Health Service Executive (HSE) Cyber Security Statement of Strategic Intent

2024 - 2027

Foreword

We are proud to share the 2024 Cyber Security Statement of Strategic Intent. This document represents a forward-looking unified approach to achieving our vision to instil trust among patients and providers by embedding security into our connected digital health services, while continuously adapting our defences to protect against the ever changing threat landscape. It further aligns with national efforts to understand and manage risk to the HSE and wider Irish healthcare eco-system.

The cyber security risks we face are complex, broad, continuously evolving and require investment, upskilling and partnerships with both external stakeholders and peer organisations. This strategic intent document brings together everything that we represent at the HSE, encapsulating our values, future aspirations and a secure health service for staff and patients. The Post Incident Review (PIR) Report[1] that was produced after the 2021 Conti cyber attack details the tactical and strategic recommendations that the HSE will have to implement to achieve the desired cyber security maturity. This report along with the associated investment case proposal and the regulatory and compliance requirements form the foundation for this Cyber Security Statement of Strategic Intent document.

This Strategic Brief will act as the cornerstone for future cyber assurance. It sets out the cyber security guiding principles for developing and operating a trusted technical environment. It recognises that we need to build a dynamic health ecosystem that is able to continually evolve to address emerging threats and that will rely heavily on contributions from all stakeholders and peer organisations.

Through implementation of the strategy, we will move quickly into the modern cyber era, leveraging the latest technologies and approaches. In addition, when implemented it has the potential to unlock significant operational and transformation efficiencies, increase public trust, leverage data securely and create a long-lasting capability for healthcare that reduces the risk of future loss of operational capability through a major cyber-attack.

Puneet Kukreja
Chief Information Security Officer
(CISO – Interim)

Fran Thompson
Chief Information Officer
(CIO)

Peter Connolly
Delivery Director
(Cyber Transformation)

[1] https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

Executive Summary

This Cyber Security Statement of Strategic Intent sets the vision and guiding principles for the HSE's cyber security programme over the next three years. It articulates our approach and key priorities for cyber security and facilitates the implementation of the Post Incident Review (PIR) recommendations made following the 2021 cyberattack on the HSE. This Cyber Security Statement of Strategic Intent sets out a coordinated and holistic approach to uplifting the HSE's cyber capability and maturity to ensure a fit-for-purpose cyber posture in response to an ever-changing cyber environment.

Through approved investment and upskilling, we will build upon our strong foundations and advance our organisational capability to securely deliver better healthcare, including the broader Sláintecare programme[2] and the Regional Health Areas[3] (RHA) established by the government. A key facet of an improved security posture will be the establishment of a new Chief Information Security Officer (CISO) and cyber team, resourced and upskilled to a level commensurate with the size and diverse nature of the HSE. The CISO Office will optimise its investments, governance and operations per the Post Incident Review (PIR) recommendations established following the 2021 Conti cyber event to uplift HSE's cyber security maturity. These will include, but is not limited to:

- Enhanced cyber resilience and the mitigation of cyber incidents and risk, such as, the incident the HSE experienced in May 2021
- Alignment to regulatory requirements, such as, Network and Information Systems (NIS) Directive[4] Compliance as the HSE is an Operator of Essential Service[5] (OES)
- Clear lines of responsibility and accountability for the management and resolution of future cyber incidents.

To implement these recommendations, a high-level estimated funding has been agreed (to build a resilient infrastructure by 2030) for the HSE estate including Voluntaries hospitals.

We are also a part of an extensive and interconnected IT ecosystem that spans the wider Irish health sector. Data being the cornerstone of health services, it is vital that the HSE has a secure environment to enable digital transformation. As the lead agency, we are commissioned to ensure information can be shared securely, quickly and easily across the wider healthcare domains to facilitate best-practice healthcare.

We recognise, in particular, the importance of collaboration, both within the wider healthcare family and with industry.

We further recognise the need to keep on top of the growing nature of threats and the dynamic nature of our work environment. We take this responsibility seriously and a key facet of our approach will be fostering an effective security ecosystem where all can contribute to the benefit of the common good.

This will manifest through healthcare forums and alignment with the emergent Regional Healthcare Areas service delivery model.

In doing so, we recognise the importance of continuously investing in an effective Computer Security Incident Response Team (CSIRT) capability.

The ability of the organisation to respond within minutes instead of hours can make a big difference between an incident being a major operational event compared to a manageable incident.

By building a CSIRT capability, we will have the capability to be proactive, to identify threats at an early stage and to respond promptly to emerging cyber events. A strategic priority for the HSE will be an investment in its people; this will manifest through the development of a strong cyber security culture, the upskilling of staff and the enhancement of mandatory annual cyber security and General Data Protection Regulation[6] (GDPR) training programmes.

Following the Conti cyber-attack, the passion to improve and reform remains strong. Ultimately, our success will be underpinned by our investments in cyber technology, security culture, secure business practices and staff behaviours at home and work. These represent a strategic imperative for our organisation and are at the core of our strategic objectives.

A target maturity level for the HSE has now been set for cyber security and by acting together on this Cyber Security Statement of Strategic Intent, we aim to build a more secure future for the Irish healthcare system.

Data is the cornerstone of the health information system, without it the system would find it impossible to function. Accordingly good quality interconnected data can only be provisioned in a secure cyber assured environment.

[2] https://www.gov.ie/en/campaigns/slaintecare-implementation-strategy/#
[3] https://www.gov.ie/en/publication/4eda4-slaintecare-regional-health-areas-rhas/
[4] https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new
[5] https://www.ncsc.gov.ie/oes/
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Contents

1. Introduction

The Health Service Executive (HSE) is Ireland's publicly funded healthcare system, responsible for providing health and personal social services. It is a geographically widespread organisation delivering public health services through hospitals and communities nationwide.

Our healthcare network operates across approximately 4,000 locations, including 54 acute hospitals and a wide variety of technology components including both Information Technology (IT) and Medical devices. We offer community-delivered care and care provided by hospitals medical devices as well as the national ambulance service. Our corporate and supporting healthcare services are supplied through a combination of national and local centres.

Our organisation, which includes direct employees and those employed by HSE-funded organisations, is the largest employer in the Irish state, with a staff of over 130,000. Therefore, it comprises an extensive community increasingly dependent on connected and reliable Information Technology (IT) solutions and varying levels of IT support from the HSE national centre to deliver clinical services. This includes the HSE's national IT infrastructure. We are considered a critical infrastructure operator according to the EU Network and Information Security Directive, also referred to as an Operator of Essential Services (OES).

1.1 Importance of Cybersecurity

We understand that with the constant advancement of technologies, the cyber threat landscape is rapidly evolving. The healthcare industry is now one of the most frequently targeted industries worldwide for multiple reasons. The following are some of the key cybersecurity perspectives we look at:

Patient Data Protection

We need to continue prioritising confidential patient data protection, ensuring privacy, preventing identity theft and instilling trust in the cyber security posture of the HSE.

Regulatory Compliance

We need to adhere to regulations and data protection laws such as but not limited to NIS directive and GDPR. Failure to comply may result in legal repercussions, financial penalties and damage to our reputation.

Data Breach Prevention

Our healthcare industry is a prime target for cybercriminals due to the value of healthcare data on the dark web. Cyberattacks like phishing, ransomware and malware can cause data breaches, disrupt services and jeopardise patient safety. Therefore, strong cyber security measures can prevent unauthorised access and lower the risk of a breach.

Continuity of Care

Cyber Security is crucial to us to provide continuous care and ensure patient safety. Disruptions to digital health services can cause delays and jeopardise our ability to provide services to our patients.

Medical Device Security

Cyber attack surface increases as medical devices and IoT tech become more integrated into healthcare. Security compromise of these devices can lead to life-threatening situations and therefore, strong cyber security measures are essential for patient safety.

Reputation and Trust

We must prioritise cyber security to protect our reputation and build trust with patients and partners to instil confidence in sharing sensitive personal and health information with us.

Financial Impact

Cyber Security incidents can lead to significant financial losses for the HSE. Investing in strong cyber security measures can help avoid these risks and expenses.

We are investing in cyber security as it is absolutely necessary to safeguard patient data, ensure seamless continuity of care, comply with regulations, maintain trust and uphold the well-being of individuals and healthcare organisations. At the HSE, we believe that the safety and security of patients, healthcare services, employee and associated information are paramount. We consider them highly critical and sensitive and take necessary measures to ensure their protection and confidentiality.

1. Introduction
2. Background
3. Cyber Security Threat Summary
4. Cyber Security Vision and Mission
5. Adhering to Compliance Requirements
6. Enterprise Security Architecture
7. Enablers
8. Cyber Security Programmes
9. Strategic Outcomes
10. Strategic Support
11. Future

1. Introduction
2. Background
3. Cyber Security Threat Summary
4. Cyber Security Vision and Mission
5. Adhering to Compliance Requirements
6. Enterprise Security Architecture
7. Enablers
8. Cyber Security Programmes
9. Strategic Outcomes
10. Strategic Support
11. Future

1.2 Cyber Security Statement of Strategic Intent

Following the HSE Conti ransomware attack in 2021, we commissioned a third party to conduct a post-incident review (PIR). The PIR report listed necessary measures to prevent future breaches and improve the HSE's cyber maturity. We thoroughly assessed these recommendations and their benefits before developing our investment case items.

The investment case outlines the direction of travel and expected cyber security outcomes spread over a period of seven years. However, the Cyber Security Statement of Intent focuses on a 36-month plan covering 27 investment case items. A detailed implementation plan for each of the twenty-seven investment case items is needed annually to secure necessary budget approvals.

The Cyber Security Statement of Strategic Intent will provide a solid foundation to help us uplift our cyber security posture while supporting the HSE's Digital Health Strategic Implementation Roadmap which is discussed under section 4.2 of this document. The HSE's Digital Health Strategic Implementation Roadmap will support the broader Sláintecare programme and the Regional Health Areas (RHA) established by the government.

1.3 Where Does Our Cyber Security Statement Of Strategic Intent Fit In?

The Cyber Security Statement of Strategic Intent outlines a 36-month plan covering 27 investment case items based on the proposal that was put together using the recommendations outlined in the PIR report. The HSE has mobilised the ICT and Cyber programme with a steering committee set up to govern the progress across six prioritised investment case groupings, which are discussed further under section 8 "Cyber Security Programmes". These recommendations are aligned to the National Institute of Standards and Technology Cyber Security Framework[7] (section 6.2 - NIST CSF), which is used to carry out a period review utilising the Capability Maturity Model Integration (CMMI) Model (Appendix 1) to inform progress and support the overall programme planning.

This will allow us to embed security into the initiatives called out in the HSE's Digital Health Strategic Implementation Roadmap and enable integrated care which requires inter connected data and data flows.

The Cyber Security Statement of Strategic Intent will be a living document that will be reviewed periodically based on the outcomes of the implementation activities.

1.4 Together We Thrive

The Cyber Security Statement of Strategic Intent aims to mature the cyber security capabilities of the HSE and the groups covered by sections 38[8] and 39[9] of The Health Act 2004[10].

By collaborating to enhance cyber security capabilities, we can improve our culture of security first mindset in the HSE. This allows us to bring our collective expertise while fully optimising our resources to respond and recover from cyber security incidents.

[7] https://www.nist.gov/cyberframework
[8] https://www.hse.ie/eng/services/publications/non-statutory-sector/section-38-documentation.html
[9] https://www.hse.ie/eng/services/publications/non-statutory-sector/section-39-documentation.html
[10] https://www.irishstatutebook.ie/eli/2004/act/42/enacted/en/print.html

2. Background

2.1 2021 Cyber Event

On the 14th of May, 2021, a major ransomware cyber attack targeted the HSE. The Conti ransomware was used to carry out the attack, which encrypted data and demanded a ransom payment in exchange for the decryption key. Extensive service disruption and the shutdown of multiple IT systems were the significant consequences of the attack, heavily affecting our processes. The disruption substantially affected healthcare institutions such as hospitals, primary care practices and other related facilities throughout Ireland.

After receiving alerts of a successful cyber attack, our critical incident process was activated, initiating a series of events that led to the decision to turn off the HSE IT systems and disconnect the National Health Network (NHN) from the internet to contain and assess the impact of the cyber attack. These steps prevented the threat actor (the Attacker) from accessing the HSE environment. We initially requested the assistance of the Garda National Cyber Crime Bureau, the International Criminal Police Organisation (Interpol) and the National Cyber Security Centre (NCSC) to support the response.

The cyber attack disrupted healthcare services throughout Ireland, as healthcare personnel lost access to essential IT systems such as patient information, clinical care and laboratory systems. The attack had severe ramifications for people who needed health services, as healthcare personnel were forced to use pen and paper to continue patient treatment, which caused delays and backlogs.

The attack also impacted non-clinical systems, disrupting healthcare services. Because of the loss of these systems, numerous administrative duties had to be completed manually, adding to the strain on non-clinical employees and further delaying the recovery of healthcare services.

Normal communication channels in the HSE's national centre and operational services were also immediately disrupted. This included email and networked phone lines. Staff switched to communicating using mobile and analogue phones, faxes and face-to-face meetings. The task was particularly challenging because of the Covid-19 pandemic.

The attacker aimed to disrupt health services and IT systems, steal data and demand a ransom for the non-publication of stolen data and the provision of a tool to restore access to data they had encrypted. The ransom note included directions on how to contact the attacker and the attacker also posted a message in a dark web internet chat room with a link to numerous examples of data allegedly taken from the HSE systems.

Upon the occurrence of the attack, the Irish government and the HSE, decided to decline any ransom to be paid after careful evaluation. We suffered a significant and prolonged aftermath from the incident, surpassing initial projections and requiring ongoing recovery work for more than four months.

To ensure a thorough investigation, a third party was chosen to conduct a Post Incident Review (PIR) of the event. Based on their findings, they provided us with a list of recommendations. As a continuation from the PIR report, an investment case was later developed by the third party, with a plan based on the ICT Cyber recommendations. This plan outlines our direction and will help us identify, cost and prioritise specific steps to be taken over the next 7 years.

2.2 Post-Incident Review (PIR)

Following the 2021 cyber-attack, the HSE Board, the CEO and the Executive Management Team (EMT), commissioned a third party with conducting a Post Incident Review[1] (PIR). The report emphasises the need for significant and fundamental advancements to the technological infrastructure of the HSE to ensure the continued provision of vital healthcare services and the essential implementation of cyber security measures.

The PIR report outlines 245 tactical and strategic recommendations in areas like Information and Communication Technologies (ICT) and cyber, clinical and operational resilience and project management office.

1. Introduction
2. Background
3. Cyber Security Threat Summary
4. Cyber Security Vision and Mission
5. Adhering to Compliance Requirements
6. Enterprise Security Architecture
7. Enablers
8. Cyber Security Programmes
9. Strategic Outcomes
10. Strategic Support
11. Future

1. Introduction
2. Background
3. Cyber Security Threat Summary
4. Cyber Security Vision and Mission
5. Adhering to Compliance Requirements
6. Enterprise Security Architecture
7. Enablers
8. Cyber Security Programmes
9. Strategic Outcomes
10. Strategic Support
11. Future

2.3 Investment Case

In August 2022, a document was published highlighting recommendations for funding to enhance the HSE's ICT and cyber capabilities followed by the PIR report. It offers a prioritised list of 27 initiatives for addressing cyber risks in line with PIR report.

The primary purpose of this Investment Case is to offer a thorough analysis of the costs associated with achieving the goals set in the PIR report through its ICT and cyber recommendations. We must develop a firm security foundation to support the expansion of digital healthcare and realise the benefits that come with it. According to the December 2021 PIR Report, the HSE's IT infrastructure currently needs the resilience required to ensure the safe and successful delivery of healthcare services. The investment proposal aims to develop a solid underlying ICT and Cyber framework for the HSE. This includes being able to adapt to the ever changing nature of the cyber threats and enabling the implementation of the HSE’s Digital Health Strategic Implementation Roadmap.

These ICT and cyber recommendations are mapped to the NIST Cyber Security Framework domains of Govern, Identify, Protect, Detect, Respond and Recover. According to the PIR report, these suggestions are further linked to three broad workstreams: ICT and cyber, Clinical and Operational Resilience and Project Management Office. These recommendations are prioritised based on the value compared to each other and the recommendations listed out connects to improving the gaps identified under each NIST domain during the assessment. Additionally, the investment requirement in this report was prepared by considering the revenue and capital costs, such as staff, hardware, software, and external vendors.

Under the section 8 - “Cyber Security Programmes”, we will further elaborate on how the 27 initiatives are planned and mobilised.

2.4 Maturity Uplift Expected

The PIR report submitted by the commissioned third party to the HSE, evaluated the HSE’s cyber security maturity against NIST CSF and similar industry peer organisations using Capability Maturity Model Integration (CMMI) levels. the CMMI model is used across industries and is intended to guide process improvement across a project, division, or an entire organisation. The CMMI cyber security process maturity ratings and associated descriptions are as captured in Appendix 1.

The report suggests implementing several tactical ICT recommendations over seven years and enhancing resilience within the organisational culture to establish a sturdy foundational infrastructure and attain an agreed state of maturity.

“The Cyber Security Statement of Strategic Intent focuses on the first three years, taking a risk-based approach to strategically implement the suggested recommendations and develop a plan that allows the HSE’s cyber security maturity growth.”

2.5 Efforts Realised

In December 2021 it was noted that the HSE’s cyber security maturity rating could be improved. Capability Maturity Model Integration (CMMI) approach was chosen. This indicated the benefit that could be derived from investment leading to achieving a leadership agreed target CMMI rating by 2030. A reassessment in June 2023 shows a CMMI maturity uplift reflective of effort and investment to date. Continuing with the strategic objectives outlined in this document, the HSE is on track to realise the 2030 target maturity uplift.

The below flow diagram (Figure 1) represents some of the key milestones since the 2021 cyber attack that the HSE has completed to help cyber security capabilities to mature.

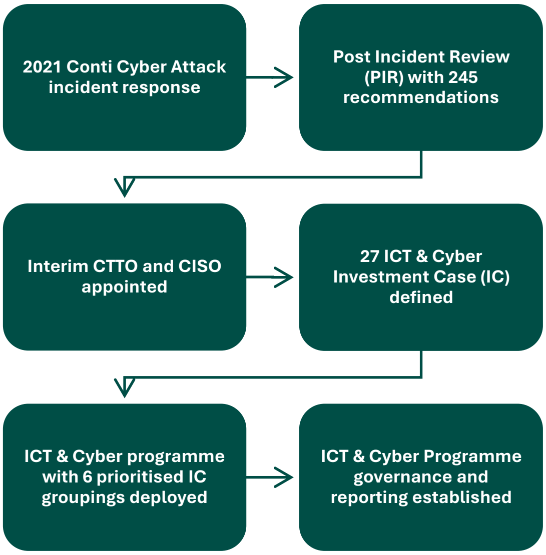

2021 Conti Cyber Attack incident response
Post Incident Review (PIR) with 245 recommendations
Interim CTTO and CISO appointed
27 ICT & Cyber Investment Case (IC) defined
ICT & Cyber programme with 6 prioritised IC groupings deployed
ICT & Cyber Programme governance and reporting established

Figure 1 : Key milestones since 2021

3. Cyber Security Threat Summary

3.1 Environment

With the rapid adoption of new technologies by the threat actors, cyber-attacks have increased in frequency, magnitude and sophistication, allowing cybercriminals to operate efficiently across jurisdictions and country borders.

While the attackers are continuously targeting various sectors, it is imperative to acknowledge that the healthcare industry is becoming more and more susceptible to cyber attacks that can result in severe outcomes. Patients' medical records are getting compromised, resulting in privacy violations and identity theft. Furthermore, the attack can interrupt the delivery of healthcare services, thereby inflicting harm to individuals. These attacks may also result in financial losses, reputational damage and legal liabilities for healthcare organisations.

Looking deeper into the healthcare threat landscape, multiple reports have disclosed significant incidents and risks that have caused immense impact to the healthcare industry and to patients. We have summarised the key takeaways from trusted cyber threat intelligence sources below:

The cyber threat landscape for the health sector issued by the European Union Agency for Cybersecurity[11] (ENISA) has disclosed in the "ENISA Threat Landscape: Health Sector (January 2021 to March 2023)" report that healthcare providers account for 53% of the total incidents reported in the EU and ransomware accounts for 54% of cyber security threats in the health sector.

The National Cyber Security Strategy[12] of Ireland for 2019-2024 produced by National Cyber Security Centre[5] (NCSC) Ireland states that despite an increased level of awareness, Cyber Crime incidents in Ireland are increasing with 61% of Irish organisations reported to have suffered cybercrime such as Fraud in the last two years with an estimated loss on average of €3.1m.

The HSE was a victim of ransomware attacks in 2021, affecting the entire country's healthcare services. The incident highlighted the importance of cyber security in the healthcare sector and the necessity for stable cyber defences underpinned by a carefully thought out strategy. It also illustrated the potentially catastrophic repercussions of a successful cyber assault on crucial infrastructure, such as healthcare systems. Even today we can see a considerable number of attack vectors being utilised to gain access to the HSE environment.

January 2024 Healthcare Data Breach Report by the HIPPA Journal[13] shows an increase of data breaches which is an increase in 2024 compared to the last 5 years that is illustrated in the figure 2.

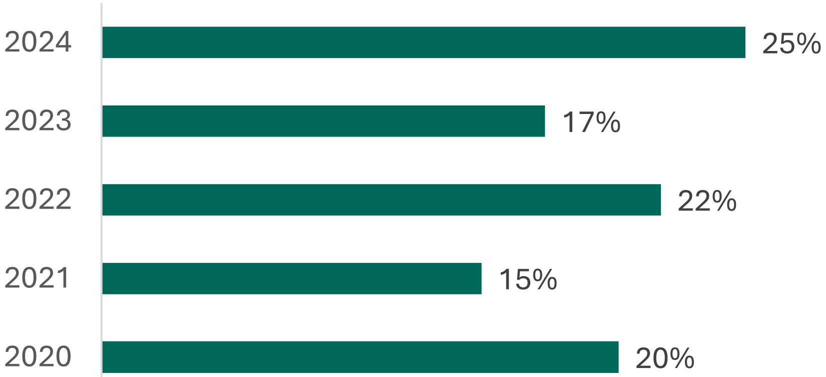


Figure 2 : 2020 to 2024 Data breaches of 500 or more records

(Source : January 2024 Healthcare Data Breach Report by the HIPPA Journal

[11] https://www.enisa.europa.eu/publications/health-threat-landscape?v2=1
[12] https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf
[13] https://www.hipaajournal.com/january-2024-healthcare-data-breach-report/

Microsoft has now highlighted[14] the emergence of human-operated ransomware which increases the complexity involved in detection. Human-operated ransomware is the result of an active attack by cybercriminals that infiltrate an organisation's on-premises or cloud IT infrastructure, elevate their privileges and deploy ransomware to critical data.

The 2024 global threat report by Crowdstrike[15] highlights that new vulnerabilities are being disclosed at a high rate and adversaries can operationalise exploits quickly. According to the report, the average time for interactive technology based intrusion activity to be detected and addressed has decreased from 84 minutes in 2022 to 63 minutes in 2023.

Looking at the most recent publication of the “Executive summary for CISOs: current and emerging healthcare cyber threat landscape”, by Health Information Sharing and Analysis Center (ISAC) in 2024[16], indicates the five healthcare threat areas looking ahead in 2024.

- Phishing/Spear Phishing Attacks
- Ransomware Deployments
- Data Breaches
- Third Party/Partner Breaches
- Social Engineering

According to the 2024 Data Breach Investigations Report (DBIR) by Verizon[17], Healthcare is among the Top 3 industries that were reported with confirmed higher number of data breaches (Figure 3). ENISA 2023 ENISA Threat Landscape: Health Sector report also confirms that both public administration and healthcare industries are heavily targeted.

Data Breach Investigations Report (DBIR) by Verizon has also highlighted that most of the patterns were seen through Miscellaneous Errors, Privilege Misuse and System Intrusion, which represent 83% of breaches. 98% of these attacks were financially motivated and 70% of the attacks were conducted by the internal threat actors.

Malicious attackers are often drawn to the healthcare and government sectors due to their potential economic and espionage motivations.

As detailed in the reports referenced above, the threat actors are continuously evolving and regularly targeting the healthcare sector. To ensure the safety of our patients and staff, it is imperative that we constantly evolve our cyber security capabilities using a threat intelligence led approach.

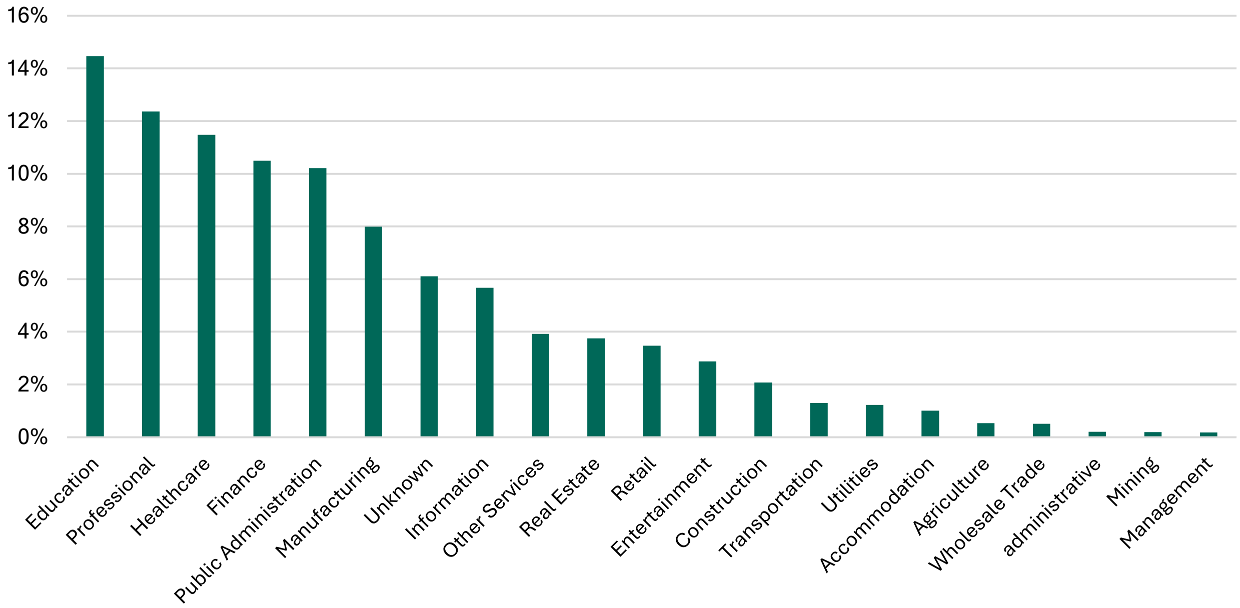


Figure 3 : Targeted sectors with confirmed data breaches

(Source – Verizon 2024 Data Breach Investigations Report)

[14] https://learn.microsoft.com/en-us/security/ransomware/human-operated-ransomware
[15] https://www.crowdstrike.com/global-threat-report/
[16] https://h-isac.org/partnered-report-healthcare-cybersecurity-benchmarking-study-2024/
[17] https://www.verizon.com/business/resources/T157/reports/2024-dbir-data-breach-investigations-report.pdf

1. Introduction
2. Background
3. Cyber Security Threat Summary
4. Cyber Security Vision and Mission
5. Adhering to Compliance Requirements
6. Enterprise Security Architecture
7. Enablers
8. Cyber Security Programmes
9. Strategic Outcomes
10. Strategic Support
11. Future

3.2 Internet of Medical Things (IoMT)

Internet of Medical Things (IoMT) covers all medical equipment and devices which are used in healthcare departments like radiology, cardiology, clinical engineering, emergency, intensive care to deliver patient care while connected over the internet or other communication channels. IoMT extends the HSE's attack surface thus requiring specific capabilities to manage cyber security risks as they cannot be treated in the same manner as general IT assets. To implement these capabilities, we understand that an organisation wide cultural change is required.

3.2.1 IoMT Cyber Security Challenges

Lack Of Visibility

Many IoMT devices work quietly in the background, always gathering and transmitting data. Since these devices are mostly network connected, managed by various vendors and require little user input, it can be challenging to identify and address security concerns that might arise. Therefore, it is challenging to have an accurate and up-to-date inventory of what needs to be protected and monitored.

Poor Testing

Many involved in developing IoMT projects and systems, often neglect the importance of security. As a result, they do not conduct thorough vulnerability testing to detect weaknesses in the IoMT systems.

Limited Security Integration

Integrating IoMT devices into security systems can be difficult due to their wide range, size and technological capabilities to manage and monitor.

Unpatched Vulnerabilities

Many IoMT devices do not have an automated system for installing security updates and patches due to their inherent availability risk. Additionally, the users may not be informed about the updates or manufacturers may not offer regular security patches for their devices, which can leave vulnerabilities unaddressed.

Vulnerable APIs

Certain IoMT devices may utilise unsecured Application Programming Interfaces (API), which could potentially expose any data transmitted between devices and servers by malicious actors.

3.2.2 How to address IoMT cyber security risks

IoMT Device Inventory

To keep track of IoMT devices in use, the HSE will maintain an inventory that includes details such as device type, location and firmware version. This helps to identify any unauthorised devices and keep track of assets.

Network Segmentation

The HSE will ensure implementation and use of secure network protocols, segmenting IoMT devices to limit the potential impact of a security breach and allow for better monitoring and control.

Security Analytics and Monitoring

The HSE will continue to mature security analytics and monitoring capabilities that can handle and analyse the large quantities of data produced by IoMT devices. This will enable the timely identification of cyber threats.

Security by Design

When designing and developing IoMT systems and solutions, the HSE will embed security into the architecture led design process, while implementing industry recognised good practices.

IoMT Security Training

The HSE will provide security training to employees and users to increase their awareness of IoMT security risks and industry recognised good practices.

The capabilities called out in the Enterprise Security Architecture (ESA – section 6) covers both IT and IoMT. Where required the underlying technology will be specifically implemented for IoMT. The multiple programmes we operate, such as ICT and cyber mobilisation, compliance, the security operation centre, foundational technology, threat and vulnerability and IT service management, are intensely focused on addressing both IT and IoMT challenges to ensure patients receive trustworthy and secure care.

4. Cyber Security Vision and Mission

4. Vision

"To instil trust among patients and providers by embedding security into our connected digital health services, while continuously adapting our defences to protect against the ever changing threat landscape."

4.1 Mission

"To enhance the effectiveness and consistency of Health and Social Care Services through strong and reliable cyber security capabilities, expertise, skilled professionals, technological coverage, unified cyber detect and response strategies and comprehensive oversight."

4.2 HSE Digital Health Strategic Implementation Roadmap

The Department of Health is developing the Digital Health Strategic Framework 2023–2030, aligned with the Government's "Harnessing Digital - The Digital Ireland Framework"[18] and the Sláintecare programme. The Department has requested that its National Digital Health Strategic Framework policy be translated and supported by a corresponding Digital Health Strategic Implementation Roadmap that the HSE has developed.

The primary purpose of the Digital Health Strategic Implementation Roadmap is to set out digital health initiatives to be undertaken from 2024 to 2030 and their benefits for patients, healthcare staff and the overall health system in Ireland. The roadmap aims to integrate and connect health and social care services, providing timely, efficient and patient-centred care with ready access to high-quality health information.

Our Cyber Security Statement of Strategic Intent is designed to offer the secure foundation required to implement the Digital Health Strategic Implementation Roadmap. Activities under this will allow the technology efforts to have incorporated security by design, allowing us, as the HSE, to deliver secure and trusted care to our patients.

We are dedicated to successfully implementing the HSE's Digital Health Strategic Implementation Roadmap, with a strong focus on cybersecurity. Our main objective is to seamlessly integrate cyber security measures into all initiatives in accordance with the Digital Health Strategic Implementation Roadmap principles in order to provide our patients with reliable and secure care as shown below.

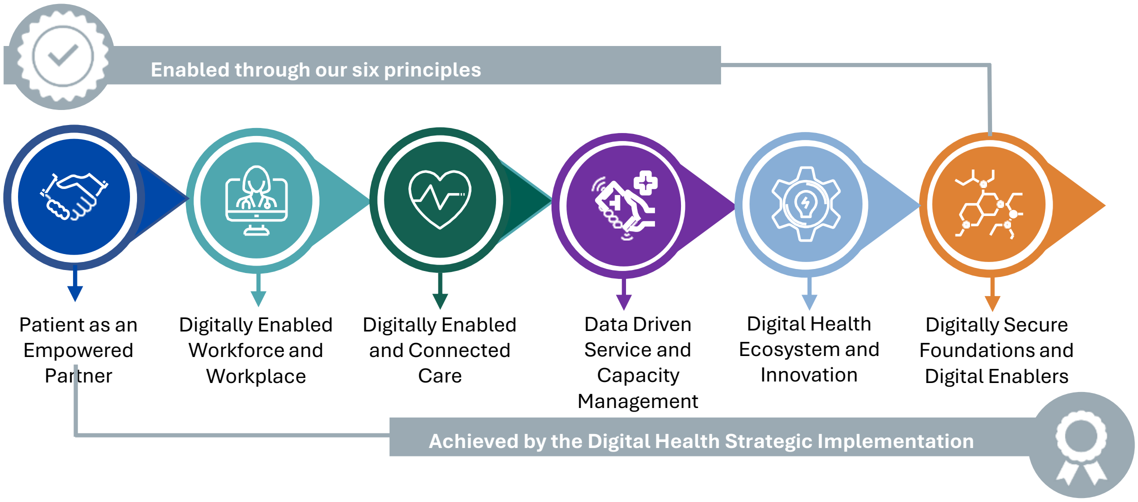

Enabled through our six principles
Patient as an Empowered Partner
Digitally Enabled Workforce and Workplace
Digitally Enabled and Connected Care
Data Driven Service and Capacity Management
Digital Health Ecosystem and Innovation
Digitally Secure Foundations and Digital Enablers
Achieved by the Digital Health Strategic Implementation

Figure 4 : The Digital Health Strategic Implementation Roadmap

[18] https://www.gov.ie/en/publication/adf42-harnessing-digital-the-digital-ireland-framework/

The Digital Health Strategic Implementation Roadmap principles detailed below, which is also illustrated in figure 4 on page 9, are supported by the Cyber Security Statement of Strategic Intent in the following manner:

Principle one: Patient as an Empowered Partner

We are taking proactive measures to enhance cyber security for our digital channels to give patients control and trust over their health information and care decisions. By doing so, patients will have greater access to services and the freedom to choose the care options that work best for them.

Principle two: Digitally Enabled Workforce & Workplace

We are supporting the HSE's Digital Health Strategic Implementation Roadmap to enhance the capabilities of the workplace while maintaining strong cyber security measures. By doing so, we aim to facilitate secure patient access to healthcare services through collaborative efforts.

Principle three: Digitally Enabled & Connected Care

We are supporting the HSE's Digital Health Strategic Implementation Roadmap by ensuring that the digital health and social care systems are equipped with sufficient cyber security controls. This enables the delivery of secure and comprehensive patient health information, leading to collaborative and evidence-based decision-making for timely improvements in patient outcomes.

Principle four: Data Driven Service and Capacity Management

We are supporting the HSE's Digital Health Strategic Implementation Roadmap by managing the cyber security risks around provision of digitally-informed services and capacity. This, in turn, will facilitate better evaluation of patient care, patient flow and workforce performance, ultimately leading to improved healthcare services.

Principle five: Digital Health Ecosystems and Innovation

We are supporting the HSE's Digital Health Strategic Implementation Roadmap by prioritising security in our Digital Service Development & Innovation. This will empower patients and healthcare workers to access innovative solutions that improve their experience throughout the healthcare ecosystem.

Principle six: Digitally Secure Foundations and Digital Enablers

We are supporting the HSE's Digital Health Strategic Implementation Roadmap by creating a strong and secure digital foundation. This foundation will enable efficient governance, promote a supportive culture and offer protection against external threats. Our approach is to align with industry standards and legislation by integrating architecture, service design, cybersecurity, agile delivery and data engineering within the health service.

The initiatives called out in the “Cyber Security Programmes”, section 8 of this document and “ICT Cyber Programme” section 6.9 in the Digital Health Strategic Implementation Roadmap document, reinforces our capability to securely deliver on the Digital Health Strategic Implementation Roadmap principles. We aim to align ourselves with industry standards, regulations and best practices to ensure that cyber security is a continuous effort and not a one-time event. We continually monitor local and global cyber activities to identify potential threats and strengthen our technology solutions with the latest cyber security controls. We ensure that cyber security is taken seriously and given utmost priority at the HSE.

4.3 Cyber Security Strategic Framework

Our framework aims to aid the HSE in implementing its Digital Health Strategic Implementation Roadmap by prioritising cyber security vision and mission. We are utilising valuable insights from the HSE's cyber attack in 2021, the Digital Health Strategic Implementation Roadmap principles and integrating crucial compliance obligations as covered under the "Adhering to Compliance Requirements", section 5 as primary factors to formulate our cyber security strategic framework.

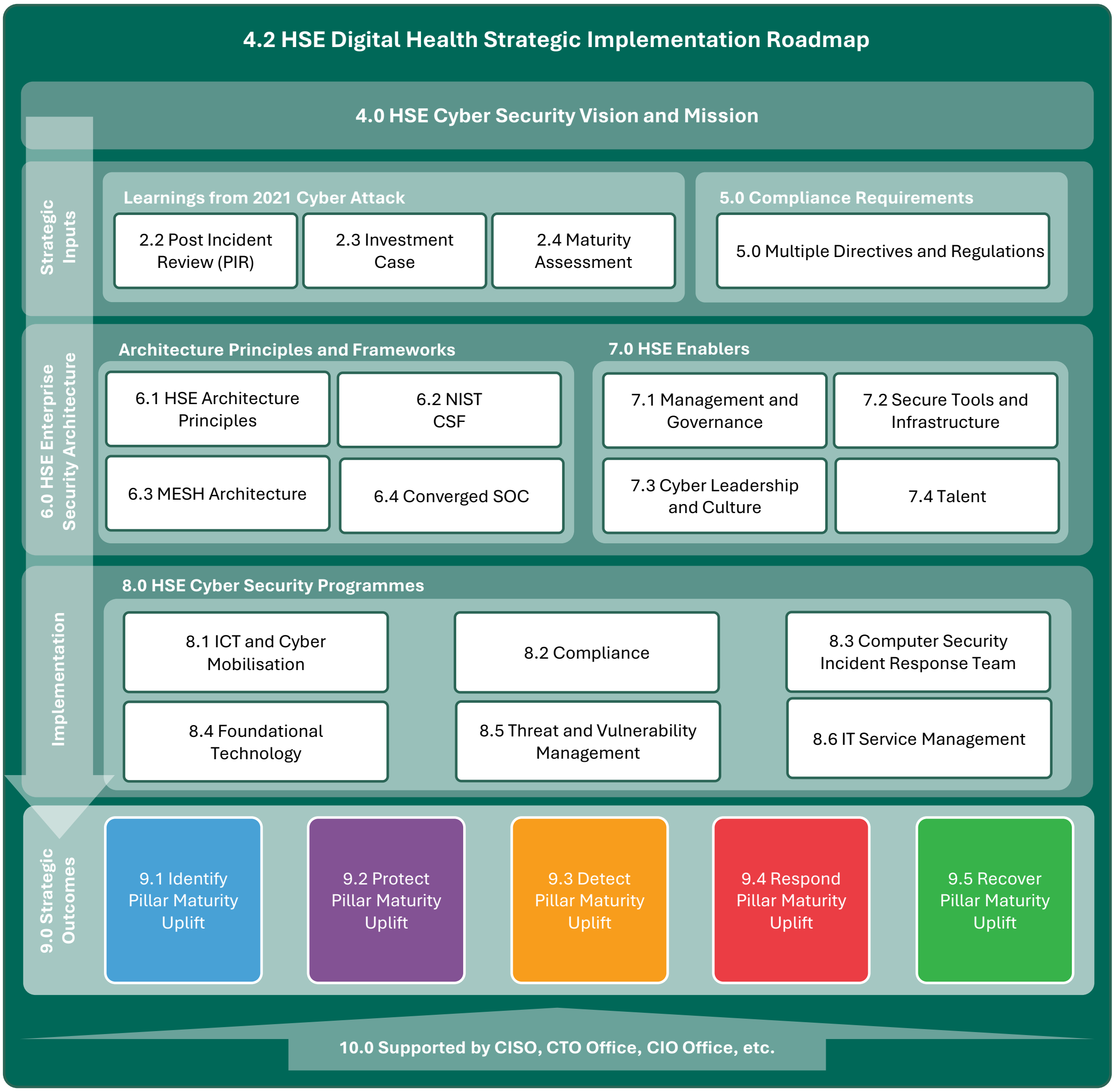
Based on these inputs, we have established our enterprise security architecture (Figure 5), which brings together security principles, frameworks and models with HSE enablers to support developing and implementing cyber security capabilities.

Through our six targeted programs, we are focused on elevating our maturity across five critical cyber security outcomes. The five strategic outcomes are based on the Post-Incident Review (PIR) recommendations and are aligned to the NIST CSF. Various organisational pillars in the HSE will support these activities, mainly through the Chief Information Security Officer's (CISO) office.

Together, the areas under this framework will unify and complement each other to secure our digital landscape and build the HSE's cyber security maturity to deliver secure and trusted healthcare to our patients.

Additionally, this framework will serve as the basis for developing a comprehensive and sustainable cyber security strategy as we move forward based on outputs from periodic NIST CSF, CMMI assessments.

This document offers further information about the sections specified within the framework.



4.2 HSE Digital Health Strategic Implementation Roadmap

4.0 HSE Cyber Security Vision and Mission

Strategic Inputs

Learnings from 2021 Cyber Attack

- 2.2 Post Incident Review (PIR)
- 2.3 Investment Case
- 2.4 Maturity Assessment

5.0 Compliance Requirements

- 5.0 Multiple Directives and Regulations

6.0 HSE Enterprise Security Architecture

Architecture Principles and Frameworks

- 6.1 HSE Architecture Principles
- 6.2 NIST CSF
- 6.3 MESH Architecture
- 6.4 Converged SOC

7.0 HSE Enablers

- 7.1 Management and Governance
- 7.2 Secure Tools and Infrastructure
- 7.3 Cyber Leadership and Culture
- 7.4 Talent

Implementation

8.0 HSE Cyber Security Programmes

- 8.1 ICT and Cyber Mobilisation
- 8.2 Compliance
- 8.3 Computer Security Incident Response Team
- 8.4 Foundational Technology
- 8.5 Threat and Vulnerability Management
- 8.6 IT Service Management

9.0 Strategic Outcomes

- 9.1 Identify Pillar Maturity Uplift
- 9.2 Protect Pillar Maturity Uplift
- 9.3 Detect Pillar Maturity Uplift
- 9.4 Respond Pillar Maturity Uplift
- 9.5 Recover Pillar Maturity Uplift

10.0 Supported by CISO, CTO Office, CIO Office, etc.

Figure 5: HSE Cyber Security Strategic Framework

5. Adhering to Compliance Requirements

We understand that it is essential for us in the healthcare industry to comply with cyber security regulations due to the criticality of the services provided. By adhering to cyber security compliance requirements, we can demonstrate our commitment to safeguarding our patients against data breaches, unauthorised access and potential harm. This ensures that critical healthcare systems and information remain confidential, available and intact, thereby preserving patient privacy and trust. It also helps us to avoid potential fines and legal consequences. Our cyber security maturity is driven by various compliance directives and standards, including but not limited to the ones listed below.

5.1 Network and Information Systems (NIS) Directive

The Network and Information Systems (NIS) directive[4] is a regulatory framework established by the European Union to enhance the cyber security and resilience of critical infrastructure operators. It imposes obligations on operators of essential services like the HSE, requiring them to implement security measures, report significant incidents and collaborate with relevant authorities.

The latest version of this directive, NIS, was released on the 27th of December 2022 and it came into effect on the 16th of January 2023. The NIS directive is crucial for the HSE because it aims to improve cyber security and safeguard critical healthcare infrastructure.

Adhering to the directive ensures that we implement strong security measures, protecting sensitive information, ensuring operational continuity and providing secure and dependable care to patients.

NIS Operators of Essential Services (OES)

The HSE is recognised as an Operator of Essential Services[19] (OES) and needs to comply with security regulations outlined in Regulation 17 of SI No. 360 of 2018 by the Network and Information Systems (NIS). To help meet these requirements, guidelines have been provided by the NCSC for OES like the HSE. The set of security guidelines comprises of the five NIST CSF functions.

NCSC Baseline Security Standard (BSS)

The NCSC, with the Office of the Government Chief Information Officer (OGCIO), has developed the BSS[20], which are meant to provide an acceptable security baseline and a broad foundation for a collection of measures that can be changed over time. Based on the NIST CSF, the BSS specifies the baseline procedures that public sector bodies such as the HSE should take to safeguard their networks.

The security capabilities called out in Enterprise Security Architecture (ESA), section 6 are designed to support the implementation and operation of NCSC BSS requirements.

5.2 General Data Protection Regulation (GDPR)

The GDPR[6] is a law in the European Union and the European Economic Area that protects data and privacy. It's a crucial part of EU privacy and human rights law, mentioned in Article 8 of the Charter of Fundamental Rights of the European Union.

This law provides guidelines for collecting, storing and processing people's personal data in the EU. Our adherence to GDPR guidelines demonstrates our commitment to safeguarding sensitive personal data and respecting their privacy rights.

Adhering to these regulations helps the HSE to handle sensitive information in an ethical manner, minimise the risk of data breaches and establish trust with patients by ensuring that their data is processed lawfully, transparently and securely.

5.3 Health Information and Quality Authority (HIQA) Standards

Health Information and Quality Authority[21] (HIQA) has defined standards for data interoperability, data security and data quality for provision of health and social care services for the benefit of the health and welfare of the public.

Adhering to these standards allows the HSE to proactively secure the collection, use and sharing of health and social care information in Ireland.

[19] https://www.ncsc.gov.ie/pdfs/NIS_Compliance_Security_Guidelines_for_OES.pdf
[20] https://ncsc.gov.ie/pdfs/Cyber_Security_Baseline_Standards_Rev_1_2022_Final.pdf
[21] https://www.hiqa.ie/

6. Enterprise Security Architecture

We have designed the HSE’s Enterprise Security Architecture (ESA) based on the National Institute of Standards and Technology Cyber Security Framework (NIST CSF - section 6.2), the Cyber Security Mesh Architecture (CSMA - section 6.3) and the Converged Security Operation Centre Model (SOC - section 6.4) and our own architecture principles. Bringing all together, we have adopted a capability based approach for designing the HSE’s ESA. Capability-based planning focuses on the planning, engineering and delivery of strategic business capabilities to the enterprise.

This architecture will allow the HSE to develop core integrated capabilities (Cyber Security Mesh Architecture approach) that will strengthen cyber security skills, resources, technologies and governance structures. This allows us to proactively manage growing cyber security threat vectors while supporting the overall HSE Digital Health Strategic Implementation Roadmap through the capabilities called out in the diagram below (Figure 6) which address people, process and technology dimensions.

The HSE’s ESA can be categorised into seven key security capability areas essential for providing a robust and resilient security posture.

The ESA is built upon two supporting foundation elements. The architectural element will help bring more sustainable ESA into the HSE and the cyber security enablers will help implement the necessary capabilities.

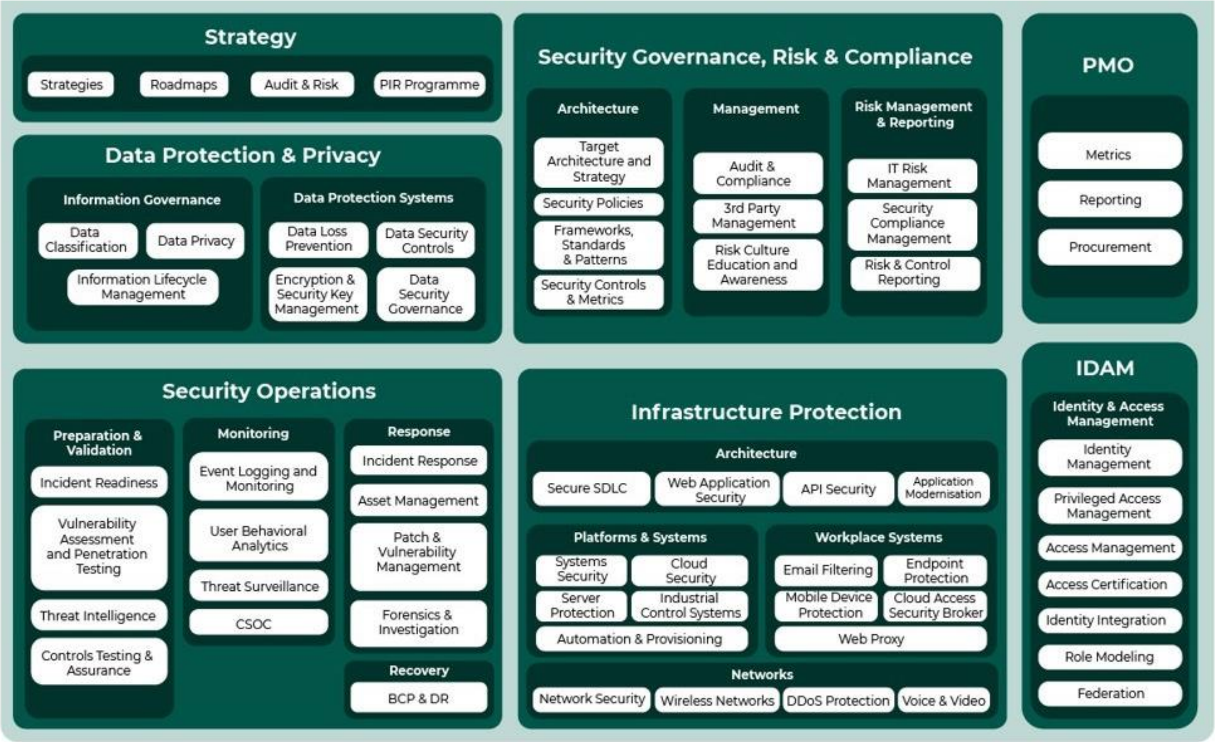


Figure 6: HSE Enterprise Security Architecture

1. Introduction
2. Background
3. Cyber Security Threat Summary
4. Cyber Security Vision and Mission
5. Adhering to Compliance Requirements
6. Enterprise Security Architecture
7. Enablers
8. Cyber Security Programmes
9. Strategic Outcomes
10. Strategic Support
11. Future

6.1 Security Architecture Principles

As part of our efforts to bolster the Enterprise Security Architecture for the HSE, we have established five fundamental cyber security principles that serve as the framework for our approach. These principles inform all actions related to deploying and utilising cyber security resources and assets across the organisation. By adhering to these principles, we can effectively support the HSE's Digital Health Strategic Implementation Roadmap and improve our overall cyber security maturity. To ensure that these principles are integrated into our implementations, we are utilising the National Institute of Standards and Technology Cyber Security Framework (NIST CSF - section 6.2), the Cyber Security Mesh Architecture (CSMA - section 6.3) and the Converged Security Operation Centre Model (SOC - section 6.4).

6.1.1 Privacy by Design

Privacy by Design is a principle that entails incorporating privacy measures into the very fabric of systems during their design phase. By doing so, privacy and data protection become integral components of the system, in addition to its intended purpose. This approach ensures that user and patient privacy is prioritised from the outset and that the system is equipped to safeguard sensitive information. The HSE will also evolve its approach to ensure optimal privacy considerations are applied to our solution sets in a seamless manner.

6.1.2 Defence in Depth

Defence in depth is an architecture principle that emphasises multiple layers of security controls with the combination of people, technology and operations to safeguard against cyber threats. This principle mainly helps to prevent the single point of failure where the systems would have to be designed in such a way that the compromise of a single security control does not result in compromise of the entire system. This layered approach will help the HSE to enhance protection against diverse threats and provide redundancy for robust cybersecurity.

6.1.3 Security by Design

A Secure-by-Design principle is a proactive approach to developing systems, products, or services with security considerations integrated from the beginning. It focuses on designing and implementing strong security measures as part of the development process rather than adding them later. By including security at the foundational level, the HSE can aim to reduce vulnerabilities, defend against threats and ensure the overall security and reliability of the system, product, or service. The HSE will also endeavour to ensure the appropriate policies, controls and checklists are applied in order to establish a strong security conscious culture and operational environment.

6.1.4 Least Privilege

The principle of Least Privilege suggests that individuals or entities should only have access to the necessary rights and permissions required to carry out their job functions or tasks. This principle helps reduce the risk of unauthorised access, accidental misuse and potential damage caused by individuals with excessive privileges. By following this principle, the HSE can lower the chance of unauthorised access, unintentional misuse and damage caused by individuals with elevated access rights.

6.1.5 Assume Breach

Assume Breach is a comprehensive approach that considerably impacts investment decisions, design choices and operational practices. This mindset entails treating applications, services, identities and networks with suspicion and assuming they are potentially compromised and insecure, regardless of their origin or location. At the HSE, we do not place blind trust in this mindset and take the necessary measures to address potential vulnerabilities and protect against them.

6.2 NIST CSF Framework

As the basis of our overall cyber security maturity improvement, we are establishing our enterprise security architecture based on the National Institute of Standards and Technology (NIST) Cyber Security Framework[7] (CSF). The NIST CSF is endorsed by the NCSC, which is being implemented through several directives within Ireland's healthcare sector. By aligning with this framework, we are ensuring that we can easily embrace changes to the cyber security domain in the future.

The NIST CSF (Figure 7) consists of internationally recognised set of guidelines, best practices and standards for managing cyber security risks. NIST created this framework to address the growing cyber threats and help organisations enhance their cyber security posture. The NIST CSF offers a versatile and adaptable method for managing cyber security risks suitable for organisations of any size or industry. It comprises six fundamental components: Govern, Identify, Protect, Detect, Respond and Recover.

6.2.1 Govern

The Governance function emphasizes the importance of establishing oversight and accountability within the HSE's cybersecurity program. It focuses on creating policies, processes, and procedures to manage risk, ensure compliance, and align cybersecurity activities with business objectives. This promotes a security-aware culture and continuous improvement within the HSE.

6.2.2 Identify

The Identify function is crucial for understanding and managing cybersecurity risks. It helps prioritize business objectives and establish reliable processes for HSE to manage cybersecurity risks. This includes creating a better understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities of the HSE.

6.2.3 Protect

The Protect function focuses on implementing safeguards to ensure the security and privacy of critical infrastructure, including measures such as access controls, training and awareness programs and data protection. With the ability to limit and contain the impact of potential cyber security events, appropriate safeguards are put in place to protect critical infrastructure. This involves using Identify and Access Management (IAM) and implementing technology and processes for information protection.

6.2.4 Detect

The Detect function aims to monitor and detect cyber security events to enable timely response continuously. This includes implementing security controls, anomaly detection and incident response capabilities. Established security continuous monitoring capabilities ensure the ability to detect and manage cyber security events in a timely manner. This helps to identify anomalies and events that may impact critical business operations.

6.2.5 Respond

The Respond function aims to create and implement plans to handle and reduce cyber incident's impact. This involves establishing communication channels, coordinating incident response and analysing the incident's aftermath. It also includes implementing appropriate processes for incident management, such as response planning and communications plans, to enable prompt response by the HSE while keeping track of critical activities.

6.2.6 Recover

The Recover function aims to restore the systems and services after a cyber incident. It includes backups, system restoration and learning from the experience to enhance future resilience. These activities are crucial in ensuring a timely return to normal operations and minimising the impact of a cyber security event on the HSE's critical business operations. The established and well-known recovery processes also enable the HSE to document and implement lessons learned into existing strategies.

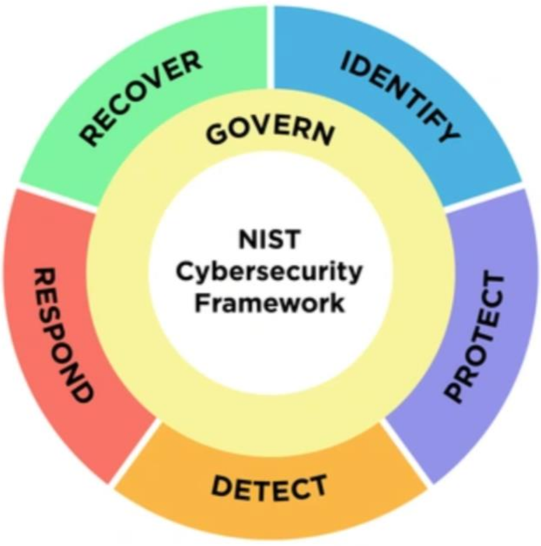


Figure 7: NIST CSF Functions

1. Introduction
2. Background
3. Cyber Security Threat Summary
4. Cyber Security Vision and Mission
5. Adhering to Compliance Requirements
6. Enterprise Security Architecture
7. Enablers
8. Cyber Security Programmes
9. Strategic Outcomes
10. Strategic Support
11. Future

6.3 Cyber Security Mesh Architecture

For us to take a holistic cyber security approach it is important to have a dependable and integrated architecture that enables the HSE in securing healthcare and social care services throughout Ireland. The HSE’s National Health Network (NHN) provides connectivity to deliver various health services across Ireland. The organisations connecting to the NHN have varying levels of cyber security maturity delivered using different cyber security tools and technologies.

Threat actors typically target the weakest link in the cyber security chain to compromise organisations. Considering the complexity of the overall HSE infrastructure, a robust architecture led approach is vital as the cyber risks associated with any connecting organisations can threaten patient care. In order to address this inherent risk, the HSE requires a flexible architecture that can cater to the decentralised nature of IT, while centrally managing the security policy and operations.

We have chosen to use the Cyber Security Mesh Architecture[22] (CSMA) as coined by Gartner, due to the holistic and “security as a platform” based approach. By implementing the PIR recommendations and building our enterprise security architecture (ESA) with a CSMA mindset, we can strengthen our cyber security foundation for the future. This enables us to integrate diverse technologies, giving us a bird's eye view and control of the cyber security threat landscape.

With the implementation of CSMA, we can consolidate diverse cyber security tools and technologies through centralised HSE cyber security policies.

CSMA is also one of the foundational inputs we have used in developing the HSE’s Enterprise Security Architecture to effectively support our efforts towards building unified cyber security capabilities to deliver secure and trusted patient care.

6.3.1 Cyber Security Mesh Architecture (CSMA)

Cyber Security Mesh Architecture (CSMA) is an architectural approach as defined by Gartner, aiming to optimise the efficiency and convenience of security and identity solutions. Rather than dictating a specific solution architecture, this approach presents a range of alternatives, such as single-vendor platforms, platforms with point solution add-ons and distributed point solutions.

The ultimate goal of the HSE leveraging CSMA is to facilitate these solution deployments, improve their effectiveness and manageability and create the best possible environment for connecting organisations. However, this is reliant on deep and more standardised integration among individual tools.

CSMA defines four foundational layers as depicted in the diagram below (Figure 8) which helps us in integrating multiple tools and technologies:

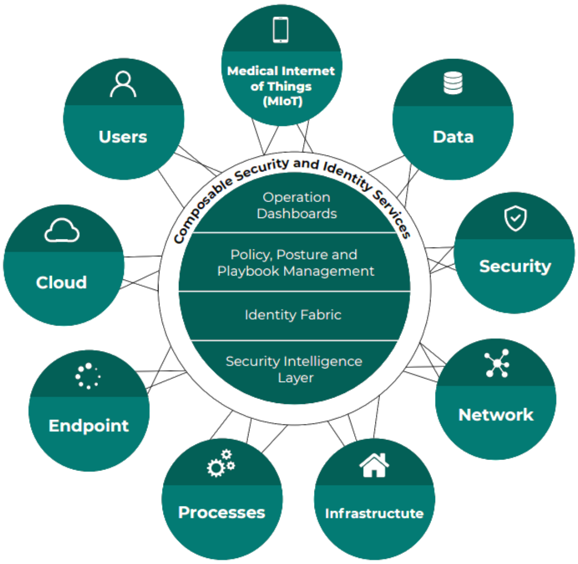

Medical Internet of Things (MIoT)
Users
Data
Composable Security and Identity Services
Operation Dashboards
Policy, Posture and Playbook Management
Identity Fabric
Security Intelligence Layer
Cloud
Security
Endpoint
Network
Processes
Infrastructute

Figure 8: Cyber Security MESH Architecture

Operation Dashboards layer assists the HSE security team by having a central hub to oversee and manage security operations. It provides complete visibility and control, enabling faster detection and more accurate response to any security incidents that may arise. The unified incident response capability covered under the SOC investment case grouping in the “Cyber Security Programmes”, section 8 will be leveraging this layer to visualise, alert and report on possible anomalies or threats before the damage is done.

[22] https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh

Policy, Posture and Playbook Management layer helps the HSE ensure that all individual security tools are set up according to the HSE's central cyber security policies and standards, which helps create a strong and consistent defence against threats. The HSE has formulated a Code of Connectivity (CoC) document to determine an appropriate set of security controls to be implemented to all connecting organisations based on the connection category. This layer enables centralised management of the security control sets.

Identity Fabric layer provides the HSE with identities, entitlements and adaptive access decisions for users and services, as well as security tools dedicated to identity and access management services. These are crucial for the HSE to move towards a successful execution of zero-trust security policy. The Healthcare Worker Identity & Access Management Platform will also be designed by the HSE to deliver identity and access management for healthcare workers using their HEALTHIRL identity platform.

Security Intelligence gathers, combines and examines security data from different tools to identify potential security risks and activate the necessary measures to counter them. The capabilities called out in the SOC investment case grouping in the "Cyber Security Programmes", section 8 of this document will leverage the security intelligence from this layer to effectively detect and respond to cyber threats.

The CSMA layers defined above are underpinned by the following fundamental concepts that collaborate to facilitate a smooth solution design.

- Optimise the distribution of enforcement, decision and policy points across the HSE environment for protecting, detecting and responding to specific asset types or channels, like email or endpoints.

- Centralising certain management functions within the HSE will create a powerful shared intelligence and policy layer, effectively supporting and enhancing the distributed elements.

- Open architectures allow connectivity between individual entities, centralised functions and components within the HSE.

- Standardise the integration process between different entities for more straightforward implementation.

The following diagram (Figure 9) represents the high-level integration of some of the key connecting organisation categories with the CSMA foundational layers.

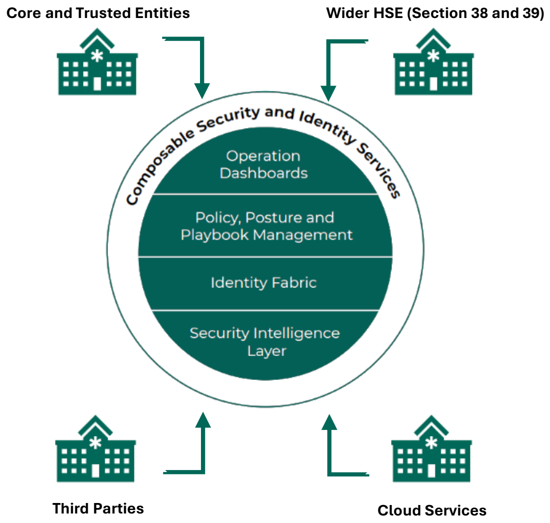

Core and Trusted Entities
Wider HSE (Section 38 and 39)
Composable Security and Identity Services
Operation Dashboards
Policy, Posture and Playbook Management
Identity Fabric
Security Intelligence Layer
Third Parties
Cloud Services

Figure 9: High-level integration of some of the key connecting organisation categories with the CSMA foundational layers

6.3.2 Key Benefits

Improved collaboration and efficiency

CSMA helps us to improve the HSE's collaboration of multiple security technologies, allowing swift response time to threats.

Cross-domain security analytics

CSMA enables an expanded view of the digital environment. It helps the HSE to safeguard the network by centrally allowing multi-domain analytics (e.g. IT, IoMT, Cloud).

Enable a more robust access management model by supporting Identity and Access Management (IAM) requests

CSMA can help codify and execute response plans for common incidents that have pre-determined resolution steps.

Unified incident response across the network

CSMA helps in unifying incident response activities through a set of centralised playbooks powered by Security Intelligence.

Enable more streamlined security tools and technology deployment and management

The CSMA architecture enables the HSE to quickly deploy and manage new security tools and technologies, making adapting to changing security standards easier.

6.4 Converged SOC Model

To support the security operational aspects of the Enterprise Security Architecture (ESA), we are leveraging a Converged Security Operations Centre[23] (SOC) model that integrates various security functions into one central unit. This approach aims to enhance overall security operations and enable the CSMA layers as defined under the CSMA section 6.3.

The converged SOC model combines technologies like threat detection and response, incident management, security analytics and automation, which provides a comprehensive view of our security operations posture. With this approach, we can monitor, analyse and respond to security incidents in real-time, improving key metrics like Mean Time To Detect (MTTD) and Mean Time to Respond (MTTR). This promotes teamwork, simplification of procedures and resource optimisation.

The key benefits of the converged SOC model are:

- Integration of security operation capabilities across the HSE
- Promote communication, coordination and collaboration among various teams in the HSE
- Holistic cyber threat management
- Promote automation of detection and response activities
- Improve scalability
- Enhance security coverage and overall visibility into the HSE threat landscape

The converged SOC will also assist in bridging the limitations and inefficiencies of siloed cyber security capabilities. It is achieved by taking into account three key capability dimensions: people, process and technology, as depicted in the Figure 10.

People: The HSE is in the process of enhancing the current Computer Security Incident Response Team (CSIRT) by introducing a combination of both internal and external skilled resources. This team will equip the HSE senior management with the necessary information needed to take crucial decisions during cyber security incidents. Additionally, the converged SOC model would support the CISRT team and other relevant teams in taking necessary actions around containment, eradication and recovery.

Processes: The HSE has processes in place for effective communication and collaboration supported by incident response playbooks. Our converged SOC model allows swift alert triage and prioritisation, with defined escalation paths. This model empowers end-to-end threat and vulnerability management combined with security intelligence.

Technology: The HSE has implemented comprehensive security technologies that includes capabilities like infrastructure protection, security information and event management, user and entity behaviour analytics, security orchestration, automation and vulnerability scanning to secure the HSE environment. This model supports effective integration of technologies underpinned by CSMA foundational layers.

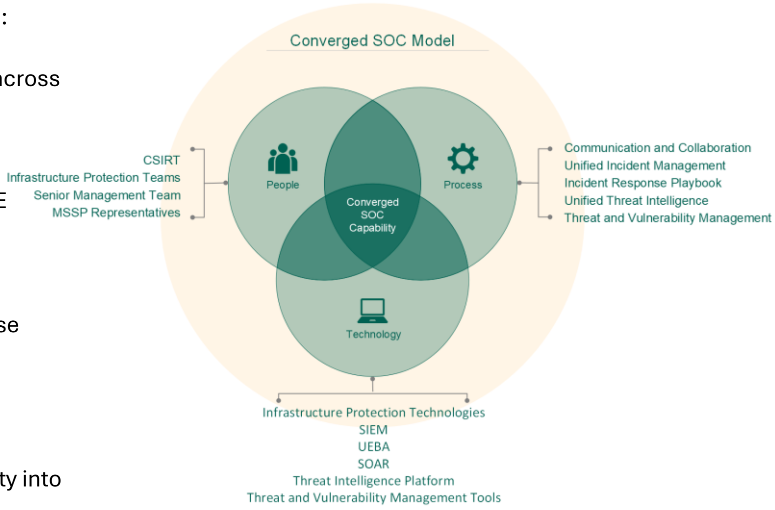

Converged SOC Model
CSIRT
Infrastructure Protection Teams
Senior Management Team
MSSP Representatives
People
Process
Converged SOC Capability
Technology
Communication and Collaboration
Unified Incident Management
Incident Response Playbook
Unified Threat Intelligence
Threat and Vulnerability Management
Infrastructure Protection Technologies
SIEM
UEBA
SOAR
Threat Intelligence Platform
Threat and Vulnerability Management Tools

Figure 10: Converged SOC Model

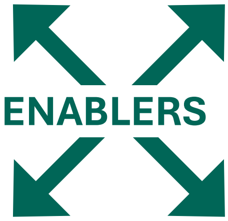
[23] https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh

7. Enablers

Whilst the multiple architectures and converged Security Operation Centre (SOC) are supporting the overall establishment of the Enterprise Security Architecture, we also have a set of cyber security enablers that enable us to strategically develop our capabilities. This allows us to strategically develop capabilities that effectively and efficiently enhance the HSE's cyber security maturity in combating the ever-evolving landscape of cyber threats that we face.

7.1 Management and Governance

We will focus on building a strong, transparent and risk-driven organisation that will allow the HSE to guarantee that cyber security is not an afterthought but is integrated into technological decisions. We will provide measurements and reporting tools to ensure cyber security is managed successfully and efficiently. These indicators can help stakeholders monitor success and identify areas for improvement, while reporting capabilities can aid stakeholders in communicating essential cyber security information. We are improving our capabilities to recognise third party risks and implementing necessary measures to effectively manage cyber security threats. Our procedures, systems and technology will be forensically-sound and have proven recovery capabilities.



7.2 Secure Tools and Infrastructure

We will provide secure technologies to employees so that they may operate more confidently, accessing and sharing HSE data with strict access control. When selecting and implementing software and hardware, we will have processes in place that take the security concerns into account, including a detailed risk assessment to detect potential vulnerabilities and threats and an evaluation of the security features and capabilities of the software and hardware. In addition, the HSE's software and hardware will be enhanced with extra contingency capabilities to enable rapid recovery during a security incident or outage with measures such as regular data backups, redundancy in essential systems and disaster recovery plans that can be deployed swiftly to mitigate the effect of any interruptions.

7.3 Cyber Leadership and Culture

We are implementing a risk-aware culture dedicated to fostering a workplace culture that prioritises cyber security awareness and empowers all employees to take informed actions. We believe that by promoting a sense of responsibility amongst our workforce, we can significantly reduce the likelihood of any security incidents. It is essential that our staff understand the importance of reporting any potential security breaches, no matter how minor they may seem. At the HSE, we are committed to being transparent about incident reporting, identifying areas for training and development and cultivating an environment that values learning from mistakes.

7.4 Talent

We aim to build a proficient cyber security workforce at the HSE that can promptly detect and tackle cyber security threats that may arise. To achieve this, we intend to analyse the current skill sets of our cyber security personnel, identify knowledge gaps and keep ourselves up-to-date with emerging cyber security trends and risks. Furthermore, we will provide specialised training and development opportunities to enhance the capabilities of our cyber security personnel. Moreover, we plan to establish partnerships with third-party cyber security service providers, provide a rich working environment, increase collaboration with government agencies and even consider outsourcing some non-critical cyber security operations to strengthen our defences against cyberattacks. By doing so, we hope to ensure that our organisation is well-equipped to deal with potential cyber threats and safeguard our valuable data and assets.

1. Introduction
2. Background
3. Cyber Security Threat Summary
4. Cyber Security Vision and Mission
5. Adhering to Compliance Requirements
6. Enterprise Security Architecture
7. Enablers
8. Cyber Security Programmes
9. Strategic Outcomes
10. Strategic Support
11. Future

8. Cyber Security Programmes

Based on related and dependent activities in the investment case items, the HSE has come up with the following six investment case groupings. Each of the investment case groupings has funding allocated and prioritised for implementation. The same set of groupings are utilised for overall cyber security programme governance and reporting. These programs are aligned to HSE's Enterprise Security Architecture (ESA), driving strategic outcomes as defined in the Post Incident Review (PIR) report. Based on the third party assessment of the HSE's cyber security maturity we can see that the programme is enhancing the maturity across the five NIST CSF functions. Furthermore, to deliver the cyber security programme, HSE also combines the capabilities through a high level target operating model.

8.1 ICT and Cyber Mobilisation

Under the Information and Communication Technologies (ICT) and Cyber Mobilisation investment case grouping, we strive to establish a multi-year cyber security transformation programme that drives the HSE's cyber security efforts in a strategic manner towards the HSE's vision while uplifting our cyber maturity level.

8.2 Compliance

Under the compliance investment case grouping, we strive to ensure that our initiatives lead to adequate compliance with directives like the Network and Information Security (NIS) Directive 2016/1148 (NIS 2 Directive) and other applicable compliance requirements and standards while establishing a thorough, ongoing, formalised cyber security training and awareness programme delivered to the HSE staff.

8.3 Computer Security Incident Response Team (CSIRT)

Under CSIRT investment case grouping, we strive to establish capabilities at the HSE to actively identify and respond to cyber security threats. These capabilities are delivered using three key services. 1.) Unified incident response, 2.) Managed threat detection and response (endpoints and network), 3.) Managed extended detection and respond for server environments. We also aim to collaborate and support various organisations connecting to the National Health Network (NHN) by extending these capabilities based on agreed upon arrangements with the HSE.

8.4 Foundational Technology

Under the foundational technology investment case grouping, we strive to manage the operating systems and applications technology footprint in the HSE. To achieve this, we will accelerate the rollout of HealthIRL to strengthen cyber security identity capabilities, improve infrastructure to support cloud migration with better backup capability and ensuring our operating systems are continuously assessed to keep up to date.

8.5 Threat and Vulnerability Management

Under the threat and vulnerability management investment case grouping, we strive to build proactive threat and vulnerability identification and timely remediation capabilities at the HSE. These capabilities will be able to proactively discover assets, scan for security vulnerabilities and help prioritise remediation efforts. It will be supported by leveraging the asset's business context and through integration with security intelligence layer as defined under CSMA in section 6.3.

8.6 IT Service Management

Under the IT service management investment case grouping, we strive to enable our IT service management capability by standardising asset register, application register and other artefacts that will be critical to support the incident response lifecycle.

1. Introduction
2. Background
3. Cyber Security Threat Summary
4. Cyber Security Vision and Mission
5. Adhering to Compliance Requirements
6. Enterprise Security Architecture
7. Enablers
8. Cyber Security Programmes
9. Strategic Outcomes
10. Strategic Support
11. Future

8.7 Progress To-Date

With the third-party reassessment of our cyber security maturity, it was highlighted that our ongoing programme initiatives have successfully contributed towards improving our level of cyber security maturity. As a result, we are now better equipped to govern, identify, protect, detect and respond to cyber security threats.

The progress is mapped to the NIST CSF functions and the HSE's cyber security strategic outcomes as follows:

Govern/Identify

Several initiatives were put in place to enhance the HSE's management and monitoring of regulatory, risk, environmental and operational requirements. This allowed us to mature our overall governance, risk and compliance capabilities.

Protect

Training the HSE personnel and partners around cyber security awareness and restricting access to the HSE assets only to authorised users, processes and devices.

Detect/Respond

Increasing our technical capability to detect cyber security incidents and respond promptly in a standardised manner.

Even with the progress we made in our capabilities, we continue to work towards improving our cyber security capabilities.

8.8 Yearly Programme Summary

Year 01– Improve Cyber Security Foundational Capabilities

In year one, our focus will be to improve the cyber security foundational capabilities at the HSE, as recommended in the PIR report. These capabilities intend to move the HSE's enterprise security architecture (ESA) from its current state to a more advanced, agreed-upon level of maturity, with an emphasis on developing each pillar of ESA in both operational and strategic aspects.

We have mobilised a range of initiatives under each of the investment case groupings to improve the foundational capabilities for swift threat identification, protection, detection, response and recovery from cyber attacks. Our efforts to implement these cyber security foundation capabilities represent a significant investment in the organisation's security infrastructure and building skilled cyber security resources.

These investments will help us improve the organisation's overall security posture, support its larger Digital Health Strategic Implementation Roadmap and provide patients with the secure and trusted medical care facilities they deserve.

Year 02 – Improve Coverage of the Cyber Security Capabilities

In year two our focus will be to improve the coverage of cyber security capabilities across the HSE's IT and medical device environment. We plan to take a data driven approach with a defined set of Key Performance Indicators (KPI) and Key Risk Indicators (KRI). The cyber security capabilities implemented in year one will be integrated into overall HSE processes and standardise across the environment.

The learnings and outcomes from year one will also be used to detail and refine the specific implementation plan for year two.

Year 03 – Further Mature the Cyber Security Capabilities

In year three our focus will be to further mature the cyber security capabilities ensuring we have processes in place to continuously improve and optimise our resources.

It will include activities such as adapting for the technical transformational changes that may have happened over the years on the deployed security tools and technologies and expanding on the reach of cyber security throughout the entire organisation, including the affiliated entities such as the groups covered by sections 38 and 39 of The Health Act 2004.

We will work closely with the teams responsible for implementing the HSE's new Information Technology (IT), Operational Technology (OT) and Internet of Medical Things (IoMT) technology to prioritise security right from the start.

Our cyber security teams will conduct regular assessments and testing on existing technologies to pinpoint and eliminate potential cyber security vulnerabilities. Our ultimate objective is to substantially reduce the HSE's cyber risks and maintain a secure environment for patient care.

9. Strategic Outcomes

Our Cyber Security Statement of Strategic Intent is designed to accomplish five primary outcomes. These outcomes derive from the PIR report, which is strongly connected to the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF). The objectives focus on improving the HSE's capability to promptly and strategically govern, identify, protect against, detect, respond to, and recover from cybersecurity risks with the support of the Enterprise Security Architecture (ESA). This involves implementing cybersecurity initiatives that are in line with the cybersecurity vision and mission, as well as providing support for the HSE's Digital Health Strategic Implementation Roadmap.

9.1 Identify Pillar Maturity Uplift

Improve the HSE's ability to effectively identify the cyber security risks by encouraging reporting and responsibility throughout the HSE, ensuring that cyber security risks are identified, assessed and managed effectively. To achieve this objective we will be carrying out multiple projects which include but are not limited to the following:

- Implementation of security resources for managing identities and access controls enhances our ability to protect critical assets and sensitive data.
- Formulation of a multi-year cyber security transformation program highlights our commitment to fortifying the security of health services and data, making them less susceptible to cyberattacks.
- Completion and management of assets capturing essential clinical and corporate services while maintaining an up-to-date inventory of all systems and applications.
- Central management of access controls across the organisation ensures consistent security measures are applied, contributing to a mature and resilient cyber security posture.

We believe that these efforts, combined with better governance structures, will facilitate reporting and accountability throughout the HSE, fostering a culture of cyber security awareness and preparedness. This comprehensive approach will further enable the HSE to make informed decisions, allocate resources efficiently and develop targeted cyber security strategies that will continuously uplift the Identify pillar maturity.

9.2 Protect Pillar Maturity Uplift

Improve HSE's ability to contain the impact of potential cyber security events via appropriate safeguards for critical infrastructure. To achieve this objective we will be carrying out multiple projects which include but not limited to the following:

- Enhance identity and access management via formal and automated mechanisms.
- Defined ‘security boundary’ for the HSE to provide a clear boundary of cyber security responsibilities.
- Establish secure methods for clinical staff in voluntary hospitals to access applications hosted by the HSE.
- Conduct comprehensive, formalised cyber security training and awareness programmes that are delivered to all staff at all grades across the organisation and is conducted on a regular basis
- Implement a process to maintain security baselines for all operational hardware and software, including but not limited to establishing preventative processes such as patch and vulnerability management processes
- Implement a process to timely identify security misconfigurations and zero-day vulnerabilities within the HSE's network perimeter.

We believe that these efforts, will enhance our cybersecurity, enabling us to better address future threats, vulnerabilities and unauthorised access and safeguard sensitive data and critical systems from attacks.

9.3 Detect Pillar Maturity Uplift

Improve automated and manual capabilities at the HSE for continuous monitoring and timely detection of cyber security events. To achieve this objective we will be carrying out multiple projects which include but not limited to the following:

- Enhance the vulnerability management capabilities for continuous scanning for vulnerabilities that can be exploited by attackers and security misconfigurations.
- Improved ability to detect and respond to cyber security events, by augmenting the existing security operations function with additional team members with experience and expertise in cyber security monitoring and response.
- Improve the security monitoring capabilities to detect and contain ransomware attacks in the early stages, ability to prevent and detect the compromise of ‘privileged’ (e.g. systems administrator) accounts and the user authentication.
- Enhance the protective technology to monitor and block traffic that could remove sensitive data from the HSE or attempt to compromise systems supporting clinical services.
- Enhance alert monitoring on all network servers, endpoint devices and firewalls for the external and internal networks.

We believe that these efforts, will enable the HSE to respond to cyber security incidents quicker thus reducing their impact. It also allows us to take preventative action to lessen the threat, improve our overall security measures and safeguard vital assets and data from potential harm.

9.4 Respond Pillar Maturity Uplift

Enhance the HSE’s capacity to respond to recognised cyber incidents through a well-defined and documented response strategy for managing and coordinating cyber security incidents involving multiple organisations connected to the NHN. To achieve this objective we will be carrying out multiple projects which include but not limited to the following:

- Enhance the documentation for managing and coordinating cyber security incidents involving multiple organisations connected to the NHN.
- Enhance the HSE's Incident Response provider’s managed defence service to detect and respond to incidents on endpoints (i.e., laptops, desktops, servers etc.) to provide protection to the entirety of the NHN.

We believe that these efforts, will enable the HSE to handle incidents quickly and efficiently, minimising downtime, reputational harm and financial losses, while monitoring and tracking progress on critical activities.

9.5 Recover Pillar Maturity Uplift

Improve the HSE's ability to withstand and recover from cyber-risks and downtimes by concentrating on cyber-risks, downtimes, necessary resources for business continuity and backup frequency while providing key responders access to communication channels and documentation to aid in risk-based decision-making.

- Improve the foundational capabilities for developing an up-to-date asset and application register, as well as plans that will assist in the response to future incidents.
- Uniform templates for collecting incident updates, action tracking and required decisions during recovery activities.
- Improve communications strategy and dedicated team to managing communications during Recovery processes.
- Enhance the mapping and document list of the people and technology resources and processes required to recover all critical systems in a pre-defined sequence.
- Improve alternative means of information sharing and communication.

We believe that these efforts, will help the HSE minimise the impact of cyber attacks, restore normal operations quickly, learn from their mistakes, build resilience against future threats and allow the HSE to document and implement lessons learned into existing strategies. This will ensure our critical services continue to operate smoothly while minimising financial and reputational damage.

10. Strategic Support

10.1 Our CISO Office

As one of our primary points to support the drive of uplifting the HSE’s cyber security maturity, we have established the Chief Information Security Officer’s (CISO) office. The team takes a proactive approach by focusing on eight work pillars aimed at increasing cyber security maturity levels. Within the CISO office, different teams cover one or more Enterprise Security Architecture pillars, providing a comprehensive framework for addressing identified risks from the Post Incident Review (PIR) report.

10.1.1 Cyber Strategy and Program

The Cyber Strategy and Program team is responsible for creating and implementing the HSE's long-term roadmap for cybersecurity. They plan investments, assess the program's maturity, manage procurement processes for the Chief Information Security Officer (CISO) and produce security metrics reports. This team ensures that the HSE follows industry good practices for cyber security in a constantly changing digital landscape.

10.1.2 Cyber Policy, Data Protection and Awareness

The Cyber Policy, Data Protection and Awareness team is responsible for overseeing data protection in the HSE. Their efforts focus on developing data protection agreements, promoting security awareness, ensuring compliance, updating policies and cultivating a culture of data security. They also support incident response reporting and communication activities in case of data breaches. This helps the HSE to establish defences and secure sensitive information.

10.1.3 Cyber Governance & Risk

The Cyber Governance and Risk team enhances the HSE's resilience against cyber threats by creating and maintaining a strong Cyber Risk Management framework. This involves identifying, assessing and mitigating cyber security risks proactively, ensuring regulatory compliance and managing audits. The team's risk based approach helps protect the HSE's critical assets and strengthens the overall cyber security posture.

10.1.4 Business Information Security Office (RHA & VOL’s)

The Business Information Security Office team oversees the security of Regional Health Areas (RHAs), Voluntary Hospitals (VOL’s) and organisations connected to the National Health Network (NHN) using established policies, procedures and standards. They enable regulatory compliance, improve security awareness and extend support for security incidents. Additionally, they handle security risks and enhance the HSE, RHA and VOL’s security through forums like Cyber Security Community of Practice and the HSE centre programme.

10.1.5 Cyber Architecture & Engineering

The Cyber Architecture & Engineering team design and implement cyber security capabilities, security controls, manages Enterprise Security Architecture and enables procurement. They ensure alignment with industry standards, conduct design reviews and validate architecture patterns. The team reinforces the HSE's resilience to evolving cyber threats through preventive measures and industry frameworks.

10.1.6 Computer Security Incident Response Team (CSIRT)

Computer Security Incident Response Team (CSIRT) is responsible for detecting, analysing and responding to the HSE's cyber security incidents. CSIRT team is also collaborating with wider HSE stakeholders, unifying response activities, sharing threat intelligence and providing guidance on security good practices to enhance the HSE's incident response capabilities.

10.1.7 Cyber Defence

The Cyber Defence team is responsible for managing the processes of Threat and Vulnerability Management (TVM) and Offensive Security. The team works on developing and implementing security management frameworks, compliance and assurance frameworks to detect and address potential cyber threats. They take proactive measures to stay ahead of evolving security threats, support the strengthening of the HSE's overall security posture and protect against potential breaches.

10.1.8 Security Operations

The Security Operations team provides operational support in managing the HSE's security technology landscape. They assist in operating advanced security solutions and support platform maintenance. The team plays a vital role in designing and implementing security operation procedures to ensure a proactive defence posture. They enable the CSIRT team by utilising the telemetry from multiple security solutions.

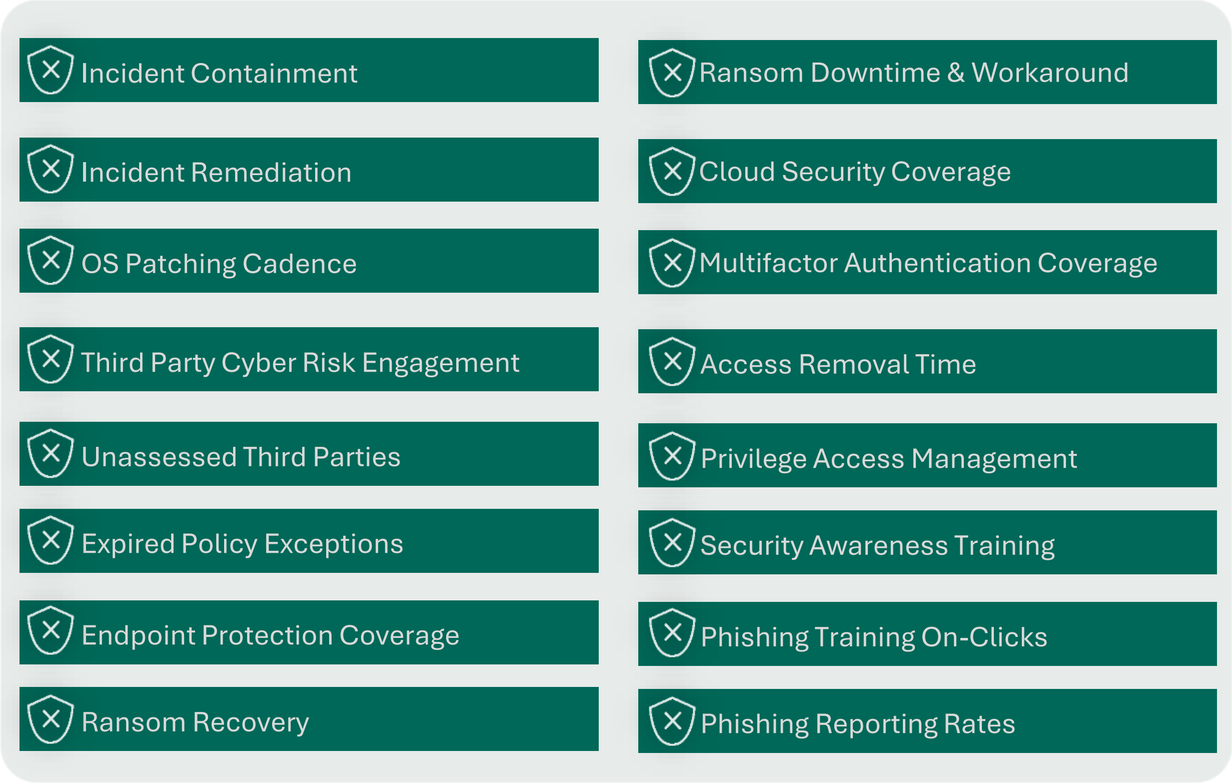
1. Introduction
2. Background
3. Cyber Security Threat Summary
4. Cyber Security Vision and Mission
5. Adhering to Compliance Requirements
6. Enterprise Security Architecture
7. Enablers
8. Cyber Security Programmes
9. Strategic Outcomes
10. Strategic Support
11. Future

10.2 Metrics and Reporting

We have taken a strategic step toward enhancing our cyber security posture by embracing Gartner's recommended 16 outcome-driven metrics[24](Figure 11). Outcome-driven metrics focus on the actual results and impact of cyber security initiatives rather than just measuring inputs or activities. These metrics collectively provide a comprehensive view of the HSE's cyber security effectiveness and help guide decision-making, investment prioritisation and continuous improvement. Each metric offers a unique perspective on various aspects of cyber security performance, enabling the HSE to better manage and enhance their cyber security posture.

In our pursuit to elevate our cyber security practices, we recognise the significance of a well-structured approach. By basing our metrics on Gartner's framework, we are setting the stage to establish a clear baseline of our current cyber posture. This baseline will not only guide us in making informed decisions about our investments but also pave the way for a more mature and resilient cyber security environment.

We are utilising the data currently available from various sources and these metrics to generate invaluable insights into our strengths and areas for improvement.



- Incident Containment
- Incident Remediation
- OS Patching Cadence
- Third Party Cyber Risk Engagement
- Unassessed Third Parties
- Expired Policy Exceptions
- Endpoint Protection Coverage
- Ransom Recovery
- Ransom Downtime & Workaround
- Cloud Security Coverage
- Multifactor Authentication Coverage
- Access Removal Time
- Privilege Access Management
- Security Awareness Training
- Phishing Training On-Clicks
- Phishing Reporting Rates

Figure 11: Gartner's 16 outcome driven metrics

[24] https://www.gartner.com/en/cybersecurity/research/cybersecurity-business-value-benchmark

11. Future

> **"We are continuously working towards providing patients with trustworthy and secure healthcare services by prioritising cyber security and building secure digital services ensuring continuous protection."**

With the cyber incident having taken place in 2021, we are committed to implementing the PIR report's suggestions to uplift our cyber security maturity. These implementation outcomes are expected to span over seven years to enhance our cyber security capabilities and achieve industry standards of maturity, while advancing patient care through secure digital interactions and innovative technology. Achieving an enhanced maturity rating will move the HSE from a reactive to a proactive security posture, ensuring the internal information security processes are managed in a robust and consistent manner.

Our Cyber Security Statement of Strategic Intent lays the high-level roadmap for the first three years, primarily focusing on improving HSE's foundational cyber security capabilities and coverage. Continued investment going forward year on year in cyber security will enable us to ensure our efforts are continuously addressing the gaps identified and monitor our threat environment, increasing cyber security posture and protection to cyber threats, reducing the likelihood of cyber-attacks being successful, proactively identify and respond to cyber security incidents, develop our skills and cultivate robust partnerships with allied security organisations.

Some of the key challenges that can potentially have significant impact on our future cyber security strategy are:

- Adoption of emerging technologies like Artificial Intelligence
- Rapid move to remote work arrangements and digital health services
- Increase in attack surface due to supply chain and third party risks
- Proliferation of targeted ransomware and extortion type attacks using automated tactics
- Use of advanced social engineering techniques like identity spoofing, watering hole attacks and spear phishing to gain foothold within organisations
- Adopting to changing regulatory and compliance landscape

We believe, continuous cyber security maturity uplift will enable contribution to the success of the HSE's Digital Health Strategic Implementation Roadmap and the Sláintecare program. Further, it will also enable the HSE to transition to a more safe and secure digitally led organisation in addition to meeting their regulatory compliance obligations with the NIS Directive.

As we progress with our roadmap, we will re-evaluate our direction and ensure that the HSE can adapt to both unprecedented challenges and transformative opportunities. The increasing adoption of integrated medical services and systems demands the need for proactive approaches to safeguarding patient data and critical healthcare systems.

12. Appendix

Appendix 1 - Capability Maturity Model Integration (CMMI)

The below diagram depicts the CMMI ratings and associated descriptions using to assess HSE's Maturity.

Level	Maturity Rating	CMMI Description
0	Absent	At this level there is no evidence to demonstrate an active process is in place.
1	Initial	At this level, there are no organised processes in place. Processes are ad hoc and informal. Security processes are reactive and not repeatable, measurable, or scalable.
2	Repeatable	At this stage of maturity, some processes become repeatable. A formal programme has been initiated to some degree, although discipline is lacking. Some processes have been established, defined and documented.
3	Defined	Here, processes have become formal, standardised and defined. This helps create consistency across the organisation.
4	Managed	At this stage, the organisation begins to measure, refine and adapt their security processes to make them more effective and efficient based on the information they receive from their programme.
5	Optimised	An organisation operating at this rating has processes that are automated, documented and constantly analysed for optimisation.

Table 1: CMMI Rating and Definitions

Figures and Tables

Abbreviations

PIR	Post Incident Review (PIR) is an independent review done by a third-party following the 2021 cyber attack
RHA	Regional Health Areas also known as Health Regions are regional bodies that should be responsible for the planning and delivery of integrated health and social care services. This is key to delivering on the Sláintecare vision of an integrated health and social care service.
CISO	Chief Information Security Officer is responsible for HSE's information security strategy, policies and protecting against cyber threats.
OES	Operators of Essential Services are wide range of critical infrastructure operators including energy, transport, health, drinking water supply and distribution and digital infrastructure.
ICT	Information and Communication Technologies (ICT) encompass digital tools and systems for data processing, communication and information exchange, enabling global connectivity.
IT	Information Technology (IT) encompasses computer systems, networks, software and data management, enabling organisations to process, store and communicate information efficiently.
CSIRT	Computer Security Incident Response Team (CSIRT) is a specialised group handling cyber security incidents, mitigating threats and ensuring digital defence.
GDPR	The General Data Protection Regulation (GDPR) is an EU privacy law governing data protection and privacy rights, applicable to individuals and organisations.
NIS	Network and Information Systems (NIS) directive is a regulatory framework established by the European Union to enhance the cyber security and resilience of critical infrastructure operators
IoT	Internet of Things (IoT) connects everyday objects to the internet, enabling data collection, communication and automation for smart and efficient applications.
IoMT	The Internet of Medical Things (IoMT) refers to interconnected medical devices and systems for remote monitoring and healthcare data exchange.
NHN	National Health Network (NHN) is the nationwide healthcare system connecting providers, patients and resources for improved medical access, efficiency and patient outcomes.
NCSC	The National Cyber Security Centre (NCSC) is a government agency responsible for protecting a nation's digital infrastructure and providing cyber security guidance.
EMT	Executive Management Team (EMT) is the leadership comprising executives responsible for strategic decision making and overall management of an organisation's operations and goals.
CMMI	Capability Maturity Model Integration (CMMI) is a framework for improving and assessing the maturity of an organisation's processes and practices.
ENISA	The European Union Agency for Cyber Security (ENISA) fosters cyber security collaboration, standards and policy development within the EU and its Member States.
ESA	Enterprise Security Architecture defines the HSE's security framework, policies and controls to safeguard assets and mitigate risks across all IT systems and processes.
API	Application Programming Interface (API) is a set of rules and protocols that allows different software applications to communicate and interact seamlessly.
BSS	Baseline Security Standard (BSS), based on the NIST Cyber Security Framework, provides the baseline measures that Public Sector Bodies should implement in order to secure their networks.

SOC Security Operations Centre (SOC) is a centralised unit that monitors and responds HSE’s information systems against cyber security threats.

CSMA Cyber Security Mesh Architecture (CSMA) is decentralised, adaptive security framework, connecting devices and applications, enhancing protection and resilience in the digital landscape.

CoC Code of Conduct (CoC) is a document formulated to determine an appropriate set of security controls to be implemented to all connecting organisations based on the connection category.

MTTR Mean Time To Respond (MTTR) measures the average time taken to address and resolve an issue or incident effectively.

MTTD Mean Time To Detect (MTTD) measures the average time taken to identify and recognise an incident or issue within a system or process.

KPI Key Performance Indicator (KPI) is a measurable metric used to evaluate the success of an organisation or specific activities.

KRI Key Risk Indicator (KRI) is a measurable metric that signals potential risks, aiding in proactive risk management and decision-making.

IAM Identity and Access Management (IAM) is a security framework managing user identities and their permissions to ensure secure system access.

BISO A Business Information Security Officer (BISO) oversees and manages cyber security and data protection strategies within a company to safeguard sensitive information.

References

1. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

2. https://www.gov.ie/en/campaigns/slaintecare-implementation-strategy/#

3. https://www.gov.ie/en/publication/4eda4-slaintecare-regional-health-areas-rhas/

4. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

5. https://www.ncsc.gov.ie/oes/

6. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

7. https://www.nist.gov/cyberframework

8. https://www.hse.ie/eng/services/publications/non-statutory-sector/section-38-documentation.html

9. https://www.hse.ie/eng/services/publications/non-statutory-sector/section-39-documentation.html

10. https://www.irishstatutebook.ie/eli/2004/act/42/enacted/en/print.html

11. https://www.enisa.europa.eu/publications/health-threat-landscape?v2=1

12. https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf

13. https://www.hipaajournal.com/january-2024-healthcare-data-breach-report/

14. https://learn.microsoft.com/en-us/security/ransomware/human-operated-ransomware

15. https://www.crowdstrike.com/global-threat-report/

16. https://h-isac.org/partnered-report-healthcare-cybersecurity-benchmarking-study-2024/

17. https://www.verizon.com/business/resources/T157/reports/2024-dbir-data-breach-investigations-report.pdf

18. https://www.gov.ie/en/publication/adf42-harnessing-digital-the-digital-ireland-framework/

19. https://www.ncsc.gov.ie/pdfs/NIS_Compliance_Security_Guidelines_for_OES.pdf

20. https://ncsc.gov.ie/pdfs/Cyber_Security_Baseline_Standards_Rev_1_2022_Final.pdf

21. https://www.hiqa.ie/

22. https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh

23. https://blogs.gartner.com/pete-shoard/use-the-gartner-soc-hit-model/

24. https://blogs.gartner.com/paul-proctor/2023/05/22/16-metrics-to-transform-cybersecurity-measurement-reporting-and-investment/