NIS Compliance Guidelines for Operators of Essential Service (OES)

August 2022

Contents

Executive Summary

On 6th July 2016, the European Union formally adopted Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive)[1]. The main objective of the NIS Directive is to ensure that there is a common high level security of network and information systems across Member States and as such, it requires Member States to take a number of significant measures with regard to Cyber Security. The Directive was formally transposed into Irish legislation under the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulation 2018 (S.I. 360 of 2018[2]) (the 'NIS Regulations') on 18th Sept 2018.

The measures required include the application of a set of binding network and information system security and incident reporting obligations to a wide range of critical infrastructure operators, termed 'Operators of Essential Services' (or OES) including energy, transport, health, drinking water supply and distribution and digital infrastructure. Note that in giving effect to the NIS Directive at national level, the NIS Regulations provide that for OES in the banking and financial market infrastructure sectors only the incident reporting obligations in the NIS Regulations apply.[3] The security obligations applicable to entities in the banking and financial market infrastructure sectors are set out in sector specific EU Regulations. The NIS Directive also requires the application of a new regulatory regime of binding security and incident reporting obligations on so called Digital Service Providers (DSPs). These include online marketplaces, cloud computing providers and search engines providers.

Regulation 25(1) of the NIS Regulations permits the Minister for Communications, Climate Action and Environment to make Guidelines for the purpose of providing practical guidance as regards compliance by Operators of Essential Services and relevant Digital Service Providers with their obligations under the Regulations. This document establishes a set of Guidelines designed to assist OES in meeting their network and information system security and incident reporting requirements under Regulations 17 and 18 of the NIS Regulations. These guidelines are both technology neutral and non-sector specific to allow OES in different sectors adapt these to meet their needs, and to

---

[1] Directive 2016/1148 concerning measures for a high common level of security of network and information systems
[2] Statutory Instrument 360 of 2018
[3] Regulation 3(2) provides that Regulation 17 (security requirements in respect of operators of essential services) does not apply to entities designated as OES in the banking and financial market infrastructures sectors.

evolve their sector specific response along with technological advances and business requirements.

While these guidelines were developed to improve cyber security risk management and incident response in Operators of Essential Services in accordance with their obligations under the NIS Regulations, they can be used by organisations in any sector or community. The guidelines enable organisations – regardless of size, degree of cyber security risk, or cyber security sophistication – to apply the principles and best practices to improve security and resilience.

The guidelines are not a universal approach to managing cyber security risk for critical infrastructure. Many sectors will have unique risks, threats and vulnerabilities which require a sector specific approach. The fundamental aim of the guidelines is to establish cross- sectoral measures to create a high common level of security of network and information systems across the Union.

Revised and updated guidelines may be adopted at a later date (again following the consultation process prescribed in Regulation 25) following feedback on implementation of these guidelines and lessons learned from security incidents.

1. Introduction: National Competent Authorities and Operators of Essential Services

Under Regulation 7 of the NIS Regulations, Ireland has designated two National Competent Authorities in respect of Operators of Essential Services who shall review the application of the Regulations:

    I.   The Minister for Communications, Climate Action and Environment is the National Competent Authority for all sectors set out in Schedule 1 of the NIS Regulations, excluding the Banking and Financial Market Infrastructures sectors; and

    II.   The Central Bank of Ireland is the National Competent Authority for the Banking and Financial Market Infrastructures sectors.

Regulation 12 permits the National Competent Authority for the relevant sector in respect of which it is the National Competent Authority to designate a person as an OES in respect of an essential service where it is satisfied that:

a) the person provides the essential service in the State,

b) the person has an establishment in the State,

c) the person is a person of a type set out in Column (3) of Schedule 1 of the NIS Regulations,

d) the sector and, where appropriate, subsector in which the essential service is provided are each a sector and subsector set out in Schedule 1 of the NIS Regulations;

e) the provision by the person of the essential service depends on network and information systems, and

f) an incident affecting the provision by the person of the essential service would have significant disruptive effects on the provision of that service in the State

Schedule 1 of the NIS Regulations sets out the types of entities in the various sectors and subsectors covered by the Regulations from which Operators of Essential Services will be designated, where they meet the criteria specified in Regulation 12. As set out in

Regulation 13, where a National Competent Authority proposes to designate a person as an OES, the person will be notified in writing and afforded an opportunity to make representations, following which a decision will be made by the relevant National Competent Authority as to whether to designate the person as an OES in respect their particular category of sector, subsector or essential service. The OES designation process is currently underway, but the list of OES will not be published for security reasons.

The following statutory powers are afforded the designated National Competent Authorities under the Regulations in respect of the sectors referred to above[4]:

➢ Both the Minister and the Central Bank of Ireland may seek information via a binding information notice (Regulation 31)

➢ The Minister (as National Competent Authority in respect of the sectors referred to above) may carry out security assessments of the compliance by an OES with its obligations under Regulation 17 and 18 (by means of a security audit or otherwise) and may appoint an independent person or auditor to carry out the assessment on his behalf (Regulation 27)

➢ The Minister (as National Competent Authority in respect of the sectors referred to above) may appoint authorised officers to examine a place owned or operated by an OES for the purpose of assessing compliance with the Regulations (Regulation 28)

➢ The Minister (as National Competent Authority in respect of the sectors referred to above) may issue a compliance notice where of the opinion that a provision of the Regulations is not being complied with, which may include directions as to the action to be taken to remedy the non-compliance and to bring the notice to the attention of the public or any person who may be affected by the non-compliance (Regulation 30)

---

[4] Part 8, Implementation and Enforcement, S.I 360 of 2018

2. Security Requirements in respect of Operators of Essential Services

Regulation 17 of the NIS Regulations sets out network and information system security obligations for operators of essential services. As above, Regulation 17 does not apply to entities designated as OES in the banking and financial market infrastructures sectors:[5] the security obligations applicable to entities in the banking and financial market infrastructure sectors are set out in sector specific EU Regulations.

Regulation 17(1) provides that operators of essential services shall –

➢ take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which it uses in its operations, and

➢ take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used by it for the provision of the essential services in respect of which it is designated as an operator of essential services with a view to ensuring the continuity of the provision by it of those services.

Regulation 17(2) goes on to provide that the measures taken shall ensure a level of security of network and information systems appropriate to the risks posed.

It will be the responsibility of the OES to demonstrate that they are complying with the security and incident notification obligations under the Regulations. These guidelines offer a sample approach for OES with regard to compliance with their obligations, identifying a best practice framework which if adopted would be likely to achieve the outcomes set out in Regulation 17 (1) and (2); taking appropriate technical and organisational measures to manage risks posed the security of the network and information systems used in its operations and minimising the impact of incidents on those systems, with a view to ensuring the continuity of the essential services.

---

[5] Regulation 3(2) provides that Regulation 17 (security requirements in respect of operators of essential services) does not apply to entities designated as OES in the banking and financial market infrastructures sectors.

Note also that the Directive proposes that OES adopt a "culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced" so that they do not face "a disproportionate financial and administrative burden".

It is recognised that it is not possible to fully protect information system from all potential security incidents. As such, the security requirements in the NIS Regulations are aimed at reducing risk throughout the incident response lifecycle, and should not be considered to render systems or entities invulnerable. Furthermore, the enforcement provisions in the NIS Regulations will apply where an OES has failed to introduce or properly apply appropriate network and information system security measures, either in the normal course of events or in the aftermath of an incident. However, the fact that an OES may have experienced an incident does not automatically mean that further enforcement action will follow. Rather, the role of the Minister in these circumstances would be to assess whether an affected OES had properly assessed the risks to their service, was managing the assessed risks appropriately and that the appropriate security measures were in place.

Lastly, when OES are formally designated as such, it will be with reference to the essential service or services that they provide. The security measures that the OES chooses to apply should specifically identify those network and information systems used for the provision or support of those services.

3. General Principles of Network & Information System Security

OES should take the following principles into account when applying security measures.

Measures should be:

➢ **Effective** in increasing the cybersecurity posture of an OES in relation to the threat landscape now and into the foreseeable future.

➢ **Tailored** to ensure effort is applied to measures which will have the most impact in relation to enhancing the security of an OES.

➢ **Compatible** to address cross-sectoral vulnerabilities, and complemented with sector specific security measures.

➢ **Proportionate** to the risks, with an emphasis on protecting systems underpinning essential services.

➢ **Concrete** and easy to understand, to ensure the measures are actually implemented in full and actively enhance the cybersecurity posture.

➢ **Verifiable** to ensure the OES can provide the Minister with evidence of the effective implementation of security measures.

➢ **Inclusive**, to ensure measures are applied to cover all five themes (Identify, Protect, Detect, Respond, Recover).

4. Overview of the NIS Guidelines in respect of OES security requirements

The technical and organisational measures identified in these guidelines, including at Appendix A and B, offers a best practice framework for ensuring the protection of network and information systems. The guidelines represent a sample approach that could be adopted by OES to manage the risks posed to the security of the network and information systems used in their operations and to minimise the impact of incidents affecting the those systems.

This framework is designed to:

➢ enable OES to describe their current cyber security status;

➢ provide an outcome-focused approach of the security principles for network and information systems;

➢ be compatible with and complement existing Risk Management, Standards and Cyber Security Programs in use by OES;

➢ enable the identification of effective cyber security improvement activities;

➢ be as straightforward to apply as possible;

➢ assist the Minister in carrying out effective security assessments (by means of security audit or otherwise) of the compliance by an OES with its obligations under Regulation 17 the NIS Regulations.

The security guidelines consist of five themes which provide a high level view of an organisation's management of cyber security risk. These five themes are Identify, Protect, Detect, Respond and Recover. The security guidelines in Appendix B describes the categories and subcategories under each theme which define a wide-ranging set of cyber security objectives, desired outcomes, and applicable references that are common across the critical infrastructure sector.

Non applicability

As the guidelines are designed for use across multiple sectors and subsectors, the outcomes described may not be relevant in all situations. As a result, it will be the

responsibility of individual OES to determine how best to satisfy the security requirements as per Regulation 17.

Standardisation

The use of internationally accepted standards and specification relevant to the security of network and information systems is encouraged in order to promote convergent implementations of the requirements in Regulation 17.

A.   Identify

OES should develop the organisational understanding, structures, polices and processes to manage cyber security risk to the network and information systems of the organisations essential services, assets, data, and capabilities.

The activities in the Identify area are critical to the understanding of the business context and resources that support critical functions and the related cyber security risks that enable an organisation to focus its efforts and resources.

  i.   **Asset Management**

All systems and/or services that are required to deliver or support essential services should be identified, understood and documented. This includes data, personnel, devices, systems and facilities.

  ii.   **Business Environment**

The organisation's mission, objectives, stakeholders, and activities are understood, prioritised and documented. This information is used to inform cyber security roles, responsibilities, and risk management decisions.

  iii.   **Governance**

The policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are identified, understood and documented, and inform the management of cyber security risk.

  iv.   **Risk Assessment**

Cybersecurity risk to organisational operations, assets, and individuals are identified and understood.

v.   Risk Management Strategy
Priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

vi.   Supply Chain Risk Management
Weaknesses in supplier security can be used to circumvent an organisations internal controls. Processes are established and implemented to identify, assess and manage supply chain risks.

B.   Protect

The protect function is based on an OES being able to protect the elements deemed as critical (data, personnel, devices, systems, facilities) to their organisation based on the people, processes and technologies in place. Critical to protecting an OES is the premise of developing and implementing the appropriate and proportionate security measures that allow the delivery and protection of the organisations essential services and systems.

The activities in the protect area should be performed consistent with the organisations risk strategy defined in the Identify function.

i.   Identity Management, Authentication and Access Control
Access to assets and associated facilities is limited to authorised users, processes, and devices, consistent with the principle of least privilege and is managed consistent with the assessed risk.

ii.   Awareness and Training
Personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related documented policies, procedures, and agreements.

iii.   Data Security
Information and records (data) are managed consistent with the risk strategy to protect the confidentiality, integrity, and availability of information and systems.

iv. **Service Protection Policies, Processes and Procedures**

Define, communicate and document appropriate policies, processes and procedures that direct the overall organisational approach to securing systems and data that support delivery of essential services.

v. **Maintenance**

Maintenance and repairs of critical system components are performed consistent with policies and procedures.

vi. **Protective Technology**

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

C.   Detect

Develop and implement the appropriate capabilities to identify, detect and defend against the occurrence of a cyber security event that may have the potential to affect essential services.

The Detect function enables a timely response and the potential to limit or contain the impact of potential cyber incidents.

i. **Anomalies and Events Detection**

Anomalous activity is detected in a timely manner and the potential impact of events is understood. All aspects in the anomalies and events detection process must be documented.

ii. **Security Continuous Monitoring**

The information system and assets are monitored in order to identify potential cyber security events and verify the effectiveness of protective measures. All aspects of the security continuous monitoring process are documented.

iii. **Detection Processes**

Detection processes and procedures are documented, maintained and tested to verify effectiveness and ensure continuous improvement.

D. Respond

The Respond function should be performed consistent with the business context and risk strategy defined in the Identify area. The activities in the Respond area should support the ability to contain and minimise the impact of a potential cyber security event.

i. Response Planning
Response processes and procedures are executed, maintained and documented, to ensure timely response to cybersecurity events with an actual or potential adverse impact.

ii. Communications
Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

iii. Analysis
Analysis is conducted and documented to ensure effective response and support recovery activities.

iv. Mitigation
Activities are performed and documented to prevent expansion of an event, mitigate its effects, and eradicate the incident.

v. Improvements
Organisational response activities are improved and documented by incorporating lessons learned from current and previous detection/response activities.

E. Recover

Develop and implement the appropriate capabilities, prioritised through the organisations risk management process, to restore the capabilities of essential services that were affected through a cyber security incident.

The activities performed in the Recover area are performed consistent with the business context and risk strategy defined in the Protect area. The activities in the Recover area support timely recovery to normal operations to reduce the impact from a cyber security incident.

i. **Recovery Planning**

Recovery processes and procedures are executed, maintained and documented to ensure timely restoration of systems or assets affected by cyber security incidents.

ii. **Improvements**

Recovery planning and processes are improved and documented by incorporating lessons learned into future activities.

iii. **Communications**

Restoration activities are coordinated with internal and external parties, such as coordinating centres, Internet Service Providers, owners of impacted systems, victims, other CSIRTs, vendors and other stakeholders. The processes used for communication will be documented.

5. Incident Notification by Operators of Essential Services

5.1 Introduction

Regulation 18 of the NIS Regulations imposes a mandatory obligation on all entities designated as OES (i.e. including entities designated as OES in the banking and financial market infrastructure sectors) to notify the computer security incident response team (CSIRT) in the Department of Communications, Climate Action and Environment of any network and information system security incidents that have a "significant impact" on the continuity of an essential service provided by it, within 72 hours of becoming aware of an incident.

> 18. (1) (a) An operator of essential services shall notify the CSIRT in accordance with paragraph (2) of any incident concerning it that has a significant impact on the continuity of an essential service provided by it in respect of which it is designated as an operator of essential services.
>
> 18. (1) (b) An operator of essential services who relies on a third-party digital service provider for the provision of an essential service in respect of which it is designated as an operator of essential services shall notify the CSIRT in accordance with paragraph (2) of an incident affecting the digital service provider which has a significant impact on the continuity of the essential service provided by the operator.
>
> 18. (2) A notification in respect of an incident shall be made under paragraph (1) without delay after the incident occurs and, in any event, not later than 72 hours after the operatory of essential services becomes aware of the occurrence of that incident.

The CSIRT is the computer security incident response team in the Department of Communications, Climate Action and Environment designated as the computer security incident response team in the State for the purposes of the Regulations.

An "incident" is defined in Regulation 2 as meaning "any event having an actual adverse effect on the security of network and information systems".

Regulation 2 defines "network and information system" as meaning:

a) an electronic communications network within the meaning of Regulation 2 of the European Communities (Electronic Communications Networks and Services) Framework) Regulations 2011(S.I. No. 333 of 2011),

b) any device or group of inter-connected or related devices, one or more of which, pursuant to a programme, perform automatic processing of digital data, or

c) digital data stored, processed, retrieved or transmitted by elements referred to in paragraph (a) or (b) for the purposes of the operation, use, protection and maintenance of the data;

"security of network and information systems" is defined as meaning "the ability of a network and information system to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the related services offered by, or accessible via, those network and information systems".

5.2   Incident notification

Taken together, the above provisions have the effect that an OES is required to report any incident affecting the security of their network and information systems that results in a significant impact on the continuity of the service for which they are designated an OES. This would include incidents affecting DSP's or any 3rd party suppliers on which the OES relies on for their essential services. The Regulations use the term 'event' – as such, there is no requirement for a third party actor to be involved or an 'attack' to have taken place for an incident to be notifiable. Rather, 'any event' includes accidents, equipment failures, software errors, or external events (such as fires or floods) – all of these may lead to notifiable incidents.

OES shall notify the CSIRT of any incident which has a significant impact on the continuity of an essential service provided by them. The notification of an incident refers to only the essential service under which the OES is designated. The timeline as stated in para 18 (2), requires OES to notify the CSIRT in respect of an incident without delay after

the incident occurs and, not later than 72 hours after the operator of essential services concerned becomes aware of the occurrence of that incident.

Once an incident that has been notified to the CSIRT under Regulation 18 (1) has been resolved, the OES is required to further notify the CSIRT that the incident has been resolved, as per Regulation 18 (9).

The timeframe within which the OES must notify the CSIRT of resolution is no later than 72 hours after resolution of the incident, as per Regulation 18 (10).

5.3   Determining the Significant Impact on the Continuity of the Essential Service

Regulation 18(4) sets out the following three parameters that must be taken into account in particular in determining whether an incident affecting an essential service provided by an OES has a significant impact on the continuity of the essential service provided:

a) the number of users affected by the disruption of the essential service;
b) the duration of the incident;
c) the geographical spread of the area affected by the incident.

By way of practical guidance to OES in the various sectors and subsectors covered by the NIS Regulations as to when an incident should be notified to the CSIRT, indicative, sector specific Incident Reporting levels are set out in **Appendix C**, at which an incident occurring in the relevant sector or subsector will likely reach the level of "significant impact" within the meaning of the Regulations, taking into account the parameters identified in Regulation 18(4).

5.4   Incident Reporting Information

As per Regulation 18 (3) of the NIS Regulations, incident notifications made to the CSIRT are required to contain certain information, to the extent to which an OES may reasonably be expected to have such information, as follows:

➤ the operator's name;
➤ the category of sector and where appropriate, subsector and the essential service provided by it which is affected by the incident;

➢ the time the incident occurred;

➢ the duration of the incident;

➢ information concerning the nature and impact of the incident;

➢ information concerning any or any likely cross-border impact of the incident;

➢ any other information that may be of assistance to the CSIRT.

5.5 Incident Reporting Procedure

The Incident Reporting template below should be used by an OES to notify the CSIRT of an incident. The template has been developed pursuant to Regulation 18(13) and will be circulated to entities designated as OES in accordance with Regulation 12.

Please email incident@ncsc.gov.ie or certreport@dccae.gov.ie to receive a copy of the incident reporting form.

NCSC — Operator of Essential Services - Incident Notification Form

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Report Type	Date	NIS Reportable Incident
First Report (no later than 72 hours after identifying incident)	Click here to enter a date.	Choose an item.
Interim Report (optional)	Click here to enter a date.	
Final Report (no later than 7 days after resolving incident)	Click here to enter a date.	

Service Provider Details			
Organisation Name			
Sector	Choose an item.		
Contact Person			
Role/Title			
Phone		**Email**	
Availability			
Other Interested Parties			

Incident Details

Description Must include time and date incident first identified.	*High level description of incident.*
Service(s) affected	*What essential services were affected:*

Nature & Impact	Duration	
	Number of Affected Users	
	Nature of Compromise (authenticity, integrity, availability, confidentiality of data or service)	
	Geographic Spread	
	Cross Border Impact	
	Data Loss/Breach	
	Material Damage	
	Financial Loss	
	Reputational Damage	
	Risk to Health, Safety or possible loss of life	

Root Cause (if known)	Please tick relevant box					
	System failure (e.g. software bug, flawed procedure, hardware failure, etc.)		**Natural disaster** (e.g. storm, earthquake, etc.)		**Human error** (e.g. mistake, negligence, etc.)	
	Malicious action (e.g. cyber-attack, vandalism, theft, software bug, DDoS attack, etc.)		**3rd party failure** (e.g. power cut, internet outage, etc.)		**Other** (please provide further detail below)	
	Root Cause narrative:					

Severity	Please tick relevant box	
	Major Impact	
	Moderate Impact	
	Minor Impact	
	Not Yet Known	
	No Impact (report for information only)	

Current Situation	
Investigation Status	Choose an item.
Actions Taken to mitigate or contain	
Expected Time to Resolve	
Support Required from CSIRT	Choose an item. Please provide further information:
Notifications Issued (Impacted Parties, Executive Management, Law Enforcement, Data Protection Commissioner)	

Information Sharing	
Full Incident Information (ICT assets affected, IoC's, etc.)	
Lessons Learned (e.g. vulnerabilities/weaknesses exposed, new threats identified, inadequate processes/controls, staff awareness training needs, success of business continuity and disaster recovery plans, etc.)	

Please email completed form to certreport@decc.gov.ie

The Incident Reporting Template covers five specific areas, which are set out in terms of guidance below;

1. Report Type
    a. First Report

       Date for submission of first report.
    b. Interim Report

       Date for submission of interim report. The interim report is optional but beneficial to the CSIRT with respect to supporting an OES during an incident.
    c. Final Report

       Date for submission of final report.

2. Service Provider Details
    a. Organisation Name

       Name of the Operator of Essential Service
    b. Sector

       The sector and sub sector under which the Operator is designated
    c. Contact person

The contact person in the OES who is the central point of contact for the incident, and who is able to provide relevant incident details to the CSIRT.

d. Role/Title

The role/title of the contact person in the Operator

e. Phone/Email

The phone number and email of the contact person in the Operator

f. Availability

The availability of the person in the Operator with respect to communications during or after the incident being reported

g. Other Interested Parties

Any other third parties who may have a legitimate interest in the incident.

3. Incident Details

a. Description

- Time/date incident first identified by the OES
- May include internal reference number for incident
- High level description of incident, meaning an overview of the incident and situation.

b. Service(s) Affected

Specification of the essential service which has been affected by the incident

c. Nature and Impact

The nature and impact of incident;

- Duration of the incident
- Number of Users affected by the incident
- Nature of the Compromise – is the incident a compromise of authenticity, integrity, availability, confidentiality of data or service. Should be specified.
- Geographic Spread of the incident.
- Cross Border Impact of the incident.
- Data Loss/Breach if they have occurred.
- Material Damage
- Financial Loss to the Operator
- Reputational Damage to the Operator
- Risk to Health, Safety or Possible Loss of Life as a result of the incident.

d. Root Cause

The root cause of the incident, if known should be specified. A number of check boxes are presented as to the category of the root cause. A narrative of the root cause should also be specified.

e. Severity

The severity of the incident. A scale from no impact to major impact is presented. The severity should be articulated here through the indication using the categories presented.

4. Current Situation

   a. Investigation Status

   The status of the incident should be outlined here based on the drop down list presented. An indication should be specified.

   b. Actions Taken To Mitigate/Contain

   A narrative or indication of the actions taken to mitigate or contain the incident should be presented.

   c. Expected Time To Resolve

   An indication on the time that is required to resolve the incident should be indicated.

   d. Support Required From CSIRT

   An indication as to whether support is required from the CSIRT is required.

   e. Notifications Issued

5. Information Sharing

   a. Full Incident Information

   The full incident information should be outlined here in full, with all details presented. This should include for example, ICT assets affected, IOC's and any other relevant technical information that will allow the CSIRT to investigate the incident.

   b. Lessons Learned

   The lessons learned should be presented here with examples such as vulnerabilities/weaknesses exposed, new threats identified, inadequate processes/controls, staff awareness training needs, success of business continuity and disaster recovery plans, but not limited to just these. All relevant information should be presented.

Appendix A: Framework Infographic

Appendix B: Security Guidelines

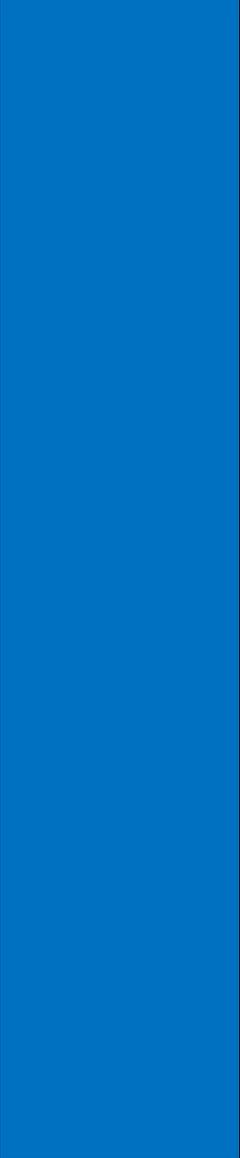Security guidelines as per Regulation 25 of S.I 360/2018

Theme	Category	Subcategory	Informative References
IDENTIFY (ID) **Develop the organisational understanding, structures, polices and processes to manage cybersecurity risk to the network and information systems of the organisations essential services,**	**Asset Management (ID.AM):** All systems and/or services that are required to deliver or support essential services must be identified, understood and documented. This includes data, personnel, devices, systems and facilities.	ID.AM-1: An up to date record of the physical and virtual devices and systems which underpins the delivery and/or support of each essential service is maintained.	• **CIS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: An up to date record of the software (information system, database, databus, applications, middleware etc) which underpins the delivery and/or support of each essential service is maintained.	• **CIS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 • **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organisational communication and data flows are mapped	• **CIS CSC** 12 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information	• **CIS CSC** 12

assets, data, and capabilities.		systems are catalogued	- **COBIT 5** APO02.02, APO10.04, DSS01.02 - **ISO/IEC 27001:2013** A.11.2.6 - **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	- **CIS CSC** 13, 14 - **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 - **ISA 62443-2-1:2009** 4.2.3.6 - **ISO/IEC 27001:2013** A.8.2.1 - **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	- **CIS CSC** 17, 19 - **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 - **ISA 62443-2-1:2009** 4.3.2.3.3 - **ISO/IEC 27001:2013** A.6.1.1 - **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organisation's mission, objectives, stakeholders, and activities are understood, prioritised and documented. This information is used to inform cybersecurity roles, responsibilities, and risk	ID.BE-1: The organisation's role in the supply chain is identified and communicated	- **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 - **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 - **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organisation's place in critical infrastructure and its industry	- **COBIT 5** APO02.06, APO03.01 - **ISO/IEC 27001:2013** Clause 4.1

management decisions.	sector is identified and communicated	· **NIST SP 800-53 Rev. 4** PM-8
	ID.BE-3: Priorities for organisational mission, objectives, and activities are established and communicated	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· **COBIT 5** APO10.01, BAI04.02, BAI09.02 · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
	ID.BE-5: Resilience requirements to support delivery of critical services are established.	· **COBIT 5** BAI03.02, DSS04.02 · **ISO 22301:2012** · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
Governance (ID.GV): Policies, procedures and processes to manage and monitor the regulatory, legal, risk, environmental and operational requirements are identified, understood and documented, and inform the management of cybersecurity risk.	ID.GV-1: Organisational cybersecurity policy is defined, documented and communicated.	· **CIS CSC** 19 · **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families
	ID.GV-2: Cybersecurity roles and	· **CIS CSC** 19

		responsibilities are coordinated and aligned with internal roles and external partners.	· **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 · **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3:Legal and regulatory requirements regarding cybersecurity obligations are understood and managed.	· **CIS CSC** 19 · **COBIT 5** BAI02.01, MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-4:Governance and risk management processes address cybersecurity risks, and ensure their ongoing adequacy and effectiveness.	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** Clause 6, Clause 9 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Risk Assessment (ID.RA): **C**ybersecurity risk to organisational operations, assets, and individuals	ID.RA-1: Asset vulnerabilities are identified and documented.	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02

	are identified and understood.		· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat (strategic, operational and tactical) and vulnerability information is received from information sharing forums and sources.	· **CIS CSC** 4 · **COBIT 5** BAI08.01 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16
		ID.RA-3: Threats, both internal and external, are identified and documented.	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified and documented.	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Threats, vulnerabilities,	· **CIS CSC** 4

		likelihoods, and impacts are used to determine risk. Risk assessments are dynamic and are updated in light of system or servcice changes, or changes to the threat environment.	▪ **COBIT 5** APO12.02 ▪ **ISO/IEC 27001:2013** A.12.6.1 ▪ **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified, prioritised and documented.	▪ **CIS CSC** 4 ▪ **COBIT 5** APO12.05, APO13.02 ▪ **ISO/IEC 27001:2013** Clause 6.1.3 ▪ **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): Priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, documented, managed, agreed to by organisational stakeholders.	▪ **CIS CSC** 4 ▪ **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ▪ **ISA 62443-2-1:2009** 4.3.4.2 ▪ **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 ▪ **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organisational risk tolerance is determined, clearly expressed and documented.	▪ **COBIT 5** APO12.06 ▪ **ISA 62443-2-1:2009** 4.3.2.6.5 ▪ **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 ▪ **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: Determination of risk tolerance is informed by the	▪ **COBIT 5** APO12.02 ▪ **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3

		organisational role in critical infrastructure and sector specific risk analysis and is documented.	▪ **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11

Supply Chain Risk Management (ID.SC): Weaknesses in supplier security can be used to circumvent an organisations internal controls. Processes are established and implemented to identify, assess and manage supply chain risks.	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organisational stakeholders	▪ **CIS CSC** 4 ▪ **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ▪ **ISA 62443-2-1:2009** 4.3.4.2 ▪ **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 ▪ **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
	ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritised, and assessed using a cyber supply chain risk assessment process	▪ **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ▪ **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ▪ **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 ▪ **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures	▪ **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ▪ **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7

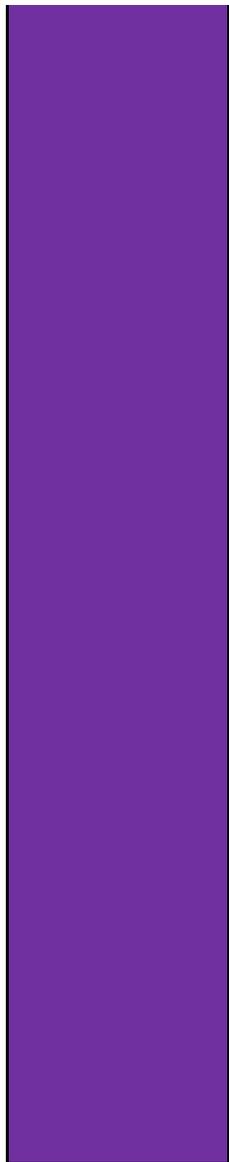|		
	designed to meet the objectives of an organisation's cybersecurity program and Cyber Supply Chain Risk Management Plan.	· **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO 22301:2012** · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

PROTECT

Theme	Category	Subcategory	Informative References
PROTECT (PR) **Develop and implement the appropriate and proportionate security measures that allow the delivery and protection of the organisations essential**	**Identity Management, Authentication and Access Control (PR.AC):** Access to assets and associated facilities is limited to authorised users, processes, and devices, consistent with the principle of least privilege and is managed consistent with the assessed risk.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, for the end to end joiners, movers and leavers lifecycle.	· **CIS CSC** 1, 5, 15, 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected.	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed and documented.	· **CIS CSC** 12 · **COBIT 5** APO13.01, DSS01.04, DSS05.03

services and systems.			· **ISA 62443-2-1:2009** 4.3.3.6.6
			· **ISA 62443-3-3:2013** SR 1.13, SR 2.6
			· **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1
			· **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties, and periodically revalidated.	· **CIS CSC** 3, 5, 12, 14, 15, 16, 18
			· **COBIT 5** DSS05.04
			· **ISA 62443-2-1:2009** 4.3.3.7.3
			· **ISA 62443-3-3:2013** SR 2.1
			· **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5
			· **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	· **CIS CSC** 9, 14, 15, 18
			· **COBIT 5** DSS01.05, DSS05.02
			· **ISA 62443-2-1:2009** 4.3.3.4
			· **ISA 62443-3-3:2013** SR 3.1, SR 3.8
			· **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
			· **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: Only individually	· **CIS CSC**, 16

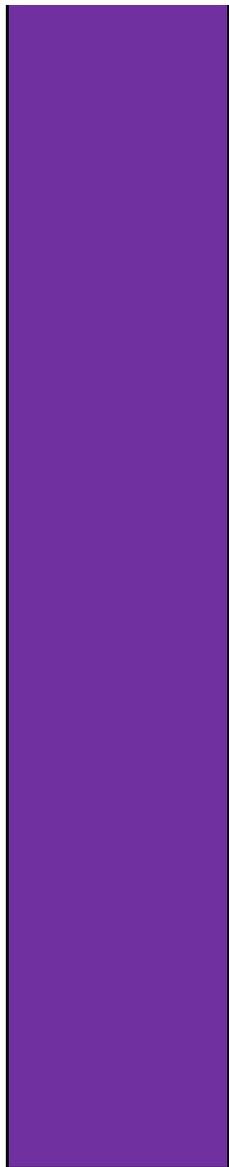|		
	authenticated and authorised users can connect to or access the organisation's networks or information systems.	• **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 • **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 • **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the access (e.g., privileged (admin, root) accounts typically require strong authentication.	• **CIS CSC** 1, 12, 15, 16 • **COBIT 5** DSS05.04, DSS05.10, DSS06.10 • **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 • **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
Awareness and Training (PR.AT): Personnel and partners are provided cybersecurity awareness education	PR.AT-1: All users are informed and trained on cyber security policies and relevent procedures, with periodic	• **CIS CSC** 17, 18 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2

and are trained to perform their cybersecurity-related duties and responsibilities consistent with related documented policies, procedures, and agreements.	updates.	· **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 · **NIST SP 800-53 Rev. 4** AT-2, PM-13
	PR.AT-2: Privileged users understand their roles and responsibilities.	· **CIS CSC** 5, 17, 18 · **COBIT 5** APO07.02, DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	· **CIS CSC** 17 · **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
	PR.AT-4: Senior executives understand their roles and responsibilities.	· **CIS CSC** 17, 19 · **COBIT 5** EDM01.01, APO01.02, APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13
	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.	· **CIS CSC** 17 · **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2

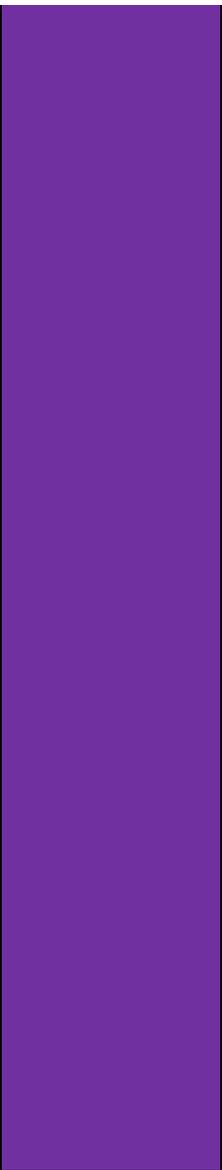|			
			· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
			· **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13
Data Security (PR.DS): Information and records (data) are managed consistent with the risk strategy to protect the confidentiality, integrity, and availability of information and systems.	PR.DS-1: Data-at-rest is protected	· **CIS CSC** 13, 14
			· **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06
			· **ISA 62443-3-3:2013** SR 3.4, SR 4.1
			· **ISO/IEC 27001:2013** A.8.2.3
			· **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
	PR.DS-2: Data-in-transit is protected	· **CIS CSC** 13, 14
			· **COBIT 5** APO01.06, DSS05.02, DSS06.06
			· **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2
			· **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
			· **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· **CIS CSC** 1
			· **COBIT 5** BAI09.03
			· **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1
			· **ISA 62443-3-3:2013** SR 4.2
			· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7
			· **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
	PR.DS-4: Adequate capacity to	· **CIS CSC** 1, 2, 13

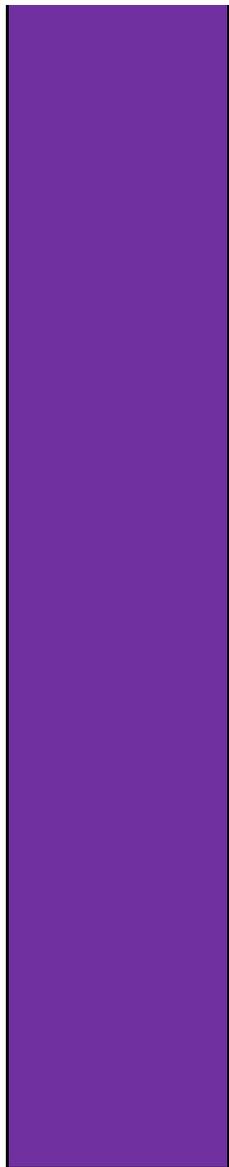| | | ensure availability is maintained. | · **COBIT 5** APO13.01, BAI04.04 |
			· **ISA 62443-3-3:2013** SR 7.1, SR 7.2
			· **ISO 22301:2012**
			· **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1
			· **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks and data loss are implemented.	· **CIS CSC** 13
			· **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02
			· **ISA 62443-3-3:2013** SR 5.2
			· **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.8.3.1, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
			· **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	· **CIS CSC** 2, 3
			· **COBIT 5** APO01.06, BAI06.01, DSS06.02
			· **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8
			· **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4
			· **NIST SP 800-53 Rev. 4** SC-16, SI-7

		PR.DS-7: The development and testing environment(s) are separate from the production environment.	· **CIS CSC** 18, 20 · **COBIT 5** BAI03.08, BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	· **COBIT 5** BAI03.05 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISO/IEC 27001:2013** A.11.2.4 · **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Service Protection Policies, Processes and Procedures (PR.SP): Define, communicate and document appropriate policies, processes and procedures that direct the overall organisational approach to securing systems and data that support delivery of essential services.	PR.SP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	· **CIS CSC** 3, 9, 11 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.SP-2: A System Development Life Cycle to manage systems is implemented with embedded security touchpoints.	· **CIS CSC** 18 · **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5

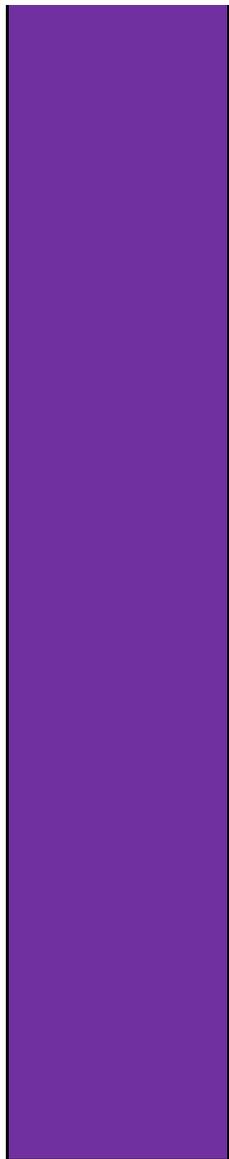|			
			• **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.SP-3: Configuration change control processes are in place	• **CIS CSC** 3, 11 • **COBIT 5** BAI01.06, BAI06.01 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.SP-4: Backups of information are conducted, maintained, and tested	• **CIS CSC** 10 • **COBIT 5** APO13.01, DSS01.01, DSS04.07 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 • **ISO 22301:2012** • **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.SP-5: Policy and regulations regarding the physical operating environment for organisational assets are met	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2,

			A.11.2.3
			· **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.SP-6: Data is destroyed according to defined policy.	· **COBIT 5** BAI09.03, DSS05.06
			· **ISA 62443-2-1:2009** 4.3.4.4.4
			· **ISA 62443-3-3:2013** SR 4.2
			· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
			· **NIST SP 800-53 Rev. 4** MP-6
		PR.SP-7: Protection processes are continuously improved.	· **COBIT 5** APO11.06, APO12.06, DSS04.05
			· **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8
			· **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10
			· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.SP-8: Effectiveness of protection technologies is shared with appropriate parties.	· **COBIT 5** BAI08.04, DSS03.04
			· **ISO/IEC 27001:2013** A.16.1.6
			· **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.SP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are	· **CIS CSC** 19
			· **COBIT 5** APO12.06, DSS04.03
			· **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1
			· **ISO 22301:2012**

		in place and managed	· **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3
			· **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.SP-10: Response and recovery plans are tested	· **CIS CSC** 19, 20
			· **COBIT 5** DSS04.04
			· **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11
			· **ISA 62443-3-3:2013** SR 3.3
			· **ISO 22301:2012**
			· **ISO/IEC 27001:2013** A.17.1.3
			· **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.SP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· **CIS CSC** 5, 16
			· **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
			· **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3
			· **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4
			· **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.SP-12: A vulnerability management plan is developed and implemented to remediate	· **CIS CSC** 4, 18, 20
			· **COBIT 5** BAI03.10, DSS05.01, DSS05.02
			· **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3,

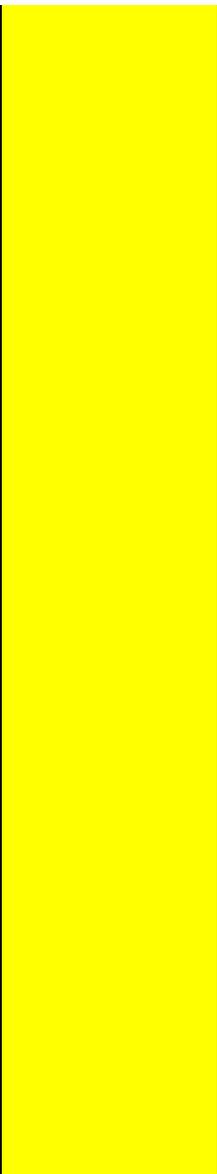|		vulnerabilities in a timely manner, commensurate with the risk.	· **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of critical system components are performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organisational assets are performed and logged, with approved and controlled tools.	· **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access.	· **CIS CSC** 3, 5 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· **CIS CSC** 1, 3, 5, 6, 14, 15, 16 · **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1

		· **NIST SP 800-53 Rev. 4** AU Family
	PR.PT-2: Removable (thumb drive etc) and mobile (smartphone, laptop etc) media is protected and its use restricted according to policy.	· **CIS CSC** 8, 13 · **COBIT 5** APO13.01, DSS05.02, DSS05.06 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	· **CIS CSC** 3, 11, 14 · **COBIT 5** DSS05.02, DSS05.05, DSS06.06 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7
	PR.PT-4: Communications and control networks are protected from	· **CIS CSC** 8, 12, 15 · **COBIT 5** DSS05.02, APO13.01

		unauthorised traffic, unauthorised access and the security mechanisms are periodically tested.	· **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 · **ISA 62443-2-1:2009** 4.3.2.5.2 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO 22301:2012** · **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

DETECT

Theme	Category	Subcategory	Informative References
DETECT (DE) **Develop and implement the appropriate capabilities to identify, detect and defend against the occurrence of a cybersecurity event that may have the potential to affect essential**	**Anomalies and Events Detection (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood. All aspects in the anomalies and events detection process must be documented.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	• **CIS CSC** 1, 4, 6, 12, 13, 15, 16 • **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• **CIS CSC** 3, 6, 13, 15 • **COBIT 5** DSS05.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	• **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 • **COBIT 5** BAI08.02 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is	• **CIS CSC** 4, 6

services.			
		determined.	• **COBIT 5** APO12.06, DSS03.01 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established.	• **CIS CSC** 6, 19 • **COBIT 5** APO12.06, DSS03.01 • **ISA 62443-2-1:2009** 4.2.3.10 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify potential cybersecurity events and verify the effectiveness of protective measures. All aspects of the security continuous monitoring process are documented.	DE.CM-1: The network is monitored to detect potential cybersecurity events.	• **CIS CSC** 1, 7, 8, 12, 13, 15, 16 • **COBIT 5** DSS01.03, DSS03.05, DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	• **COBIT 5** DSS01.04, DSS01.05 • **ISA 62443-2-1:2009** 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 • **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• **CIS CSC** 5, 7, 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3

		· **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
	DE.CM-4: Malicious code is detected	· **CIS CSC** 4, 7, 8, 12 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3, SI-8
	DE.CM-5: Unauthorized mobile code is detected	· **CIS CSC** 7, 8 · **COBIT 5** DSS05.01 · **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 · **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· **COBIT 5** APO07.06, APO10.05 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 · **COBIT 5** DSS05.02, DSS05.05 · **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
	DE.CM-8: Vulnerability scans are	· **CIS CSC** 4, 20

		performed	· **COBIT 5** BAI03.10, DSS05.01
			· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7
			· **ISO/IEC 27001:2013** A.12.6.1
			· **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are documented, maintained and tested to verify effectiveness and ensure continuous improvement.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	· **CIS CSC** 19
			· **COBIT 5** APO01.02**,** DSS05.01, DSS06.03
			· **ISA 62443-2-1:2009** 4.4.3.1
			· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
			· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	· **COBIT 5** DSS06.01, MEA03.03, MEA03.04
			· **ISA 62443-2-1:2009** 4.4.3.2
			· **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3
			· **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Detection processes are periodically tested against 'real world' scenarios.	· **COBIT 5** APO13.02, DSS05.02
			· **ISA 62443-2-1:2009** 4.4.3.2
			· **ISA 62443-3-3:2013** SR 3.3
			· **ISO/IEC 27001:2013** A.14.2.8
			· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated to appropriate	· **CIS CSC** 19
			· **COBIT 5** APO08.04, APO12.06, DSS02.05

		stakeholders.	▪ **ISA 62443-2-1:2009** 4.3.4.5.9
			▪ **ISA 62443-3-3:2013** SR 6.1
			▪ **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3
			▪ **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved.	▪ **COBIT 5** APO11.06, APO12.06, DSS04.05
			▪ **ISA 62443-2-1:2009** 4.4.3.4
			▪ **ISO/IEC 27001:2013** A.16.1.6
			▪ **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

RESPOND

Theme	Category	Subcategory	Informative References
RESPOND (RS) **Develop and implement the appropriate activities, prioritised through the organisations risk management process to take action to contain and minimise the impacts relating to a cybersecurity**	**Response Planning (RS.RP):** Response processes and procedures are executed, maintained and documented, to ensure timely response to cybersecurity events with an actual or potential adverse impact.	RS.RP-1: Response plan is executed during a cybersecurity event with an actual or potential adverse impact.	• **CIS CSC** 19 • **COBIT 5** APO12.06, BAI01.10 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27035:2016** • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-1: Personnel know their roles and order of operations when a response is needed	• **CIS CSC** 19 • **COBIT 5** EDM03.02, APO01.02, APO12.03 • **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported in line with established criteria, consistent with legal and regulatory requirements.	• **CIS CSC** 19 • **COBIT 5** DSS01.03 • **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	• **CIS CSC** 19 • **COBIT 5** DSS03.04 • **ISA 62443-2-1:2009** 4.3.4.5.2

event.			· **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2
			· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· **CIS CSC** 19 · **COBIT 5** BAI08.04 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Analysis (RS.AN): Analysis is conducted and documented to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated	· **CIS CSC** 4, 6, 8, 19 · **COBIT 5** DSS02.04, DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	· **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8

			· **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6
			· **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	· **COBIT 5** APO12.06, DSS03.02, DSS05.07
			· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
			· **ISO/IEC 27001:2013** A.16.1.7
			· **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	· **CIS CSC** 19
			· **COBIT 5** DSS02.02
			· **ISA 62443-2-1:2009** 4.3.4.5.6
			· **ISO/IEC 27001:2013** A.16.1.4
			· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the Organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	· **CIS CSC** 4, 19
			· **COBIT 5** EDM03.02, DSS05.07
			· **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigation (RS.MI): Activities are performed and documented to prevent expansion of an event,	RS.MI-1: Incidents are contained	· **CIS CSC** 19
			· **COBIT 5** APO12.06
			· **ISA 62443-2-1:2009** 4.3.4.5.6

mitigate its effects, and eradicate the incident.		· **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4	
	RS.MI-2: Incidents are mitigated	· **CIS CSC** 4, 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4	
	RS.MI-3: Newly identified vulnerabilities are remediated, mitigated or documented as accepted risks, in line with organisational risk tolerance.	· **CIS CSC** 4 · **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5	
Improvements (RS.IM): Response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8	
	RS.IM-1: Response strategies are updated	· **COBIT 5** BAI01.13, DSS04.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8	

RECOVER

Theme	Category	Subcategory	Informative References
RECOVER (RC) **Develop and implement the appropriate capabilities, prioritised through the organisations risk management process, to restore essential services that were affected through a cybersecurity**	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed, maintained and documented to ensure restoration of systems or assets affected by cybersecurity incidents.	RC.RP-1: Recovery plan is executed during or after a cybersecurity response.	▪ **CIS CSC** 10 ▪ **COBIT 5** APO12.06, DSS02.05, DSS03.04 ▪ **ISO 22301:2012** ▪ **ISO/IEC 27001:2013** A.16.1.5 ▪ **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	▪ **COBIT 5** APO12.06, BAI05.07, DSS04.08 ▪ **ISA 62443-2-1:2009** 4.4.3.4 ▪ **ISO 22301:2012** ▪ **ISO/IEC 27035:2016** Clause 5.6 ▪ **ISO/IEC 27001:2013** A.16.1.6, Clause 10 ▪ **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	▪ **COBIT 5** APO12.06, BAI07.08 ▪ **ISO/IEC 27001:2013** A.16.1.6, Clause 10 ▪ **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties e.g. coordinating centers, Internet Service Providers, owners of	RC.CO-1: Public relations are managed	▪ **COBIT 5** EDM03.02 ▪ **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: Reputational impacts are assessed and addressed.	▪ **COBIT 5** MEA03.02 ▪ **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Recovery activities are	▪ **COBIT 5** APO12.06

event.	impacted systems, victims, other CSIRTs, vendors and other stakeholders. The processes used for communication will be documented.	communicated to internal and external stakeholders as well as executive and management teams	· **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4

Appendix C: Indicative Incident Reporting Levels

Sector (1)	Subsector (2)	Type of person (3)	Incident Reporting Level
1. Energy	(a) Electricity	- Electricity undertakings within the meaning of section 2(1) of the Electricity Regulation Act 1999 (No. 23 of 1999)	Loss of 10 GWh or greater of generation capacity in a seven day period
		- Distribution system operators within the meaning of section 2(1) of the Electricity Regulation Act 1999	Loss of 10 GWh or greater of electricity distribution in a seven day period
		- Transmission system operators within the meaning of section 2(1) of the Electricity Regulation Act 1999 and electricity transmission system operators within the meaning of Regulation 2 of the European Communities (Internal Market in Natural Gas and Electricity)(Amendment) Regulations 2015 (S.I. No. 16 of 2015)	Loss of 10 GWh or greater of electricity transmission in a seven day period
	(b) Oil	- Operators of oil transmission pipelines	Not Applicable
		- Operators of oil production, refining and treatment	Loss of oil production, refining and treatment, or storage and transmission greater than 50,000

		facilities, storage and transmission	barrels (or BOE) per day
	(c) Gas	- Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009[6]	Not Applicable
		- Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009[6]	Loss of 200 GWh of gas distributed in a 7 day period
		- Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009[6]	Loss of 200 GWh of gas transmitted in a 7 day period
		- Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009[6]	Not Applicable
		- LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009[6]	Not Applicable
		- Natural gas undertakings as defined in point (1) of	Loss of 200 GWh of gas transmitted in a 7 day

[6] O.J. No. L 211, 14.08.2009, p.94

		Article 2 of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009[6]	period
		- Operators of natural gas refining and treatment facilities	Not Applicable
2. Transport	(a) Air transport	- Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008[7]	Any incident which results in more than 25% of the air carrier's scheduled flights in the State being cancelled in a 24 hour period
		- Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009[8], airports as defined in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013[9], and entities operating ancillary installations contained within airports	Any incident which results in more than 25% of the airport managing bodies scheduled flights in the State being cancelled in a 24 hour period
		- Traffic management control operators providing air traffic control (ATC) services as defined in point (1) of	Any incident that has an effect on the operation of Air Traffic Management Services within the State

		Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004[10]	
	(b) Rail transport	- Infrastructure managers within the meaning of Regulation 2(1) of the European Union (Regulation of Railways) Regulations 2015 (S.I. No. 249 of 2015)	Any incident which results in 25% of a train operator's services being cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations
		- Railway undertakings within the meaning of Regulation 2(1) of the European Union (Regulation of Railways) Regulations 2015, including operators of service facilities within the meaning of that Regulation	Any incident which results in 25% of a train operator's services being cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations
	(c) Water transport	- Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No. 725/2004 of the European Parliament and of the Council of 31 March 2004[11], not including the individual vessels operated by those companies	Any incident which results in the suspension of sailings from any port within the State for a period of two hours or more; or Any incident which results in 25% of scheduled sailings from a port being cancelled or delayed by 2 hours or more

---

[10] O.J. No. L 96, 31.3.2004, p.1
[11] O.J. No. L 129, 29.4.2004, p.6

		- Managing bodies of ports within the meaning of Regulation 2(1) of the European Communities (Port Security) Regulations 2007 (S.I. No. 284 of 2007), including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No. 725/2004 of the European Parliament and of the Council of 31 March 2004[11], and entities operating works and equipment contained within ports	For passengers and roll-on roll-off traffic: Any incident that results in the port being closed for two hours or more; or 25% of scheduled sailings being cancelled or delayed by 2 hours or more.

For LOLO, Liquid Bulk, Dry Bulk and Break Bulk traffic: Any incident which results in suspension of throughput at the port for 4 hours or more. |
		- Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002[12]	Any incident which results in the loss or disruption of a VTS system that causes delays in excess of two hours for 20% of ship movements within a 24 hour period or the port being closed for two hours or more
	(d) Road transport	- Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 of 18 December 2014[13]	Not Applicable
		- Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the	For Operators of ITS in area over 500,00 people; A single incident that results in a loss of capacity of 100% to the flow of traffic on a road in one or both

---

[12] O.J. No. L 208, 5.8.2002, p. 10
[13] O.J. No. L 157, 23.6.2015, p.21

		European Parliament and of the Council of 7 July 2010[14]	directions for a period of more than 2 hours. For Operators of ITS in area under 500,000 people; A single incident that results in a loss of capacity of 100% to the flow of traffic on a road in one or both directions for a period of more than 6 hours.
3. Banking[15]	Credit institutions	Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 - Payment Services provided to non-Monetary Financial Institutions in the State	Based on transactions affected; > 25% of the Credit Institution's regular level[16] of transactions (in terms of number of transactions)or > EUR 15 million Based on payment services users > 50 000 or > 25% of the credit institution's payment service users Based on economic impact; > Max. (0.1% Tier 1 capital,* EUR 200 000) or

---

[14] O.J. No. L 207,6.8.2010, p.1

[15] Incident reporting thresholds for the Banking sector are aligned with PSD2

[16] Regular level is the daily annual average of transactions, taking the previous year as the reference period for calculations.

			> EUR 5 million
		Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 - Cash Services provided in the State	Based on transactions affected; > 25% of the credit Institution's regular level[17] of transactions (in terms of number of transactions) or > EUR 5 million Based on customers > 50 000 or > 25% of the credit institution's customers Based on economic impact; > Max. (0.1% Tier 1 capital,* EUR 200 000) or > EUR 5 million
		Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 - Access to retail	Based on transactions affected; > 25% of the regular level[18] of transactions by the credit institutions that are provided with access to

---

[17] Regular level is the daily annual average of transactions, taking the previous year as the reference period for calculations.

[18] Regular level is the daily annual average of transactions, taking the previous year as the reference period for calculations.

		payment systems provided to credit institutions in the State	retail payment systems via the operator of essential services. transactions (in terms of number of transactions) or > EUR 5 million Based on payment services users in the credit institutions gaining access. > 50 000 or > 25% of the credit institution's payment service users Based on economic impact; > Max. (0.1% Tier 1 capital,* EUR 200 000) or > EUR 5 million
4. Financial Market Infrastructure	Operators of Trading Venues	Operators of trading venues within the meaning of Regulation 3(1) of the European Union (Markets in Financial Instruments) Regulations 2017 (S.I. No. 375 of 2017 – listing and trading of Irish equities in the State	Any incident affecting the institution's ability to list or trade Irish equities in the State.
5. Health	Health care	Healthcare providers as defined in Regulation 3 of the	Any incident that affects the ability of an operator to

sector	settings (including hospitals and private clinics)	European Union (Application of Patients' Rights in Cross-Border Healthcare) Regulations 2014 (S.I. No. 203 of 2014)	provide continuity of essential services to users and where applicable the operator has greater than 500 total beds (In-Patient and Day Bed Spaces)
6. Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption within the meaning of Regulation 3(1) of the European Communities (Drinking Water) Regulations 2014 (S.I. No. 122 of 2014) but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services	Any incident that effects the ability of an OES to supply and distribute water intended for human consumption to greater than 200,000 users within the state
7. Digital Infrastructure		- IXPs	Loss or significant degradation of connectivity to 25% of connected global routes for greater than 1 hour or loss of greater than 75% of total port capacity for greater than 1 hour
		- DNS service providers	Loss or significant degradation of the service to greater than 50% of clients in 30 minutes or loss or significant degradation of service for greater than 25% of domains
		- TLD name registries	Loss or significant degradation of greater than 25%

			of name resolution capability for greater than 1 hour