9 Assessing cyber security in the public sector

9.1 The term 'cyber security' refers to the full range of measures designed to protect information and communications technology (ICT) systems to ensure the confidentiality, integrity, authenticity and availability of networks, devices and data services.

9.2 Cyber security is critically important. The amount of data stored by public bodies is growing and digital technology is performing vital functions across public services. At the same time, public bodies are facing an ever-growing range of cyber threats, and as demonstrated by the significant ransomware cyber attack against the health services in 2021, these events can have a devastating impact.[1]

9.3 The Department of the Environment, Climate and Communications (the Department) is responsible for cyber security policy in Ireland and for co-ordinating government's emergency response to any national-level cyber security incidents. The Department discharges these responsibilities through the National Cyber Security Centre (NCSC).[2]

9.4 In November 2021, the NCSC published public sector Cyber Security Baseline Standards (CSBS) which set out the measures that public sector bodies should implement in order to secure their networks.[3,4] The standards are aligned with the US National Institute of Standards and Technology (NIST) framework and cover five key themes (see Figure 9.1).[5]

Figure 9.1 Themes underpinning the framework for cyber security measures

Theme	Description
Identify	Understand the structures, policies and processes required to manage cyber security risk to systems, assets, data and capabilities.
Protect	Develop and implement appropriate and proportionate cyber security measures to deliver and protect an organisation's essential services and systems.
Detect	Develop and implement appropriate capabilities to identify, detect and defend against a cyber security event that may have the potential to affect essential services and systems.
Respond	Develop and implement appropriate activities, prioritised through an organisation's risk management process to take action to contain and minimise the impacts related to a cyber security event.
Recover	Develop and implement appropriate capabilities, prioritised through an organisation's risk management process, to restore essential services affected by a security event.

Source: Department of the Environment, Climate and Communications, Public Sector Cyber Security Baseline Standards

1 Chapter 12 'Financial impact of cyber security attack' of the *Report on the Accounts of the Public Services 2021* examined the impact of the cyber attack on the HSE and other bodies.

2 The NCSC was established in 2011 pursuant to Government decision S180/20/10/481.

3 Measure 8 of the National Cyber Security Strategy 2019 – 2024 states that the NCSC will develop a baseline security standard to be applied by all government departments and key agencies.

4 The baseline standards are subject to ongoing revision. They were last revised in November 2022 to enhance the clarity of some existing narrative.

5 The NIST cyber security framework is an internationally recognised framework offering voluntary guidance based on existing standards, guidelines and practices for organisations to better manage and reduce cyber security risk. The latest version of the framework was published in April 2018.

9.5 Subsequently, in November 2022, the NCSC published a cyber security baseline standards self-assessment form. The form is a checklist (in excel format) that public sector bodies can use internally to assess their cyber security posture against the baseline standards.[1]

9.6 This examination was undertaken to provide an overview of the cyber security self-assessment form developed and published by the NCSC and to share some user experience from its application. The examination was assisted by a consultant experienced in the area of cyber security to provide technical expertise.

An overview of the NCSC's self-assessment form

9.7 The self-assessment form describes the cyber security controls that an entity would be expected to have in place, where relevant to its operations, under 43 categories, split across the five key cyber security themes (see Annex 9A).[2] The form facilitates the assessment of each of the 43 categories against four control measures – control design, implementation, operation effectiveness and review (see Figure 9.2).

Figure 9.2 Cyber security control measures

Control measure assessment	Description
Cyber security policy management system i.e. **control design objectives**	The correct practices and procedures are in place to ensure that ▪ the relevant risks are addressed ▪ the scope is adequate ▪ the controls cannot be by-passed ▪ correct systems and processes are covered
Implementation	The controls implemented ▪ are operated by appropriate individuals ▪ operate at the adequate frequency ▪ allow the control operator to access reliable information ▪ allow issues identified to be adequately addressed
Operation effectiveness	The controls continue to operate effectively and ▪ are still valid ▪ have not been degraded over time ▪ non-compliance/control breaches have not increased
Review of controls	The controls are reviewed regularly to ensure they continue to achieve the desired outcomes

Source: The National Cyber Security Centre, Cyber Security Baseline Standards self-assessment form

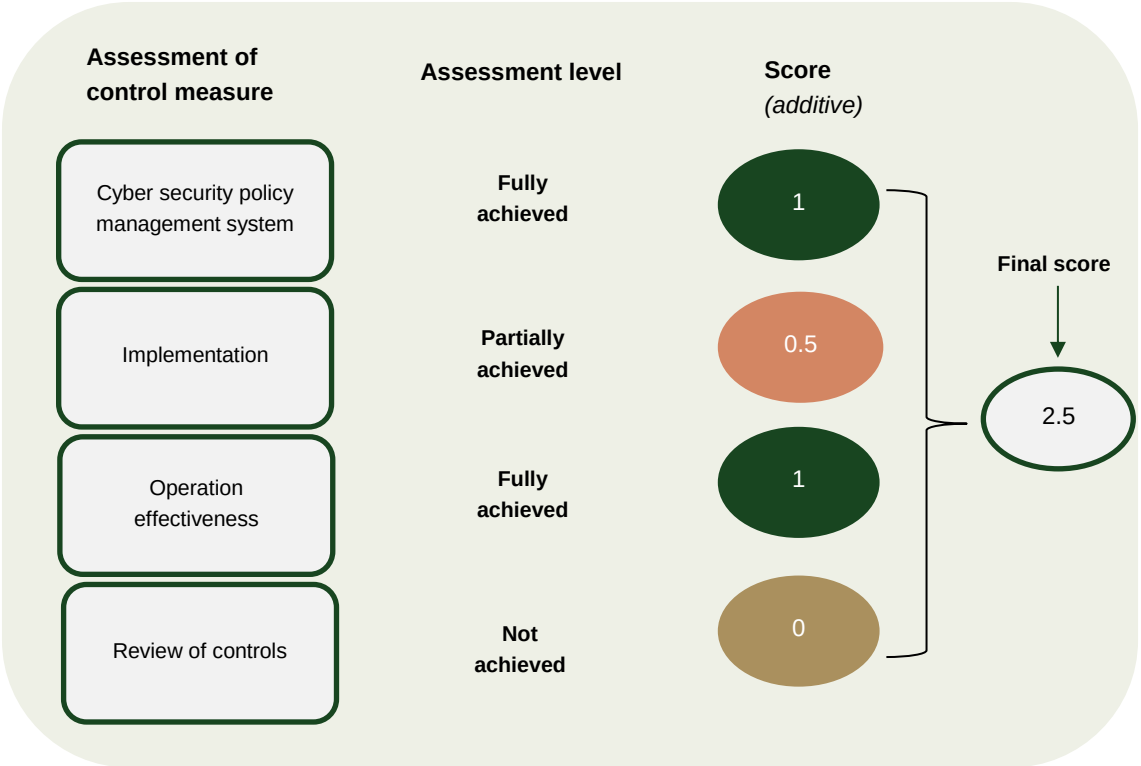
1 The self-assessment form can be found at www.ncsc.gov.ie/guidance.

2 Some categories are further divided into subcategories. There are around 100 subcategories in total, across the five themes.

9.8 To facilitate the identification of cyber security gaps and risks in relation to cyber security, the self-assessment form defines three assessment levels of fully, partially or not achieved for each cyber security control across each of the control measures. A score is assigned for each level (see Figure 9.3). The overall score for each of the 43 categories can range from zero to four as the four control measure assessments in Figure 9.2 are applied to each of the categories and scored from zero to 1.

Figure 9.3 Assessment of cyber security controls

Assessment level	Overview of control level achieved	Score
Fully achieved	Defines an organisation fully achieving the implementation and operation of a comprehensive set of policies and practices. It is intended that all positive indicators would normally be present to support an assessment of 'fully achieved'.[a]	1
Partially achieved	Defines an organisation partially achieving the implementation and operation of a comprehensive set of policies and practices. It is also important that partial achievement is delivering specific worthwhile cyber security benefits. An assessment of 'partially achieved' should represent a significant effort has been made to implement and operate a set of practices and procedures for each relevant sub category.	0.5
Not achieved	Defines an organisation not achieving the implementation and operation of a comprehensive set of policies and practices. It is intended that the presence of any one indicator would normally be sufficient to justify a control review assessment of 'not achieved'.	0



Source: National Cyber Security Centre, Cyber Security Baseline Standards self-assessment form

Note: a All positive indicators refer to all elements of the relevant control being in place.

9.9 The appropriate level of cyber security controls and practices for an organisation is best determined by those charged with governance. The benefits of operating at a higher level must be balanced with the increased cost associated with moving to that level.[1] However, it is not appropriate for a public sector organisation to be operating at the 'not achieved' level, unless the control was deemed irrelevant for the organisation.

9.10 The NCSC has stated that it developed the form for self-assessment purposes, and therefore it is considered a compliance support rather than a compliance-driving tool.

9.11 Our review found that the form is well aligned with the cyber security baseline standards. It includes tabulated result calculations that should enable efficient reporting and dashboards for effective leadership for those public bodies that use it as intended to support the development of their ICT security regime. The ratings are straightforward and easy to apply based on the questions presented.

9.12 The assessment tool provides useful features beyond the main self-assessment excel spreadsheet, which include

- tabular results scorecard and summary reporting dashboard
- self-assessment worksheets for each of the five baseline themes with detailed guidance
- a corrective action plan worksheet with risk ratings and status tracking
- a detailed statistical breakdown of results.

9.13 However, the example questions given to users to help them consider their organisation's cyber security level of maturity do not mention documentation or recording. In the absence of complete and robust documented and/or recorded policies and procedures, it is likely some controls are operating in an ad hoc environment. The self-assessment form may infer documentation/recording but it would benefit from stating explicitly that a good policy management system will have documented/recorded policies and procedures that are updated as any changes are introduced.

9.14 This review also found that the self-assessment form is detailed and lengthy, as would be expected. However, it requires a significant amount of effort to complete and will likely require a collaborative effort within any organisation to conduct the self-assessment.

User experience on the application of the self-assessment form

9.15 The Department of Foreign Affairs (DFA) was selected for the purpose of this examination as it is involved in direct and critical service provision to citizens. It has been actively reviewing its cyber security, and its Evaluation and Audit Unit (EAU) engaged a third party service provider in early 2022 to undertake an assessment of the DFA's cyber security preparedness against the NCSC's baseline standards — the NCSC's self-assessment tool was not available at that time.[2] For the purposes of this examination, the DFA agreed also to complete the NCSC's self-assessment form and to provide feedback on its use (see Figure 9.4).

9.16 The DFA stated that the assessment of an organisation using a tool like the self-assessment form should be carried out by the organisation itself, with testing of the findings conducted by a suitably qualified person to get the best value from the exercise; to ensure risks and gaps are correctly understood and noted; and to avoid the risk of false positives/negatives in the assessment.

1 The benefits to an organisation of operating at a higher level of cyber security depend on its nature, complexity and activities. An organisation should assess whether the benefits outweigh the costs associated with operating at the higher standard.

2 This assessment facilitated the DFA's subsequent completion of the NCSC's self-assessment tool requested by the examination team.

9.17 The internal audit report was finalised in September 2022 and included five high, 33 medium and eleven low risk recommendations, which broadly covered the areas of policies and procedures; logging and monitoring; and business continuity planning. The DFA developed a detailed implementation plan to address the recommendations. The DFA's management board is overseeing the progress on implementation and reports on the progress to the DFA audit committee.

Figure 9.4 Department of Foreign Affairs — feedback on use of the self-assessment form[a]

Control	Description
About the self-assessment form	▪ Straightforward ▪ Logical ▪ Aligned with the international NIST cyber security framework
Challenges	▪ Sending sensitive information and security designs to external support partners — can be overcome by more on-site demonstrations, on-site evidence gathering and consultations with key technical staff [b] ▪ Challenge around legacy software and replacement timelines to achieve some key standards — resulting in some recommendations being outstanding for long periods ▪ Challenge around business continuity standard outcomes – responsibility to implement recommendations may reside outside of the IT unit ▪ Due to some overlap between the baseline standards, where multiple outcomes can be addressed by implementing one recommendation, the failure of one large outcome in a particular standard could result in several standards not being achieved across a number of themes ▪ Results from the application of the self-assessment form become a very confidential output — usually in documented form — which needs to be appropriately stored, protected and access restricted ▪ Effort involved to complete the assessment — the DFA stated that the assessment took approximately two weeks to complete, while the testing and evidence gathering phase lasted approximately four months
What worked well	▪ The form structure is aligned to the NIST cyber security framework but is designed with public bodies in mind i.e. not using an assessment purely designed for private entities ▪ When the assessment has been completed once, this allows the mapping of the baseline cyber security landscape, and therefore the exercise should be easy to repeat ▪ The implementation of the NCSC baseline standards in essence, ensures compliance with the NIST cyber security framework
Lessons learned	▪ Giving a point in time measurement, it should be used to create a baseline that can be measured against subsequently ▪ It should not be seen as a measure of IT performance ▪ Gaps and risks identified should be used to roadmap future investment or any required implementation activities in ICT strategy/business plans ▪ Important to highlight any instances of good practice and what is being achieved

Source: Department of Foreign Affairs

Notes: a The feedback also reflects the DFA's experience from the cyber security assessment undertaken in 2022.

b External support partners relate to any third party body utilised during the assessment.

9.18 The NCSC currently uses the provisions of the Network and Information System (NIS) Directive to frame the national effort to protect critical national infrastructure.[1] In December 2022, a revised Directive — NIS 2 — was published.[2] Under the NIS 2 Directive, there is a requirement for a national competent authority to check compliance of public administration with the provisions of the Directive.

9.19 Member states are required to adopt and publish the measures necessary to comply with the NIS 2 Directive by mid October 2024. The Department has stated that it plans to seek Government approval for the NIS 2 transposition model during 2023.

Conclusions and recommendations

9.20 Cyber security is a critical issue for most public bodies, who increasingly are relying on ICT to assist in providing public services. Those charged with governance and management of public bodies need to be able to provide assurance publicly to taxpayers and to service users that a high level of ICT security is in place. Such public assurance has to be achieved without providing assistance to malefactors who might seek to exploit weaknesses in public bodies' systems.

9.21 The NCSC has published cyber security standards that set out the baseline measures that public sector bodies should implement to secure their networks. It has also published a cyber security baseline standards self-assessment checklist to help public sector bodies assess their cyber security posture against the standards. The form was developed for self-assessment purposes rather than as a compliance-driving tool.

9.22 Our review of the guidance material indicates that the self-assessment form is well developed and comprehensive. It is well aligned with the cyber security baseline standards. It includes tabulated result calculations that should enable efficient reporting and dashboards for effective leadership for those public bodies that use it as intended to support the development of their ICT security regime. The ratings are straightforward and easy to apply based on the questions presented.

9.23 The self-assessment form is detailed and lengthy (as would be expected) and requires a significant amount of effort and collaboration to complete. It would benefit from stating explicitly that a good ICT management system will have documented/recorded policies and procedures that are updated as any changes are introduced.

9.24 The DFA completed the self-assessment form and found that it was straightforward and logical to use. While it identified a number of challenges with the self-assessment process, which included the significant effort involved in completing the assessment, it cited that once the assessment has been completed, facilitating the mapping of the baseline cyber security landscape, it should be easier to repeat. It recommended that following the self-assessment, testing of findings should be conducted by a suitably-qualified independent person to get the best value from the exercise.

9.25 Overall, the self-assessment checklist is a good model for public sector bodies to assess their cyber security practices and controls and such bodies are encouraged to build the self-assessment process into their existing cyber security review processes. There is also scope for the NCSC to work closely with users of the self-assessment form until it becomes embedded within public sector bodies' cyber security assessment practices.

1 The Directive (EU) 2016/1148 was formally adopted by the EU in July 2016 and was transposed into national law in September 2018 under SI 360 of 2018. The main objective of the Directive is to ensure that there is a common high level of cyber security across member states.

2 The NIS 2 Directive was published in the Official Journal of the European Union as Directive (EU) 2022/2555 on Measures for a high common level of cyber security across the Union.

Recommendation 9.1

The NCSC should promote compliance with the Public Sector Cyber Security Baseline Standards by actively promoting use of the self-assessment form through communications and outreach.

Accounting Officer's response

Agreed

The NCSC agrees with this finding and believes that widespread adoption of the cyber security baseline standards (CSBS) by public sector bodies will significantly enhance the security of Ireland's public services.

Timeline for implementation

The NCSC will promote the CSBS in a planned Cyber Security Month campaign in October 2023 in the context of the upcoming NIS 2 Directive which puts public administration in scope of regulation. Additionally, the NCSC will continue to raise awareness of the guidance and associated self-assessment tool in its public and private engagements on an ongoing basis.

Recommendation 9.2

The NCSC should introduce a feedback mechanism whereby public bodies can share any issues or challenges identified from using the self-assessment form that the NCSC can address in future iterations of the form.

Accounting Officer's response

Agreed

The NCSC agrees that feedback from users that have implemented the CSBS is useful to ensure continued improvement in order to keep abreast of technological change.

Timeline for implementation

The NCSC will establish a dedicated mailbox and invite users to submit feedback on their experience implementing the CSBS by Q4 2023. The NCSC will also undertake a review and update (as required) of the CSBS before Q4 2024, in particular ensuring that the guidance is in compliance with the Cybersecurity Risk Management measures outlined in the NIS 2 Directive.

9.26 The NIS 2 Directive places a range of cyber security requirements on entities and sectors covered by the Directive, including the requirement for a national competent authority to check public administration compliance with the provisions of the Directive.

9.27 As yet, no such authority has been appointed although the NCSC stated that the Department is currently drafting the necessary 'heads of bill' including provisions relating to the designation of a competent authority. The NCSC stated that the aim is to have the legislation to give effect to the NIS 2 Directive enacted in 2024.

Annex 9A Cyber security categories by theme

Source: Department of the Environment, Climate and Communications, Public Sector Cyber Security Baseline Standards