TLP - Clear

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NIS 2 Risk Management Measures Guidance

Draft

04/06/2025

ncsc.gov.ie

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Version Control		
Description of Change	**Changed by**	**Date**
Draft	NCSC	04/06/2025

DRAFT

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Contents

Introduction: 4

Implementing Regulation for 'main establishment' entities and Trust service providers in the digital infrastructure sector 5

Other EU Legislation 5

Cybersecurity Risk Management Measures for Essential and Important Entities in Scope for NIS 2 7

Implementation guidance: for the Cybersecurity Risk Management Measures 10

RMM001 – Registration 11

RMM002 – Governance – Management board commitment and accountability 12

RMM003 – Network and Information Security Policy 13

RMM004 – Risk Management Policy 15

RMM005 – Continuous improvement - assess effectiveness and improve cybersecurity risk management measures. 17

RMM006 – Basic Cyber Hygiene Practices and Security Training 18

RMM007 – Asset Management 20

RMM008 – Human Resources Security 22

RMM009 – Access Control 24

RMM010 – Environmental and physical security 27

RMM011 – Cryptography, Encryption and Authentication 28

RMM012 – Supply chain policy 29

RMM013 - Security in network and information systems acquisition, development and maintenance 31

RMM014 – Incident Handling 35

RMM015 – Incident Reporting 38

RMM016 – Business Continuity and Crisis Management 40

Reference material 42

Abbreviations 43

Addendum for ECN/ECS entities only 44

Appendix I - Foundational indicative control mapping 47

DRAFT

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Introduction:

Directive (EU)2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), will be transposed into Irish legislation by the upcoming National Cybersecurity Bill.

The Directive can be viewed here: Publications Office (europa.eu)[1]

The Directive requires that Member States take a number of actions to ensure the resilience of key infrastructure and services. These actions include the placing of legal obligations on the management boards[2] of two different categories of entity, termed 'Essential Entities' and 'Important Entities', to both meet a set of cybersecurity risk management measures and to report cybersecurity incidents. The risk management measures are required to *"ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services".*

The Directive covers entities operating in multiple sectors which are critical to the functioning of our society.

For essential and important entities operating in the digital infrastructure (with the exception of Internet Exchange Point providers & Providers of publicly available electronic communications services), ICT service management (B2B) and digital provider sectors, a single set of Union wide risk management measures have been agreed at EU level in Commission Implementing Regulation (EU) 2024/2690.

For other entities subject to the Directive it is up to individual Member States to determine which precise risk management measures will apply to entities in their State, provided they meet the minimum requirements of Article 21(2) of the Directive.

This document focuses on the primary obligations for entities in scope that are contained in articles 3, 20, 21 and 23 of the Directive.[3] It is a cross-sector general guidance document, derived from these obligations that will come into effect in Ireland following the implementation of the forthcoming National Cybersecurity Bill. Once signed into legislation, the then Act will transpose the NIS 2 directive in Ireland.

This guidance will be updated over time, as appropriate and remains in draft pending the final content of the forthcoming National Cybersecurity Bill

Comments on this guidance can be sent to nisdirective@ncsc.gov.ie.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555Intro
[2] "management board", in relation to Essential and Important Entities (EIE), means the senior body of the EIE performing executive and administrative functions and which is responsible and accountable for the day-to-day management of the EIE.
[3] Other obligations include Article 29(4) of the Directive –the requirement of entities to notify competent authorities in regard to participation in information sharing arrangements.

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Implementing Regulation for 'main establishment' entities and Trust service providers in the digital infrastructure sector

The European Commission has adopted an Implementing Regulation regarding the cybersecurity risk management measures with regard to:

- DNS service providers,
- TLD name registries,
- Entities providing domain name registration services,
- Cloud computing service providers,
- Data centre service providers,
- Content delivery network providers,
- Managed service providers and managed security service providers,
- Digital providers i.e. providers of online marketplaces, of online search engines or of social networking services platforms and
- Trust service providers.

These entities should refer to the Implementing Regulation instead of RMM003 to RMM014 and RMM016. The implementing regulation for the entities within scope of the regulation also defines criteria as set out in Article 23(3) of the NIS 2 directive for what constitutes significant incidents. These criteria replace those set out in RMM015.

This Implementing Regulation is available here: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

Other EU Legislation

(EU)2022/2554 and Financial Entities

Regulation - 2022/2554 - EN - DORA - EUR-Lex of the European Parliament and of the Council is considered to have sector specific Cybersecurity Risk Management Measures equivalent to NIS 2 in effect and should be applied in place of the specified NIS 2 Cybersecurity Risk Management Measures for financial entities. Therefore, the guidance in this document does not apply to financial entities covered by DORA (EU)2022/2554.

It should be noted that financial entities exempted from DORA in Ireland are also exempted from NIS 2, however, the NCSC recommends that they identify and assess their risks and implement measures to appropriately address them.

DRAFT

(EU)2022/2557, the CER directive/ S.I. No. 559/2024

(EU)2022/2557, the Critical Entities Resilience directive requires Member States to carry out a risk assessment to identify critical entities. This is to be completed by January 17th 2026. Any entity determined to be critical under the CER directive will be deemed an essential entity under the NIS 2 directive.

S.I. No. 559/2024 gives effect to the CER Directive in Irish legislation. This is available here: S.I. No. 559/2024 - European Union (Resilience of Critical Entities) Regulations 2024 (irishstatutebook.ie).

Electronic Communications (Security Measures)

The NIS 2 risk management measures may be amended to include specific additional requirements for providers of Electronic Communications Services/Networks (ECS/N). These additional measures will include measures arising from the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 (No. 4 of 2023) which are not already covered by these NIS 2 Risk Management Measures and will be applicable to providers of ECS/ECN which are not covered by the Implementing Regulation (EU) 2024/2690.

DRAFT

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Cybersecurity Risk Management Measures for Essential and Important Entities in Scope for NIS 2

The requirement for each risk management measure (RMM) in the guidance below derive directly from the upcoming National Cybersecurity Bill giving effect to the NIS 2 Directive (EU)2022/2555).

These cybersecurity risk management measures will be applicable to essential and important entities.

Summary Table: Risk Management Measures required by the NIS 2 Directive.

RMM001 - Registration	The upcoming National Cybersecurity Bill transposing the NIS 2 Directive defines the criteria, whereby entities are considered 'essential' or 'important' entities. Entities that meet these criteria must register with the NCSC on the registration portal on the NCSC's website. Note: this measure also applies to entities providing domain name registration services
RMM002 – Governance – Management board commitment and accountability	Management boards of essential and important entities must approve the cybersecurity risk management measures taken by those entities and oversee their implementation.
RMM003 – Network and Information Security Policy	Essential and important entities must establish and maintain an appropriate network and information security policy and topic specific policies.
RMM004 – Risk Management Policy	Essential and important entities must implement, operate, and maintain an appropriate network and information security risk management framework to identify and address the network and information system cybersecurity risks posed to the security of the network and information systems. Essential and important entities must also ensure that network and information system risk management is fully supported at management board level, supports decision making and is an integral part of day-to-day operations. It must be implemented uniformly at all levels and the level of governance and oversight is appropriate and proportionate to the severity of any identified risks.

DRAFT

RMM005 – Continuous improvement/assess effectiveness & improve cybersecurity risk management measures.	Essential and important entities must regularly carry out cybersecurity risk assessments on their network and information systems, encompassing an all-hazards approach to assess and update their cybersecurity risks. The risk treatments implemented must be regularly reviewed to ensure they are providing the expected mitigations. Where treatments fail to deliver the expected/mandated level of mitigation, the risk treatments must be adjusted to bring them into line with the approved risk tolerance level.
RMM006 – Basic Cyber Hygiene Practices and Security Training	Essential and important entities must implement, operate and maintain basic cyber hygiene practices for network and information systems used to support their operations or delivery of their services
RMM007 – Asset Management	Essential and important entities must implement, operate, and maintain asset management for network and information systems supporting their operations or delivery of their services.
RMM008 – Human Resources Security	Essential and important entities must, in the context of managing the risks to network and information systems used in their operations or for the delivery of their services, take into account the human factor.
RMM009 – Access Control	As part of the risk management measures, essential and important entities must put in place, access management for both human and non-human identities. To do this they will need to implement, operate, and maintain appropriate access control polices.
RMM010 – Environmental and physical security	Essential and important entities must take physical and environmental considerations into account for cybersecurity risk assessments of network and information systems used in their operations or for the delivery of their services.
RMM011 – Cryptography, Encryption and Authentication	Essential and important entities must implement, operate and maintain policies and procedures for the appropriate use of cryptography and where appropriate, encryption by and within their network and information systems used in their operations or for the delivery of their services. These policies and procedures are required on the basis of cybersecurity risk assessments, resulting in the identification of risks, and implemented as appropriate to the risk treatment plan.
RMM012 – Supply chain policy	Essential and important entities must implement, operate and maintain an organisational approved network and information system supply chain policy that includes the security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.
RMM013 - Security in network and information systems acquisition,	Essential and important entities must manage the cybersecurity risks to network and information systems used in their operations or for the delivery of their services from both the process of obtaining those

DRAFT

development and maintenance, including vulnerability handling and disclosure.	systems and then in the maintenance of those systems. This must include both vulnerability handling and disclosure.
RMM014 – Incident Handling	Essential and important entities must have measures in place that define roles, responsibilities, and procedures for preventing, detecting, responding to, containing, or analysing, cybersecurity incidents in a timely manner, meeting all mandated legal and regulatory requirements.
RMM015 – Incident Reporting	Essential and important entities must notify, without undue delay, the NCSC (CSIRT) of any significant incident. Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Essential and important entities must report, inter alia, any information enabling the CSIRT to determine any cross-border impact of a significant incident.
RMM016 – Business Continuity and Crisis Management	Essential and important entities must implement, operate, and maintain a continuity plan including but not limited to business continuity and disaster recovery plans to enact in the case of an incident.

DRAFT

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Implementation guidance: for the Cybersecurity Risk Management Measures

While the cybersecurity risk management measures are applicable to essential and important entities, the level to which each control is implemented should be appropriate and proportionate to the degree of the entity's exposure to risks and to the societal and economic impact that an incident will have.

The risk management measures are divided into two categories:

1. Foundation Actions:

These are controls, which the NCSC consider to be the minimum required to meet the legislative obligations of the Directive, as transposed into national legislation. They establish a baseline of security practices that all entities are expected to uphold.

2. Supporting Actions:

Further controls may be required, depending on specific risks faced by the organisation. They supplement the foundation actions to provide enhanced security, where necessary to reduce risk to a target level or to reach a desired security maturity level in line with the risk appetite of the organisation.

It should be noted in this guidance that the "appropriate and proportionate" provision is a recognition that one size does not fit all. Variations in multiple risks occur and can vary across sectors, within sectors, within business models, across different network and information system architecture's, within geographical areas, across different data sets, etc. As such, risk management measures and the level of risk mitigation required when implementing them, will also vary in accordance with the individual entity risks.

Determining Which Actions to Implement:

All entities are expected to implement the foundation actions as a baseline. To determine whether supporting actions are also required, organisations should conduct a thorough risk assessment considering several factors, including those set out in recital 82 of the Directive.

Exposure to Risk: Evaluate how vulnerable your organisation is to potential risks. This includes assessing both internal and external risks that could impact your operations.

Size of the Entity: Larger organisations may have more complex systems and processes, potentially increasing exposure to risk. Consider whether your size necessitates additional controls.

Likelihood and Severity of Incidents: Analyse the probability of incidents occurring and the potential impact they could have on your organisation and stakeholders.

Societal and Economic Impact: Consider the broader implications of a security incident, including potential effects on society and the economy. Organisations critical to societal functions may require more robust measures.

DRAFT

Cost of Implementing Measures: Weigh the financial implications of implementing supporting actions against the benefits of enhanced security. Ensure that measures are proportionate and cost-effective.

RMM001 – Registration

The forthcoming National Cybersecurity Bill will set out, in line with the NIS 2 Directive, the criteria whereby entities are considered 'essential' or 'important' entities. Every entity that meets these criteria must register with the NCSC[4].

It should be noted that it is not the act of registration that determines if an entity is subject to the measures as an essential or important entity. Rather, every entity that meets the defined criteria for applicability laid out in the forthcoming National Cybersecurity Bill will be subject to the requirements of the legislation and the mandated legally and regulatory binding measures therein.

In general, medium and large enterprises, operating in the sectors in scope for NIS 2, will be subject to the National Cybersecurity Bill giving effect to the NIS 2 Directive. However, this is not the only criteria. Other criteria can apply, organisations should consult the National Cybersecurity Bill when available or review relevant sections of the NIS 2 Directive to determine if they are essential or important entities.

Please avail of the NCSC's 'Am I in Scope' tool for further clarity: NCSC: NIS 2[5] which helps organisations to determine if they are subject to the Directive's requirements.

Note: this measure also applies to entities providing domain name registration services

To meet this risk management measure:

Foundational actions:

RMM001.FA01: Entities operating in the sectors mandated under Annex I and II of the NIS 2 Directive, or subject to the other criteria for inclusion in the scope of forthcoming National Cyber Security Bill need to review the criteria and based on their assessment determine if they are in scope.

RMM001.FA02: When the National Cybersecurity Bill comes into effect, register with the NCSC, submitting such information as set out for registration.

RMM001.FA03: For entities covered by the main establishment principle, they need to register in the member state of their main establishment.

RMM001.FA04: Registered entities are required to keep their registration detail up to date, modifying as appropriate as circumstances warrant over time.

[4] A portal will be available on www.ncsc.gov.ie when the legal requirements come in to effect.
[5] https://www.ncsc.gov.ie/nis2/amiinscope/

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

RMM002 – Governance – Management board commitment and accountability

It is a requirement of the NIS 2 Directive that the management board of essential and important entities must approve the cybersecurity risk management measures taken by those entities and oversee their implementation.

To meet this risk management measure:

Foundational actions:

RMM002.FA01: Management board to undertake Cybersecurity Risk Management training that enables them to adequately assess the cybersecurity risks that are being presented, their potential impact on their services and enable them to recognise appropriate remediations for the presented risks, in line with the risk appetite of the entity. This training should be both documented and should be repeated as necessary to ensure it keeps pace with the requirement.

RMM002.FA02: Management board to approve, appropriate and proportionate to their organisation, the cybersecurity risk-management measures required to address identified cybersecurity risks.

RMM002.FA03: Management board to commit the resources needed to implement, operate, and maintain the cybersecurity risk management measures, they have approved.

RMM002.FA04: Management Board to ensure that an effective governance structure is in place.

RMM002.FA05: Management Board to approve a network and information security policy suite, to include the polices required by the NIS 2 directive, with the security objectives and the risk acceptance criteria that are compatible with the risk appetite of the entity.

Supporting actions:

RMM002.SA01: Management Board to ensure personnel apply network and information security in accordance with the established policies and procedures of the entity.

RMM002.SA02: Management Board to ensure communication of the importance of effective network and information security management.

RMM002.SA03: Management Board to ensure the recording, monitoring, and updating of cybersecurity risks identified from cybersecurity risk assessments.

RMM002.SA04: Management Board to ensure identified significant cybersecurity risks are presented to the management board, to ensure the body is properly informed and updated about the current status of the entity's cybersecurity risk and level of network and information security.

RMM002.SA05: Management Board to ensure implementation of cybersecurity technical, operational, and organisational risk-management measures appropriate and proportionate to the degree of the entity's risk exposure. This should be done with due account of the criticality of the entity, the risks, to which it is exposed, the entity's size and the likelihood of occurrence of incidents and their potential severity, including their societal and national/regional economic impacts.

DRAFT

RMM002.SA06: Management Board to regularly review the progress of both the cybersecurity risk management measures and the cybersecurity risk reporting lifecycle (cybersecurity risks change over time, thus cybersecurity risk assessments are not static, rather will need to be routinely reviewed/updated).

RMM002.SA07: Management Board to promote continual improvement.

RMM003 – Network and Information Security Policy

Essential and important entities establish and maintain an appropriate network and information security policy and topic specific policies.

To meet this risk management measure requirement:

Foundational actions:

RMM003.FA01: Create, communicate, maintain, and operate an organisation defined network and information security policy and topic specific policies. These policies are to be practical, usable, and appropriate for an organisation's essential function and technologies.

RMM003.FA02: Policies are reviewed at regular intervals and when significant changes to technology, business, legal or regulatory requirements take place, or when a significant incident occurs, to ensure they remain relevant to the organisation's cybersecurity risk.

RMM003.FA03: Policies are communicated effectively across the organisation and personnel acknowledge receipt of such policies when first hired, contracted, annually, or whenever a policy is updated.

RMM003.FA04: Network and information security policy is approved by the management board in accordance with RMM002 FA05.

Supporting actions:

RMM003.SA01: The network and information security policy sets out the entity's approach to managing its network and information security requirements, the entity's risk management measures and their implementation. It covers people, processes, and technologies incorporating the following:

- Is appropriate to the purpose and risk appetite of the entity, while being proportionate to the risks identified to the entity's network and information systems, operations or the provision of their services.
- Includes network and information security objectives.
- Includes a commitment to satisfy applicable cybersecurity risk management measures related to network and information security.
- Includes a commitment to continual improvement of the network and information security policy.
- Requires all personnel and third parties to apply network and information security in accordance with the established security policy, topic-specific policies, and procedures of the entity.

DRAFT

RMM003.SA02: The policy, as well as the topic specific policies (policy suite), follows a defined, documented, and managed lifecycle.

RMM003.SA03: Topic specific policies are reviewed and approved by designated, documented, and authorised personnel at planned intervals or when significant changes or significant incidents occur.

RMM003.SA04: The result of reviews, as well as any changes, including the authorisation for the change, should be documented providing a documented history of the policy suite lifecycle.

RMM003.SA05: Assess whether the network and information security policy, as well as topic specific polices, conform to the entity's own requirements, the requirements of the Directive, and if the policy suite is effectively implemented and maintained.

- Assessment of the network and information security policy to include available security assessments and any available security testing results of the network and information systems.
- Undertake security assessments and/or security testing of network and information systems specifically to support the policy suite assessment.

RMM003.SA06: When measuring compliance with the policy suite, the following should be taken into account:

- The security measures that need to be monitored and measured, including processes and controls to assess the effectiveness of the network and information security policy suite implementation and compliance.
- The methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results are targeted to the required evaluation criteria. The criteria to include the impact to the risk the measure is being implemented to address.
- When the monitoring and measuring should be performed.
- Who should monitor and measure.
- When the results from monitoring and measurement should be analysed and evaluated.
- Who should analyse and evaluate these results.
- Actions arising

RMM003.SA07: Set out in the network and information security policy or policy suite (a separate policy on roles and responsibilities could be used) responsibilities and authorities that should be defined, assigned to roles, and allocated according to the entity's needs.

- These should be documented, communicated, and approved at a management level appropriate to the requirements of the entity in managing its risk.
- The roles could establish a person(s), responsible for network and information security and this role should report directly to an appropriate senior role based on risk.

RMM003.SA08: Depending on the size and resourcing of an entity, information security should be covered by dedicated roles or duties carried out in addition to existing roles.

DRAFT

RMM003.SA09: Conflicting duties and conflicting areas of responsibility should be segregated, if applicable. The roles and responsibilities should be documented.

RMM003.SA10: The entity could describe and assign corresponding responsibilities regarding the following roles (or comparable equivalents depending on the organisation): Chief Information Officer (CIO), Chief Information Security Officer (CISO) and IT security incident handling officer.

RMM004 – Risk Management Policy

Essential and important entities must implement, operate, and maintain an appropriate network and information security risk management framework to identify and address the risks posed to the security of the network and information systems.

Essential and important entities must also ensure that network and information system risk management is fully supported at management board level, supports decision making and is an integral part of day-to-day operations.

It must be implemented uniformly at all levels and the level of governance and oversight is appropriate and proportionate to the severity of any identified risks.

To meet this risk management measure requirement:

Foundational actions:

RMM004.FA01: Create, communicate, maintain, and enforce, an organisation defined network and information system risk management policy and topic specific policies, including policies and instructions on identification, analysis, evaluation, and treatment of cybersecurity risks.

RMM004.FA02: The policy requires that the organisation perform and document network and information system security risk assessments and, based on the results, implement, and monitor a cybersecurity risk treatment plan. Residual risks to be either treated or risk accepted by risk owners, with adequate reporting to the management board.

RMM004.FA03: To ensure full coverage of the risk assessments to fully capture the risks, the polices must set out that the entity:

- Identify and document the network and information systems which they use for their operations or for the provision of their services.
- Understand the business impact from disruption to their network and information systems used in its operations or services (business impact analysis).
- Risk assesses the network and information systems which they use for their operations or for the provision of their services.
- Categorise systems according to the level of criticality to the organisation for their operations or for the provision of their services.

RMM004.FA04: Mandate that the network and information system risk management process is an integral part of the overall organisation's risk management.

DRAFT

Supporting actions:

RMM004.SA01: Establish a cybersecurity risk management process for the network and information systems which the entity uses in its operations or for the delivery of its services, in line with its policies. This process to:

- Be an integral part of the overall organisation's risk management.
- Follow an all-hazards approach and ensure that corporate governance and risk management processes address cybersecurity risks, including risks from third parties.
- Adopt a risk management methodology and/or tools based on well-known standards.
- Establish and maintain risk criteria relevant to the entity.
- Identify and document the risks posed to the security of network and information systems, including the identification of single point of failures.
- Identify risk owners and document their responsibilities.
- Analyse the risks posed to the security of network and information systems (threat, likelihood, impact, risk level), taking into account cyber threat intelligence and vulnerabilities.
- Evaluate the identified risks based on risk criteria.
- Identify and prioritize appropriate risk treatment measures, taking account of the risk assessment results and the results of the procedure to assess the effectiveness of security measures. Where risk treatment is 'accept', the rationale for acceptance, should be documented to include who, what, why, when and condition for review.
- Identify who is responsible for implementing decided measures and when the measure should be implemented.
- Make key personnel aware of the main risks and of the security measures.
- Document the chosen security measures and the reasons to justify the acceptance of residual risks in a comprehensive manner to include who, what, why, when and condition for review.

RMM004.SA02: Assess those network and information systems for the entity's operations or the delivery of their services, prioritise and categorise those network and information systems.

- To enable a structured, managed approach, the entity could define classification levels to assign and categorise its network and information systems. This will facilitate the implementation of required levels of risk management measures.
- The categorisation should take in both cybersecurity risks and business risks to its operations or service provision.
- The classification level should incorporate the cybersecurity measures based on risk to the confidentiality, integrity, authenticity, and availability requirements, to indicate the risk management measures required according to their sensitivity/criticality, risk and business value.

For example, the entity could assign systems into:

  - Low risk to their operations or provision of their services and low risk to the security of their network.
  - High risk to their operations or provision of their services and/or have a high risk to the security of their network.
  - Systems supporting critical national infrastructure and/or the systems for which an incident would have a societal and national/regional economic impact.

DRAFT

- Availability requirements should be aligned with the business requirement of operations/service delivery and recovery time objectives.

RMM005 – Continuous improvement - assess effectiveness and improve cybersecurity risk management measures.

Essential and important entities must regularly carry out cybersecurity risk assessments on their network and information systems, encompassing an all-hazards approach to assess and update their cybersecurity risks.

The risk treatments implemented must be regularly reviewed to ensure they are providing the expected mitigations.

Where treatments fail to deliver the expected/mandated level of mitigation, the risk treatments must be adjusted to bring them into line with the approved risk tolerance level.

To meet this risk management measure requirement:

Foundational actions:

RMM005.FA01: Carry out regular cybersecurity risk assessments on their network and information systems, including after significant cybersecurity incidents or after major changes to network and information systems and services.

RMM005.FA02: Determine and implement appropriate and proportionate risk treatments.

RMM005.FA03: Regularly review risk treatments for effectiveness and adjust where necessary.

RMM005.FA04: Look for, identify, and embrace opportunities to improve both risk posture and risk treatments to ensure effective, appropriate and proportionate ongoing cybersecurity risk management.

Supporting actions:

RMM005.SA01: Based on a risk analysis, define the need and the frequency of security test types (penetration tests, system tests, etc.) and the risk management measures, components, systems or services, commensurate with the risk, to ensure secure operation of those network and information systems.

RMM005.SA02: Network and information systems are tested at installation, after upgrades or changes to the infrastructure or applications that the entity deems significant, or after maintenance to ensure the risk treatments are delivering the expected results.

RMM005.SA03: Organisation wide tests are carried out at planned intervals or when significant incidents or changes occur to ensure the correct application and effectiveness of the risk management measures, as well as to find any potential gaps or weaknesses not captured in the original cybersecurity risk assessments that the risk treatments were based on.

DRAFT

RMM005.SA04: Security tests are carried out according to a documented test methodology and cover the network and information systems that have been identified in a risk analysis. Evidence should be recorded while testing. The type, scope, time/period and results should be documented in a manner that is comprehensible to an expert third party.

RMM005.SA05: Findings from security testing, if applicable, should be used to update the policies and procedures to assess the effectiveness of security measures.

RMM005.SA06: Independent review of network and information security policies where appropriate.

RMM005.SA07: Residual risks are either accepted by risk owners as part of the normal risk management process, or mitigated with an appropriate risk mitigation measure, with adequate reporting to top management.

RMM005.SA08: Findings are assessed and followed up, remediated where the risk has not been accepted, particularly in the case of the risk being assessed as medium to very high criticality with respect to the confidentiality, integrity, authenticity or availability of the service provided.

RMM005.SA09: The assessment of criticality and mitigating actions for each finding is documented.

RMM006 – Basic Cyber Hygiene Practices and Security Training

Essential and important entities implement, operate and maintain basic cyber hygiene practices for network and information systems used to support their operations or delivery of their services.

These practices entail those actions comprising a common baseline set of practices, including software and hardware updates, password changes, the management of new installations, the limitation of administrator-level access accounts, and the backing-up of data, necessary to address basic cybersecurity risks in essential and important entities. The makeup of which will be determined in a manner appropriate and proportionate to the assessed risks.

To meet this risk management measure requirement:

Foundational actions:

RMM006.FA01: Have a defined, communicated and operated cybersecurity policy suite. (see RMM003).

RMM006.FA02: Implement cybersecurity design practices.

- Manage the implementation, operation, maintenance and decommissioning of network and information systems, both hardware and software to minimise cyber risk. (see RMM007).
- Limit privilege access. (RMM008, RMM009).
- Implement a risk-based approval and tracking control process for exceptions.
- Implement network segmentation, where appropriate.

RMM006.FA03: Implement appropriate and proportionate cybersecurity technical controls.

- Ensure privilege access is controlled and monitored.

- Ensure unique accounts with complex passwords are required and defined password changes are enforced.
- Remove default accounts or rename default accounts where they cannot be removed and change the password on default accounts. Minimise permissions on default accounts that cannot be removed and implement alerting on use.
- Backup both systems and data in-line with identified mandated recovery criteria.
- Deploy available updates in a timely manner.
- Operate a risk-based approval and tracking control for exceptions.
- Install and automatically update endpoint protection on all relevant assets.

RMM006.FA04: Ensure cybersecurity training (training/awareness) is provided to foster personnel behaviours in line with the policy suite and to minimise cybersecurity risk.

Supporting actions:

RMM006.SA01: An awareness raising programme for all employees, regardless of their job function and including top management.

- Scheduled over time, so that the activities are repeated and cover new personnel.
- Established in line with the network and information security policy, topic-specific policies and relevant procedures on network and information security.
- Covering security measures in place (e.g. information security incident reporting), contact points, resources for additional information, and advice on information security matters raising awareness of cyber threats, phishing or social engineering techniques, as well as cyber hygiene practices for end users.
- Include:
  - Clear desk and screen policy,
  - Use of passwords and other authentication means,
  - Recommended email use and web browsing,
  - Protection from phishing and social engineering,
  - Using a secure connection,
  - Backup practices,
  - Secure teleworking practices,
  - Any other security measures relevant to the organisation.

RMM006.SA02: Cybersecurity training for specific information systems provided in line with the network and information security policy, topic-specific policies and relevant procedures on network and information security.

- Targeted training that reflects the required cybersecurity knowledge the entity has determined is needed for certain positions and for certain roles.
- This training to be relevant to the job function of the employee and its effectiveness assessed.
- This training to take into consideration the security measures the entity has in place. This may include regular instructions regarding the secure configuration and operation of the network and information systems relevant to the job function of the employee, including mobile devices.
- Regular briefings on known threats.
- Regular behavioural training on security-relevant events.

RMM006.SA03: Provide initial training for new personnel and retraining to those who transfer to new positions or roles with substantially different network and information security requirements.

DRAFT

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

RMM007 – Asset Management

Essential and important entities must implement, operate and maintain asset management for network and information systems supporting their operations or delivery of their services.

This is a fundamental measure in identifying, assessing, and treating network and information system cybersecurity risks. Entities need to know their equipment, both hardware and software, as well as the data, that is being used by their network and information systems. It is impossible to identify, assess, quantify or understand the risks associated with those assets or to allow for appropriate treatment without this information.

To meet this risk management measure requirement:

Foundational actions:

RMM007.FA01: Asset inventory: Create and maintain with regular updates and/or on systems changes/acquisitions, a catalogue (inventory) of their network and information systems assets, hardware/software/Cloud/third party/Data, used in their operations or to support their services.

RMM007.FA02: Asset classification: For each identified asset, understand its importance to the business and service delivery, taking into account relevant factors such as its position within the network and information system architecture, etc.

RMM007.FA03: Asset handling: Network and information system assets to be handled in an appropriate manner to the risks around each asset during its lifecycle, from configuration, deployment, maintenance and finally decommissioning. Asset handling to include measures such as recovery on termination of contract for staff, safe disposal, physical considerations such as access, moisture, temperature, etc.

Supporting actions:

RMM007.SA01: Understand the significance of assets and thus risk to the entity's operations or delivery of its services.

RMM007.SA02: Categorise systems that make up the network and information services supporting the entities operations or services, allowing at least matching categorisation of the assets that underpin or deliver the operations or services.

RMM007.SA03: Understand an asset's position within a network and information system architecture as this can increase the significance of any weakness or vulnerability inherent in its design, operation, configuration, or maintenance. As such both its business significance and its network and information system cybersecurity risk need to be taken into account.

RMM007.SA04: Develop and maintain an inventory of network and information systems and associated assets. Ensure that this inventory remains complete, accurate, current, and consistent. Changes to the entries in the inventory are documented in a traceable manner.

DRAFT

RMM007.SA05: All assets are associated with a classification level, ideally at or greater than the classification of the system it is part of delivering or supporting. Similar to operations and system classification, the asset classification is to be based on risk and take into consideration the confidentiality, integrity, authenticity and availability requirements, as well as business risk to indicate the protection level required.

- Data that an entity holds, creates or processes is also an asset and treated as such. To support this, the entity should institute a data classification scheme. The classification for sensitive information should be defined and communicated and enforced. e.g. a data classification could have various levels such as "public" – no restriction, internally or externally, "Internal only" - accessible only to members of your organisation, "confidential" – restricted to those who have been authorised. Entities should use classifications derived by national law, international agreements or international accepted strategies for information sharing, like the Traffic Light Protocol (TLP).[6]

RMM007.SA06: Ensure assets are controlled in a manner consistent with the risk requirements of the entity. To ensure this the entity should create, document, communicate, maintain and provide policies, standards and guidelines for the proper handling of assets in accordance with the network and information security policy, throughout their life cycle of acquisition, use, storage, transportation and disposal.

RMM007.SA07: Asset policies and guidelines should also cover the appropriate use, storage, transport, and the irretrievable deletion and destruction of assets, both physical and virtual (virtual machines, software or data).

RMM007.SA08: Equipment, hardware, software or data are only transferred externally with the entities approval and in a manner authorized by the entity in line with the risks. Where warranted by the risk and mandated by the entity, the transfer should take place in a secure manner, in accordance with the type of asset to be transferred. The policies and guidelines should cover the correct usage of any asset used outside the organisation's premises (e.g. mobile device).

RMM007.SA09: Removable media – due to the particular risk profile of removeable media, specific controls to be mandated.

- Create, document, communicate, and maintain a policy on the management of removable storage media and communicate it to anyone authorised to use or handle removable storage media. The policy should:
  - Provide for technical measures to prohibit the connection of personal, or unauthorised third-party removable storage media.
  - Use technical measures to prohibit the connection of removable media unless there is both an organisational reason and authorisation for its use, ideally in a limited, documented, controlled manner, using authorised entity removable storage media.
  - Provide for disabling the execution of autoruns from such media.
  - Mandate and provide for scanning of authorised removeable storage media for malicious code before they are used on organisation's systems.

[6] https://www.first.org/tlp/

- Include control and protection of portable storage devices while in transit and in storage.
- Where appropriate to the use case of the removeable storage media, the use of cryptographic techniques should be enforced to protect information on removable storage media, if required for confidentiality or integrity reasons.
- Each of the approved and authorised removeable storage media should have full lifecycle tracking, including where appropriate to the use case, the data classification it is being used for and the protections enabled for that data (e.g. encryption for PII).

RMM007.SA10: All internal employees, external employees, contractors or third parties in possession of entity assets, to return or irrevocably delete these assets under their control in a manner and to a level specified by the entity, in line with the risk profile of the asset. This should be done as soon as the employment or contractual relationship is terminated, with an acceptable, mandated level of assurance. This should be reflected and traceable through the asset inventory.

RMM008 – Human Resources Security

Essential and important entities, in the context of managing the risks to network and information systems used in their operations or for the delivery of their services, take into account the human factor.

An entity's human resource security is a fundamental measure in identifying, assessing, and treating cybersecurity risks. Entities need to know and control who should, who can and who is accessing network and information systems used in their operations or delivery of their services.

To meet this risk management measure requirement:

Foundational actions:

RMM008.FA01: Ensure that employees, contractors and third parties are aware of, understand and adhere to the security requirements of the organisation.

RMM008.FA02: Ensure access to network and information systems is controlled, access is limited to only that required, regularly reviewed and the level of access is approved by the appropriate authority before it is granted.

RMM008.FA03: Security roles are defined in accordance with the role/access/risk requirements of the access they will have and the potential impact of compromise.

RMM008.FA04: Background verification checks are performed where appropriate/possible/required.

RMM008.FA05: Increased control and/or monitoring where appropriate such as for privileged/high risk/contractor/third party access.

RMM008.FA06: Implement ongoing and targeted role based cybersecurity/risk training.

RMM008.FA07: Strict processes for the authorisation/review/update/monitoring of role-based permissions in line with the defined role risk appetite.

DRAFT

Supporting actions:

RMM008.SA01: Employees, and where applicable, direct suppliers, service providers, contractors, maintenance or support personnel understand and adhere to their security responsibilities, appropriate to the services and function offered, the access they have been provided and in line with the entity's network and information security policies.

(Security responsibilities will differ depending on access and associated risk profile of the role that personnel are assigned to.)

RMM008.SA02: All users for their particular role/access understand and adhere to the security requirements of that role and the standard cyber hygiene practices of the entity.

RMM008.SA03: All users with administrative or privileged access are aware of and follow their network and information security roles, responsibilities, and authorities.

RMM008.SA04: Top management understand their role, responsibilities and authorities regarding network and information security.

RMM008.SA05: Those staff with delegated authority to authorise access for a given role/system/service understand the network and information system risks associated with providing that level of access and utilise the requisite level of caution in providing any such authorisation for that level of access.

RMM008.SA06: Based on an entity's risk assessments of its network and information systems used for its operations or delivery of its services, determine if background verification checks (e.g. reference check, validation of certifications, written tests) are appropriate, possible, or required for a role.

- Where it is determined by the entity that background verification checks are appropriate, possible, or required background verification checks should at least take into consideration:
  - Applicable laws.
  - Regulations.
  - Ethics.

RMM008.SA07: When granting access, take into account the risks, business requirements, the classification of the information and the network and information systems to be accessed.

RMM008.SA08: Responsibilities and duties that must continue to be met, after termination of employment or of a contract, should be contained in the individual's terms and conditions of employment, contract or agreement, e.g. confidentiality clauses.

RMM008.SA09: Logical and physical access control policies, such as a joiner/movers/leavers HR policy should ensure that access rights are modified accordingly upon termination or change of employment (e.g. revocation of access rights along with the granting of the new access rights, account deactivation, etc.).

RMM008.SA10: On a change of employment within the entity, it should be ensured that the employee can perform the new tasks to an appropriate level on a consistent basis and a familiarisation mechanism provided for the employee to ensure full understanding of the requirements of the new role and to determine if further training is needed.

RMM008.SA11: Encourage a "no blame" culture and reporting of mistakes, errors, misconfigurations, etc.

DRAFT

RMM008.SA12: Establish, communicate, and maintain a disciplinary process for handling wilful, malicious or negligent violations of network and information security policies. The process should take into consideration relevant legal, statutory, contractual and business requirements.

RMM009 – Access Control

As part of the risk management measures essential and important entities put in place, they must address identity and access management for both human and non-human identities. To do this they will need to implement, operate, and maintain appropriate access control polices.

To meet this risk management measure requirement:

Foundational actions:

RMM009.FA01: Establish and implement logical and physical access control policies for the access of persons and processes on network and information systems, with an appropriate and proportionate level of authentication, based on cybersecurity risk assessments.

RMM009.FA02: As part of the access control policies, develop, implement, and operate a JML (joiners, movers, leavers) process. Then create, deploy, operate, and review appropriate access control, both to control access and to manage the risk of cumulative permissions assigned over time.

RMM009.FA03: Limit the use of shared/generic/default/well known user accounts to a documented controlled exception basis only, involving a documented, authorised, controlled, monitored, verified and limited number of identifiable individuals, with compensating controls and or heightened monitoring/alerting.

RMM009.FA04: Limit both the number and type of administrator level access accounts to unique accounts and to only those strictly necessary. In exceptional circumstances where this is not technically possible or feasible, these accounts should be limited to a controlled exception basis only, involving a documented, authorised, controlled, monitored, verified and limited number of identifiable individuals, with compensating controls and/or heightened monitoring/alerting.

RMM009.FA05: Use segregation of administrative or privileged access where possible, limiting the extent of privilege of any single account according to the associated risk.

RMM009.FA06: Failed privilege login attempts to be logged and flagged, in line with risk.

Supporting actions:

RMM009.SA01: The access control policies should be based on business, as well as network and information security requirements, in order to prevent unauthorised access to related assets, including information.

- Policies addressing access by (a) persons, both staff members and external entities, such as suppliers and service providers, and (b) processes – e.g. one network and information system connecting to another.
- Access control policies and processes supporting them should be documented. The entity should implement and maintain network and information system access restrictions based on these access-control policies.

DRAFT

- Access should be granted only when the user has been correctly authenticated.

RMM009.SA02: Manage access rights to network and information systems which should be provisioned, modified, removed and documented in accordance with the organisation's topic-specific policy on access control.

- Assign and revoke access rights based on the need-to-know, least privilege principles and separation of duties.
- Access rights are modified accordingly upon termination or change of employment (e.g. revocation of access rights, account deactivation, etc.).
- Access to network and information systems is authorised by their owner.
- Access rights appropriately address third-party access, such as suppliers, service providers, contractors and maintenance or support personnel. It is particularly important to limit such access rights, both in scope and in their duration.
- Maintain a register of access rights granted to users.
- Apply appropriate logging to access rights management.

RMM009.SA03: Maintain policies for management of privileged and administration accounts.

- Set up specific accounts to be used for administration operations only, such as installation, configuration, management, or maintenance.
- Individualise and restrict administration privileges as much as possible.
- Only use such accounts for system administration purposes.
- Use strong identification, authentication, and authorisation procedures for such accounts.

RMM009.SA04: Where administration systems are used, restrict and control the use of those administration systems.

- Only use such systems for administration purposes, and not for any other operations.
- Logically separate such systems from application software not used for administrative purposes.
- Protect access to administration systems with authentication and encryption.

RMM009.SA05: Manage the full life cycle of identities of users and systems accessing information and related assets.

- Require the use of unique identities for users and systems:
  - For users, link the identity to a single person to allow traceability/attribution of actions and to hold the person linked to the identity accountable for actions performed with that specific identity.
  - Where identities are assigned to multiple persons or are allowed to be used by multiple persons (e.g. shared identities), these should be only permitted where they are necessary for business or operational reasons and are subject to dedicated approval, documentation, heightened control, monitoring, to include logging and alerting.
  - Use an exception process for these shared identities, with stricter controls where appropriate such as activation on request, with strict limits to both access and duration (see FA04 and FA05).

DRAFT

- Provide human oversight of system identities.
- Apply appropriate logging for the management of identities.

RMM009.SA06: Implement secure authentication procedures and technologies based on access restrictions and the topic-specific policy on access control.

- Ensure the strength of authentication is appropriate to the classification of the asset to be accessed.
- Enforce the specified authentication methods based on risk and unique authentication information.
- Control the allocation of secret authentication information by a process, that ensures the confidentiality of the information, including advising personnel on appropriate handling of authentication information.
- Require the change of authentication credentials initially, periodically, and when there is suspicion that the credential has been compromised.
- Require the reset of authentication credentials and the blocking of users after a predefined number of unsuccessful log-on attempts.
- Generate an alert if a potential, attempted or successful breach of log-on controls is detected, and have a defined mandated or automated response for such an event that is in line with the risk.
- Terminate inactive sessions after a predefined period of inactivity.
- Require separate credentials for privileged access or administrative accounts, based on the risk, limit these accounts to performing the privilege access or administrative functions they have been authorised for e.g. don't allow the use of the domain administrative account to browse the internet or access emails.

RMM009.SA07: In accordance with the classification of the asset to be accessed and where appropriate, users, devices and other assets should be authenticated by multiple authentication factors and/or continuous authentication mechanisms for accessing the entity's networks and information systems.

- The multi factor authentication should be appropriate for the classification of the asset to be accessed.
- Multi factor authentication when accessing systems from a remote location, accessing administration systems, access to sensitive information, etc.
- Multi factor authentication can be combined with other techniques that require additional factors under specific circumstances, based on predefined rules and patterns, such as restricting access based on location, device, or timeframe. This could be combined with altering for access attempts from an unusual location, from an unusual device or at an unusual time.

DRAFT

RMM010 – Environmental and physical security

Essential and important entities must take physical and environmental considerations into account for cybersecurity risk assessments of network and information systems used in their operations or for the delivery of their services.

For the risks identified in the assessments, appropriate and proportionate measures for the treatment of the risks must be developed and incorporated into the cybersecurity posture of the entities.

To meet this risk management measure requirement:

Foundational actions:

RMM010.FA01: Physical and environmental considerations will need to be taken into account for cybersecurity risk assessments of network and information systems. These will include:

- System failures
- Human error
- Malicious acts
- Natural phenomena

RMM010.FA02: Implement appropriate and proportionate measures to address the identified risks.

RMM010.FA03: Regularly review the adequacy of the measures in addressing the risks.

RMM010.FA04: Regularly renew/update the risk assessments to take account of change in equipment, threat landscape, known risks and changes to risk levels.

RMM010 FA05: Implement appropriate physical access control measures.

Supporting actions:

RMM010.SA01: Prevent and monitor for unauthorized physical access (physical security measures designed to Deter, Detect, Deny, Delay), damage and interference to the organisation's network and information systems.

- Ensure that critical remote installations have a level of security appropriate to their criticality.
- Security perimeters defined and used to protect areas that contain network and information systems and other associated assets.
- Secure areas protected by appropriate entry controls and access points.
- Physical security for offices, rooms and facilities.
- Premises continuously monitored for unauthorized physical access.
- Physical access control procedures and measures are tested and reviewed at planned intervals or when significant changes to operations or risks or significant incidents occur.

RMM010.SA02: Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure. Examples of such threats include fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions:

DRAFT

- The security measures should take into account risk assessment results, local topography and urban threats. Environmental parameters should be monitored and lead to an event being reported, if the permitted control range is exceeded.
- Protection measures against physical and environmental threats should be tested, as well as reviewed at planned intervals and when there are significant changes to operations or risks, or when significant incidents occur.

RMM010.SA03: Facilities are protected from power failures and other disruptions caused by failures in supporting utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning). Where applicable, consider the use of redundancy for utility services.

RMM010.SA04: Utility services such as electricity and telecommunications, which transport data or supply information systems, are protected against interception and damage.

RMM010.SA05: The utility services are monitored. If the permissible control range is exceeded, alarm messages are generated and forwarded to the responsible unit for event management.

RMM010.SA06: Contracts for the maintenance of the emergency supply with a corresponding service provider have been concluded (e.g. for the fuel for the emergency power supply).

RMM010.SA07: The supply of IT systems necessary for the operation of the service offered (e.g. electricity, temperature, humidity control, telecommunications, and internet connection) are monitored, regularly maintained, and tested to ensure continuous effectiveness. Therefore, policies/instructions are documented, communicated, and made available, which describe the maintenance (especially remote maintenance), deletion, updating, reuse of assets in information processing in outsourced premises or by external personnel.

RMM010.SA08: IT systems should be equipped with automatic fail-safes and other redundancies.

RMM011 – Cryptography, Encryption and Authentication

Essential and important entities must implement, operate and maintain policies and procedures for the appropriate use of cryptography and where appropriate, encryption by and within their network and information systems used in their operations or for the delivery of their services.

To meet this risk management measure requirement:

Foundational actions:

RMM011.FA01: The confidentiality, integrity, and availability (CIA) of the data required to deliver services is protected.

RMM011.FA02: Based on the cybersecurity risk assessments, entities will need to create, communicate, maintain and enforce policies and procedures for the appropriate use of cryptography and where appropriate encryption by, and within, their network and information systems.

DRAFT

RMM011.FA03: The adequacy of these measures is supervised and reviewed as part of the entities compliance operation specifically to ensure the measures remain adequate for the risks as they evolve over time.

RMM011.FA04: Multi factor and/or continuous authentication is used for remote access or privileged accounts where appropriate and proportionate to the risk.

RMM011.FA05: Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, entities shall include the use of secured voice, secured video, secured text communications and the use of secured emergency communication systems within the entity, where appropriate to the risks posed.

Supporting actions:

RMM011.SA01: Establish and implement a policy and procedures related to cryptography, with the aim of ensuring, in line with the risk, appropriate use of cryptography.

- Protocols to be adopted, cryptographic algorithms, cipher strength, cryptographic solutions and usage practices that are approved or required for use in the entity, e.g. end-to end encryption of communication, hard disk encryption of data at rest, etc.
- Identification of the required level of protection and the classification of assets, including the establishment of the required type, strength, and quality of the cryptographic algorithms.
- The approach to key management, including methods for:
  - Generating keys for different cryptographic systems and different applications.
  - Issuing and obtaining public key certificates.
  - Distributing keys to intended entities, including how to activate keys once received.
  - Storing keys, including how authorized users obtain access to keys.
  - Changing or updating keys including rules on when and how to change keys.
  - Dealing with compromised keys.
  - Revoking keys including how to withdraw or deactivate keys.
  - Recovering keys that are lost or corrupted.
  - Backing up or archiving keys.
  - Secure destruction of keys appropriate to the classification level.
  - Logging and auditing of key management related activities.
  - Setting activation and deactivation dates for keys so that the keys can only be used for the period of time according to the organisation's rules on key management.
  - Handling legal requests for access to cryptographic keys.

RMM012 – Supply chain policy

Essential and important entities must implement, operate and maintain an organisation approved network and information system supply chain policy that includes the security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

It should be noted that the risks to third party supplied network and information systems, even where fully managed, and the resulting risks to the entity's operations or services, are the responsibility of the entity themselves.

As such they will need to be recognised and addressed in an appropriate and proportionate manner, in line with the risk management framework set out by the entity's risk management policy (RMM004).

DRAFT

To meet this risk management measure requirement:

Foundational actions:

RMM012.FA01: Create, communicate, maintain, and enforce an organisation defined network and information system supply chain policy that includes the security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

- Entities shall take into account the risks specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.
- When considering which measures are appropriate entities will need to take into account the results of the coordinated security risk assessments of critical supply chains carried out by the co-operation group in accordance with Article 22(1) of the Directive.

RMM012.FA02: Identify direct suppliers or service provider relationships, particularly for the network and information system supply chain (e.g. ICT, ICS, OT), to ensure that potential risks can be identified.

RMM012.FA03: Maintain and keep up to date a registry of direct suppliers or service providers, including:

- Contact points for each one, in particular those with access to, or managing the entity's critical assets.
- List of network and information systems, services, or products provided by the supplier or service provider.

RMM012.FA04: Ensure via service level agreements (SLA) and/or auditing mechanisms that suppliers and providers, including cloud computing providers, establish and continue to operate adequate security measures which address the entity's security requirements. Ensuring they are and remain appropriate and proportionate to the risk.

RMM012.FA05: Considers the information security policy measures (RMM003), risk management policy measures (RMM004) and any other mandated measures.

Supporting actions:

RMM012.SA01: Define criteria to select suppliers or service providers in the supply chain policy.

- Ability of the supplier or service provider to meet cybersecurity specifications.
- Risks and classification level of the ICT services, ICT systems or ICT products that the supplier or service provider delivers.
- The risk tolerance of the supplier should be taken into account.
- Ability of the entity to diversify sources of supply and limit vendor lock-in.
- Results of the coordinated security risk assessments of critical supply chains carried out in accordance with article 22(1) of NIS 2, are taken into consideration, if applicable.

RMM012.SA02: Contracts with direct suppliers or service providers should include clauses on (non-exhaustive list):

- Security clauses in contracts/SLA's/etc. (required by the entity's own security requirements, NIS 2 or other legal requirements, e.g. confidentiality clauses).

DRAFT

- Obligation of the supplier to notify the entity of all relevant incidents as soon as they become aware of the incident, with adequate information disclosure to allow the entity to understand, risk assess and implement appropriate responses.
- Right to audit and/or right to receive audit reports.
- Skills and training required from the supplier's personnel.
- Security certifications required by personnel of the supplier or provider.
- Background verification checks of the supplier's personnel, if critical assets are managed/maintained by the supplier (required by the entity's own security requirements).
- Agreement on repair times.
- Obligation to perform vulnerability management.
- Subcontracting details/agreements and (if allowed) security measures for subcontractors.
- Obligations of the supplier at the termination of the agreement (e.g. retrieval and disposal of the information).

RMM012.SA03: Take into account security requirements as part of the selection process of new direct suppliers and providers, as well as when planning, preparing, managing, and terminating the procurement of an ICT product, service, or process.

RMM012.SA04: Monitor, review, evaluate and manage changes in the cybersecurity practices of direct suppliers or service providers at planned intervals or after an incident related to the provision of services by direct suppliers or service providers.

RMM012.SA05: Review of the security requirements passed on to the direct suppliers or service providers:

- Regular monitoring of service reports (e.g. SLA reporting).
- Review of security-related incidents, operational failures or outages, and interruptions related to the service.
- Unscheduled reviews following significant changes in requirements or environment. The need for unscheduled reviews will need to be assessed and documented in a comprehensible manner.
- Conduct a risk analysis of all identified deviations so that they can be addressed in a timely and effective manner through risk mitigation measures.

RMM013 - Security in network and information systems acquisition, development and maintenance

Essential and important entities must manage the cybersecurity risks to network and information systems used in their operations or for the delivery of their services from both the process of obtaining those systems and then in the maintenance of those systems. This must include both vulnerability handling and disclosure.

To meet this risk management measure requirement:

Foundational actions:

RMM013.FA01: Create, communicate, enforce, and maintain appropriate and proportionate policies and procedures, in line with the management of the cybersecurity risks for:

- patch management,

- configuration management
- change management
- logging and monitoring

RMM013.FA02: In an entity's acquisition of network and information systems, take into account risks in relation to the maintenance of those systems, to include life cycle, support, etc. including any inherent risks of those systems.

RMM013.FA03: When developing systems, or parts thereof, use or cause to be used, Secure Software Development methods such as SSDLC in order to minimise the cybersecurity risks of the product when deployed into production.

RMM013.FA04: Address network and information system vulnerabilities and undertake vulnerability disclosure to the extent that it is within their ability, to an appropriate and proportional extent, in line with the management of the cybersecurity risks.

RMM013.FA05: Take into account any changes to the risk structures within the organisation due to the acquisition of new systems during the acquisition process.

Supporting actions:

RMM013.SA01: Establish, document, implement, and monitor configurations, including security configurations of hardware, software, services, and networks (e.g. create baselines).

RMM013.SA02: Define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services, and networks, for newly installed systems as well as for operational systems over their lifetime.

RMM013.SA03: Changes, repairs and maintenance to network and information systems subject to change management procedures and be consistent with the entity's policies. The procedures should be documented and communicated.

RMM013.SA04: Change control procedures applied for releases, modifications and emergency changes of any operational software, hardware, or changes to the configuration. The procedures should be documented and communicated.

RMM013.SA05: In case of emergency changes, the outcome of the change should be documented, as well as an explanation of why the regular change process could not be followed and what the consequences would have been of a delay by following the regular change process. Tests that were skipped due to the emergency change should be carried out afterwards.

RMM013.SA06: Changes tested first in an environment that is different and separate from the production environment (operational environment) before that change is effectively implemented. That way, the effect of those changes can be analysed, and adjustments can be made without disrupting operational activities.

RMM013.SA07: Procedures for changes include:

- Request for change.
- Risk assessment.

DRAFT

- Criteria for categorization and prioritization of changes and associated requirements for the type, and scope of the tests to be carried out and the approvals to be obtained.
- Requirements for performing rollbacks.
- Documentation and approval of the changes including information to stakeholders.

RMM013.SA08: Changes, maintenance and repairs of network and information systems are performed and logged, with approved and controlled tools.

RMM013.SA09: Remote maintenance of network and information systems should be approved, logged, and performed in a manner that prevents unauthorized access.

RMM013.SA10: Obtain information about technical vulnerabilities of network and information systems, evaluate the organisation's exposure to such vulnerabilities and take appropriate measures to manage the vulnerabilities. Follow different channels, for example announcements of the national competent authorities (e.g. national CSIRT), or supplier information.

RMM013.SA11: Perform vulnerability scans when appropriate and record evidence.

RMM013.SA12: For any vulnerability, given the potential impact, create and implement a plan to mitigate the vulnerability or document the reason why the vulnerability does not require remediation. The vulnerability handling should be aligned with change management and incident management. Vulnerabilities assigned to a criticality level of "Critical" (or equivalent) should be addressed without undue delay.

RMM013.SA13: Security patches are:

- applied within a reasonable time after they become available.
- tested before being applied in production systems.
- verified as coming from trusted sources and are checked for integrity.
- are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them.

RMM013.SA14: The reasons for not applying any security patches are documented.

RMM013.SA15: Additional measures are implemented, such as compensating controls and/or heightened logging/alerting are put in place where patches are not applied.

RMM013.SA16: Any residual risks are put through the standard risk framework process with an appropriate and proportionate risk treatment defined. Should the risk be accepted, particularly where a patch is not available, the risk should be reviewed regularly.

RMM013.SA17: Patch management is aligned with the change management procedures.

RMM013.SA18: Define and implement processes and procedures to manage cybersecurity risks associated with the acquisition of network and information services, systems, or products throughout their entire lifecycle. Such as:

- Security requirements to apply to the services, systems, or products to be acquired.

DRAFT

- Security updates throughout the entire lifetime of services, systems or products or replacement after the end of the support period, where applicable.
- Information describing the hardware and software components used in services, systems, or products.
- Information describing the implemented cybersecurity functions of the product and the configuration required for its secure operation.
- Obtaining assurance that the services, systems, or products achieve the required security levels.
- Processes and acceptable methods for validating that the delivered services, systems, or products are compliant to stated security requirements, as well as documentation of the validation results.

RMM013.SA19: A product lifecycle management policy and the derived procedures and measures applied to both software and hardware products, regardless of whether they were developed in-house or acquired.

RMM013.SA20: Rules for the secure development of software and systems should be established and applied when entities acquire or develop network and information systems. Such as:

- An analysis of security requirements carried out at the specification and design phases of any systems development or acquisition project undertaken by the entity or on behalf of the entity.
- Principles for engineering secure systems and secure coding principles applied to any information system development activities, e.g. promoting cybersecurity-by-design, zero trust architectures.
- Security requirements for development environments are defined.
- Security testing processes defined and implemented in the development life cycle and test information appropriately selected, protected, and managed.
- Testing data is sanitised and anonymised according to information classification and a risk assessment.

RMM013.SA21: Protect network and information systems from cybersecurity threats:

- Apply controls (e.g. firewalls) to protect the entity's internal network domains from unauthorized access.
- Configure network and information systems to prevent all protocols and accesses not required for the operation of the entity.
- Segmentation of systems into networks or zones considering functional, logical, and physical (including location) relationship between trustworthy systems and services.
- Application of the same security measures to all systems co-located in the same zone.
- Keeping all systems that are critical to the entity's operation or to safety in one or more secured zone(s), according to their risk assessment.
- Restrict access and communications between zones to those necessary for the operation of the entity or for safety, according to their risk assessment.
- Separate dedicated network for administration of network and information systems and the entity's operational network.
- Segregate network administration channels from other network traffic.
- Separate the production systems for the entity's services from systems used in development and testing.
- Reinforce controls for remote access (proxy, VPN) to network and information systems, including access from authorised or trusted third parties such as service providers.

DRAFT

- Prohibit the use of administration systems for other purposes.
- Explicitly forbid or deactivate unnecessary connections and services.
- Authorised devices managed by the entity only and explicitly forbid all other devices.
- Actively control the connections of trusted third parties or service providers, only allowing the connection after an authorization request and where possible, for a set time period (e.g. duration of a maintenance).
- Establish communication between distinct systems only through trusted channels that are isolated using logical, cryptographic, or physical separation from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.
- Document the architecture of the network in a comprehensible and up-to-date manner.
- Network and information systems should be protected against malicious and unauthorized software. These systems should be equipped with malware detection and repair software, which is at least updated daily.
- In particular:
    - Implement rules and controls that prevent or detect the use of unauthorized software.
    - Implement controls that prevent or detect the use of known or suspected malicious websites.
    - Reduce vulnerabilities that can be exploited by malware.
    - Control the execution of applications on user workstations or user end devices.
    - Control the use of removable media.
    - Employ email and web application filters to reduce exposure to malicious content.

RMM014 – Incident Handling

Essential and important entities must have measures in place that define roles, responsibilities and procedures for preventing, detecting, analysing, containing or responding to, cybersecurity incidents in a timely manner, meeting all mandated legal and regulatory requirements.

To meet this risk management measure requirement:

Foundational actions:

RMM014.FA01: Create, communicate, enforce, and maintain a policy that includes incident handling which mandates the creation, maintenance and use of an incident response plan. This plan to include effective communication plans, categorization of incidents, escalation and reporting.

RMM014.FA02: Assign roles to detect and appropriately respond to incidents, to appropriate personnel.

RMM014.FA03: Create, communicate, enforce, and maintain documentation to be employed in the course of incident detection and response, in line with the incident response plan. This may include incident response manuals, escalation charts, contact lists and templates.

RMM014.FA04: Create, communicate, enforce, and maintain interfaces between the incident handling and business continuity management arrangements, e.g. when does an incident trigger the BCP plan.

RMM014.FA05: Create, communicate, enforce, and maintain reporting obligations according to national legislative frameworks (e.g. NIS 2) and with relevant internal and external stakeholders in accordance with agreed communication plans.

DRAFT

RMM014.FA06: Create, communicate, enforce, and maintain a mechanism allowing personnel, suppliers, and customers to report suspicious events.

RMM014.FA07: Create, communicate, enforce, and maintain a defined mechanism to ensure suspicious events are assessed to determine whether they constitute network and information security incidents and, if so, to determine their nature and severity.

RMM014.FA08: Test the security incident management process through periodic incident response exercises and scenarios.

Supporting actions:

RMM014.SA01: The entity should ensure personnel assigned to an incident handling role have the necessary competency, skills, knowledge, and experience for the assigned role.

RMM014.SA02: Appropriate documentation is employed or generated in the course of incident detection and response.

RMM014.SA03: Response to incidents is carried out in accordance with documented procedures and in a timely manner. This may include incident response manuals, escalation charts, contact lists and templates.

RMM014.SA04: Procedures should include the following stages:

- Incident containment, to prevent the consequences of the incident from spreading.
- Eradication, to prevent the incident from continuing or reappearing.
- Where required, recovery from the incident.

RMM014.SA05: Communicate:

- With national competent authorities and NCSC, according to the national legal provisions related to incident notification.
- With relevant internal and external stakeholders in accordance with agreed communication plans.

RMM014.SA06: Log incident response activities, and record evidence. This should include as appropriate, forensic methods to ensure that the evidence is admissible in a court of law.

RMM014.SA07: Use of appropriate and proportionate tools and processes to monitor and log activities on the entity's network and information systems. This is to detect events that could be considered a security incident and use alerting to enable them to respond accordingly and in a timely manner to mitigate the impact.

RMM014.SA08: Maintain, document, and review logs, with automatic alerting on at least the critical systems/access/data.

RMM014.SA09: Items to include in logging (non-exhaustive):

- Outbound and inbound network traffic.
- The creation, modification or deletion of users and extension of their permissions.
- Access to systems and applications.
- All privileged access to systems and applications.
- All activities performed by administrative accounts.

DRAFT

- Access and changes to critical configuration and backup files.
- Event logs and logs from security tools, e.g. antivirus, intrusion detection systems or firewalls.
- Use of system resources, as well as their performance.
- Physical access to its facilities.
- Access to and use of its network equipment and devices.
- Environmental events, such as flooding alarms.

RMM014.SA10: Review logs for any unusual or unwanted trends and the entity should define appropriate alarm thresholds. If the defined threshold values are exceeded, an alarm should be triggered. The responsible personnel should ensure that in the case of an alarm an appropriate response is initiated.

RMM014.SA11: Implement monitoring in a way which minimises false positive and false negative alerting.

RMM014.SA12: To the extent feasible, monitoring should be automated (e.g. intrusion detection systems) and should be carried out either in real time or in periodic intervals, subject to business capabilities.

RMM014.SA13: Maintain and back up logs for a predefined period, stored at a central location and protected from unauthorized access or changes. The logging should include defined events that may affect the security and availability of the service provided, including logging of the activation, stopping and pausing of the various logs.

RMM014.SA14: The implemented measures should be able to detect network-based attacks based on anomalous ingress or egress traffic patterns and/or distributed denial of service (DDoS) attacks in a timely manner.

RMM014.SA15: All systems have synchronised time (sources) to be able to correlate logs between systems for incident assessment.

RMM014.SA16: Document a list of all assets that are being logged.

RMM014.SA17: Monitoring and logging systems have redundancy to ensure the security of the provided services, in line with the risk.

RMM014.SA18: Availability of the monitoring and logging systems is monitored independently.

RMM014.SA19: Suspicious events should be assessed to determine whether they constitute network and information security incidents and, if so, to determine their nature and severity.

RMM014.SA20: Assessments are carried out based on predefined criteria, and through triage by personnel with the competency to determine the nature of the suspicious event and assign an appropriate classification, prioritisation assigned if determined to be an incident, containment steps and eradication. The entity should review the appropriate logs for the purposes of event assessment and classification. The entity should put in

DRAFT

place a process for log correlation and analysis. The entity should reassess and reclassify events if and when new information becomes available.

RMM014.SA21: Evidence is recorded in a way that ensures that the evidence is admissible in a court of law, if applicable.

RMM014.SA22: Deploy a Security Information and Event Management tool (SIEM) that will facilitate the correlation and analysis of data where appropriate.

RMM014.SA23: Post-incident reviews to identify the root cause of the incident should take place and result in lessons learned to reduce the occurrence and consequences of future incidents.

RMM014.SA24: Post-incident reviews feed into continuous improvement of the entity's approach to network and information security, to risk treatment measures, and to incident handling, detection, and response procedures.

RMM015 – Incident Reporting

Essential and important entities must notify, without undue delay, the NCSC CSIRT of any significant incident. They must also indicate if the significant incident is a cross-border incident.

Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services.

An incident shall be considered to be significant if:

- It has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned.
- It has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

The following incident notification timelines are applicable:

- Early warning, without undue delay and in any case within 24 hours of becoming aware of the significant incident. This incident notification shall indicate:
  - Any cross-border impact.
  - Whether the significant incident is suspected of being caused by unlawful or malicious acts.
- Formal incident notification without undue delay and in any case within 72 hours of becoming aware of the significant incident.
  - This incident notification shall:
    - Provide an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise.
- Status updates: To the CSIRT or NCA, upon request.
- Final report not later than one month after the submission of the Formal incident notification, which includes the following:
  - A detailed description of the incident, including its severity and impact.
  - The type of threat or root cause that is likely to have triggered the incident.
  - Applied and ongoing mitigation measures.
  - Where applicable, the cross-border impact of the incident.

- In the event of an ongoing incident one month after formal incident notification, the entity concerned shall provide a progress report at that time, ongoing progress reports at the request of the NCSC or the NCA and in any event, monthly. These progress reports shall explain the progress

DRAFT

of service restoration and their handling of the incident. A final report not later than one month after the closure of the incident shall be submitted by the entity.

For trust service providers – the formal notification period, for significant incidents is without undue delay, and in any case within 24 hours of becoming aware of the significant incident.

General or sector specific guidance for incident reporting may be issued by the Minister, the NCSC or other relevant National Competent Authorities.

There is an implementing regulation EU/2024/2690 that sets out the reporting requirements for the following types of entities:

- DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

To meet this risk management measure:

Foundational actions:

RMM015.FA01: Report any significant incident to the NCSC within the mandated timeframes for incident reporting. This incident notification shall indicate:
- Any cross-border impact.
- Whether the significant incident is suspected of being caused by unlawful or malicious acts.

RMM015.FA02: Where the incident may potentially pose a (significant) cyber threat to the recipients of their services, the entity concerned shall notify those recipients, without undue delay. They shall also advise them of remedies that those recipients are able to take in response to that threat.

Supporting actions:

RMM015.SA01: Include the reporting requirements within its incident handling policy and guidelines.

- A definition of what a significant incident is, including those events capable of causing a significant incident, in the context of the entities network and information systems.
- Clearly outline in advance of any incident the mandatory reporting timelines with clearly articulated authorisation and reporting structures, i.e.
  - Who can authorise an incident report and who will report it.
  - What are the required reporting timelines at each stage.
  - Where is the incident to be reported e.g. to senior management and/or competent authorities and/or recipients of their services.
  - What information will be required for each reporting type at each stage of the incident reporting cycle.

DRAFT

- How an incident can/will be reported i.e. what mechanism will be required to report the incident, particularly where normal communications channels may be compromised by the incident.

RMM016 – Business Continuity and Crisis Management

Essential and important entities must implement, operate and maintain a continuity plan including but not limited to business continuity and disaster recovery plans to enact in the case of an incident.

The scope of which will be all network and information systems used in their operations or for the delivery of their services.

To meet this risk management measure requirement:

Foundational actions:

RMM016.FA01: The entity creates, communicates, maintains, reviews, and enforces a continuity plan, including but not limited to business continuity and disaster recovery plans to enact in the case of an incident.

RMM016.FA02: Put in place processes for crisis management, particularly in case of serious incidents.

RMM016.FA03: The entity implements a process for managing and making use of information received from the National CSIRT or, where applicable, competent authority, e.g. incidents, vulnerabilities, threats, and security controls

RMM016.FA04: Plans are regularly reviewed, updated and tested.

Supporting actions:

RMM016.SA01: Operations should be restored according to the business continuity plan.

RMM016.SA02: The plan should be based on the results of the risk assessment process which includes (non-exhaustive list):

- Purpose, scope and audience.
- Roles and responsibilities.
- Key contacts and communication channels – both internal and external.
- Conditions for plan activation and deactivation.
- Order of recovery for operations.
- Recovery plans for specific operations, including recovery objectives.
- Estimated required resources, including backups and redundancies.
- Restoring and resuming activities from temporary measures.
- Interfaces to incident handling.

RMM016.SA03: Crisis management processes addressing the following:

- Maintenance of network and information security in crisis situations by way of applying appropriate controls, such as supporting systems, processes, and additional capacity.
- Roles and responsibilities for personnel, including clear decision-making contingencies, ensuring that all staff know their roles in crisis situations, with specific steps to follow.

DRAFT

- Appropriate communication means between the entity and relevant competent authorities. This flow of information to include both obligatory communications, such as incident reports and related timelines (e.g., under NIS 2), and non-obligatory communications.

RMM016.SA04: Carry out a comprehensive business impact analysis (BIA). Based on the results of the BIA and risk assessments, establish for network and information systems used in its operations or delivery or a service, appropriate:

- Recovery time objectives (RTOs) to determine the maximum amount of time accepted for the recovery of a system, application or process after a disaster occurs.
- Recovery point objectives (RPOs) to determine how much data can acceptably be lost by systems, applications or processes as a result of an outage.
- Service delivery objectives (SDOs) to determine the minimum level of performance that needs to be reached by business functions during the alternate processing mode.

RMM016.SA05: RPOs, RTOs and SDOs should be used to help determine backup and redundancy requirements.

RMM016.SA06: To meet the objectives, adequate backup copies of information and sufficient availability of resources, including facilities, network and information systems and personnel, maintained and tested regularly, are required.

RMM016.SA07: Backup plans considerations:

- Recovery times.
- Assurance that backup copies are complete and accurate and include configuration data and information stored in cloud service environments they may utilise.
- Storing (online or offline) backup copies in a safe remote location or locations, which are not on the same network as the system on which the original data resides.
- Applying appropriate physical/environmental (such as access restrictions) and logical (such as encryption) controls to backup copies, in accordance with their information classification level.
- A determined retention period based on business, legal and regulatory requirements.
- Restoring information from backup copies (including approval processes).
- Regular managed and documented integrity checks on the backup copies.

RMM016.SA08: Availability of resources ensured by redundancy, in part or in full:

- Network and information systems, i.e. hardware, software, services, data, etc. (e.g. redundant network devices, servers with load balancing, raid arrays, backup services, multiple datacentres). Particularly for critical systems supporting services.
- Non-human assets, including facilities, equipment, and supplies.
- Personnel with the necessary responsibility, authority, competence, with appropriate communication channels and content (e.g. plans, contact lists, etc.).

RMM016.SA09: Consider appropriate controls for the handling of backup systems, data, communications, alerting, integrity checks, in line with the risks from handling sensitive data outside the normal direct control/authorisation/monitoring/reporting structures.

DRAFT

Reference material

The NIS 2 Directive

The NIS 2 directive ((EU)2022/2555) is available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

The Implementing Regulation

The implementing regulation (EU)2024/2690 is available at: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

This covers:

- DNS service providers,
- TLD name registries,
- Entities providing domain name registration services,
- Cloud computing service providers,
- Data centre service providers,
- Content delivery network providers,
- Managed service providers and managed security service providers,
- Digital providers i.e. providers of online marketplaces, of online search engines or of social networking services platforms and
- Trust service providers.

For these entities, refer to the Implementing Regulation instead of RMM003 to RMM014 and RMM016.

The implementing regulation also provides further specification of the cases in which an incident is considered to be significant.

DRAFT

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Abbreviations

Term	Meaning
AIW	Acceptable interruption window
BCP	Business Continuity Plan
BIA	Business Impact Assessment
CBI	Central Bank of Ireland
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ComReg	Commission for Communications Regulation
CRR	Commission for Railway Regulation
CRU	Commission for the Regulation of Utilities
DECC	The Department of Environment, Climate and Communications
DR	Disaster Recovery
ECSM	Electronic Communications Security Measures
GRC	Governance, Risk and Compliance
IAA	Irish Aviation Authority
ICT	Information and communications technology
ICS	Industrial control systems
JML	Joiners, Movers, Leavers
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
NCSC	National Cybersecurity Centre
NIS	Network and Information System
NTA	National Transport Authority
OT	Operational technology
PII	Personal Identifiable Information
SSDLC	Secure Software Development Lifecycle
TLP	Traffic Light Protocol

DRAFT

Addendum for ECN/ECS entities only

Background Information

The security measures in this section are based on the security measures which were consulted upon under Part 2 of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 to implement the security measures of the EU 5G Toolbox of Risk Mitigating Measures. While the majority of those security measures are now incorporated in the Risk Management Measures contained in the main body of this document, **there are some additional security measures that are only applicable to providers of publicly available ECN/ECS Networks.** These security measures are Foundational Actions and are contained in this addendum.

Network Management and Access Control

With reference to RMM007.FA01, ECN/ECS providers must ensure and document management plane asset management.

ECN/ECS providers must ensure that the management plane is under the oversight and ultimate control of the provider at all times.

For ECN/ECS providers, ensure that access to the management plane is through a dedicated jump server and requires multi factor authentication, wherever feasible. Any exceptions to this requirement must follow a pre-defined emergency access procedure and be fully documented.

ECN/ECS Providers must ensure that all access to and activity undertaken on the management plane is logged and monitored.

ECN/ECS providers must ensure that the management plane is only accessible from secure devices or PAWs, which are trusted and have been authenticated, and whose attack surface has been minimised.

ECN/ECS providers must ensure that managed equipment is locked-down, only necessary management protocols are enabled and, where technically feasible, management traffic uses secure encrypted protocols.

Where virtualization is implemented in ECN/ECS, providers must ensure that the security measures outlined in this document also apply to the administration of any virtualisation infrastructure.

Signalling Plane Security

ECN/ECS providers must ensure they understand how signalling interface and associated equipment could be impacted by malicious signalling. This includes understanding what user or network data could be compromised as a result of malicious signalling.

ECN/ECS providers must put in place suitable mechanisms to

- ensure that only trusted external signalling is accepted into its network.
- where technically feasible, only allow legitimate signalling traffic into and out of their networks.

DRAFT

- monitor and analyse inbound and outbound signalling traffic for malicious or malformed signalling messages.
- identify and block malicious or malformed signalling messages.
- design its networks to inhibit the leakage of network or user data.

ECN/ECS providers must ensure

- signalling nodes are hardened, unused interfaces are closed, and only authorised interfaces are used to establish communications links with the network elements.
- conduct security testing of its signalling network to ensure it functions as operationally expected and is sufficiently robust and secure.

ECN/ECS providers using Border Gateway Protocol (BGP) must implement technical and organisational measures

- which detect and mitigate against border gateway protocol misuse and which have regard to recognised industry standards, guidance and best practice.
- which minimise incorrect routing information being propagated and mitigates spoofed BGP traffic.
- to ensure that when implementing these measures, they collaborate with other network providers where appropriate.

Virtualisation Security

ECN/ECS providers using virtualisation must take the following virtualisation security measures:

- Ensure the retention of sufficient expertise to manage the virtualised infrastructure.
- Ensure that they understand the functioning of its virtual network; including but not limited to data flows, trust domains and the location and status of the physical hosts on which the virtual network resides.
- Ensure that the hardware & software involved in providing the virtualisation infrastructure is kept up to date and is able to withstand known vulnerabilities.
- Ensure that the hardware providing the virtualisation infrastructure supports silicon chip-based security functionality with a trusted platform module that stores measurements of the entire virtualisation layer and boot process, and is hardened.
- Ensure that communication between physical hosts is restricted to the minimum necessary, that interfaces are restricted to trusted hosts and that hard-coded configurations are reduced to the minimum necessary.
- Ensure where technically feasible, that sensitive virtual workloads or those providing a security boundary do not directly address the physical hardware on which they run. Document, risk assess and justify any exceptions to this.
- Ensure that the virtualisation layer is validated during boot up using a trusted platform module.
- Ensure that the virtualisation layer is hardened, Only the minimum services and processes necessary to operate VNFs shall be included, and other services shall be removed by default.
- Monitor the virtualisation layer to detect potential intrusion and take protective actions.
- Allocate a trust domain to virtual workloads based on their sensitivity.
- Separate trust domains using full virtualisation.

DRAFT

- Ensure that containers are not used to separate trust domains.
- Categorise physical hosts based on risk and each category shall be tagged with the trust domains that they can execute.
- Provide the management and orchestration function with enhanced level of security protection and monitoring.
- Ensure that administration of the virtualisation infrastructure or management and orchestration function is automated wherever possible.
- Ensure that the code used for automated administration is stored securely, monitored and audited.
- Ensure changes to the code used for automated administration are peer reviewed and signed off by appropriate senior employees.
- Ensure that administrators of their virtual infrastructure do not have access to the workloads within the virtualised environment. All exceptions to this requirement are documented, risk assessed and justified.

ECN/ECS Providers must:

- Ensure that it manages its network elements using either its own resources, the resources of a European Union or a European Economic Area registered entity or the resources of an entity operating in a manner compliant with European electronic communications, security and data protection legislation

ECN/ECS Providers must:

- Retain sufficient expertise to adequately monitor and supervise third parties accessing its network.
- Require suppliers to achieve suitable European cybersecurity certifications for critical products and services provided for under the EU Cybersecurity Act (Regulation (EU) 2019/881) or equivalent schemes.

ECN/ECS Providers must

- Ensure that there is an adequate stock of spare or replacement equipment available to the provider, to support critical network equipment.

DRAFT

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Appendix I - Foundational indicative control mapping

	NIS 2 Risk Management Measures Guidance		National Frameworks		International Standards	
Risk Management Measure	**Foundation Action**	**Title**	**BE-CyFun®2023**	**Draft CyFun2025**	**ISO 27001:2022**	**NIST CSF v2.0**
Governance – Management board commitment and accountability	2.1	RMM002.FA01	BASIC: PR.AT-1.1, IMPORTANT: ID.AM-6.1, PR.AT-4.1,	IMPORTANT: PR.AT-02.1, ID.IM-03.3	5.1, 5.3, 7.2, 7.3, A.5.2, A.5.4, A.6.3,	ID.IM-03, PR.AT-02,
Governance – Management board commitment and accountability	2.2	RMM002.FA02	IMPORTANT: ID.RM-1.1, ID.RM-2.1, ID.RM-3.1,	BASIC: GV.RM-03.1 IMPORTANT: GV.RM-01.1, GV.RM-02.1, GV.RM-03.2, GV.RM-04.1	6.1, 6.2, 6.3, 8.1, 8.2, 8.3, A.5.4	GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04
Governance – Management board commitment and accountability	2.3	RMM002.FA03	BASIC: ID.GV-4.1, IMPORTANT: ID.GV-4.2, ID.AM-6.1	IMPORTANT: GV.RR-03.1,	5.1, 7.1, 7.2, A.5.4	GV.RR-03,
Governance – Management board commitment and accountability	2.4	RMM002.FA04	BASIC: ID.GV-1.1, ID.GV-3.1, ID.GV-4.1, ID.AM-5.1 IMPORTANT: ID.AM-6.1, ID.GV-1.2, ID.GV-3.2, ID.GV-4.2, ID.RM-1.1, ID.RM-2.1, ID.RM-3.1, ID.SC-2.1, ID.SC-3.1, ID.SC-4.1, PR.IP-7.1, ESSENTIAL: ID.GV-1.2, ID.GV-4.2, ID.SC-1.1, ID.SC-2.2, ID.SC-3.2, ID.SC-3.3, ID.SC-4.2, PR.IP-7.2, PR.IP-7.3,	IMPORTANT: GV.OC-01.1, GV.OC-03.2, GV.RM-01.1, GV.RM-03.2, GV.RR-03-01, GV.SC-07.1, ID.RA-05.2, ID.IM-03.3, ID.IM-04.1, RC.CO-03.1 ESSENTIAL: GV.OC-02.1, GV.RM-07.1, GV.RR-01.1, GV.RR-02.2, GV.OV-02.1, GV.OV-03.1, GV.SC-03.1, ID.RA-05.3, ID.IM-03.9, ID.IM-04.2, DE.AE-04.1,	5.1, 5.2, 5.3, 6.1, 6.2, 6.3, 8.1, 8.2, 8.3, 9.1, 9.3, 10.1, 10.2, A.5.4	GV.OC-01, GV.OC-02, GV.OC-03, GV.RM-01, GV.RM-03, GV.RM-07, GV.RR-01, GV.RR-02, GV.RR-03, GV.SC-03, GV.SC-07, GV.OV-02, GV.OV-03, ID.RA-05, ID.IM-03, ID.IM-04, DE.AE-04, RC.CO-03

DRAFT

Governance – Management board commitment and accountability	2.5	RMM002.FA05	BASIC: ID.GV-1.1, ID.GV-4.1, IMPORTANT: ID.BE-3.1, ID.GV-1.2, ID.GV-4.2,	BASIC: GV.PO-01.1, IMPORTANT: GV.OC-04.2, GV.RM-01.1, GV.RM-02.1, GV.RM-03.2, GV.PO-01.2,	5.2, A.5.4	GV.PO-01, GV.OC-04, GV.RM-01, GV.RM-02, GV.RM-03,
Network and Information Security Policy	3.1	RMM003.FA01	BASIC: ID.GV-1.1 IMPORTANT: ID.GV-1.2	Basic: GV.PO-01.1 Important: GV.PO-01.2	5.1, 5.2, A.5.1, A.5.36	GV.PO-01
Network and Information Security Policy	3.2	RMM003.FA02	BASIC: ID.GV-1.1 IMPORTANT: ID.GV-1.2	Basic: GV.PO-01.1 Important: GV.PO-01.2	5.1, 5.2, A.5.1, A.5.36	GV.PO-01
Network and Information Security Policy	3.3	RMM003.FA03	BASIC: ID.GV-1.1 IMPORTANT: ID.GV-1.2	Basic: GV.PO-01.1 Important: GV.PO-01.2	5.1, 5.2, A.5.1	GV.PO-01
Network and Information Security Policy	3.4	RMM003.FA04	BASIC: ID.GV-1.1 IMPORTANT: ID.GV-1.2	Basic: GV.PO-01.1 Important: GV.PO-01.2	5.1, 5.2, A.5.1	GV.PO-01
Risk Management Policy	4.1	RMM004.FA01	BASIC: ID.GV-4.1, IMPORTANT: ID.GV-4.2, ID.RA-6.1	Basic: GV.RM-03.1 Important: GV.RM-01.1, GV.RM-03.2, ID.RA-06.1	5.1, 5.2, 8.1, 8.2, 8.3, A.5.1	GV.RM-01, GV.RM-03, ID.RA-06
Risk Management Policy	4.2	RMM004.FA02	IMPORTANT: ID.GV-4.2, ID.RA-6.1, RS.MI-3.1	BASIC: GV.RM-03.1 ID.RA-05.1, Important: GV.RM-03.2, GV.RM-04.1, ID.RA-05.2, ID.RA-06.1 ESSENTIAL: ID.RA-05.3	5.1, 5.2, 8.1, 8.2, 8.3, 9.1, 9.3, A.5.1, A.5.36	GV.RM-03, GV.RM-04, ID.RA-05, ID.RA-06,

DRAFT

Risk Management Policy	4.3	RMM004.FA03	BASIC: ID.RA-1.1, ID.RA-5.1 IMPORTANT: ID.GV-4.2, ID.RA-1.2,ID.RA-2.1 ID.RA-5.2, ID.RA-6.1 ESSENTIAL: ID.RA-5.3,	Basic: ID.AM-05.1, ID.RA-01.1, ID.RA-05.1 Important: GV.OC-04.1, GV.OC-04.2, GV.RM-03.2, ID.RA-05.2, ID.RA-06.1 ESSENTIAL: GV.OC-04.3, GV.OC-04.4,	5.1, 5.2, 5.3, 6.1, 6.2, 6.3, 7.4, 7.5, 8.1, 8.2, 8.3, 9.1, 9.3, 10.1, 10.2, A.5.9, A.5.10, A.5.36,	GV.OC-04, GV.RM-03, ID.AM-05, ID.RA-01, ID.RA-05, ID.RA-06,
Risk Management Policy	4.4	RMM004.FA04	IMPORTANT: ID.GV-4.2, ID.RA-6.1	BASIC: GV.RM-03.1, Important: GV.OC-01.1, GV.RM-03.2, ID.RA-06.1 ESSENTIAL: GV.OC-02.1	5.1, 5.3, 6.1, 6.2, 6.3, A.5.4	GV.RM-03, GV.OC-01, GV.OC-02, ID.RA-06,
Continuous improvement/assess the effectiveness of Cybersecurity risk management measures	5.1	RMM005.FA01	BASIC: ID.RA-1.1, ID.RA-5.1 IMPORTANT: ID.GV-4.2, ID.RA-1.2,ID.RA-2.1 ID.RA-5.2, ID.RA-6.1 ESSENTIAL: ID.RA-5.3,	Basic: ID.RA-01.1, ID.RA-05.1 Important: GV.RM-03.2, GV.RM-04.1, ID.RA-05.2, ID.RA-06.1 ESSENTIAL: ID.RA-05.3	6.1, 8.1, 8.2, 9.1, 9.2, 10.1	GV.RM-03, GV.RM-04, ID.RA-01, ID.RA-05, ID.RA-06,
Continuous improvement/assess the effectiveness of Cybersecurity risk management measures	5.2	RMM005.FA02	IMPORTANT: ID.GV-4.2, ID.RA-6.1, RS.MI-3.1	BASIC: GV.RM-03.1, ID.RA-05.1 Important: GV.RM-03.2, ID.RA-05.2, ID.RA-06.1, RS.MI-01.1	6.1, 8.3,	GV.RM-03, ID.RA-05, ID.RA-06, RS.MI-01
Continuous improvement/assess the effectiveness of Cybersecurity risk management measures	5.3	RMM005.FA03	BASIC: RS.IM-1.1 IMPORTANT: ID.GV-4.2, PR.IP-7.1, PR.IP-8.1, PR.IP-8.2, PR.IP-9.1, DE.DP-3.1, RS.IM-1.2, RC.IM-1.1 ESSENTIAL: PR.IP-7.2, PR.IP-7.3, PR.IP-9.2	Basic: ID.RA-05.1, ID.IM-03.1 Important: ID.RA-05.2, ID.IM-03.2, ID.IM-03.3, ID.IM-03.4, ID.IM-03.5, ID.IM-03.6, ID.IM-03.10 ESSENTIAL: ID.IM-03.7, ID.IM-03.8, ID.IM-03.9	9.1, 9.2, 9.3, A.5.36,	ID.RA-05, ID.IM-03,

DRAFT

Continuous improvement/assess the effectiveness of Cybersecurity risk management measures	5.4	RMM005.FA04	BASIC: RS.IM-1.1 IMPORTANT: ID.GV-4.2, PR.IP-7.1, PR.IP-8.1, PR.IP-8.2, PR.IP-9.1, DE.DP-3.1, RS.IM-1.2, RC.IM-1.1 ESSENTIAL: PR.IP-7.2, PR.IP-7.3, PR.IP-9.2	Basic: ID.IM-03.1 Important: GV.OC-01.1, ID.IM-03.2, ID.IM-03.3, ID.IM-03.4, ID.IM-03.5, ID.IM-03.6, ID.IM-03.10 ESSENTIAL: GV.OC-01.2, GV.RM-07.1, ID.IM-03.7, ID.IM-03.8, ID.IM-03.9	9.1, 9.2, 9.3, 10.1, 10.2, A.5.36,	GV.OC-01, GV.RM-07, ID.IM-03,
Basic Cyber hygiene practices and security training	6.1	RMM006.FA01	BASIC: ID.GV-1.1 IMPORTANT: ID.GV-1.2	Basic: GV.PO-01.1 Important: GV.PO-01.2	5.1, 5.2, A.5.1, A.5.36	GV.PO-01
Basic Cyber hygiene practices and security training	6.2	RMM006.FA02	BASIC: ID.AM-1.1, ID.AM-3.1, PR.AC-1.1, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.AC-4.4, PR.AC-5.1, PR.AC-5.2 IMPORTANT: ID.AM-1.2, ID.AM-1.3, ID.AM-2.4, ID.AM-6.1, ID.GV-4.2, PR.AC-5.3, PR.AC-5.4, PR.DS-3.1, PR.DS-3.2, PR.DS-3.3 ESSENTIAL: PR.AC-5.5, PR.AC-5.6, PR.PT-3.3, PR.PT-4.3	BASIC: GV.RR-04.1, GV.RM-03.1, ID.AM-08.1, ID.AM-08.2, ID.RA-05.1, PR.AA-01.1, PR.AA-03.1, PR.AA-03.2, PR.AA-05.1, PR.AA-05.2, PR.AA-05.3, PR.AA-05.4, PR.IR-01.1, PR.IR-01.2, Important: GV.RM-03.2, GV.RM-04.1, ID.AM-08.3, ID.AM-08.4, ID.AM-08.6, ID.AM-08.8, ID.AM-08.11, ID.AM-08.12, ID.RA-05.2, PR.AA-01.2, PR.AA-02.1, PR.AA-03.3, PR.AA-03.6, PR.AA-05.5, PR.AA-05.6, PR.AA-05.7, PR.IR-01.3, PR.IR-01.4,	6.1, 6.2, 6.3, 8.1, A.5.9, A.5.11, A.5.15, A.5.16, A.5.17, A.5.18, A.5.36, A.5.37, A.6.5, A.7.13, A.7.14, A.8.1, A.8.2, A.8.5, A.8.8, A.8.9, A.8.10, A.8.13, A.8.15, A.8.16, A.8.18, A.8.20, A.8.21, A.8.22, A.8.32	GV.RR-04, GV.RM-03, GV.RM-04, ID.AM-08, ID.RA-05.1, PR.AA-01, PR.AA-03, PR.AA-05, PR.IR-01, PR.AA-02,

DRAFT

				ESSENTIAL: ID.AM-08.5,ID.AM-08.7, ID.AM-08.9, ID.AM-08.10, ID.AM-08.13, PR.AA-01.3, PR.AA-01.4, PR.AA-01.5, PR.AA-02.2, PR.AA-03.4, PR.AA-03.5, PR.AA-05.8, PR.IR-01.5, PR.IR-01.6, PR.IR-01.7, PR.IR-01.8, PR.IR-01.9		
Basic Cyber hygiene practices and security training	6.3	RMM006.FA03	BASIC: PR.AC-1.1, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.AC-4.4, PR.IP-4.1, PR.MA-1.1, DE.CM-4.1 IMPORTANT: ID.GV-4.2, PR.AC-4.2, PR.AC-4.7, PR.AT-2.1, PR.AT-5.1, PR.DS-3.3, PR.DS-5.1, PR.MA-1.2, PR.MA-1.3, PR.MA-1.4, DE.CM-5.1 ESSENTIAL: PR.AC-3.3, PR.DS-1.1, PR.IP-4.2, PR.IP-4.3, PR.IP-4.4, PR.IP-4.5, PR.MA-1.6	BASIC: GV.RM-03.1, GV.RR-04.1, ID.RA-05.1, PR.AA-01.1, PR.AA-03.1, PR.AA-03.2, PR.AA-05.1, PR.AA-05.2, PR.AA-05.3, PR.AA-05.4, PR.DS-11.1, DE.CM-01.2 Important: GV.RM-03.2, ID.RA-05.1, PR.AA-01.2, PR.AA-02.1, PR.AA-03.3, PR.AA-03.6, PR.AA-05.5, PR.AA-05.6, PR.AA-05.7, DE.CM-01.3, PR.DS-11.2, PR.DS-11.3, PR.PS-02.1, PR.PS-03.1, DE.CM-01.3, ESSENTIAL: PR.AA-01.3, PR.AA-01.4, PR.AA-01.5, PR.AA-02.2, PR.AA-03.4,	6.1, 6.2, 6.3, 8.1, A.5.9, A.5.11, A.5.15, A.5.16, A.5.17, A.5.18, A.5.36, A.5.37, A.6.5, A.7.13, A.7.14, A.8.1, A.8.2, A.8.5, A.8.8, A.8.9, A.8.10, A.8.13, A.8.15, A.8.16, A.8.18, A.8.20, A.8.21, A.8.22, A.8.32	GV.RM-03, GV.RR-04, ID.RA-05, PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05, PR.DS-11, PR.PS-02, PR.PS-03, DE.CM-01,

DRAFT

				PR.AA-03.5, PR.AA-05.8, DE.CM-01.4, PR.DS-11.4, PR.DS-11.5, DE.CM-01.4,		
Basic Cyber hygiene practices and security training	6.4	RMM006.FA04	BASIC: PR.AT-1.1, IMPORTANT: PR.AT-1.2, PR.AT-2.1, PR.AT-3.1, PR.AT-3.2, PR.AT-3.3, PR.AT-4.1, PR.AT-5.1 ESSENTIAL: PR.AT-1.3, PR.AT-3.4	BASIC: PR.AT-01.1, IMPORTANT: PR.AT-01.2, PR.AT-01.4, PR.AT-02.1, PR.AT-02.2, PR.AT-02.3 ESSENTIAL: PR.AT-01.3	5.2, 7.3, 8.2, 8.3, A.5.1, A.6.3	PR.AT-01, PR.AT-02,
Asset Management	7.1	RMM007.FA01	BASIC: ID.AM-1.1, ID.AM-2.1, ID.AM-3.1, ID.AM-4.1, IMPORTANT: ID.AM-1.2, ID.AM-1.3, ID.AM-2.2, ID.AM-2.3, ID.AM-2.4, ID.AM-3.2, ESSENTIAL: ID.SC-1.1	BASIC: ID.AM-01.1, ID.AM-02.1, ID.RA-05.1 IMPORTANT: ID.AM-01.2, ID.AM-01.3, ID.AM-02.2, ID.AM-02.3, ID.AM-02.4, ID.AM-03.2, ID.AM-04-1, ID.AM-07.1, ID.RA-05.2 ESSENTIAL: ID.AM-01.4, ID.AM-02.5, ID.AM-03.3, ID.AM-04.2, ID.AM-07.2,	A.5.9	ID.AM-01, ID.AM-02, ID.RA-05, ID.AM-03, ID.AM-04, ID.AM-07,
Asset Management	7.2	RMM007.FA02	BASIC: ID.AM-5.1	BASIC: ID.RA-05.1, ID.AM-05.1 IMPORTANT: ID.RA-05.2	A.5.9, A.5.10, A.5.12, A.5.13, A.7.10	ID.RA-05,

DRAFT

Asset Management	7.3	RMM007.FA03	BASIC: PR.DS-3.1, PR.MA-1.1, IMPORTANT: PR.DS-3.2, PR.DS-3.3, PR.IP-1.1, PR.IP-2.1, PR.IP-3.1, DE.CM-2.1 ESSENTIAL: PR.DS-3.4, PR.IP-2.2, PR.IP-3.2	BASIC: ID.AM-08.1, ID.AM-08.2, ID.RA-05.1 IMPORTANT: ID.AM-08.3, ID.AM-08.4, ID.AM-08.6, ID.AM-08.8, ID.AM-08.11, ID.AM-08.12, ID.RA-05.2 ESSENTIAL: ID.AM-08.5,ID.AM-08.7, ID.AM-08.9, ID.AM-08.10, ID.AM-08.13,	6.3, A.5.9, A.5.10, A.5.11, A.5.13, A.6.5, A.7.10, A.7.13, A.7.14, A.8.9, A.8.10,	ID.AM-08, ID.RA-05,
Human Resources Security	8.1	RMM008.FA01	BASIC: PR.AT-1.1 IMPORTANT: PR.AT-1.2, PR.AT-2.1, PR.AT-4.1, PR.AT-5.1 ESSENTIAL: PR.AT-1.3,	BASIC: PR.AT-01.1, IMPORTANT: PR.AT-01.2, PR.AT-01.4, PR.AT-02.1, PR.AT-02.2, PR.AT-02.3 ESSENTIAL: PR.AT-01.3	5.1, 5.2, 5.3, 7.3, A.5.1, A.6.2, A.6.3,	PR.AT-01, PR.AT-02,
Human Resources Security	8.2	RMM008.FA02	BASIC: PR.AC-1.1, PR.AC-2.1, PR.AC-3.1, PR.AC-3.2, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.AC-4.4 IMPORTANT: PR.AC-1.2, PR.AC-2.2, PR.AC-3.3, PR.AC-4.5, PR.AC-4.6, PR.AC-4.7, PR.AC-6.1, PR.AC-7.1 ESSENTIAL: PR.AC-1.3, PR.AC-1.4, PR.AC-1.5,PR.AC-2.3, PR.AC-2.4, PR.AC-3.4, PR.AC-3.5, PR.AC-4.8, PR.AC-6.2	BASIC: PR.AA-01.1, PR.AA-03.1, PR.AA-03.2, PR.AA-05.1, PR.AA-05.2, PR.AA-05.3, PR.AA-05.4, IMPORTANT: PR.AA-01.2, PR.AA-02.1, PR.AA-03.3, PR.AA-03.6, PR.AA-05.5, PR.AA-05.6, PR.AA-05.7, ESSENTIAL: PR.AA-01.3, PR.AA-01.4, PR.AA-01.5, PR.AA-02.2, PR.AA-03.4,	A.5.3, A.5.15, A.5.16, A.5.18, A.8.3,	PR.AA-01,PR.AA-02, PR.AA-03, PR.AA-05,

DRAFT

				PR.AA-03.5, PR.AA-05.8,		
Human Resources Security	6.3	RMM008.FA03	BASIC: PR.AT-1.1, RS.RP-1.1, RC.RP-1.1 IMPORTANT: PR.AT-2.1, PR.AT-3.1, PR.AT-3.2, PR.AT-4.1, PR.AT-5.1	IMPORTANT: GV.RR-02.1, GV.RR-03.1, GV.RR-04.2 ESSENTIAL: GV.RR-02.2,	5.3, A.5.2, A.5.4,	GV.RR-02, GV.RR-03, GV.RR-04,
Human Resources Security	8.4	RMM008.FA04	BASIC: PR.IP-11.1, IMPORTANT: PR.IP-11.2	IMPORTANT: PR.AA-02.1, ESSENTIAL: PR.AA-02.2,	A.6.1	PR.AA-02,
Human Resources Security	8.5	RMM008.FA05	BASIC: PR.AC-3.1, PR.AC-3.2, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.AC-4.4, IMPORTANT: PR.AC-4.7,	BASIC: PR.AA-01.1, PR.AA-03.1, PR.AA-03.2, PR.AA-05.1, PR.AA-05.2, PR.AA-05.3, PR.AA-05.4, IMPORTANT: PR.AA-01.2, PR.AA-02.1, PR.AA-03.3, PR.AA-03.6, PR.AA-05.5, PR.AA-05.6, PR.AA-05.7, ESSENTIAL: PR.AA-01.3, PR.AA-01.4, PR.AA-01.5, PR.AA-02.2, PR.AA-03.4, PR.AA-03.5, PR.AA-05.8,	A.5.15, A.5.16, A.5.18, A.8.2, A.8.3, A.8.16	PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05,

DRAFT

Human Resources Security	8.6	RMM008.FA06	BASIC: PR.AT-1.1 IMPORTANT: PR.AT-1.2, PR.AT-2.1, PR.AT-4.1, PR.AT-5.1 ESSENTIAL: PR.AT-1.3	BASIC: PR.AT-01.1, IMPORTANT: PR.AT-01.2, PR.AT-01.4, PR.AT-02.1, PR.AT-02.2, PR.AT-02.3 ESSENTIAL: PR.AT-01.3	A.5.1, 7.3, 8.2, 8.3, A.6.3	PR.AT-01,PR.AT-02,
Human Resources Security	8.7	RMM008.FA07	BASIC: PR.AT-1.1, RS.RP-1.1, RC.RP-1.1,PR.AC-1.1, PR.AC-2.1, PR.AC-3.1, PR.AC-3.2, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.AC-4.4 IMPORTANT: PR.AC-1.2, PR.AC-2.2, PR.AC-3.3, PR.AC-4.5, PR.AC-4.6, PR.AC-4.7, PR.AC-6.1, PR.AC-7.1 ESSENTIAL: PR.AC-1.3, PR.AC-1.4, PR.AC-1.5,PR.AC-2.3, PR.AC-2.4, PR.AC-3.4, PR.AC-3.5, PR.AC-4.8, PR.AC-6.2	BASIC: PR.AA-01.1, PR.AA-03.1, PR.AA-03.2, PR.AA-05.1, PR.AA-05.2, PR.AA-05.3, PR.AA-05.4, IMPORTANT: PR.AA-01.2, PR.AA-02.1, PR.AA-03.3, PR.AA-03.6, PR.AA-05.5, PR.AA-05.6, PR.AA-05.7, ESSENTIAL: PR.AA-01.3, PR.AA-01.4, PR.AA-01.5, PR.AA-02.2, PR.AA-03.4, PR.AA-03.5, PR.AA-05.8,	5.3, A.5.2, A.5.3, A.5.4, A.5.15, A.5.16, A.5.18, A.8.3,	PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05,
Access Control	9.1	RMM009.FA01	BASIC: ID.GV-1.1, PR.AC-1.1, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.AC-4.4, PR.IP-11.1, IMPORTANT: ID.GV-1.2, ID.GV-4.2, PR.AC-1.2, PR.AC-6.1, PR.AC-4.7, PR.AC-7.1, PR.AT-3.2, PR.DS-5.1, PR.IP-11.2, DE.CM-7.1,	Basic: GV.PO-01.1, ID.RA-05.1, PR.AA-01.1, PR.AA-03.1, PR.AA-03.2, PR.AA-05.1, PR.AA-05.2, PR.AA-05.3, PR.AA-05.4, Important: GV.PO-01.2, GV.RM-03.2, ID.RA-05.2, PR.AA-01.2, PR.AA-02.1, PR.AA-03.3, PR.AA-03.6, PR.AA-05.5, PR.AA-05.6,	A.5.1, A.5.15, A.5.16, A.5.17, A.5.18, A.7.2, A.8.2, A.8.3, A.8.5,	GV.PO-01, GV.RM-03, ID.RA-05, PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05,

DRAFT

				PR.AA-05.7, ESSENTIAL: PR.AA-01.3, PR.AA-01.4, PR.AA-01.5, PR.AA-02.2, PR.AA-03.4, PR.AA-03.5, PR.AA-05.8,		
Access Control	9.2	RMM009.FA02	BASIC: ID.GV-1.1, PR.AC-1.1, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.AC-4.4, PR.IP-11.1, IMPORTANT: ID.GV-1.2, PR.AC-1.2, PR.AC-6.1, PR.AC-4.7, PR.AC-7.1, PR.AT-3.2, PR.DS-5.1, PR.IP-11.2, DE.CM-7.1,	Basic: GV.PO-01.1, PR.AA-01.1, PR.AA-03.1, PR.AA-03.2, PR.AA-05.1, PR.AA-05.2, PR.AA-05.3, PR.AA-05.4, Important: GV.PO-01.2, GV.RM-03.2, PR.AA-01.2, PR.AA-02.1, PR.AA-03.3, PR.AA-03.6, PR.AA-05.5, PR.AA-05.6, PR.AA-05.7, ESSENTIAL: PR.AA-01.3, PR.AA-01.4, PR.AA-01.5, PR.AA-02.2, PR.AA-03.4, PR.AA-03.5, PR.AA-05.8,	A.5.15, A.5.16, A.5.17, A.5.18, A.6.5, A.7.2, A.8.2, A.8.3, A.8.5,	GV.PO-01, GV.RM-03, PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05,

DRAFT

Access Control	9.3	RMM009.FA03	BASIC: ID.GV-1.1, PR.AC-1.1, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.AC-4.4, PR.IP-11.1, IMPORTANT: ID.GV-1.2, PR.AC-1.2, PR.AC-6.1, PR.AC-7.1, PR.AC-4.7, PR.AT-3.2, PR.DS-5.1, PR.IP-11.2, DE.CM-7.1,	BASIC: PR.AA-01.1, PR.AA-03.1, PR.AA-03.2, PR.AA-05.1, PR.AA-05.2, PR.AA-05.3, PR.AA-05.4, IMPORTANT: PR.AA-01.2, PR.AA-02.1, PR.AA-03.3, PR.AA-03.6, PR.AA-05.5, PR.AA-05.6, PR.AA-05.7, ESSENTIAL: PR.AA-01.3, PR.AA-01.4, PR.AA-01.5, PR.AA-02.2, PR.AA-03.4, PR.AA-03.5, PR.AA-05.8,	8.2, A.5.15, A.5.16, A.5.17, A.5.18, A.7.2, A.7.4, A.8.2, A.8.3, A.8.5, A.8.16,	PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05,
Access Control	9.4	RMM009.FA04	BASIC: PR.AC-1.1, IMPORTANT: PR.AC-4.2, PR.AC-4.7, PR.AC-7.1 ESSENTIAL: PR.AC-4.8	BASIC: PR.AA-01.1, PR.AA-03.1, PR.AA-03.2, PR.AA-05.1, PR.AA-05.2, PR.AA-05.3, PR.AA-05.4, IMPORTANT: PR.AA-01.2, PR.AA-02.1, PR.AA-03.3, PR.AA-03.6, PR.AA-05.5, PR.AA-05.6, PR.AA-05.7, ESSENTIAL: PR.AA-01.3, PR.AA-01.4, PR.AA-01.5, PR.AA-02.2, PR.AA-03.4, PR.AA-03.5, PR.AA-05.8,	8.2, A.5.15, A.5.16, A.5.17, A.5.18, A.7.2, A.7.4, A.8.2, A.8.3, A.8.5, A.8.16,	PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05,

DRAFT

Access Control	9.5	RMM009.FA05	BASIC: PR.AC-1.1, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.AC-4.4, IMPORTANT: PR.AC-4.2, PR.AC-4.5, PR.AC-4.6, PR.AC-4.7, PR.AC-7.1 ESSENTIAL: PR.AC-4.8	BASIC: ID.RA-05.1, PR.AA-01.1, PR.AA-03.1, PR.AA-03.2, PR.AA-05.1, PR.AA-05.2, PR.AA-05.3, PR.AA-05.4, IMPORTANT: ID.RA-05.1, PR.AA-01.2, PR.AA-02.1, PR.AA-03.3, PR.AA-03.6, PR.AA-05.5, PR.AA-05.6, PR.AA-05.7, ESSENTIAL: PR.AA-01.3, PR.AA-01.4, PR.AA-01.5, PR.AA-02.2, PR.AA-03.4, PR.AA-03.5, PR.AA-05.8,	8.2, A.5.15, A.5.16, A.5.17, A.5.18, A.7.2, A.7.4, A.8.2, A.8.3, A.8.5, A.8.16,	ID.RA-05, PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-05,
Access Control	9.6	RMM009.FA06	BASIC: PR.AC-1.1, PR.AC-4.1, PR.AC-4.2, PR.AC-4.3, PR.AC-4.4, IMPORTANT: PR.AC-4.2, PR.AC-4.5, PR.AC-4.6, PR.AC-4.7, PR.AC-7.1 ESSENTIAL: PR.AC-4.8	BASIC: ID.RA-05.1, IMPORTANT: ID.RA-05.2, PR.AA-05.5, PR.AA-05.6, PR.AA-05.7, ESSENTIAL: PR.AA-05.8, PR.AA-05.9	8.2, A.5.15, A.5.16, A.5.17, A.5.18, A.7.2, A.7.4, A.8.2, A.8.3, A.8.5, A.8.16,	ID.RA-05, PR.AA-05,
Environmental and physical security	10.1	RMM010.FA01	BASIC: ID.GV-1.1, PR.AC-2.1, IMPORTANT: PR.IP-5.1, ID.GV-4.2,v ESSENTIAL: PR.IP-5.2,	Basic: GV.PO-01.1, ID.RA-05.1 PR.AA-06.1 Important: GV.RM-03.2, ID.RA-05.2 PR.AA-06.2, ESSENTIAL: PR.AA-06.3, PR.AA-06.4,	8.2, A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6, A.7.7, A.7.8, A.7.9, A.7.10, A.7.11, A.7.12, A.7.13, A.7.14,	GV.PO-01, GV.RM-03, ID.RA-05, PR.AA-06,
Environmental and physical security	10.2	RMM010.FA02	BASIC: PR.AC-2.1, IMPORTANT: PR.IP-5.1, ESSENTIAL: PR.IP-5.2,	BASIC: PR.AA-06.1 IMPORTANT: PR.AA-06.2, ESSENTIAL:	8.1, 8.2, 8.3, 9.1, 9.2, A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6, A.7.7, A.7.8,	PR.AA-06,

DRAFT

				PR.AA-06.3, PR.AA-06.4,	A.7.9, A.7.10, A.7.11, A.7.12, A.7.13, A.7.14,	
Environmental and physical security	10.3	RMM010.FA03	BASIC: RS.IM-1.1 IMPORTANT: ID.GV-4.2, PR.IP-7.1, PR.IP-9.1, DE.DP-3.1, DE.DP-5.1, RS.IM-1.2, RS.IM-2.1, RC.IM-1.1 ESSENTIAL: PR.IP-7.2, PR.IP-7.3, PR.IP-9.1, DE.DP-5.2	BASIC: ID.IM-03.1, Important: GV.RM-03.2, ID.IM-03.2, ID.IM-03.3, ESSENTIAL: ID.IM-03.7, ID.IM-03.8, ID.IM-03.9	8.1, 8.2, 8.3, 9.1, 9.2, A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6, A.7.7, A.7.8, A.7.9, A.7.10, A.7.11, A.7.12, A.7.13, A.7.14,	GV.RM-03, ID.IM-03,
Environmental and physical security	10.4	RMM010.FA04	BASIC: RS.IM-1.1 IMPORTANT: PR.IP-7.1, PR.IP-9.1, DE.DP-3.1, DE.DP-5.1, RS.IM-1.2, RS.IM-2.1, RC.IM-1.1 ESSENTIAL: PR.IP-7.2, PR.IP-7.3, PR.IP-9.1, DE.DP-5.2	BASIC: ID.IM-03.1, ID.RA-05.1 Important: GV.RM-03.2, ID.RA-05.2, ID.IM-03.2, ID.IM-03.3, ESSENTIAL: ID.IM-03.7, ID.IM-03.8, ID.IM-03.9	8.1, 8.2, 8.3, 9.1, 9.2, A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6, A.7.7, A.7.8, A.7.9, A.7.10, A.7.11, A.7.12, A.7.13, A.7.14,	GV.RM-03, ID.RA-05, ID.IM-03,
Cyrptography, encryption and authentication	11.1	RMM011.FA01	BASIC: PR.DS-3.1, PR.DS-7.1 IMPORTANT: PR.DS-3.2, PR.DS-3.3, PR.DS-5.1, PR.DS-6.1, ESSENTIAL: PR.DS-1.1, PR.DS-2.1, PR.DS-6.2, PR.DS-6.3, PR.DS-8.1, PR.DS-8.2,	IMPORTANT: PR.DS-01.1, PR.DS-01.4, PR.DS-01.5, PR.DS-02.1 ESSENTIAL: PR.DS-01.2, PR.DS-01.3, PR.DS-01.6, PR.DS-01.7, PR.DS-01.8	8.1, 8.2, 8.3, A.5.14, A.5.33, A.5.34, A.7.10, A.8.11, A.8.12, A.8.13, A.8.14, A.8.24,	PR.DS-01, PR.DS-02,
Cyrptography, encryption and authentication	11.2	RMM011.FA02	BASIC: ID.GV-1.1 IMPORTANT: ID.GV-4.2, PR.DS-3.2, PR.DS-3.3 ESSENTIAL: PR.DS-1.1, PR.DS-2.1,	Basic: GV.PO-01.1, ID.RA-05.1 Important: GV.RM-03.2, ID.RA-05.2 ESSENTIAL: PR.DS-01.7, PR.DS-01.8	8.2, 8.3, A.5.1, A.8.24,	GV.RM-03, GV.PO-01, ID.RA-05, PR.DS-01,
Cryptography, encryption and authentication	11.3	RMM011.FA03	IMPORTANT: PR.IP-7.1	BASIC: ID.RA-05.1, IMPORTANT: ID.RA-05.2, ID.IM-03.3	8.2, 8.3, 9.1, 9.2, A.5.1, A.8.24,	ID.RA-05, ID.IM-03,

DRAFT

Cryptography, encryption and authentication	11.4	RMM011.FA04	BASIC: PR.AC-3.2, IMPORTANT: PR.AC-7.1 ESSENTIAL: PR.AC-1.4,	BASIC: PR.AA-03.2, ID.RA-05.1 IMPORTANT: ID.RA-05.2, PR.AA-03.6, ID.AM-08.12 ESSENTIAL: PR.AA-03.5	8.2, 8.3, A.5.1, A.8.2, A.8.5, A.8.24,	ID.RA-05, ID.AM-08, PR.AA-03,
Cryptography, encryption and authentication	11.5	RMM011.FA05	ESSENTIAL: PR.PT-4.2	BASIC: ID.RA-05.1, PR.IR-01.1, PR.IR-01.2 IMPORTANT: ID.RA-05.2, PR.IR-01.3, PR.IR-01.4 ESSENTIAL: PR.IR-01.5, PR.IR-01.8, PR.IR-01.9	8.2, 8.3, A.5.1, A.8.11, A.8.12, A.8.21, 8.22, A.8.24, A.8.26, A.8.27,	ID.RA-05, PR.IR-01,
Supply chain policy	12.1	RMM012.FA01	IMPORTANT: ID.GV-1.2, ID.SC-2.1, ID.SC-3.1, ESSENTIAL: ID.SC-1.1, ID.BE-1.2, ID.SC-3.2, ID.SC-3.3, ID.SC-4.2	BASIC: GV.PO-01.1, ID.RA-05.1 Important: GV.PO-01.2, GV.SC-05.1, GV.SC-07.1, ID.RA-05.2 ESSENTIAL: GV.SC-01.1, GV.SC-01.2, GV.SC-03.1, GV.SC-05.2, GV.SC-05.3, GV.SC-06.1, GV.SC-07.2, GV.SC-07.3, GV.SC-07.4,	A.5.1, A.5.19, A.5.20, A.5.21, A.5.22, A.5.23,	GV.PO-01, GV.SC-01, GV.SC-03, GV.SC-05, GV.SC-06, GV.SC-07, ID.RA-05
Supply chain policy	12.2	RMM012.FA02	BASIC: IMPORTANT: ID.BE-1.1, ID.BE-2.1, ID.BE-4.1, ID.SC-2.1, ID.SC-3.1, ID.SC-4.1, DE.CM-6.1, DE.CM-6.2 ESSENTIAL: ID.BE-1.2, ID.SC-1.1, ID.SC-3.2, ID.SC-3.3, ID.SC-4.2	IMPORTANT: GV.OC-05.1, GV.SC-08.1, ID.AM-04.1, ID.RA-05.1 ESSENTIAL: GV.SC-08.2, ID.AM-04.2, GV.SC-07.2, ID.RA-05.2	A.5.1, A.5.19, A.5.20, A.5.21, A.5.22, A.5.23,	GV.OC-05, GV.SC-07, GV.SC-08, ID.AM-04, ID.RA-05,

DRAFT

Supply chain policy	12.3	RMM012.FA03	BASIC: IMPORTANT: ID.SC-2.1, ID.SC-3.1, ID.SC-4.1, DE.CM-6.1, DE.CM-6.2 ESSENTIAL: ID.SC-3.2, ID.SC-3.3, ID.SC-4.2	IMPORTANT: GV.OC-05.1, GV.SC-08.1, ID.AM-04.1 ESSENTIAL: GV.SC-08.2, ID.AM-04.2, GV.SC-07.2	A.5.1, A.5.19, A.5.20, A.5.21, A.5.22, A.5.23,	GV.OC-05, GV.SC-07, GV.SC-08, ID.AM-04,
Supply chain policy	12.4	RMM012.FA04	BASIC: IMPORTANT: ID.BE-1.1, ID.BE-2.1, ID.BE-4.1, ID.RM-1.1, ID.SC-2.1, ID.SC-3.1, ID.SC-4.1, PR.AC-7.1, DE.CM-6.1, DE.CM-6.2 ESSENTIAL: ID.SC-1.1, ID.SC-2.2, ID.SC-3.2, ID.SC-3.3, ID.SC-4.2	IMPORTANT: GV.SC-05.1 ESSENTIAL: GV.SC-05.2, GV.SC-05.3	A.5.1, A.5.19, A.5.20, A.5.21, A.5.22, A.5.23,	GV.SC-05
Supply chain policy	12.5	RMM012.FA05	Reference to previous RMMs. See RMM003&004			
Security in network and information systems acquisition, development and maintenance	13.1	RMM013.FA01	BASIC: ID.AM-1.1, ID.AM-2.1, ID.GV-1.1, PR.MA-1.1, IMPORTANT: PR.IP-1.1, PR.MA-1.2, ID.AM-3.2, PR.IP-1.1, ID.AM-1.2, ID.AM-2.2, ID.AM-4.1, ID.GV-1.2, PR.DS-6.1, PR.MA-1.2, PR.MA-1.3, PR.IP-3.1, ESSENTIAL: ID.SC-3.2, PR.MA-1.7, PR.IP-1.2, PR.IP-2.2, DE.CM-7.2	BASIC: GV.PO-01.1, ID.AM-08.2, PR.PS-04.1, Important: GV.PO-01.2, ID.AM-08.6, ID.AM-08.8, ID.AM-08.11, PR.PS-01.1, PR.PS-02.1, PR.PS-03.1, PR.PS-04.2, PR.PS-06.2, ESSENTIAL: ID.AM-08.7, ID.AM-08.9, ID.AM-08.10, ID.AM-08.13, PR.PS-01.2, PR.PS-01.3, PR.PS-01.4, PR.PS-01.5, PR.PS-04.3, PR.PS-04.4, PR.PS-06.4,	6.1, 6.3, A.5.1, A.8.8, A.8.9, A.8.15, A.8.16, A.8.26, A.8.27, A.8.32,	GV.PO-01, ID.AM-08, PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04, PR.PS-06,

DRAFT

Security in network and information systems acquisition, development and maintenance	13.2	RMM013.FA02	BASIC: ID.GV-4.1 IMPORTANT: ID.RM-1.1, ID.GV-4.2, ID.SC-3.1, ID.SC-4.1, DE.CM-6.2 ESSENTIAL: ID.SC-2.2, ID.SC-3.2, ID.SC-4.2, ID.SC-3.3	Basic: GV.RM-03.1, ID.RA-05.1 Important: GV.RM-03.2, ID.RA-05.2, GV.SC-05.1 ESSENTIAL: GV.SC-05.2, GV.SC-05.3, GV.SC-06.1, GV.SC-10.1	A.5.21, A.5.23, A.8.27	GV.RM-03, GV.SC-05, GV.SC-06, GV.SC-10, ID.RA-05,
Security in network and information systems acquisition, development and maintenance	13.3	RMM013.FA03	BASIC: ID.GV-1.1, IMPORTANT: ID.GV-1.2, PR.IP-2.1 ESSENTIAL: PR.DS-7.1, PR.IP-2.2	Basic: GV.PO-01.1 Important: GV.PO-01.2, PR.PS-06.1, PR.PS-06.2 ESSENTIAL: PR.PS-06.3, PR.PS-06.4	A.8.27, A.8.28, A.8.29, A.8.30, A.8.31, A.8.33,	GV.PO-01, PR.PS-06,
Security in network and information systems acquisition, development and maintenance	13.4	RMM013.FA04	BASIC: ID.RA-1.1 IMPORTANT: ID.RA-1.2, ID.RA-2.1, DE.CM-8.1, DE.CM-8.2, DE.DP-4.1, RS.AN-5.1 ESSENTIAL: DE.AE-3.3, DE.DP-5.2, RS.AN-5.2	BASIC: ID.RA-01.1, ID.RA-05.1 IMPORTANT: GV.RM-03.2, ID.RA-01.2, ID.RA-01.3, ID.RA-01.5, GV.RM-04.1, ID.RA-05.2, ID.RA-06.1, ID.RA-08.1 ESSENTIAL: ID.RA-05.3, ID.RA-01.4, ID.RA-02.2, ID.RA-08.2	8.2, 8.3, A.8.8	GV.RM-03, GV.RM-04, ID.RA-01, ID.RA-05, ID.RA-06, ID.RA-08,
Security in network and information systems acquisition, development and maintenance	13.5	RMM013.FA05	BASIC: ID.GV-4.1 IMPORTANT: ID.RM-1.1, ID.GV-4.2, ID.SC-3.1, ID.SC-4.1, DE.CM-6.2 ESSENTIAL: ID.SC-2.2, ID.SC-3.2, ID.SC-4.2, ID.SC-3.3	Basic: GV.RM-03.1 Important: GV.RM-03.2, GV.SC-05.1 ESSENTIAL: GV.SC-05.2, GV.SC-05.3, GV.SC-06.1	8.2, A.5.21, A.5.23, A.8.27	GV.RM-03, GV.RM-03, GV.SC-05, GV.SC-06,

DRAFT

Incident Handling	14.1	RMM014.FA01	BASIC: ID.GV-1.1, RS.RP-1.1, IMPORTANT: PR.IP-9.1, RS.CO-1.1, RS.CO-2.1, RS.CO-3.1, RS.CO-3.2,RS.CO-4.1, RS.CO-5.1, RC.RP-1.1	Basic: GV.PO-01.1, RS.MA-01.1, RC.RP-01.1 IMPORTANT: ID.IM-04.1, RS.MA-01.2 ESSENTIAL: ID.IM-04.2, RC.RP-02.1,	A.5.1, A.5.24, A.5.25, A.5.26	GV.PO-01, ID.IM-04, RS.MA-01, RC.RP-01, RC.RP-02,
Incident Handling	14.2	RMM014.FA02	BASIC: RS.RP-1.1, RC.RP-1.1 IMPORTANT: ID.AM-6.1, ID.GV-1.2, PR.IP-9.1 RS.CO-1.1, RS.CO-2.1, RS.CO-4.1, RS.CO-5.1, ESSENTIAL: PR.IP-9.2	BASIC: RS.MA-01.1, Important: GV.PO-01.2, RS.MA-01.2	5.3, A.5.2, A.5.24	GV.PO-01, RS.MA-01
Incident Handling	14.3	RMM014.FA03	BASIC: ID.GV-1.1, RS.RP-1.1, RS.CO-3.1, RS.IM-1.1, RC.RP-1.1, IMPORTANT: PR.IP-9.1, RS.CO-3.1, RS.CO-5.1, RS.AN-4.1, ESSENTIAL: PR.IP-9.2,	Basic: GV.PO-01.1, RS.MA-01.1, RC.RP-01.1 IMPORTANT: ID.IM-04.1, RS.MA-01.2 ESSENTIAL: ID.IM-04.2, RC.RP-02.1,	7.4, 7.5, A.5.1, A.5.24,	GV.PO-01, ID.IM-04, RS.MA-01, RC.RP-02,
Incident Handling	14.4	RMM014.FA04	BASIC: RS.RP-1.1, RC.RP-1.1, IMPORTANT: ID.BE-5.1, PR.IP-9.1, RS.CO-1.1, RS.CO-2.1, RS.CO-3.1,, RS.CO-4.1, RS.CO-5.1, RS.MI-1.1, RS.MI-2.1, ESSENTIAL: PR.IP-9.2, RS.MI-3.1,	Basic: GV.PO-01.1, IMPORTANT: RS.MA-02.1, RS.MA-03.1, RS.MA-05.1, RS.MI-01.1 ESSENTIAL: RS.MA-02.2	7.4, 7.5, A.5.1, A.5.24, A.5.25, A.5.26	GV.PO-01, RS.MA-02, RS.MA-03, RS.MA-05, RS.MI-01,
Incident Handling	14.5	RMM014.FA05	BASIC: ID.GV-3.1, RS.RP-1, RC.RP-1.1, IMPORTANT: PR.IP-9.1, RS.CO-2.1, RS.CO-3.1,, RS.CO-4.1, RS.CO-5.1, ESSENTIAL: PR.IP-9.2,	BASIC: GV.OC-03.1, RS.CO-02.1 IMPORTANT: GV.OC-03.2, RS.CO-02.2	7.4, 7.5, A.5.1, A.5.5, A.5.6, A.5.24, A.5.31	GV.OC-03, RS.CO-02,

DRAFT

Incident Handling	14.6	RMM014.FA06	IMPORTANT: RS.CO-2.1 ESSENTIAL: RS.CO-2.2	BASIC: RS.CO-02.1 IMPORTANT: RS.MA-02.1, RS.CO-02.2	7.4, 7.5, A.5.1, A.5.24, A.6.8,	RS.CO-02, RS.MA-02,
Incident Handling	14.7	RMM014.FA07	IMPORTANT: RS.AN-1.1, RS.AN-2.1, RS.AN-4.1, RS.AN-5.1, ESSENTIAL: RS.AN-1.2, RS.AN-2.2, RS.AN-3.1, RS.AN-3.2, RS.AN-5.2	IMPORTANT: RS.MA-02.1, RS.MA-03.1, RS.MA-05.1, ESSENTIAL: RS.MA-02.2, RS.AN-03.1, RS.AN-06.1, RS.AN-07.1, RS.AN-08.1,	7.4, 7.5, A.5.1, A.5.24, A.5.25, A.6.8,	RS.MA-02, RS.MA-03, RS.MA-05, RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08,
Incident Handling	14.8	RMM014.FA08	IMPORTANT: PR.IP-7.1, PR.IP-9.1, RS.IM-1.1, RS.IM-1.2, RS.IM-2.1 ESSENTIAL: PR.IP-7.2, PR.IP-7.3, PR.IP-9.2,	BASIC: ID.IM-03.1 IMPORTANT: ID.IM-02.1, ID.IM-03.2, ID.IM-03.3, ID.IM-03.4, ID.IM-03.5, ID.IM-03.6, ID.IM-03.10, ID.IM-04.1, ESSENTIAL: ID.IM-03.7, ID.IM-03.8, ID.IM-03.9, ID.IM-04.2	9.1, 9.2, 10.1, A.5.1, A.5.24, A.5.27,	ID.IM-02, ID.IM-03, ID.IM-04,
Incident Reporting	15.1	RMM015.FA01	BASIC: ID.GV-3.1, RS.RP-1, RC.RP-1.1, IMPORTANT: PR.IP-9.1, RS.CO-2.1, RS.CO-3.1, RS.CO-4.1, RS.CO-5.1, ESSENTIAL: PR.IP-9.2	BASIC: GV.OC-03.1, RS.MA-01.1 IMPORTANT: GV.OC-03.2, RS.MA-01.2	7.4, 7.5, A.5.1, A.5.5, A.5.6, A.5.24, A.5.31	GV.OC-03, RS.MA-01,
Incident Reporting	15.2	RMM015.FA02	BASIC: ID.GV-3.1, RS.RP-1, RC.RP-1.1, IMPORTANT: PR.IP-9.1, RS.CO-2.1, RS.CO-3.1, RS.CO-4.1, RS.CO-5.1, ESSENTIAL: PR.IP-9.2	BASIC: GV.OC-03.1, RS.MA-01.1 IMPORTANT: GV.OC-03.2, RS.MA-01.2, RC.CO-03.1, RC.CO-04.1, ESSENTIAL: RC.CO-04.2, RC.CO-04.3	7.4, 7.5, A.5.1, A.5.5, A.5.6, A.5.24, A.5.31	GV.OC-03, RS.MA-01, RC.CO-03, RC.CO-04,

DRAFT

Business continuity and crisis management	16.1	RMM016.FA01	BASIC: ID.GV-1.1, IMPORTANT: ID.SC-5.1, PR.IP-9.1 ESSENTIAL: ID.SC-5.2, PR.IP-9.2, RC.RP-1.2	Basic: GV.PO-01.1, RC.RP-01.1 IMPORTANT: ID.IM-04.1, RC.RP-05.1, RC.RP-06.1 ESSENTIAL: ID.IM-04.2,	7.4, 7.5, 9.1, 9.2, 10.1, A.5.1, A.5.24,	GV.PO-01, ID.IM-04, RC.RP-01, RC.RP-05, RC.RP-06
Business continuity and crisis management	16.2	RMM016.FA02	BASIC: RS.CO-3.1 IMPORTANT: PR.IP-8.1, DE.DP-4.1, RS.CO-3.2 ESSENTIAL: PR.IP-4.4, PR.IP-9.2, RC.CO-2.1, RS.CO-2.2	Basic: GV.PO-01.1, RC.RP-01.1 IMPORTANT: ID.IM-04.1, RC.RP-05.1, RC.RP-06.1 ESSENTIAL: ID.IM-04.2,	A.5.1, A.5.24, A.5.37	GV.PO-01, ID.IM-04, RC.RP-01, RC.RP-05, RC.RP-06
Business continuity and crisis management	16.3	RMM016.FA03	IMPORTANT: ID.RA-2.1, ESSENTIAL: ID.RA-2.2,	IMPORTANT: ID.RA-02.1, ESSENTIAL: ID.RA-02.2,	A.5.1, A.5.5, A.5.6, A.5.7, A.5.24, A.5.37	ID.RA-02,
Business continuity and crisis management	16.4	RMM016.FA04	IMPORTANT: PR.IP-7.1, RS.IM-1.1, RS.IM-1.2, RS.IM-2.1, RC.IM-1.1 ESSENTIAL: PR.IP-7.2, PR.IP-7.3, RS.MI-3.1,	BASIC: ID.IM-03.1, Important: ID.IM-03.2, ID.IM-03.3, ID.IM-03.4, ID.IM-03.5, ID.IM-03.6, ID.IM-03.10, RS.MI-01.1 ESSENTIAL: ID.IM-03.7, ID.IM-03.8, ID.IM-03.9	9.1, 9.2, 10.1, A.5.24, A.5.27	ID.IM-03, RS.MI-01,

DRAFT