5.3 Focus area 3 - preparedness of the HSE to manage cyber risks

Focus area 1	Focus area 2	Focus area 3
Review the technical investigation and response	Review the organisation-wide preparedness and strategic response	Review the preparedness of the HSE to manage cyber risks
		Approach to focus area 3
		Key findings and recommendations
		Conclusion

Approach to focus area 3

To facilitate this review, PwC developed a PIR Cybersecurity Framework for the HSE which was based on the NIST CSF and the Information Systems Audit and Control Association Control Objectives for Information and Related Technologies (COBIT). Both NIST CSF and COBIT are internationally recognised standards that organisations frequently use to assess their information security capabilities and IT governance processes. The PIR Cybersecurity Framework incorporates NIST's 5 key domains and 23 supporting sub-domains along with the governance aspects from COBIT.

The PIR Cybersecurity Framework

The following table illustrates the 5 key domains of the PIR Cybersecurity Framework and their associated definitions:

Figure 14: The PIR domains and domain definitions

The PIR Cybersecurity Framework		
Domain	**Domain definition**	**Sub domains**
Identify	The **Identify** function assists in developing an organisation with understanding and managing cybersecurity risk to systems, people, assets, data, and capabilities.	• Asset Management • Business Environment • Governance • Regulation Compliance • Risk Management • Supply Chain Risk Management
Protect	The **Protect** function outlines appropriate safeguards to ensure the secure delivery of critical infrastructure services.	• People Security • Access Control • Data Security • Protective Technology including: Information Protection Processes and Procedures • IT Baseline Maintenance
Detect	The **Detect** function defines the appropriate activities to identify the occurrence of a cybersecurity event.	• IT Events & Threat Monitoring including: Detection Technology • Continuous Monitoring • Detection Processes
Respond	The **Respond** function includes the appropriate activities regarding a detected cybersecurity incident.	• Response Planning • Communications • Analysis • Mitigation Improvements
Recover	The **Recover** function identifies appropriate activities for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	• Recovery Planning • Improvements • Communications

Capability Maturity Model Integration

Each domain and subdomain were allocated a rating in accordance with the definitions below. Ratings are based on the Capability Maturity Model Integration (CMMI) cybersecurity process maturity. ISACA's CMMI cyber maturity model helps CISO's, CIO's, and large organisations build cyber maturity, and manage enterprise cybersecurity resilience, readiness and provide assurance to the Board.

Figure 15: ISACA CMMI cybersecurity process maturity ratings and associated descriptions

Level	Maturity rating	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 program 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 program.
5	**Optimised**	An organisation operating at this rating has processes that are automated, documented, and constantly analysed for optimisation.

Key findings and recommendations

Figure 16: Focus area 3 summary of key findings and recommendations

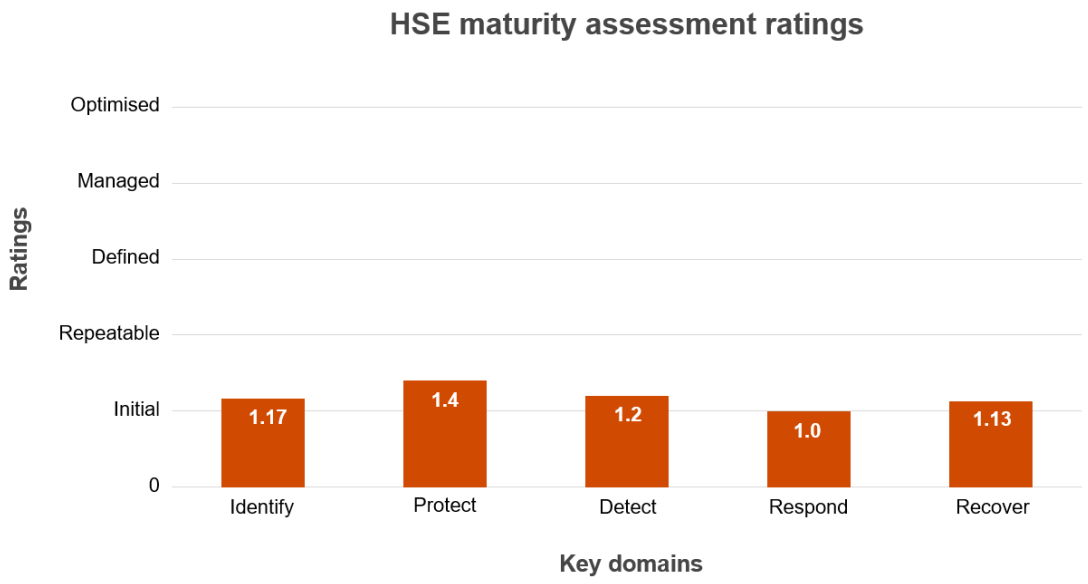
Area	No. of key findings	No. of key recommendations
Identify	6	6
Protect	5	5
Detect	3	3
Respond	5	5
Recovery	3	3
Total no. of key findings & recommendations	**22**	**22**

HSE maturity assessment ratings

Using the PIR Cybersecurity Framework, PwC conducted interviews with key stakeholders and reviewed key documents from the HSE and relevant third parties. This provided PwC with sufficient evidence to enable each of the 23 sub-domains to be assessed against the CMMI model. Assessments were then averaged per their domain and an overall maturity rating achieved.

A summary of the maturity ratings by key domain is illustrated below. Our assessment demonstrated that the HSE is at an *"initial"* CMMI maturity stage across the 5 key domains. Cybersecurity and governance processes are predominantly ad hoc, informal, and not well organised. This represents a very low level of maturity for cybersecurity and is significantly behind where an organisation of its size and risk profile should be. It is our experience that organisations with this level of maturity carry an unacceptable level of risk and frequently fall victim to cyber attack, and often regulatory action. An organisation like the HSE should be aiming for a rating of at least 3 and higher. The HSE OoCIO has an ambition[324] to reach a maturity rating of between 2.6 and 3.5. Considerable resources and investment will be required to achieve this ambition across all 5 NIST domains. It should be noted that similar organisations that PwC has reviewed have ratings of between 2.6 to 2.95.

Figure 17: The assessment ratings of the key domains



324 Cybersecurity effectiveness assessment, IVI August 2018 (extract reported to the HSE Board November 2020)

Identify - The rating reflects the immaturity in the understanding of cybersecurity within the HSE. There was a lack of understanding of the business context, the resources that supported critical functions, and the related cybersecurity risks.

Protect - The rating is based on the lack of appropriate safeguards that should have ensured delivery of critical infrastructure services. A mature protect function would support the ability to limit or contain the impact of a cybersecurity event.

Detect - The rating reflects the absence of appropriate activities that were used to identify the occurrence of the cybersecurity event. The incident indicates that the HSE lacked the ability for timely discovery of the cybersecurity event.

Respond - The rating indicates that the appropriate activities to act regarding a detected cybersecurity incident were lacking in the HSE. The impact of a cybersecurity incident was widespread and was only contained by shutting down the network.

Recover - The rating reflects the immaturity in maintaining plans for resilience and the restoration of any capabilities or services that were impaired due to a cybersecurity incident in a timely manner, in a way to reduce the incident's impact.

Summary of NIST recommendations

Note: Recommendations are categorised as immediate (starting immediately and completed within six months) and medium-term (with a phased plan for implementation to be developed and completed within 18 months).

Figure 18: Focus area 3 key NIST recommendations

Immediate term	1. **Governance *(see tactical recommendation 1.5 in Section 4.2)* -** The HSE should recruit a senior leader to act as an interim Chief Information Security Officer (CISO) to begin with the implementation of a cybersecurity incident management process to include detection and response strategies and to assign roles and responsibilities for cybersecurity incident response throughout the HSE. A tactical cybersecurity improvement programme with appropriate governance and dedicated resources that reports into the interim CISO and can provide updates on the programme's progress into the Board. 2. **Monitoring *(see tactical recommendation 2.1 in Section 4.2)* -** The HSE should accelerate the deployment of a Security Incident Event Management ("SIEM") technology and build a Security Operations Centre ("SOC") to leverage the SIEM functionality. The SIEM, in conjunction with anti-virus tools and the threat intelligence inputs, will provide the HSE with greater threat management and the ability to detect and respond effectively to any future cybersecurity incident. 3. **Vulnerability management *(see strategic recommendation 3.2 in Section 4.1)* -** The HSE should begin a formal process of addressing all known vulnerabilities highlighted by Internal Audit and ICT across the HSE network. Acquire protective technology to monitor and block traffic that could remove sensitive data from the HSE or attempt to compromise systems supporting clinical services. Empower administrative staff via a phased deployment of Privileged Access Management and Network Administrator Software to enable the central and standard management of servers and network infrastructure. Continue with employee cybersecurity awareness training and run a phishing campaign to reinforce good cybersecurity hygiene in all employees.

Medium term	1. **Recruit a permanent CISO with a supporting team *(see strategic recommendation 3.1 in Section 4.1)* -** The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the EMT and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. The CISO should be responsible for cybersecurity operations as well as driving strategic and tactical actions to transform cybersecurity capability. The CISO should be provided with the resources to build a supporting cybersecurity team structure in the HSE. This structure would include all aspects of cybersecurity capability including operations, risk management, strategy, architecture, engineering, and investigations. 2. **Develop a specific cybersecurity strategy for the HSE *(see strategic recommendation 4.1 in Section 4.1)* -** to provide the HSE with a multi-year transformation programme to address highlighted issues from this PIR and build defence in depth over time. Such issues would include a complete IT asset register, a completed and managed CMDB that is aligned to a Service Catalogue to capture key Clinical and Corporate services, as well as a roadmap to address open Internal Audit findings each year. 3. **Governance *(see strategic recommendation 1.1 in Section 4.1)* -** Implement a dedicated cybersecurity Board oversight committee to report on risks on a regular basis. This committee should report on all relevant technology updates, patching, audit findings and threat intelligence. This committee should provide the Board with a contextualised perspective of cybersecurity risk across the HSE.

Summary of key findings and recommendations

From our assessment, PwC has identified cybersecurity capability gaps in the form of findings and designed tactical and strategic recommendations for each domain and subdomain. A summary of key findings and their corresponding recommendations are included below.

Figure 19: PIR Cybersecurity Framework

The PIR Cybersecurity Framework				
NIST domain	**Rating**	**NIST CSF category/ sub-domain**	**Key findings**	**Key recommendations**
Identify	**Initial**	**Asset Management**	**FA3. KF1** The HSE did not have a complete and accurate IT asset register, a Configuration Management Database (CMDB) or a defined asset management methodology.	**FA3. KR1** ***(see tactical recommendation 1.3 in Section 4.2)*** The HSE should continue to develop an asset register that is aligned to clinical and corporate services, as well as underpinning a process to ensure the register is maintained up to date. Doing so will allow the HSE to determine the potential impact of any future incident and effectively respond in a controlled and structured manner.
		Business Environment	**FA3. KF2** The HSE did not have a defined and agreed cybersecurity strategy nor a formalised risk appetite statement that it could be aligned to.	**FA3. KR2** ***(see tactical recommendation 1.4 in Section 4.2)*** The HSE should create a cybersecurity strategy, covering at a minimum incident detection, incident response and business recovery. It will also need to be aligned to the HSE strategy objectives and signed off by the HSE Board.
		Governance	**FA3. KF3.1** An information cybersecurity governance framework (policy, process, standards) to manage cyber risk did not exist within the HSE.	**FA3. KR3** ***(see strategic recommendation 3.2 in Section 4.1)*** The HSE should establish an appropriate cybersecurity risk and governance framework to ensure there is a consistent and clear allocation of responsibility, authority, and accountability. Including the need to establish reporting processes to ensure potential cybersecurity incidents are appropriately reported in all cases. This should provide a forum for key stakeholders e.g., Clinical Operations, Corporate Services, Third Party service managers, Sections 38s and 39s have a forum to discuss and align on cybersecurity priorities. Providing required assurance to the Board and facilitating effective management at Board level. The HSE should appoint a senior leader for cybersecurity (a CISO) who has experience rapidly reducing organisations vulnerability to threat, designing cyber security transformation programmes, and providing assurance to Boards of management. This should provide the required assurance to the Board in facilitating effective cybersecurity management.
			FA3. KF3.2 The HSE did not have a structured and robust process to ensure suspicious activity that was detected and/ or reported on applications or infrastructure (servers or on the NHN) was properly investigated and appropriately reported to the OoCIO SMT and the HSE EMT.	
			FA3. KF3.3 The HSE did not have adequate assurance processes in place to ensure the HSE EMT and Board had oversight of OoCIO operational processes. In the absence of assurance processes the HSE Board did not have sufficient visibility over the operation of these processes or comfort they were operating in line with HSE Policy and standards.	
			FA3. KF3.4 The HSE did not have a CISO or dedicated senior executive with responsibility for cybersecurity governance.	
			FA3. KF3.5 There was no dedicated committee that provided direction and oversight of cybersecurity and the activities required to reduce the HSE's cyber risk exposure.	

Identify	**Initial**	**Regulation**	**FA3. KF4** The HSE had not completed its Operator of Essential Services (OES) return to comply with the Network and Information Systems Directive (NISD) since 2019. In addition, while continual progress was made to resolve HSE Internal Audit issues, a number remained unresolved.	**FA3. KR4** ***(see tactical recommendation 2 in Section 4.2)*** The HSE should complete its required OES returns on an annual basis to ensure compliance with NISD regulations and to understand potential cybersecurity weaknesses with critical services.
		Risk Management	**FA3. KF5** A cybersecurity risk framework for the HSE did not exist.	**FA3. KR5** ***(see tactical recommendation 3 in Section 4.2)*** The HSE should develop a formal cybersecurity risk framework aligned to the business' operational risks and strategic plans.
		Supply Chain Risk Management	**FA3. KF6** Third Party Risk (TPR) was not effectively managed as no formal process existed that would assess suppliers and manage this risk appropriately. Processes did not ensure Business System Managers were appointed in all cases to be responsible and accountable for the delivery of services within the assigned service area in line with nationally defined frameworks, standards and policies.	**FA3. KR6** ***(see strategic recommendation 4.2 in Section 4.1)*** The HSE should implement a Third Party Risk Management framework that defines how third parties to the HSE are assessed for cybersecurity risks and what risk treatment plans are appropriate to address residual cyber risk.

The PIR Cybersecurity Framework				
NIST domain	**Rating**	**NIST CSF category/ sub-domain**	**Key findings**	**Key recommendations**
Protect	**Initial**	**People Security**	**FA3. KF7** There was no comprehensive formal cybersecurity awareness or training program in the HSE that ensured people were sufficiently trained to perform their duties in a manner consistent with policy.	**FA3. KR7** ***(see strategic recommendation 3.2 in Section 4.1)*** The HSE should introduce a comprehensive, formalised cybersecurity training and awareness programme that is delivered to all staff at all grades across the organisation. This should be conducted on a regular basis.
		Access Control	**FA3. KF8** The HSE Access Control Policy was last reviewed in 2014 and was not fit for purpose. In addition, there was no central access control process for all HSE applications.	**FA3. KR8** ***(see tactical recommendation 3.1 in Section 4.2)*** The HSE should introduce centralised processes and procedures to manage and review the appropriate access and identities that require access to services and data. This should be in the form of an Identity Access Management (IAM) solution that would consistently manage access across users, System Admins and third parties.
		Data Security	**FA3. KF9** ICT HSE should formalise a backup strategy to enable the efficient restoration of services.	**FA3. KR9** ***(see strategic recommendation 4.1 in Section 4.1)*** ICT HSE should implement a structured process for performing data backups and storing this data off site. Regular testing of this data should take place to ensure success recovery.
		Protective Technology	**FA3. KF10** Protective technology e.g., AV software was implemented in an ad-hoc manner, not consistently or against a clear set of threat-based requirements.	**FA3. KR10** ***(see strategic recommendation 3.1 in Section 4.1)*** The HSE should develop a strategy for adopting the appropriate protective technologies and ensure consistent deployment across the HSE network.
		IT Baseline Maintenance	**FA3. KF11** The HSE did not maintain security baselines for all operational hardware and software, and the patching processes did not ensure preventative maintenance and vulnerability management was performed in a timely manner.	**FA3. KR11** ***(see strategic recommendation 3.1 in Section 4.1)*** The HSE should develop 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.

The PIR Cybersecurity Framework				
NIST domain	**Rating**	**NIST CSF category/ sub-domain**	**Key findings**	**Key recommendations**
Detect	**Initial**	**IT Events and Threat Management (including: Detection Technology)**	**FA3. KF12** The HSE did not have the capability to detect security events relating to this incident, across its network due to a lack of technology deployed, ad hoc processes and very limited resources to monitor events.	**FA3. KR12** ***(see tactical recommendation 4 in Section 4.2)*** The HSE should develop a cybersecurity threat profile that is informed by relevant sources to enable an effective monitoring capability. This should include threat intelligence feeds to provide an informed view of the latest cyber threats relevant to the HSE. These feeds should be used in conjunction with a SIEM to inform and provide IOCs for monitoring and detecting across the HSE ICT estate. Aligned to this the HSE should implement anti-virus consistently across the estate, ensure it as well as logging and EDR outputs are aggregated and obtain a 24x7 security operations centre (SOC) to monitor the entire business and detect anomalous behaviour and events.
		Continuous Monitoring	**FA3. KF13** The HSE did not have an effective continuous monitoring capability that would identify and manage security events.	**FA3. KR13** ***(see tactical recommendation 2 in Section 4.2)*** The HSE should implement alert monitoring on all network servers, endpoint devices, and firewalls for the external and internal networks. Specific use cases for each alert should be developed for the chosen SIEM.
		Detection Processes	**FA3. KF14** The HSE did not have a structured and robust process to detect and respond to activity on the network, nor an effective escalation path to senior management for reporting and validation of events	**FA3. KR14** ***(see strategic recommendation 2 in Section 4.1)*** The HSE should implement a holistic network detection and response functionality with a dedicated team to continually monitor for and respond to alerts.

The PIR Cybersecurity Framework				
NIST domain	**Rating**	**NIST CSF category/ sub-domain**	**Key findings**	**Main recommendations**
Respond	**Initial**	**Response Planning**	**FA3. KF15** The HSE had not identified the viable clinical and services continuity options across people, process and technology, nor had the HSE defined requirements for achieving clinical and services continuity in accordance with its risk appetite. In particular the HSE did not have an appropriate response policy, plan, or run books for cybersecurity incidents.	**FA3. KR15** ***(see tactical recommendation 3 in Section 4.2)*** The HSE should develop an appropriate cybersecurity response policy, supported by plans and/or run books for cybersecurity incidents that are regularly reviewed and exercised so that it can mount an effective and efficient response in the event of a future incident.
		Communications	**FA3. KF16** The HSE did not have an internal communication plan or a crisis communication system for sharing messages in the event of a cybersecurity incident.	**FA3. KR16** ***(see strategic recommendation 4.2 in Section 4.1)*** The HSE should develop a formal internal communications plan where key internal parties such as senior leadership, voluntary hospitals, CHOs are receiving timely and consistent messages. Specifically, the HSE should develop specific runbooks and template responses for specific scenarios to aid a speedy response and ensure there is consistent communication.
		Analysis	**FA3. KF17** The HSE lacked skilled resources to respond immediately to the Incident. The HSE was reliant on third party assistance.	**FA3. KR17** ***(see strategic recommendation 2.1 in Section 4.1)*** The HSE should ensure that an appropriate response policy, plan, and process are in place to manage multiple security incidents, perform response investigations, and collect evidence to assess the best potential mitigation plan.
		Mitigation	**FA3. KF18** The HSE did not have formal mitigation strategies and tactics to isolate, remove, and monitor threats.	**FA3. KR18** ***(see tactical recommendation 3 in Section 4.2)*** The HSE should develop formal mitigation strategies and tactics to isolate, remove, and monitor threats. Key Performance Indicators (KPIs) should be put in place so that performance can be optimised.
		Improvements	**FA3. KF19** The HSE Incident Management process did not have formal processes to ensure lessons were learnt and codified from all incidents.	**FA3. KR19** ***(see strategic recommendation 4.2 in Section 4.1)*** The HSE should establish a formal process, as well as resources to ensure lessons were learnt and codified from all incidents and are maintained to reflect operational and organisational change.

The PIR Cybersecurity Framework				
NIST domain	**Rating**	**NIST CSF category/ sub-domain**	**Key findings**	**Main recommendations**
Recover	**Initial**	**Recovery Planning**	**FA3. KF20** The HSE did not have appropriate recovery plans for cybersecurity incidents. Clinical and services continuity requirements are not aligned to a formally defined risk appetite statement. Both contributed to the initial recovery response being focused on foundational technology and not clinical services.	**FA3. KR20** ***(see strategic recommendation 4.1 in Section 4.1)*** The HSE should implement a cybersecurity recovery plan that links to an asset register detailing clinical, corporate, and other priorities and test this plan on a regular basis.
		Improvements	**FA3. KF21** The HSE should formally document lessons learnt from all cybersecurity incidents to develop a continuous improvement methodology to manage any future cybersecurity incident.	**FA3. KR21** ***(see strategic recommendation 1.1 in Section 4.1)*** The HSE should develop a formal process for capturing improvements/lessons learnt following an incident.
		Communications	**FA3. KF22** The HSE's internal communications relating to the cybersecurity incident were ad-hoc and lacked an appropriately resourced team dedicated to manage the message to the organisation.	**FA3. KR22** ***(see strategic recommendation 4.2 in Section 4.1)*** The HSE should consider developing a communications strategy for cybersecurity incidents.

Focus area 3 conclusion

PwC's NIST and COBIT based assessment of cybersecurity capability within the HSE clearly indicates that the organisation is operating at a level of maturity that is reactive, ad-hoc and significantly below the level needed to afford a basic level of protection against the rapidly increasing level of cyber threats that the organisation faces. Despite efforts and endeavours at the time of the Incident, the HSE was not well prepared to identify, understand, and respond to cybersecurity attacks. Significant gaps exist across all 5 NIST domains. The cyber attack was not detected prior to the ransomware execution, protective controls and technologies were not robust enough to prevent the spread of the ransomware. Furthermore, the response and recovery was based on ad hoc structures, including processes to identify and prioritise applications and systems to be recovered. Considerable resources and sustained investment will be required to remediate the gaps across all 5 NIST domains. However, the recommendations herein, which are both tactical and strategic, will support the HSE to safeguard and protect against future cyber attacks and will also significantly improve its cybersecurity maturity ratings across all 5 domains of NIST.