. It supports organisations in managing IT risks and measuring performance. COBIT encompasses over 40 IT management processes, provides a matrix linking business and IT goals, and uses a maturity model to evaluate process performance. Primarily used for auditing and regulatory compliance, COBIT emphasises the alignment between IT and business, with a strong focus on security, risk management, and governance.

2. COBIT 2019 6 Governance System Principles and 3 Governance Framework Principles.

   a) Governance System Principles

   i) Deliver Value to Stakeholders

   ii) Comprehensive Perspective: IT governance is connected to every part of the organisation and considers all elements comprehensively.

   iii) Adaptable Governance to meet changing environments and demands.

   iv) Separation of Governance and Management

   v) Tailored to Organisational Requirements according to an organisation's characteristics and needs.

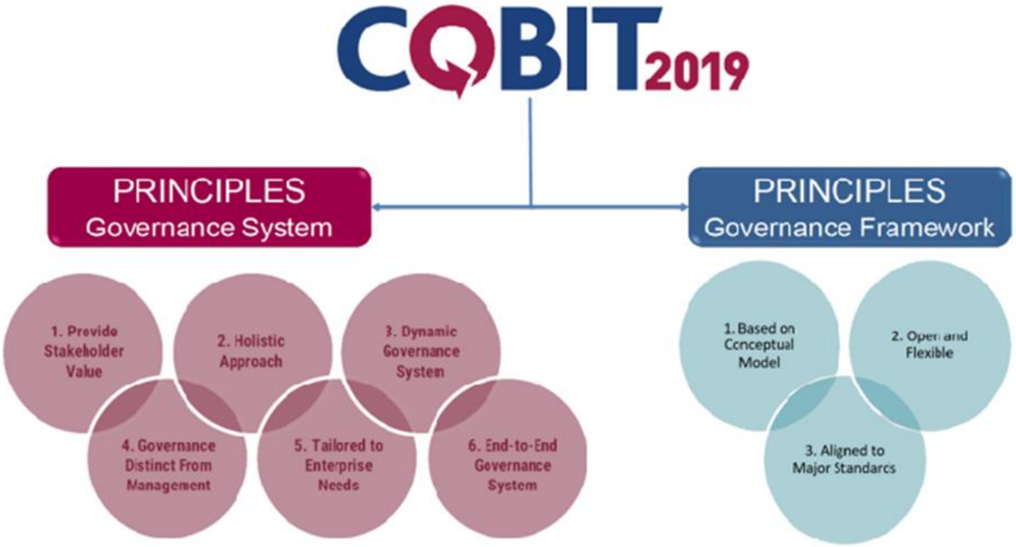
   vi) Comprehensive Governance Framework: It encompasses all IT activities within an organisation.

   b) Governance Framework Principles.

   i) Based on Conceptual Framework

ii) Inclusive and Adaptable Framework to various organisations.

iii) Aligned to Major Standards: e.g. ITIL 4, ISO/IEC 27001, ISO/IEC 38500, ISO/IEC 20000.


COBIT 2019
PRINCIPLES
Governance System
PRINCIPLES
Governance Framework
1. Provide Stakeholder Value
2. Holistic Approach
3. Dynamic Governance System
4. Governance Distinct From Management
5. Tailored to Enterprise Needs
6. End-to-End Governance System
1. Based on Conceptual Model
2. Open and Flexible
3. Aligned to Major Standards

https://www.researchgate.net/figure/COBIT-2019-Principles-COBIT-2019-is-a-Framework-issued-by-the-ISACA-association-an_fig4_375554316

3. COBIT structure

COBIT structure is crucial because it aligns IT with business goals, ensuring IT supports business strategy and enhances overall performance. It optimises resource usage, reduces costs, minimises risks, and helps meet legal and regulatory requirements. COBIT structure consists of the following three key elements: Business requirements, IT resources and IT processes.

a) Business requirements

i) Effectiveness

ii) Efficiency

iii) Confidentiality

iv) Integrity

v) Availability

vi) Compliance

vii) Reliability

b) IT resources

i) Applications

ii) Information

iii) Infrastructure

iv) People

c) IT processes

i) Domains

(1) APO: Align, Plan and Organise

(2) BAI: Build, Acquire and Implement

(3) DSS: Deliver, Service and Support

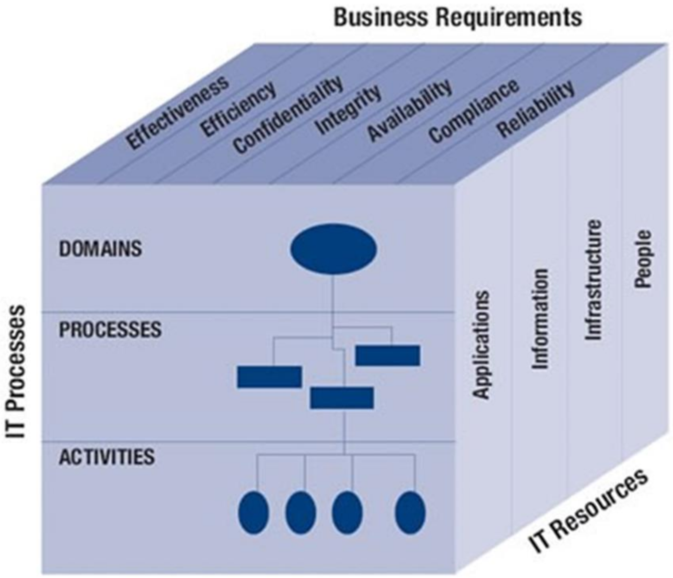
(4) MEA: Monitor, Evaluate and Assess

(5) EDM: Evaluate, Direct and Monitor

ii) Processes

Various 40 processes under sub-domains.

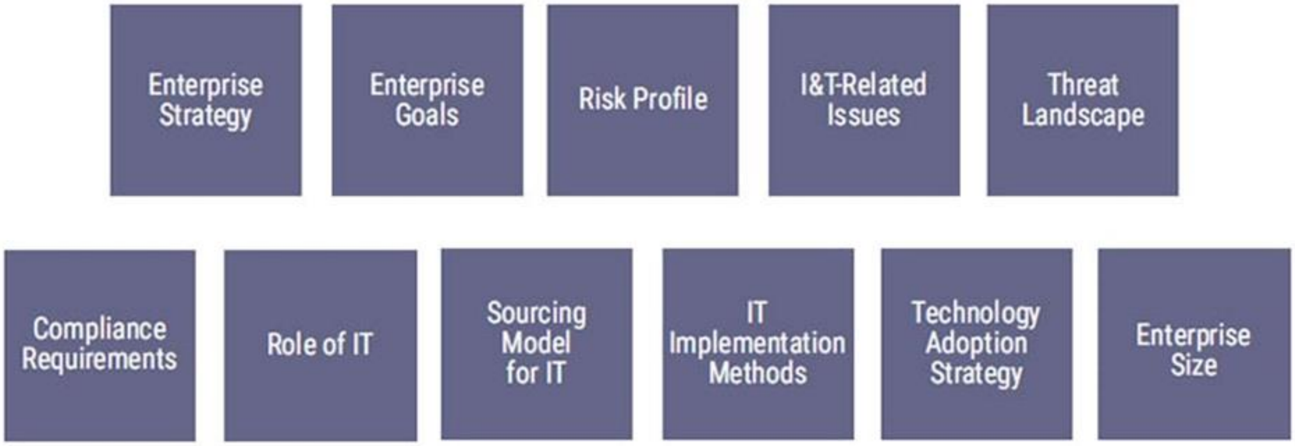
iii) Activities



https://www.bmc.com/blogs/cobit/

4. Design Factors

In COBIT 2019, the concept of enablers was removed for simplification and replaced by Design Factors. Design Factors are elements to consider when designing an IT governance system for an organisation, helping to tailor the system according to the organisation's needs and environment.

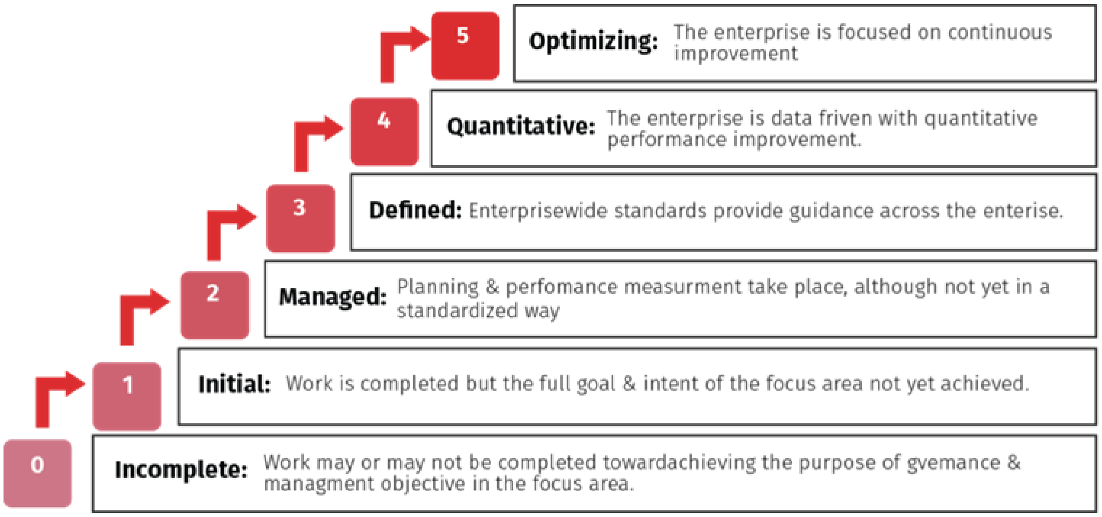


https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

5. Effort for continuous improvement

a) COBIT Performance Management (CPM, Maturity Model)

It describes capability levels and maturity levels from 0 to 5. At Level 0, processes are non-existent or ad hoc, lacking any structured approach. Level 1 represents initial stages where processes are unpredictable and reactive. Level 2 is characterised by repeatable processes that are documented but still largely reactive. At Level 3, processes become defined and standardised across the organisation. Level 4 sees processes being managed and measured with quantitative performance indicators in place. Finally, Level 5 represents optimised processes that are continuously improved through feedback and innovation. This maturity model helps organisations assess their current state and identify areas for improvement.



Optimizing: The enterprise is focused on continuous improvement

Quantitative: The enterprise is data friven with quantitative performance improvement.

Defined: Enterprisewide standards provide guidance across the enterise.

Managed: Planning & perfomance measurment take place, although not yet in a standardized way

Initial: Work is completed but the full goal & intent of the focus area not yet achieved.

Incomplete: Work may or may not be completed towardachieving the purpose of gvemance & managment objective in the focus area.

https://www.businessbeam.com/consulting/capability-assessment-and-performance/

b) Utilise an open-source model
To identify potential improvements, examine feedback from communities.

c) COBIT online training, documentation on specific areas

6. Case study

The case study titled “Information and Communications Technology study of Public Health Institutions in Mexico” explores the impact of ICT on Mexico’s public health sector and utilises COBIT frameworks, particularly regarding the governance and management of IT resources. COBIT is referenced in relation to improving the strategic alignment and performance of ICT systems within the health sector. The study highlights how COBIT principles helped address challenges such as inadequate IT infrastructure and lack of standardised processes. For example, they implemented the APO (Align, Plan, and Organise) domain, which means creating a clear plan for IT investments, such as improving electronic health records and patient management systems.

By implementing COBIT practices, the institutions were able to better align their ICT strategies with organisational goals, ensure more efficient use of resources, and improve overall IT governance. The framework provided a structured approach to assess and enhance ICT management, ultimately leading more effective and reliable public health services.

https://www.isaca.org/resources/news-and-trends/industry-news/2014/information-and-communications-technology-study-of-public-health-institutions-in-mexico

ii. ITIL

1. What is ITIL?

The ITIL (Information Technology Infrastructure Library) framework was developed by the Central Computer and Telecommunications Agency (CCTA) in the UK during the 1980s, and focuses on IT service management, providing guidelines for effectively delivering, managing IT services, and reducing cost. It aims to enhance the quality and efficiency of IT services, offering guidelines across the service life cycle, which includes service strategy, design, transition, operation, and continual improvement, and covers various functions within IT organisations, such as the service desk, technical management, and application management. It clearly defines roles and responsibilities for each process and function. Primarily used for service delivery and management, ITIL emphasises customer-centric services and aims for continual service improvement. Key areas of allocation include IT service desk operations, problem management, incident management, and the continual improvement of IT services. The current version, ITIL 4 emphasises a flexible, value-driven approach and integrates modern methodologies like Agile and DevOps. Additionally, the ITIL certification path starts with the Foundation level and progresses to advanced modules like ITIL Managing Professional (MP) and ITIL Strategic Leader (SL), equipping professionals to effectively implement and manage ITIL practices.

2. ITIL 4 Key Components

a. Service Value System (SVS)

The SVS illustrates how an organisation’s various components and activities collaborate to create value through IT-enabled services. These elements can be combined flexibly, necessitating integration and coordination to maintain organisational coherence. The ITIL SVS aids in this integration and coordination, offering a robust, unified, value-driven direction for the organisation.

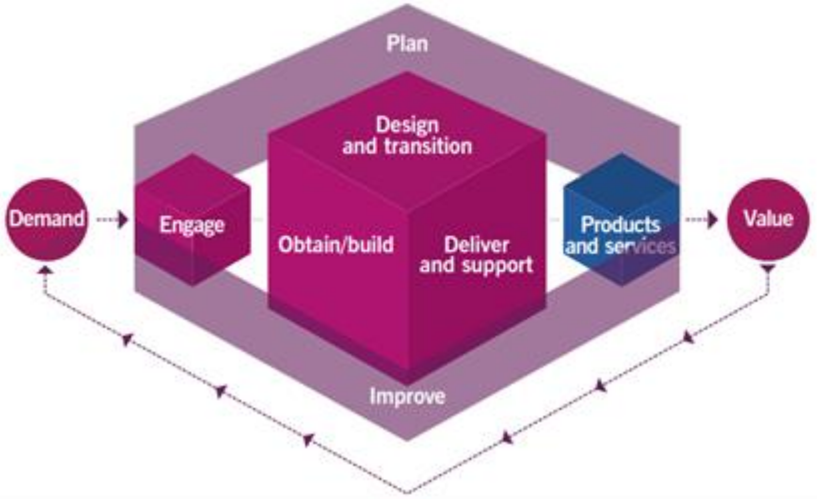
The core components of the ITIL SVS are SVC, ITIL Practices, ITIL guiding Principles, Governance, Continual Improvement, Certificate Scheme

I. The ITIL Service Value Chain (SVC):

This outlines an operational framework for developing, delivering, and continuously enhancing services. It specifies six essential activities that can be integrated in various combinations to create different value streams.

The main activities of the SVC are as follows:

1. Plan
2. Improve
3. Engage
4. Design and Transition
5. Obtain/Build
6. Deliver and Support



https://www.itsmf.co.uk/wp-content/uploads/2020/11/Introductory-Overview-of-ITIL4.pdf

b. Four Dimensions Model:

- Organisations and People:
  It focuses on the organisational structure, culture, and people involved in delivering and managing services, ensuring they have the right skills and roles.

- Information and Technology:
  It encompasses the information, knowledge, and technologies needed to deliver services, including data management and IT infrastructure.

- Partners and Suppliers:
  It looks at the relationships with external parties, including suppliers and partners, and how they support service delivery

and management.

- Value Streams and Processes:
  It examines how activities and workflows are organised to create value, focusing on optimising processes and ensuring efficient value streams.

c. Continual Improvement

d. The ITIL 4 certification scheme

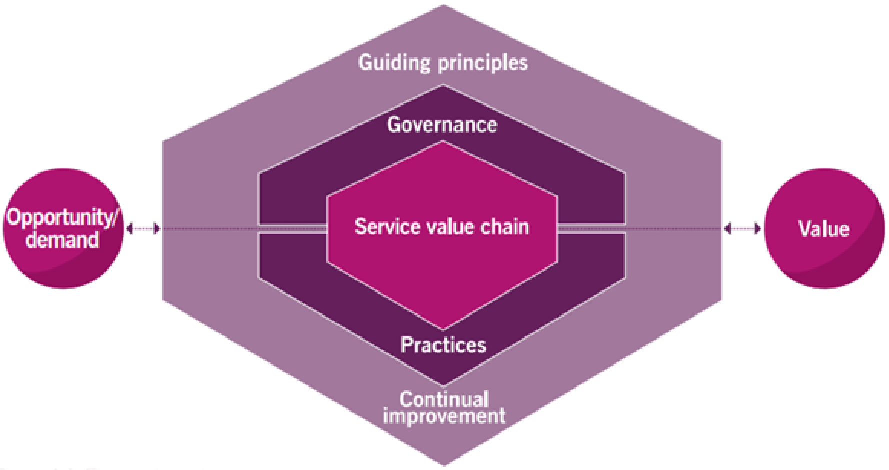


Figure 1.1 The service value system
https://www.itsmf.co.uk/wp-content/uploads/2020/11/Introductory-Overview-of-ITIL4.pdf

3. Core ITIL 4 Practices
The ITIL 4 framework includes a comprehensive set of practices designed to help organisations manage IT services effectively. These practices are categorised into 3 concepts: Service Management Practices, General Management Practices, and Technical Management Practices. Each category addresses different aspects of IT service management to ensure that services are delivered and maintained efficiently.

a. Service Management Practices

I. Availability Management

ii. Business Analysis

iii. Capacity and Performance Management

iv. Change Control

v. Incident Management

vi. IT Asset Management

vii. Monitoring and Event Management

viii. Problem Management

ix. Release Management

x. Service Catalogue Management

xi. Service Configuration Management

xii. Service Continuity Management

xiii. Service Design

xiv. Service Desk

xv. Service Level management

xvi. Service Request Management

xvii. Service Validation and Testing

b. General Management Practices

i. Architecture Management

ii. Continual Improvement

iii. Information Security Management

iv. Knowledge Management

v. Measurement and Reporting

vi. Organisational Change Management

vii. Portfolio Management

viii. Project Management

ix. Relationship Management

x. Risk Management

xi. Service Financial Management

xii. Strategy Management

xiii. Supplier Management

xiv. Workforce and Talent Management

c. Technical Management Practices

i. Deployment Management

ii. Infrastructure and Platform Management

iii. Software Development and Management

4. Case Study

Title: ITIL Adoption in Healthcare: A Study Of Process Impact At A New England Hospital

Author: Dawn Almeida, Regis University

This paper investigates how New England Hospital implemented ITIL to improve service management. ITIL provides a framework for aligning IT services with business needs and enhancing service quality. The hospital adopted ITIL to address issues with inefficient, ad-hoc processes, and the study analyses the impact of ITIL adoption on service quality and alignment with organisational needs, as well as the barriers encountered during implementation. Using action research, the study collected data through observations and unstructured interviews in the IT department. Before ITIL, the hospital's knowledge management processes were decentralised with inadequate updates and maintenance, and no document approval procedures. After implementing ITIL, improvements included document integration and adoption led to systematic management of IT assets and software, consistent incident management, and improved information collection and communication. However, challenges such as staff training, departmental culture, lack of executive support, and project time constraints were noted. The study highlights that while ITIL adoption enhances IT service quality, there are still significant challenges, and there is a need for further research on ITIL adoption in different stages and various healthcare institutions.

https://epublications.regis.edu/cgi/viewcontent.cgi?article=1796&context=theses

V. Key Incident Response Strategies

i. NIST Incident response plan (NIST SP 800-61r2)

NIST Incident response plan provides a guide for computer security incident response, emphasising the importance of having an effective response capability due to the increasing number and variety of cybersecurity attacks. Incident response is essential for quickly detecting incidents, minimising losses, mitigating exploited vulnerabilities, and restarting IT services. The guide primarily targets federal agencies, outlining the requirements and recommendations for creating and maintaining an effective incident response capability.

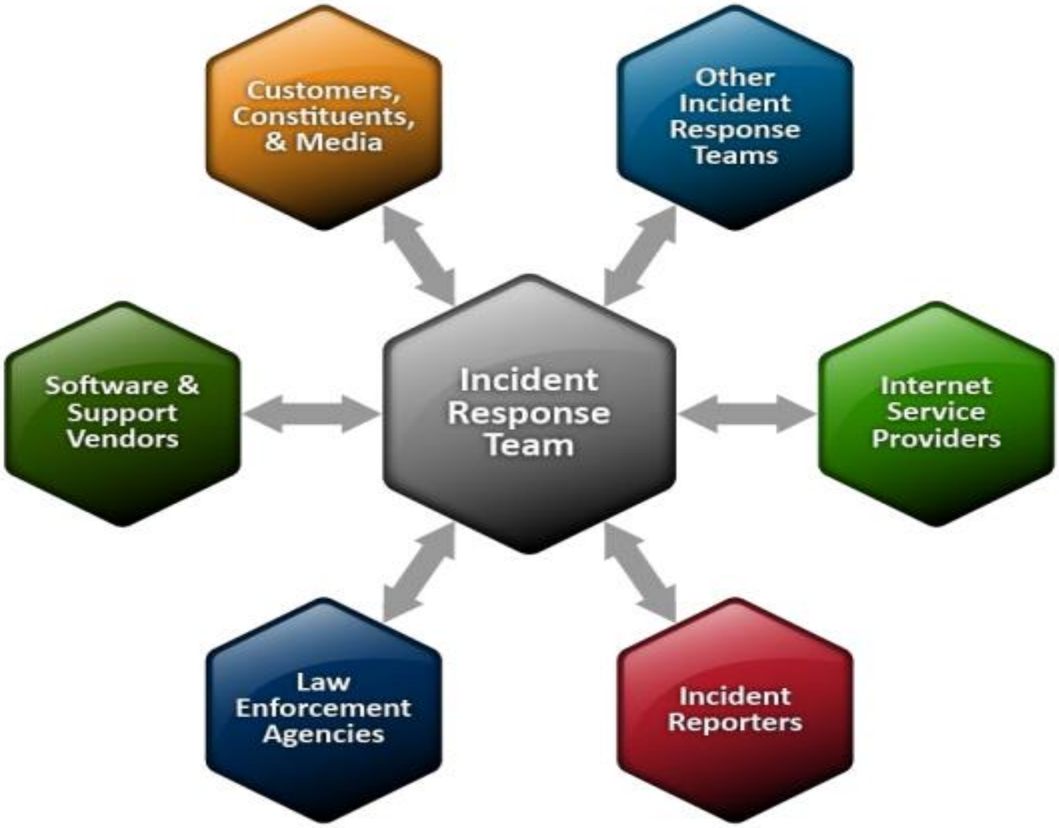
Key points include:

1. Establishing Incident Response Capability: It involves creating an incident response policy and plan, developing handling and reporting procedures, setting communication guidelines with external parties, choosing a team structure, establishing relationships with internal and external groups, determining the services to be provided, and staffing and training the response team.
   Standard Operating Procedures (SOPs) outline the detailed technical processes, methods, checklists, and documentation utilised by the incident response team to minimise any errors due to stressful incident handling circumstances.

2. Incident Prevention: Organisations should secure networks, systems, and applications to reduce the frequency of incidents. Prevention is more cost-effective and efficient than reacting to incidents. This includes training IT staff on security standards and educating users about proper use of systems.

3. Communication with External Parties: Organisations should document guidelines for communication with external entities such as other response teams, law enforcement, the media, ISPs, and the vendors related to the incident, ensuring that only appropriate information is shared. Otherwise, information about incidents may be leaked to unrelated parties, and it causes additional adverse impact on the organisation. When discussing with the media about incidents, organisations often find it useful to appoint a primary point of contact (POC) along with at least alternate contact. To effectively prepare designated contacts and others who may interact with the media, it is advised to conduct training sessions focused on media communication during incidents, highlighting the importance of protecting sensitive information. Additionally, ensure that a current status update on the incident is consistently maintained, remind all staff of the established procedures for managing

media inquiries, and incorporate simulated interviews and press conferences into incident response drills to enhance readiness.


Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

Communications with outside parties

4. Handling Common Attack Vectors: Organisations should focus on being prepared to handle incidents related to common attack vectors such as external media, web-based attacks, email threats, improper usage by authorised users, and loss or theft of equipment.

5. Incident Detection and Analysis: Automation is crucial for analysing vast amounts of data from logs and security software. Organisations should establish logging standards and regularly review the collected data to ensure effective incident defection. By utilising automation, it supports responding to incidents systematically and helps with legal issues that may arise.

6. Prioritising Incidents: Incidents should be prioritised based on their impact on business functions, information security, and the resources needed for recovery.

7. Law Enforcement: To ensure that security incidents result in convictions, the Australian Federal Police (AFP) and the Australian Cyber Security Centre (ACSC),

state police, and local authorities, can investigate incidents. International law enforcement may also become involved if attackers affect locations outside Australia. Incident response teams should proactively engage with local law enforcement to understand the reporting process, evidence collection requirements, and appropriate methods for gathering evidence.
Organisations should designate a POC to communicate with law enforcement, following legal and procedural guidelines. To avoid jurisdictional conflicts, organisations should contact only one agency and be aware of potential jurisdictional issues.

8. Learning from Incidents: After handling major incidents, organisations should hold lessons learned meetings to improve the incident handling process and address systemic weaknesses. These meetings can also help train new team members and refine future response strategies. Once an organisation establishes a plan, at least annual review should be conducted to ensure if the organisation adheres to the roadmap for maturing the capability and successfully reach their desired goals.

Incident Response Team structure

The effectiveness of the incident response team relies on the active involvement and collaboration of people across the organisation.

Organisations can choose between two main incident response models:

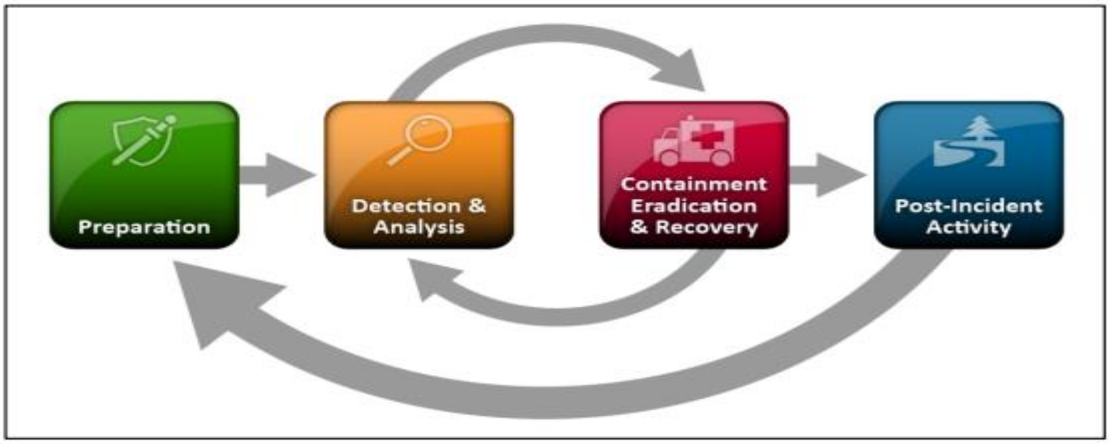
1. The Central Incident Response Team involves a single team handling all incidents, which is effective for smaller organisations or those with minimal geographic spread.
2. Distributed Incident Response Teams model assigns multiple teams to different segments of the organisation, making it suitable for larger organisations or those with significant computing resources across various locations.

Incident response team involves in three staffing models:

1. Employees:
2. Partially Outsourced
3. Fully Outsourced

Incident handling procedures

The incident response process has 4 phases: Preparation, Detection and Analysis, Containment, Eradication, and Recovery, and Post-Incident Activity. While processes generally follow a sequential order, there are instances where activities cycle back to earlier phases. For instance, when eradicating a malware incident, it might be required to revisit the detection and analysis phase to check if other hosts have been affected.



Incident Response Life Cycle

1. Preparation (Establishing an incident response capability)
    a. Contact information
    b. On-call information
    c. Issue tracking system and resources (e.g. Port lists, Documentation for software, network topology, current baselines, cryptographic hashes)
    d. Smartphones
    e. Encryption software
    f. War room
    g. Secure storage facility
    h. Incident analysis hardware (e.g. Laptops, Forensic workstations, backup devices, spare servers, and virtualized equipment)
    i. Incident analysis software (e.g. Packet sniffers, protocol analysers, and forensic software)
    j. Jump kit for investigation
    k. Maintain recommended practices (e.g. Periodic Risk Assessment, Host security, Network security, Malware prevention, and User Awareness and Training)

2. Detection and Analysis
    a. Attack Vectors (e.g. Removable Media, Web, Email, Impersonation, and Loss of equipment)
    b. Signs of an Incident

i. Precursors: signs before an attack happens
ii. Indicators: evidence observed after an attack has occurred or is occurring.
iii. Source: IDPs, SIEMs, Antivirus and antispam software, File integrity checking software, Third-party monitoring services, Logs, publicly available information, People within the organisation or other organisation.

c. Incident Analysis (processes to analysis an incident)
i. Measure and Understand Normal Behaviours
ii. Create a Log Retention Policy
iii. Perform Event Correlation
iv. Keep All Host Clocks Synchronised
v. Maintain and Use a Knowledge Base of Information
vi. Use Internet Search Engines for Research
vii. Run Packet Sniffers to Collect Additional Data
viii. Filter the Data
ix. Seek Assistance from Others

d. Incident Documentation
i. Logbook, laptops, audio recorders, and digital cameras.
ii. Documenting system events, conversations, and observed changed in files
iii. Must be dated and signed by the incident handler

e. Incident Prioritization
i. Based on relevant factors
ii. Rating functional impact (None, Low, Medium, and High)
iii. Rating Information impact (None, Privacy Breach, Proprietary Breach, and Integrity Loss)
iv. Rating recoverability effort (Regular, Supplemented, Extended, and Not Recoverable)

f. Incident Notification
CIO, Head of information security, Security officer, other incident response teams, System owner, Human resources, public affairs, Legal department, ACSC, Law enforcement

3. Containment, Eradication, and Recovery
a. Choosing a Containment Strategy
i. Redirect the attacker to a sandbox
ii. Duration of the solution

Solution Type	Description	Removal Time
Emergency Workaround	An immediate response to address urgent issues (system downtime)	Within 4 hours
Temporary Workaround	A longer-term response but temporary fix, Not a permanent solution	Within 2 weeks
Permanent Solution	A final fix to address the root cause of the problem	Permanent

iii. Conduct containment to avoid liability issues, potential data deletion, activation of a self-destruct mechanism, or permanent data loss.

b. Evidence Gathering and Handling
   i. Chain of Custody
   ii. Initial system snapshot

c. Identifying the Attacking Hosts
   i. Not solely focusing on an attacker’s IP - Address spoofing, Dynamic address
   ii. Using Search Engines
   iii. Using Incident databases
   iv. Monitoring communication channels (Internet Relay Chat, IRC)

d. Eradication and Recovery
   i. Deleting malware
   ii. Disabling compromised user accounts
   iii. Mitigating vulnerabilities
   iv. Backup or rebuilding systems and files
   v. Installing patches
   vi. Changing passwords
   vii. Tightening network perimeter security
   viii. Deploy hardened network monitoring

4. Post-Incident Activity
   a. Hold a Lesson learned meeting
      i. Good material for training
      ii. Updating incident response policies
      iii. Create a follow-up report
   b. Evidence Retention
      Depends on prosecution, Data Retention, and Cost.

Part B – Final Summary Report:

Health Sector

Background / Scenario

You are a cyber security professional working for a small Cybersecurity Compliance company, you work as part of a team that is responsible for implementing and monitoring the organisation's compliance with relevant Australian standards and laws. The company you work for specialises in cyber law at Federal and State levels within Australia and has clients that operate their businesses internationally. The team you are part of must ensure the Cybersecurity Compliance company has selected and implemented appropriate frameworks, policies, and standards for its business operations.

You have been tasked to do a compliance check for a client in the health care sector. You are required to analyse and interpret frameworks, policies, and standards that are relevant to the organisation's cyber security legal and operational requirements. As an individual you will conduct further research and make recommendations for the selection and implementation of appropriate frameworks, policies, and standards for the Cybersecurity Compliance Company.

You and your team must take into consideration in its discussion the areas of DLP, Privacy and relevant law. Your recommendations must also consider DLP, Privacy and relevant laws. Also include in your discussion and report the organisational process "before" and "after" the implementation.

I. Recommendations of Implementation - General

AOJC Cybersecurity & Compliance is a company dedicated to helping healthcare organisations protect sensitive data and maintain compliance with relevant laws and standards. As part of our commitment to securing patient and healthcare operations, we have outlined essential recommendations for enhancing privacy, securing network and security devices, and ensuring reliable backups. These recommendations are designed to minimise risks and ensure that your organisation is well-prepared to handle cybersecurity challenges effectively. Below, we provide a detailed overview of these key areas.

i. Privacy

We can recommend the implementation of a DLP solution to monitor and control sensitive data flows within the network. It is important to ensure that personal and healthcare data are not leaked or misused.

Encryption of all stored and transmitted sensitive patient information to safeguard it from unauthorised access and breaches.

Adhere to the seven principles of GDPR to protect patient information and maintain compliance with international privacy regulations.

Establish protocols for sharing cybersecurity threat information with government agencies, as permitted by CISA 2015, to enhance privacy protection.

Conduct regular audits to ensure compliance with privacy standards and to identify potential gaps in data protection.

If data that is held on premises other than the warrant premises is accessed under subsection 201(1) and it is practicable to notify the occupier of the other premises that the data has been accessed under a warrant.

The executing officer must:

- Do so as soon as practicable and if the executing officer has arranged or intends to arrange for continued access to the data under subsection 201(1A) or (2) - include that information in the notification.

A notification under subsection (1) must include sufficient information to allow the occupier of the other premises to contact the executing officer.

ii. Network & Device Security

We recommend segmenting the network to isolate sensitive data and critical systems. The goal is to reduce the impact of potential ransomware or DDoS attack.

Implement Multi-Factor Authentication (MFA) and application whitelisting to prevent unauthorised access and mitigate phishing attacks (Essential Eight).

Regularly update and patch network devices and systems to protect against known vulnerabilities that could be exploited in cyberattacks (Essential Eight).

Deployment of an Intrusion Detection System (IDS) to monitor network traffic for suspicious activities and potential intrusions.

Implement a Next-Generation Firewall (NGFW) to filter incoming and outgoing traffic, blocking malicious attempts to access the network.

Implement specific endpoints protection tools like antivirus software, anti-malware solutions to secure all devices connected to the network from malware and unauthorised access.

Implement software to monitor, manage and secure employees' devices used in the workplace (BYOD protection).

iii. Backups

Conduct daily automated backups of critical data, software and settings to ensure availability in case of ransomware attack (Essential Eight).

Limit backup management to three trusted personnel to reduce the risk of unauthorised access and use a reputable third-party backup solution to enhance data security (Essential Eight).

Perform regular test backup and recovery process to ensure data integrity and availability in case of a cyber incident (Essential Eight).

Establish and enforce backup retention policies to ensure that backups are kept for the required duration.

Ensure cross-border data backups comply with international regulations (CISA 2015 – ENISA standards) to avoid legal complications.

II. Recommendations of Implementation – Acts / Standards

When it comes to cybersecurity, following established standards and regulations is vital. At AOJC Cybersecurity and compliance, we emphasise the importance of adhering to guidelines that help safeguard sensitive information and maintain legal compliance. In this section, we provide specific recommendations for implementing well-known standards and acts like NIST, HIPAA and CIS Security Controls. This framework will guide your organisation in creating a strong cybersecurity foundation. Below, we explore these standards and their relevance to your operations.

i. NIST – Small Business Information Security: The Fundamentals

The NIST - Small Business Information Security guide provides an overview about the steps small businesses should follow to protect their information and ensure confidentiality, integrity and availability. This is relevant to the health organisation we are currently assessing as it is a small business. As mentioned earlier, these are the main threats in the health sector:

- Ransomware attacks which can encrypt essential data and demand a payment to decrypt it.
- Malware attacks which can disrupt health organisation operations.
- Phishing and social engineering against health sector employees which could trick them and lead to stealing credentials or install malicious software on the systems.
- Insider threats could use their privileges to access sensitive information, steal it and use it for malicious purposes.
- Outdated medical devices and healthcare systems could lead to vulnerabilities in the software which can be used later by an attacker.
- Medical devices which are connected to networks which are not secured properly could be exploited by an attacker and disrupt the operations or have sensitive data leaked.

Understanding the risks of the small business is part of the steps which needs to be followed according to the NIST - Small Business Information Security guide.

The next part is focussing on protecting the information of the company against the risks and it is highly recommended to follow those steps and ensure your business is more protected against cyber security incidents. We are recommending following the following main steps:

- Encrypting sensitive data in transit and at rest.
- Collect and store the minimum data of patients and delete it once it's no longer in need.
- Monitor loggings to patient data to detect and respond to any unauthorised access.
- Make sure the business is complying with the GTPR if handling data of EU citizens and the Australian Privacy Act 1988.
- Have access control in place, such as multi-factor authentication.
- Perform regular encrypted backups of sensitive data and sore it offline to protect it as much as possible.
- Patch management should be in place to ensure all systems and medical devices are updated with the latest updates and security patches.
- Segment the network so the medical devices, guest Wi-Fi and administrative functions are separated to limit damage of breaches.
- Training your employees regularly to ensure they use a strong password and recognize phishing attempts for instance.
- Have incident response plans in place which include each step of preparation, detection and analysis, containment and eradication, recovery and post-incident analysis.
- Consider hiring an IT security employee to manage and monitor the systems regularly.
- Use simple security solutions, such as firewalls, antivirus and VPNs.
- Decide on a budget for security purposes to minimise the risk of cyber incidents.

ii. Health Insurance Portability and Accountability Act (HIPAA)

According to HIPAA, there are several key requirements that organisations must follow to ensure the protection of sensitive health information. Upon conducting regular audits, organisations should review all system configurations and adopt and adapt the latest security best practices.

HIPAA mandates that all employees undergo regular security training. Security awareness training helps minimise insider threats and human errors while preventing social engineering attacks.

It is essential to strengthen email security to prevent phishing attacks. This includes using spam filters and implementing tools to detect malicious links and attachments. By enhancing email security measures, organisations can better protect sensitive information and reduce the risk of data breaches.

Applying the principle of least privilege ensures that each employee has access only to the minimum information and systems necessary for their job functions. This principle is crucial for enhancing security and preventing unnecessary exposure of sensitive information.

Establishing a system for continuously monitoring all system logs and responding promptly when suspicious activities are detected. This proactive approach enables early detection of security threats and allows for swift action to be taken. As cyber-attacks in the healthcare sector have increased recently, the importance of a robust log monitoring system and rapid incident response has become critical. To address this, a strategy is proposed that integrates the log and monitoring requirements of HIPAA with the NIST Incident Response Plan.

How to implement the integration of HIPAA and the NIST Incident Response Plan:

1. Log collection in accordance with HIPAA requirements and NIST log analysis
2. Establish incident response procedures
3. Regular training that integrates HIPAA and NIST
4. Utilise automated monitoring tools
5. Evaluate NIST post-Incident analysis and identify improvement for HIPAA compliance

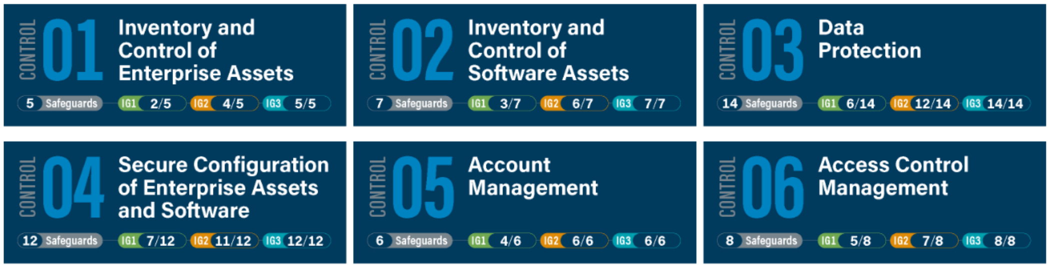
iii. Center for Internet Security (CIS) Security Controls

We recommend using CIS which contains 18 security controls that can help your business to be protected from common cyber incidents. Those controls are valuable for a health sector business as they help to protect sensitive patient data, esure the system availability and ensure that the company is complying with the latest regulatory compliance and industry standards.

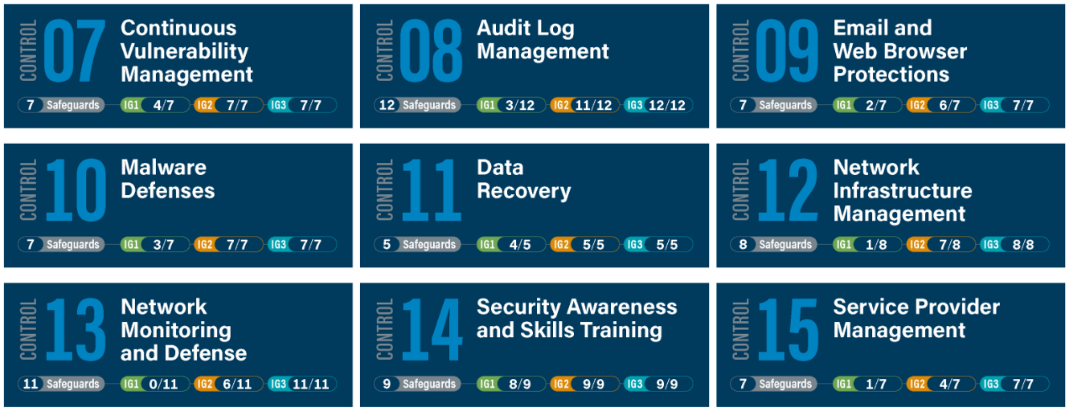
Before the implementation phase, it is required to assess your current security posture by conducting a risk assessment which can identify security gaps in the systems, networks or medical devices and review the current compliance of the company with known regulations, such as HIPAA, Privacy Act 1988 or GTPR.

After assessing the security posture and the compliance level of the business, we will categorise the CIS 18 controls into three main categories:

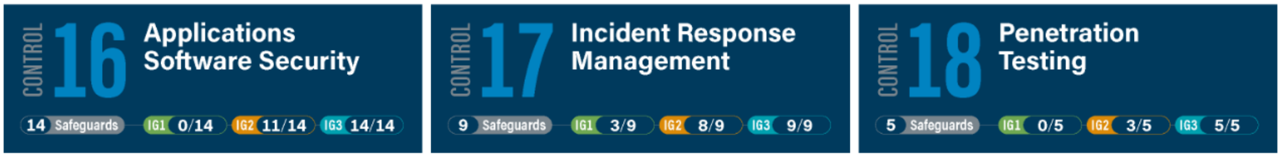
1. Controls 1-6: basic controls for minimising the risks which were found in the previous phase as soon as possible.


CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5
CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7
CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12
CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6
CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8

2. Controls 7-15: foundational controls to level up the security posture of the company.


CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7
CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12
CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7
CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7
CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5
CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8
CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11
CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9
CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7

3. Controls 16-18: organisational controls to improve cybersecurity governance and reach an advanced level of cyber defence.



First, we will implement the basic controls as an immediate action to reduce the risk of cyber security events, and then we will move to advanced controls which will improve the overall security posture of the business.

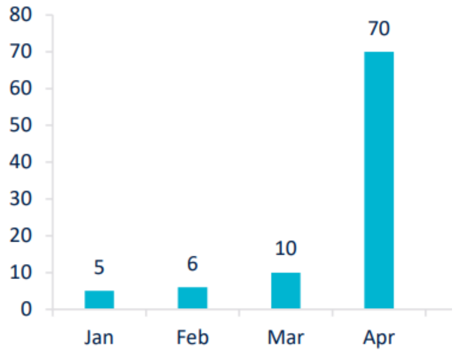
It is important to make sure that the CIS controls implementation is aligning with regulation and common standards, such as HIPAA, Australian Privacy Act 1988 and GDPR (if dealing with EU citizens). Also, using automated tools for monitoring the systems and detecting threats (SIEM) along with automated patches is critical.

It is recommended to monitor the process and its effectiveness regularly and to make sure the security controls are relevant, up-to-date and followed by your staff.

III. Monitor the Organisation's Security Implementation and Incident Mitigation

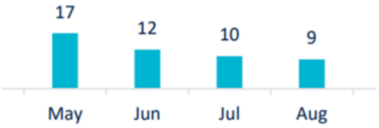
The client has collated two data sets for your analysis. The first set describes cyber incidents during the first quarter, the second dataset shows cyber incidents for the second reporting quarter. Your final task is to analyse the data sets provided and ascertain the effectiveness of the recommended implementation and mitigation strategies.
Prior to the client being audited, they have supplied you with a dataset called dataset A. This dataset outlines the number of attacks the organisation is subject to over the last month.
You have now been supplied with a second dataset set, called dataset 2. Your job is to analyse the difference in attacks that the organisation has been subject to. Using graphs and charts, you will determine the implications that have been recommended in Part A1 and Part B have been successful.

Dataset 1:
During the first quarter of the reporting period of 2023, there were 91 cyber security incidents reported by the organisation. Most of the reported incidents were for compromised host systems and other incidents.



Dataset 2:

Dataset recorded in the second quarter of the reporting period of 2023, is now provided by the health organisation for review. It is below for your review and recommendation. Based on this data, determine if the recommended mitigations have been successful.



Industry characteristics

After the COVID-19 pandemic, cybercriminals are focusing on the health sector, motivated mainly because it provides them with a significant economic benefit.

Any service interruption, even if it is temporary or momentary, creates a strong social alarm and reputational damage, making healthcare organisations potentially willing to give in to possible blackmail and pay to recover “normality”. Health data is highly valuable on the black market. Not only has the volume and heterogeneity of data generated, transmitted and processed increased, but they are also interconnected, both within and outside the organisation itself. All this complexity and the poor cybersecurity practices have expanded the attack surface for cybercriminals.

Main threats to the sector

Based on studies published by ENISA (2023), the most frequent attack vectors in the health sector are:

- Poor security configurations (68%)
- Insiders/Human errors in the operation (16%)
- Social engineering/phishing (4%)
- Unpatched software or hardware vulnerabilities, as well as downloading and installing malware or malicious programs within the technological infrastructure (9% and 3% respectively).

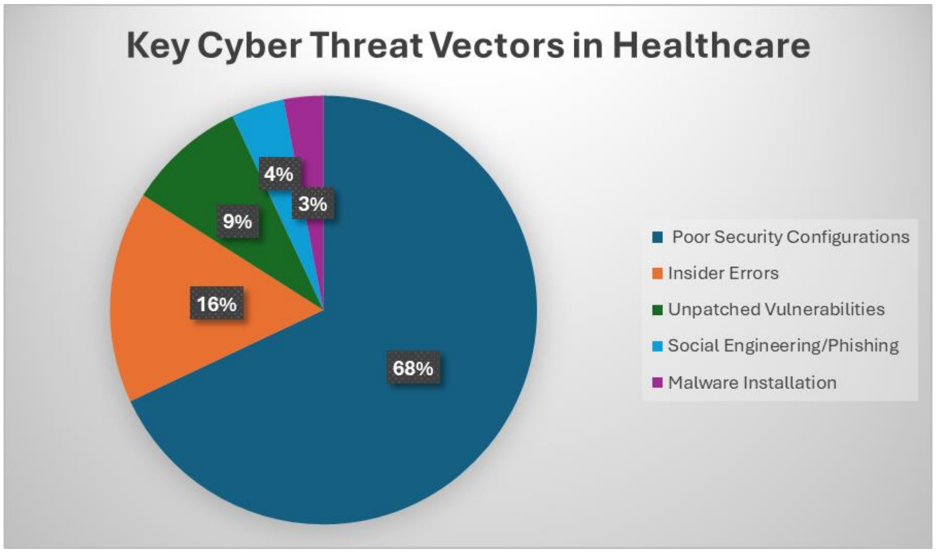


Figure 1 - Key cyber threat vectors in healthcare

According to the dataset for the first quarter, 52% of the incidents were ransomware attacks, causing service disruption and data theft. Phishing accounted for 30% of the incidents, mainly involving stolen credentials. Malware was responsible for 13% of the incidents, leading to breaches of patient data, including medical records and financial information. DDoS attacks made up 5% of incidents, causing temporary disruptions.

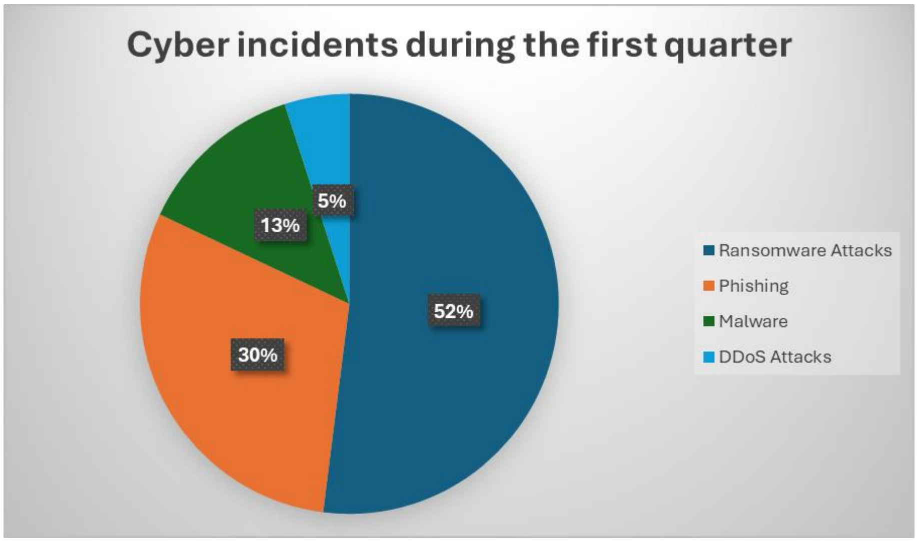


Figure 2 - Cyber incidents during the first quarter

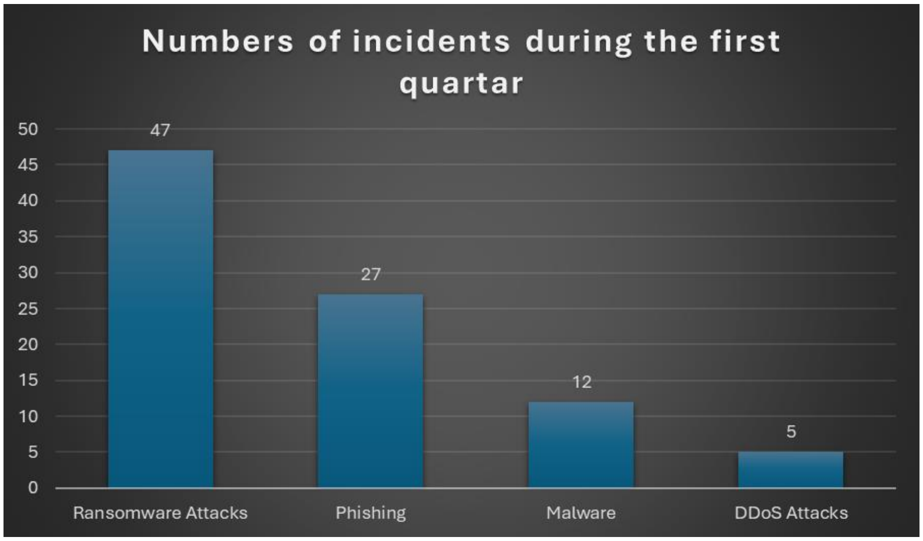


Figure 3 - Numbers of incidents during the first quarter

Types of assets affected:

- Patient medical data (medical records, laboratory results), demographic and administrative data (65%), which allowed cybercriminals to carry out impersonation, fraud or extortion to the provider or the patient.
- ICT infrastructure data by 28%
- Corporate data with 7% of the incidents reported.

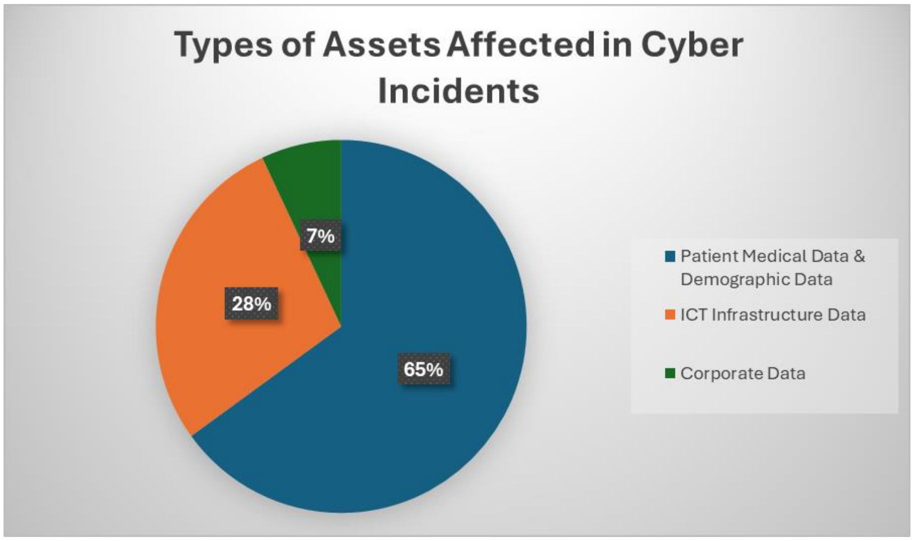
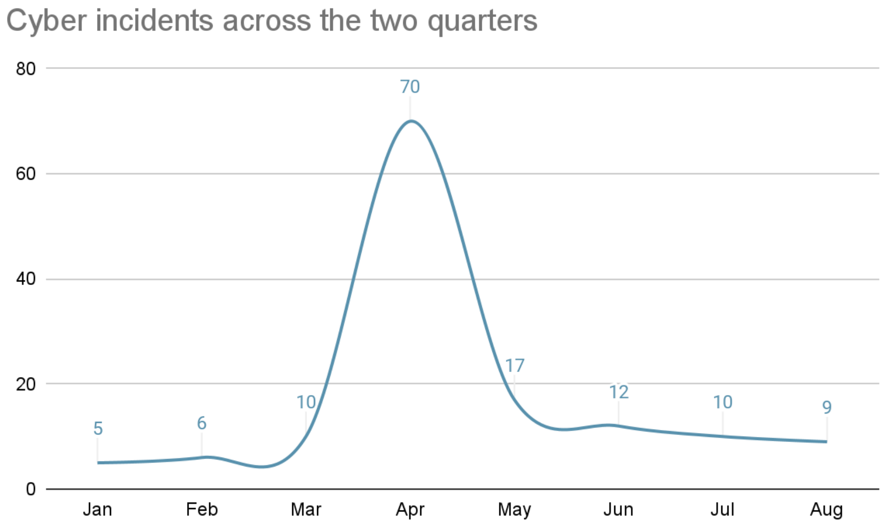


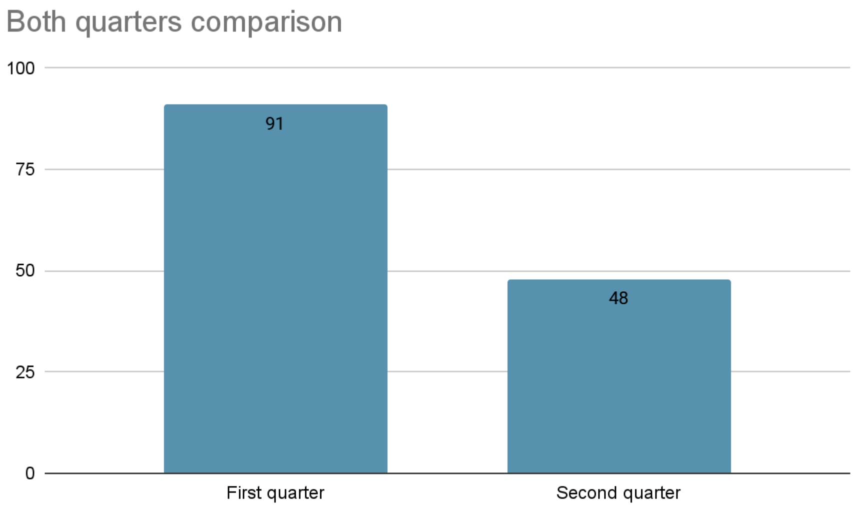
Figure 4 - Types of Assets Affected in Cyber Incidents

Post Implementation - Second Dataset

As your business begins to implement our general recommendations along with our Act/Standards recommendations we outlined before, we analysed both datasets which gave us an overview about the cyber incidents rate the company experienced before and after the implementation of our recommendations.

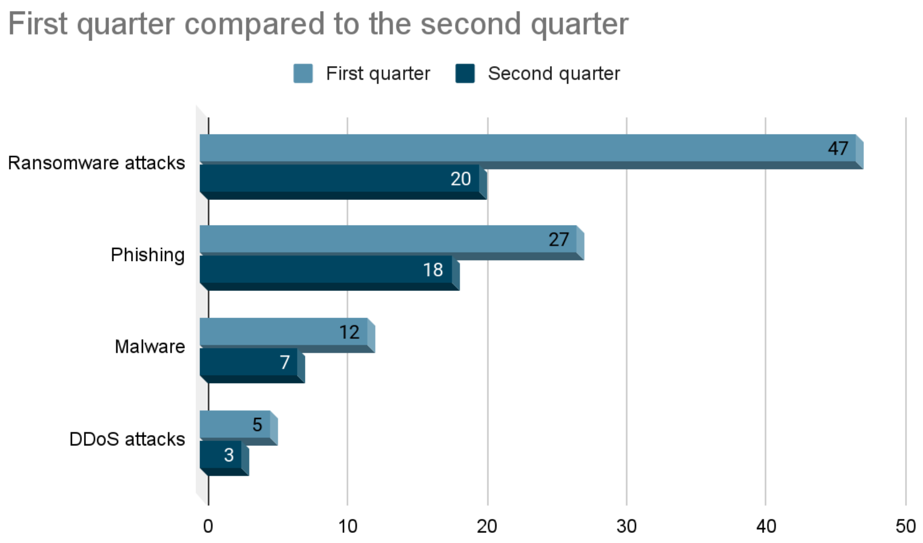
Before the implementations your business experienced 91 cyber incidents over the first quarter (Jan, Feb, Mar, Apr) and once you started implementing our recommendation you experienced 48 cyber incidents over the next quarter (May, Jun, Jul, Aug) which is a decrease of 47% in cyber incidents compared to the first quarter. The company had 70 cyber incidents in April and only 17 cyber incidents in May which is a decrease of 76% in cyber incidents after starting to implement our recommendations. Furthermore, the company had a decrease of 87% in cyber incidents if we compare May (70 incidents) to August (9 incidents). On the graphs below you could view the comparison between each month.



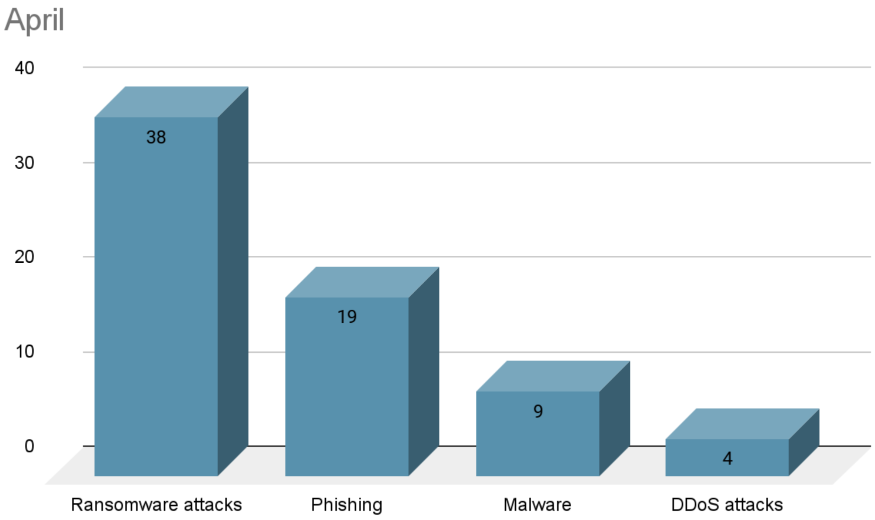

Both quarters comparison

In the first quarter 47 (53%) of the cyber incidents were due to ransomware attacks, 27 (30%) to phishing, 12 (13%) to malware and 5 (5%) to DDoS attacks.

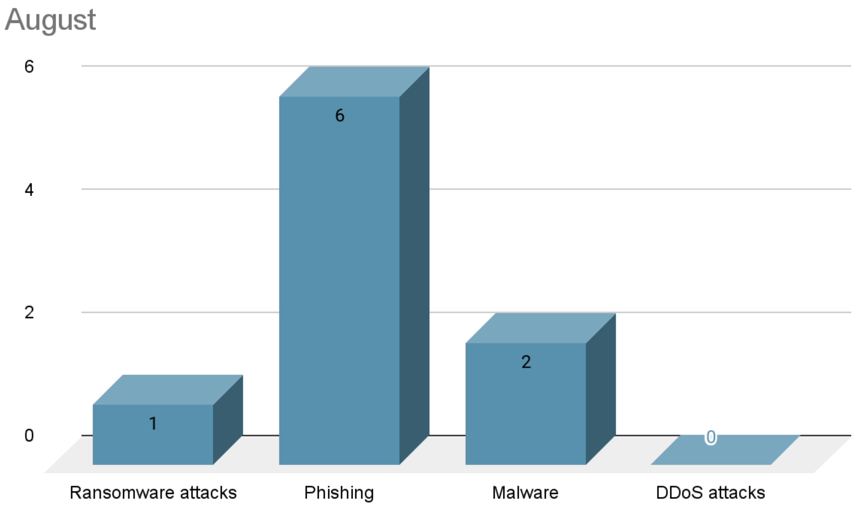
In the second quarter we can confirm that the numbers of each kind of incident reduced as 20 (42%) of the incidents were due to ransomware attacks, 18 (38%) to phishing, 7 (15%) to malware and 3 (6%) to DDoS out of 48 incidents in the whole quarter.


First quarter compared to the second quarter

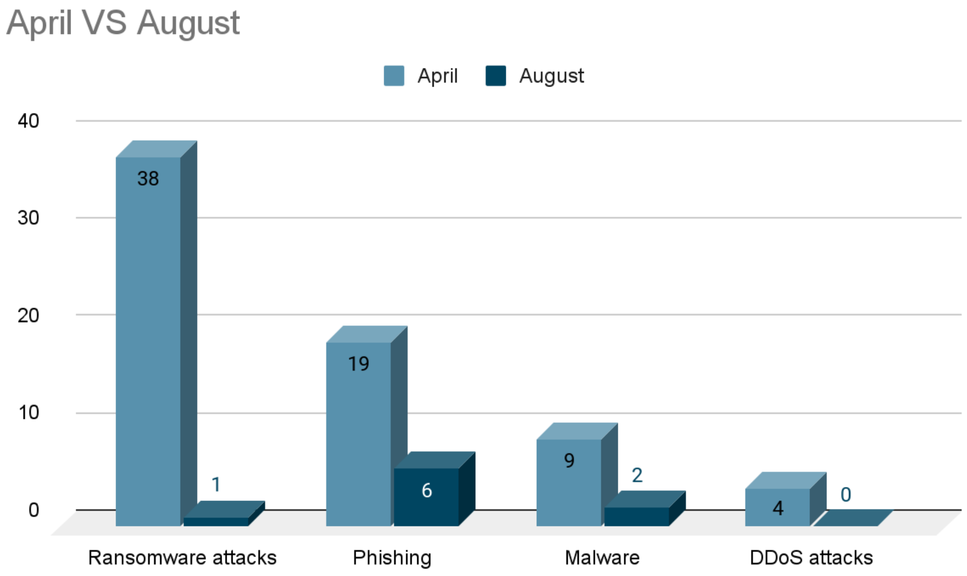
In April your business experienced an increased number of 70 cyber incidents which were reduced to only 9 incidents in August. We can confirm that 38 of the cyber incidents across April were due to ransomware attacks, 19 to phishing, 9 to malware and 4 to DDoS attacks.



4 months later, in August, after you implemented most of our recommendations, your business experienced only 9 cyber incidents across the whole month with 1 ransomware attacks, 6 phishing, 2 malware and no DDoS attacks.



If we compare April to August with a graph, you will see the dramatically decreased numbers of cyber incidents as you can view below. August showing a decrease of 87% in cyber incidents compared to April.



With the data before us we can confirm that the implementation of our recommendations was beneficial to your business. Following our recommendations for privacy, network & device security and backup along with following strong acts and standards, such as NIST, HIPAA and CIS Security Controls, reduced the attack surface of your business and made it more difficult for the attacker to proceed and succeed with his planned attacks.

However, you still experienced 6 phishing attacks in August. Human mistakes are one of the weakest points in every company. Phishing attacks can be a click away from being exploited if your staff members do not take safety measures and recognize phishing emails in advance. We recommend that you perform more education sessions for your staff in the upcoming months and launch a phishing campaign to monitor which staff members are interacting with those phishing attacks. Education is one of the best ways to minimise this threat.

Remember to monitor your systems regularly, follow our recommendations every single day and implement new security tools. As attackers find new tactics quite often, it is important to view your security posture regularly and be up to date with any new additions of the current acts and standards or with new frameworks, standards and best practices which will be released in the future and will be worth to be considered.

IV. References

https://www.digitalhealth.gov.au/healthcare-providers/cyber-security

https://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

https://uncitral.un.org/en/commission

https://lawcouncil.asn.au/policy-agenda/international-law/uncitral

http://www.austlii.edu.au/au/journals/QldJSchol/2016/26.pdf

https://www.business.gov.au/Planning/New-businesses/Legal-essentials-for-business

https://www.legislation.gov.au/Details/C2004C01213

https://www.legislation.gov.au/Details/C2019C00296

https://www.legislation.gov.au/Details/C2020C00248

https://www.legislation.gov.au/Details/C2020C00248

https://www.legislation.vic.gov.au/in-force/acts/privacy-and-data-protection-act-2014/025

https://www.giac.org/paper/gsec/4017/synopsis-cybercrime-act-2001/106427

https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities/

https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

https://www.techtarget.com/searchsecurity/definition/ENISA-European-Network-and-Information-Security-Agency

https://www.nist.gov/cyberframework

https://www.securitymetrics.com/blog/improve-your-security-posture-nist-cybersecurity-framework

https://www.iso.org/isoiec-27001-information-security.html

https://www.isaca.org/resources/cobit

https://www.cynet.com/incident-response/nist-incident-response/

https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/

https://www.asd.gov.au/about/what-we-do/cyber-security#:~:text=The%20Australian%20Signals%20Directorate's%20Australian,Visit%20cyber.gov.au

https://econofact.org/the-cybersecurity-threat-ailing-healthcare#:~:text=The%20Issue%3A&text=Hospitals%20and%20other%20healthcare%20organizations,interface%20with%20specialized%20medical%20technologies.

https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cyber-security/securing-customer-personal-data https://www.enisa.europa.eu/

https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015

https://www.cadwalader.com/resources/clients-friends-memos/potential-risks-and-rewards-of-cybersecurity-information-sharing-under-cisa

https://gdpr.eu/what-is-gdpr/

https://epublications.regis.edu/cgi/viewcontent.cgi?article=1796&context=theses

https://www.itsmf.co.uk/wp-content/uploads/2020/11/Introductory-Overview-of-ITIL4.pdf

https://www.mizekhedmat.com/wp-content/uploads/2022/07/ITILFoundation-ITIL4Edition.pdf

https://www.isaca.org/resources/news-and-trends/industry-news/2014/information-and-communications-technology-study-of-public-health-institutions-in-mexico

https://www.businessbeam.com/consulting/capability-assessment-and-performance/

https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

https://www.bmc.com/blogs/cobit/

https://www.researchgate.net/figure/COBIT-2019-Principles-COBIT-2019-is-a-Framework-issued-by-the-ISACA-association-an_fig4_375554316

https://www.oaic.gov.au/__data/assets/pdf_file/0011/2090/guide-to-health-privacy.pdf

https://ovic.vic.gov.au/privacy/resources-for-organisations/information-privacy-principles-full-text/#principle-6access-and-correction

https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/the-pdp-act-a-deep-dive/#enforcement

https://ovic.vic.gov.au/privacy/for-the-public/your-privacy-rights/#health-information

https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-133#sec.12

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

https://www.archives.sa.gov.au/managing-information/privacy-in-south-australia/information-privacy-principles-instruction

https://www.legislation.tas.gov.au/view/whole/html/inforce/current/act-2004-046

https://www.legislation.qld.gov.au/view/html/inforce/current/act-2009-014#sec.26

https://legislation.nt.gov.au/en/Legislation/INFORMATION-ACT-2002

https://www.itgovernance.co.uk/iso27001#:~:text=ISO%2FIEC%2027001%20is%20the,(information%20security%20management%20system).

https://www.cisecurity.org/controls/implementation-groups

https://www.privacyengine.io/resources/glossary/cross-border-data-transfer/#:~:text=Cross%2Dborder%20data%20transfer%20involves,virtual%20private%20networks%20(VPNs)

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

https://www.hipaajournal.com/healthcare-data-breach-statistics/

https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf