TLP:GREEN

NIST CSF 2.0 and ISO 27001:2022 (mapping)

1.0, 01.03.2024

NIST CSF 2.0 NIST Cybersecurity Framework 2.0

https://www.nist.gov/cyberframework

ISO 27001 ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

https://www.iso.org/standard/27001

CSF Functions and Categories

1. **Govern (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	• Organizational Context (GV.OC) • Risk Management Strategy (GV.RM) • Roles, Responsibilities, and Authorities (GV.RR) • Policy (GV.PO) • Oversight (GV.OV) • Cybersecurity Supply Chain Risk Management (GV.SC)
2. **Identify (ID):** The organization's current cybersecurity risks are understood	• Asset Management (ID.AM) • Risk Assessment (ID.RA) • Improvement (ID.IM)
3. **Protect (PR):** Safeguards to manage the organization's cybersecurity risks are used	• Identity Management, Authentication, and Access Control (PR.AA) • Awareness and Training (PR.AT) • Data Security (PR.DS) • Platform Security (PR.PS) • Technology Infrastructure Resilience (PR.IR)
4. **Detect (DE):** Possible cybersecurity attacks and compromises are found and analyzed	• Continuous Monitoring (DE.CM) • Adverse Event Analysis (DE.AE)
5. **Respond (RS):** Actions regarding a detected cybersecurity incident are taken	• Incident Management (RS.MA) • Incident Analysis (RS.AN) • Incident Response Reporting and Communication (RS.CO) • Incident Mitigation (RS.MI)
6. **Recover (RC):** Assets and operations affected by a cybersecurity incident are restored	• Incident Recovery Plan Execution (RC.RP) • Incident Recovery Communication (RC.CO)

CSF Core: A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. Its components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome.

CSF Function: The highest level of organization for cybersecurity outcomes. There are six CSF Functions: Govern, Identify, Protect, Detect, Respond, and Recover.

CSF Category: A group of related cybersecurity outcomes that collectively comprise a CSF Function.

CSF Subcategory: A group of more specific outcomes of technical and management cybersecurity activities that comprise a CSF Category.

See also:

CSF 2.0 Informative References and Implementation Examples - https://www.nist.gov/informative-references

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

#	NIST CSF 2.0	ISO 27001:2022
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
1.	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties 4.3 Determining the scope of the information security management system 4.4 Information security management system 5.2 Policy
2.	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	4.2 Understanding the needs and expectations of interested parties A.5.5. Contact with authorities A.5.6. Contact with special interest groups
3.	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties A.5.31. Legal, statutory, regulatory and contractual requirements A.5.32. Intellectual property rights A.5.34. Privacy and protection of PII
4.	GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	4.2 Understanding the needs and expectations of interested parties 7.4 Communication
5.	GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	4.2 Understanding the needs and expectations of interested parties 7.4 Communication 8.1 Operational planning and control A.5.19. Information security in supplier relationships A.5.20. Addressing information security within supplier agreements A.8.30. Outsourced development
Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions		
6.	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	6.1 Actions to address risks and opportunities 6.2 Information security objectives and planning to achieve them
7.	GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	6.1 Actions to address risks and opportunities
8.	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	6.1 Actions to address risks and opportunities 8.2 Information security risk assessment 8.3 Information security risk treatment
9.	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	6.1 Actions to address risks and opportunities 6.3 Planning of changes 8.3 Information security risk treatment

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

10.	GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	6.1 Actions to address risks and opportunities 7.4 Communication A.5.19. Information security in supplier relationships
11.	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	6.1 Actions to address risks and opportunities
12.	GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	6.1 Actions to address risks and opportunities 8.2 Information security risk assessment
Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated		
13.	GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	5.1 Leadership and commitment 5.3 Organizational roles, responsibilities and authorities A.5.4. Management responsibilities
14.	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	5.3 Organizational roles, responsibilities and authorities A.5.2. Information security roles and responsibilities A.5.4. Management responsibilities
15.	GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	7.1 Resources
16.	GV.RR-04: Cybersecurity is included in human resources practices	7.2 Competence 7.3 Awareness A.6.1. Screening A.6.2. Terms and conditions of employment A.6.3. Information security awareness, educationand training A.6.4. Disciplinary process A.6.5. Responsibilities after termination or change of employment A.6.6. Confidentiality or non-disclosure agreements
Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced		
17.	GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	5.2 Policy A.5.1. Policies for information security
18.	GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	5.2 Policy 7.5 Documented information A.5.1. Policies for information security
Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy		
19.	GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	5.1 Leadership and commitment 8.3 Information security risk treatment 9.3 Management review
20.	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	9.3 Management review

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

21.	GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	9.1 Monitoring, measurement, analysis and evaluation 9.3 Management review
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders		
22.	GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	6.1 Actions to address risks and opportunities 8.1 Operational planning and control A.5.8. Information security in project management A.5.19. Information security in supplier relationships A.5.20. Addressing information security within supplier agreements A.5.21. Managing information security in the ICT supply chain A.5.22. Monitoring, review and change management of supplier services A.5.23. Information security for use of cloud services
23.	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	5.3 Organizational roles, responsibilities and authorities 7.4 Communication A.5.2. Information security roles and responsibilities A.5.19. Information security in supplier relationships
24.	GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	6.1 Actions to address risks and opportunities 8.1 Operational planning and control 8.2 Information security risk assessment 10.1 Continual improvement A.5.22. Monitoring, review and change management of supplier services
25.	GV.SC-04: Suppliers are known and prioritized by criticality	A.5.19. Information security in supplier relationships A.5.21. Managing information security in the ICT supply chain A.5.23. Information security for use of cloud services
26.	GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	8.1 Operational planning and control A.5.20. Addressing information security within supplier agreements
27.	GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	A.5.19. Information security in supplier relationships A.5.22. Monitoring, review and change management of supplier services
28.	GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	6.1 Actions to address risks and opportunities 8.1 Operational planning and control 8.2 Information security risk assessment A.5.19. Information security in supplier relationships A.5.22. Monitoring, review and change management of supplier services
29.	GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	A.5.19. Information security in supplier relationships A.5.24. Information security incident management planning and preparation

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

30.	GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	6.1 Actions to address risks and opportunities 8.1 Operational planning and control 8.2 Information security risk assessment A.5.19. Information security in supplier relationships A.8.25. Secure development life cycle A.8.27. Secure system architecture and engineering principles A.8.29. Security testing in development and acceptance A.8.30. Outsourced development
31.	GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	A.5.19. Information security in supplier relationships A.5.20. Addressing information security within supplier agreements A.5.21. Managing information security in the ICT supply chain A.5.22. Monitoring, review and change management of supplier services A.5.23. Information security for use of cloud services
Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy		
32.	ID.AM-01: Inventories of hardware managed by the organization are maintained	A.5.9. Inventory of information and other associated assets
33.	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	A.5.9. Inventory of information and other associated assets
34.	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	A.8.20. Network security A.8.21. Security of network services A.8.22. Segregation of networks
35.	ID.AM-04: Inventories of services provided by suppliers are maintained	A.5.9. Inventory of information and other associated assets A.5.19. Information security in supplier relationships
36.	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	A.5.9. Inventory of information and other associated assets A.5.12. Classification of information
37.	ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	A.5.9. Inventory of information and other associated assets A.5.12. Classification of information A.5.13. Labelling of information
38.	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	A.5.10. Acceptable use of information and other associated assets A.5.11. Return of assets A.5.37. Documented operating procedures A.6.5. Responsibilities after termination or change of employment A.7.8. Equipment siting and protection A.7.9. Security of assets off-premises A.7.10. Storage media A.7.13. Equipment maintenance A.7.14. Secure disposal or re-use of equipment
Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization		
39.	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	A.8.8. Management of technical vulnerabilities

40.	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	A.5.5. Contact with authorities A.5.6. Contact with special interest groups A.5.7. Threat intelligence
41.	ID.RA-03: Internal and external threats to the organization are identified and recorded	6.1 Actions to address risks and opportunities 8.2 Information security risk assessment A.5.7. Threat intelligence
42.	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	A.5.7. Threat intelligence A.8.8. Management of technical vulnerabilities
43.	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	6.1 Actions to address risks and opportunities 8.2 Information security risk assessment A.5.7. Threat intelligence A.8.8. Management of technical vulnerabilities
44.	ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	6.1 Actions to address risks and opportunities 6.3 Planning of changes 8.3 Information security risk treatment
45.	ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	6.1 Actions to address risks and opportunities 6.3 Planning of changes 8.3 Information security risk treatment
46.	ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established	A.5.7. Threat intelligence A.8.8. Management of technical vulnerabilities
47.	ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use	A.5.32. Intellectual property rights A.5.37. Documented operating procedures A.8.4. Access to source code A.8.19. Installation of software on operational systems A.8.26. Application security requirements A.8.29. Security testing in development and acceptance A.8.32. Change management
48.	ID.RA-10: Critical suppliers are assessed prior to acquisition	A.5.19. Information security in supplier relationships
Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions		
49.	ID.IM-01: Improvements are identified from evaluations	9.1 Monitoring, measurement, analysis and evaluation 10.1 Continual improvement
50.	ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	9.2 Internal audit 10.2 Nonconformity and corrective action A.5.35. Independent review of information security A.5.36. Compliance with policies, rules and standards for information security
51.	ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities	9.2 Internal audit 10.2 Nonconformity and corrective action A.5.35. Independent review of information security A.5.36. Compliance with policies, rules and standards for information security
52.	ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	A.5.24. Information security incident management planning and preparation

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access		
53.	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	A.5.15. Access control A.5.16. Identity management A.5.17. Authentication information A.5.18. Access rights A.8.2. Privileged access rights A.8.3. Information access restriction A.8.4. Access to source code A.8.5. Secure authentication
54.	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	A.5.16. Identity management
55.	PR.AA-03: Users, services, and hardware are authenticated	A.5.17. Authentication information A.8.5. Secure authentication
56.	PR.AA-04: Identity assertions are protected, conveyed, and verified	A.5.16. Identity management A.8.11. Data masking
57.	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	A.5.3. Segregation of duties A.5.18. Access rights A.8.2. Privileged access rights A.8.3. Information access restriction
58.	PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	A.5.37. Documented operating procedures A.7.1. Physical security perimeter A.7.2. Physical entry A.7.3. Securing offices, rooms and facilities A.7.4. Physical security monitoring A.7.6. Working in secure areas
Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks		
59.	PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	7.2 Competence 7.3 Awareness A.6.3. Information security awareness, education and training
60.	PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	7.2 Competence 7.3 Awareness A.6.3. Information security awareness, education and training
Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information		
61.	PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	A.8.1. User end point devices A.8.3. Information access restriction A.8.4. Access to source code A.8.7. Protection against malware A.8.10. Information deletion A.8.11. Data masking A.8.12. Data leakage prevention A.8.18. Use of privileged utility programs A.8.19. Installation of software on operational systems A.8.24. Use of cryptography A.8.26. Application security requirements A.8.32. Change management

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

62.	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	A.5.14. Information transfer A.8.11. Data masking A.8.12. Data leakage prevention A.8.20. Network security A.8.21. Security of network services A.8.23. Web filtering A.8.24. Use of cryptography
63.	PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	A.5.10. Acceptable use of information and other associated assets A.8.1. User end point devices A.8.3. Information access restriction A.8.4. Access to source code A.8.7. Protection against malware A.8.10. Information deletion A.8.11. Data masking A.8.12. Data leakage prevention A.8.18. Use of privileged utility programs A.8.19. Installation of software on operational systems A.8.24. Use of cryptography A.8.26. Application security requirements A.8.28. Secure coding A.8.32. Change management A.8.34. Protection of information systems during audit testing
64.	PR.DS-11: Backups of data are created, protected, maintained, and tested	A.5.37. Documented operating procedures A.8.13. Information backup
Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability		
65.	PR.PS-01: Configuration management practices are established and applied	A.5.37. Documented operating procedures A.8.9. Configuration management A.8.32. Change management
66.	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	A.5.37. Documented operating procedures A.8.9. Configuration management A.8.18. Use of privileged utility programs A.8.19. Installation of software on operational systems A.8.32. Change management
67.	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	A.5.37. Documented operating procedures A.7.6. Working in secure areas A.7.7. Clear desk and clear screen A.7.8. Equipment siting and protection A.7.13. Equipment maintenance A.7.14. Secure disposal or re-use of equipment A.8.32. Change management
68.	PR.PS-04: Log records are generated and made available for continuous monitoring	A.5.37. Documented operating procedures A.8.15. Logging A.8.16. Monitoring activities A.8.17. Clock synchronization
69.	PR.PS-05: Installation and execution of unauthorized software are prevented	A.5.37. Documented operating procedures A.8.2. Privileged access rights A.8.7. Protection against malware A.8.18. Use of privileged utility programs A.8.19. Installation of software on operational systems

70.	PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	A.5.37. Documented operating procedures A.8.25. Secure development life cycle A.8.26. Application security requirements A.8.27. Secure system architecture and engineering principles A.8.28. Secure coding A.8.29. Security testing in development and acceptance A.8.30. Outsourced development A.8.31. Separation of development, test and production environments A.8.32. Change management A.8.33. Test information A.8.34. Protection of information systems during audit testing
Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience		
71.	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	A.8.20. Network security A.8.21. Security of network services A.8.22. Segregation of networks A.8.23. Web filtering
72.	PR.IR-02: The organization's technology assets are protected from environmental threats	A.7.1. Physical security perimeter A.7.2. Physical entry A.7.3. Securing offices,rooms and facilities A.7.4. Physical security monitoring A.7.5. Protecting against physical and environmental threats A.7.6. Working in secure areas A.7.7. Clear desk and clear screen A.7.8. Equipment siting and protection A.7.9. Security of assets off-premises A.7.10. Storage media A.7.11. Supporting utilities A.7.12. Cabling security A.7.13. Equipment maintenance A.7.14. Secure disposal or re-use of equipment
73.	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	A.5.29. Information security during disruption A.5.30. ICT readiness for business continuity A.8.14. Redundancy of information processing facilities
74.	PR.IR-04: Adequate resource capacity to ensure availability is maintained	A.8.6. Capacity management A.8.14. Redundancy of information processing facilities
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events		
75.	DE.CM-01: Networks and network services are monitored to find potentially adverse events	A.5.25. Assessment and decision on information security events A.5.37. Documented operating procedures A.8.16. Monitoring activities
76.	DE.CM-02: The physical environment is monitored to find potentially adverse events	A.5.37. Documented operating procedures A.7.4. Physical security monitoring
77.	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	A.5.37. Documented operating procedures A.6.8. Information security event reporting A.8.12. Data leakage prevention A.8.16. Monitoring activities

78.	DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	A.5.22. Monitoring, review and change management of supplier services A.5.37. Documented operating procedures
79.	DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	A.5.37. Documented operating procedures A.8.4. Access to source code A.8.7. Protection against malware A.8.16. Monitoring activities A.8.18. Use of privileged utility programs
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents		
80.	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	A.5.7. Threat intelligence A.5.25. Assessment and decision on information security events
81.	DE.AE-03: Information is correlated from multiple sources	A.6.8. Information security event reporting A.8.15. Logging A.8.16. Monitoring activities
82.	DE.AE-04: The estimated impact and scope of adverse events are understood	A.5.25. Assessment and decision on information security events
83.	DE.AE-06: Information on adverse events is provided to authorized staff and tools	A.5.7. Threat intelligence A.5.24. Information security incident management planning and preparation
84.	DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	A.5.7. Threat intelligence A.5.25. Assessment and decision on information security events
85.	DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	A.5.25. Assessment and decision on information security events
Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed		
86.	RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	A.5.26. Response to information security incidents A.5.37. Documented operating procedures
87.	RS.MA-02: Incident reports are triaged and validated	A.5.26. Response to information security incidents A.5.27. Learning from information security incidents A.5.28. Collection of evidence
88.	RS.MA-03: Incidents are categorized and prioritized	A.5.25. Assessment and decision on information security events A.5.26. Response to information security incidents
89.	RS.MA-04: Incidents are escalated or elevated as needed	A.5.26. Response to information security incidents
90.	RS.MA-05: The criteria for initiating incident recovery are applied	A.5.24. Information security incident management planning and preparation A.5.26. Response to information security incidents
Incident Analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities		
91.	RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	A.5.27. Learning from information security incidents
92.	RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	A.5.27. Learning from information security incidents A.5.28. Collection of evidence
93.	RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	A.5.27. Learning from information security incidents A.5.28. Collection of evidence

94.	RS.AN-08: An incident's magnitude is estimated and validated	A.5.25. Assessment and decision on information security events A.5.27. Learning from information security incidents
Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies		
95.	RS.CO-02: Internal and external stakeholders are notified of incidents	7.4 Communication A.5.5. Contact with authorities A.5.6. Contact with special interest groups A.5.26. Response to information security incidents
96.	RS.CO-03: Information is shared with designated internal and external stakeholders	7.4 Communication A.5.5. Contact with authorities A.5.6. Contact with special interest groups A.5.26. Response to information security incidents
Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects		
97.	RS.MI-01: Incidents are contained	A.5.26. Response to information security incidents
98.	RS.MI-02: Incidents are eradicated	A.5.26. Response to information security incidents
Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents		
99.	RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	A.5.26. Response to information security incidents
100.	RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	A.5.26. Response to information security incidents
101.	RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	A.5.30. ICT readiness for business continuity A.5.37. Documented operating procedures A.8.13. Information backup
102.	RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	A.5.30. ICT readiness for business continuity
103.	RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	A.5.30. ICT readiness for business continuity A.5.37. Documented operating procedures A.8.13. Information backup
104.	RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed	A.5.26. Response to information security incidents A.5.27. Learning from information security incidents
Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties		
105.	RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	7.4 Communication A.5.5. Contact with authorities A.5.6. Contact with special interest groups
106.	RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	7.4 Communication 5.7. Threat intelligence