INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2013-2016

COM 17 – LS 078 – E

Original: English

Question(s):	4/17
Source:	ITU-T Study Group 17
Title:	LS/o on NIST preliminary cybersecurity framework [to NIST]

LIAISON STATEMENT

For action to:		
For comment to:	NIST	
For information to:		
Approval:	ITU-T SG17 management team by electronic correspondence (13 December 2013)	
Deadline:	N/A	
Contact:	Youki Kadobayashi Rapporteur of ITU-T Question 4/17	Tel: +81 743 72 52 11 E-mail: youki-k@is.aist-nara.ac.jp

ITU-T Study Group 17, Security, in its Question 4/17, Cybersecurity, reviewed the NIST preliminary cybersecurity framework, pursuant to open solicitation for review. In the highly interdependent cyberspace with its basis on open, interoperable technologies, critical infrastructure sectors are likely to benefit from existing open standards: the NIST framework is an important initiative to proliferate key standards and best practices into those sectors.

Our collective findings are summarized in the following points, which we hope to be useful to further improve the framework:

1 Scope of the framework

We understand that the current version of the framework is intended to improve the cybersecurity of individual enterprises, rather than that of industries/sectors. As such, automated indicator sharing and supply chain risk management are left out of the Framework Core, as documented in Appendix C. The scope of the current version of the framework could be better articulated by incorporating a concise summary of Appendix C into Section 1.1, *Overview of the Framework*.

2 Suggested reference to knowledge-base standards

We find that the current framework could be improved by incorporating references to cybersecurity knowledge-base standards. The Annex to this document contains suggested additional references to the NIST Preliminary Cybersecurity Framework – Framework Core.

As indicated in the clause 2.1 of the Framework, the Framework Core is not a checklist of activities to perform; however, it is our understanding that traditional process-centric approach of risk management alone – without awareness of cybersecurity knowledge bases and enumeration standards – may not facilitate precise estimation of cybersecurity risks or communication about risks amongst organizations.

As cybersecurity risks can exhibit high degree of volatility due to variety of factors such as vulnerability discovery as well as cascading effects across systems, it is important to understand the fundamentally different nature of the risk from both business and management perspectives. As such, awareness of cybersecurity knowledge bases and enumeration standards are crucial.

In accordance with the cooperative agreements between NIST and ITU-T, we are looking forward to further our continuing collaboration.

Annex
Suggested additional references to NIST Preliminary Cybersecurity Framework – Framework Core.

Subcategory	Informative References	Suggested Additional References
ID.AM-1: Physical devices and systems within the organization are inventoried	**• ISA 99.02.01 4.2.3.4 • COBIT BAI03.04, BAI09.01, BAI09, BAI09.05 • ISO/IEC 27001 A.7.1.1, A.7.1.2 • NIST SP 800-53 Rev. 4 CM-8 • CCS CSC1**	
ID.AM-2: Software platforms and applications within the organization are inventoried	**• ISA 99.02.01 4.2.3.4 • COBIT BAI03.04, BAI09.01, BAI09, BAI09.05 • ISO/IEC 27001 A.7.1.1, A.7.1.2 • NIST SP 800-53 Rev. 4 CM-8 • CCS CSC 2**	**CPE (Rec. ITU-T X.1528 -- Common platform enumeration)**
ID.AM-3: The organizational communication and data flow is mapped	**• ISA 99.02.01 4.2.3.4 • COBIT DSS05.02 • ISO/IEC 27001 A.7.1.1 • NIST SP 800-53 Rev. 4 CA-3, CM-8, CA-9 • CCS CSC 1**	
ID.AM-4: External information systems are mapped and catalogued	**• NIST SP 500-291 3, 4 • NIST SP 800-53 Rev. 4 AC-20, SA-9**	
ID.AM-5: Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software	**• ISA 99.02.01 4.2.3.6 • COBIT APO03.03, APO03.04, BAI09.02 • NIST SP 800-53 Rev. 4 RA-2, CP-2 • NIST SP 800-34 Rev 1 • ISO/IEC 27001 A.7.2.1**	
ID.AM-6: Workforce roles and responsibilities for business functions, including cybersecurity, are established	**• ISA 99.02.01 4.3.2.3.3 • COBIT APO01.02, BAI01.12, DSS06.03 • ISO/IEC 27001 A.8.1.1 • NIST SP 800-53 Rev. 4 CP-2, PM-11 • NIST SP 800-34 Rev 1**	
ID.BE-1: The organization's role in the supply chain and is identified and communicated	**• COBIT APO08.01, APO08.02, APO08.03, APO08.04, APO08.05, APO10.03, DSS01.02 • ISO/IEC 27001 A.10.2 • NIST SP 800-53 Rev. 4 CP-2**	
ID.BE-2: The organization's place in critical infrastructure and their industry ecosystem is identified and communicated	**• COBIT APO02.06, APO03.01 • NIST SP 800-53 Rev. 4 PM-8**	
ID.BE-3: Priorities for organizational mission, objectives, and activities are established	**• ISA 99.02.01 4.2.2.1, 4.2.3.6 • COBIT APO02.01, APO02.06, APO03.01 • NIST SP 800-53 Rev. 4 PM-11**	
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**• COBIT DSS01.03 • ISO/IEC 27001 9.2.2 • NIST SP 800-53 Rev 4 CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PM-8**	

Subcategory	Informative References	Suggested Additional References
ID.BE-5: Resilience requirements to support delivery of critical services are established	• **NIST SP 800-53 Rev. 4 CP-2, SA-14**	
ID.GV-1: Organizational information security policy is established	• **ISA 99.02.01 4.3.2.6** • **COBIT APO01.03, EA01.01** • **ISO/IEC 27001 A.6.1.1** • **NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)**	
ID.GV-2: Information security roles & responsibility are coordinated and aligned	• **ISA 99.02.01 4.3.2.3.3** • **ISO/IEC 27001 A.6.1.3** • **NIST SP 800-53 Rev. 4 AC-21, PM-1, PS-7**	
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	• **ISA 99.02.01 4.4.3.7** • **COBIT MEA03.01, MEA03.04** • **ISO/IEC 27001 A.15.1.1** • **NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)**	
ID.GV-4: Governance and risk management processes address cybersecurity risks	• **NIST SP 800-53 Rev. 4 PM-9, PM-11**	
ID.RA-1: Asset vulnerabilities are identified and documented	• **ISA 99.02.01 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12** • **COBIT APO12.01, APO12.02, APO12.03, APO12.04** • **ISO/IEC 27001 A.6.2.1, A.6.2.2, A.6.2.3** • **CCS CSC4** • **NIST SP 800-53 Rev. 4 CA-2, RA-3, RA-5, SI-5**	**CVE (Rec. ITU-T X.1520 -- Common vulnerabilities and exposures)**
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	• **ISA 99.02.01 4.2.3, 4.2.3.9, 4.2.3.12** • **ISO/IEC 27001 A.13.1.2** • **NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5**	**CAPEC (Rec. ITU-T X.1544 -- Common attack pattern enumeration and classification)**
ID.RA-3: Threats to organizational assets are identified and documented	• **ISA 99.02.01 4.2.3, 4.2.3.9, 4.2.3.12** • **COBIT APO12.01, APO12.02, APO12.03, APO12.04** • **NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-16**	**CAPEC (Rec. ITU-T X.1544 -- Common attack pattern enumeration and classification)**
ID.RA-4: Potential impacts are analyzed	• **ISA 99.02.01 4.2.3, 4.2.3.9, 4.2.3.12** • **NIST SP 800-53 Rev. 4 RA-3**	**CVSS (Rec. ITU-T X.1521 -- Common vulnerability scoring system)**
ID.RA-5: Risk responses are identified	• **NIST SP 800-53 Rev. 4 PM-9**	
ID.RM-1: Risk management processes are managed and agreed to	• **ISA 99.02.01 4.3.4.2** • **COBIT APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02** • **NIST SP 800-53 Rev. 4 PM-9** • **NIST SP 800-39**	
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• **ISA 99.02.01 4.3.2.6.5** • **COBIT APO10.04, APO10.05, APO12.06** • **NIST SP 800-53 Rev. 4 PM-9** • **NIST SP 800-39**	

Subcategory	Informative References	Suggested Additional References
ID.RM-3: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	**• NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11**	
PR.AC-1: Identities and credentials are managed for authorized devices and users	**• ISA 99.02.01 4.3.3.5.1** **• COBIT DSS05.04, DSS06.03** **• ISO/IEC 27001 A.11** **• NIST SP 800-53 Rev. 4 AC-2, AC-5, AC-6, IA Family** **• CCS CSC 16**	
PR.AC-2: Physical access to resources is managed and secured	**• ISA 99.02.01 4.3.3.3.2, 4.3.3.3.8** **• COBIT DSS01.04, DSS05.05** **• ISO/IEC 27001 A.9.1, A.9.2, A.11.4, A.11.6** **• NIST SP 800-53 Rev 4 PE-2, PE-3, PE-4, PE-6, PE-9**	
PR.AC-3: Remote access is managed	**• ISA 99.02.01 4.3.3.6.6** **• COBIT APO13.01, DSS01.04, DSS05.03** **• ISO/IEC 27001 A.11.4, A.11.7** **• NIST SP 800-53 Rev. 4 AC 17, AC-19, AC-20**	
PR.AC-4: Access permissions are managed	**• ISA 99.02.01 4.3.3.7.3** **• ISO/IEC 27001 A.11.1.1** **• NIST SP 800-53 Rev. 4 AC-3, AC-4, AC-6, AC-16** **• CCS CSC 12, 15**	
PR.AC-5: Network integrity is protected	**• ISA 99.02.01 4.3.3.4** **• ISO/IEC 27001 A.10.1.4, A.11.4.5** **• NIST SP 800-53 Rev 4 AC-4**	
PR.AT-1: General users are informed and trained	**• ISA 99.02.01 4.3.2.4.2** **• COBIT APO07.03, BAI05.07** **• ISO/IEC 27001 A.8.2.2** **• NIST SP 800-53 Rev. 4 AT-2** **• CCS CSC 9**	
PR.AT-2: Privileged users understand roles & responsibilities	**• ISA 99.02.01 4.3.2.4.2, 4.3.2.4.3** **• COBIT APO07.02** **• ISO/IEC 27001 A.8.2.2** **• NIST SP 800-53 Rev. 4 AT-3** **• CCS CSC 9**	
PR.AT-3: Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities	**• ISA 99.02.01 4.3.2.4.2** **• COBIT APO07.03, APO10.04, APO10.05** **• ISO/IEC 27001 A.8.2.2** **• NIST SP 800-53 Rev. 4 AT-3** **• CCS CSC 9**	
PR.AT-4: Senior executives understand roles & responsibilities	**• ISA 99.02.01 4.3.2.4.2** **• COBIT APO07.03** **• ISO/IEC 27001 A.8.2.2** **• NIST SP 800-53 Rev. 4 AT-3** **• CCS CSC 9**	

Subcategory	Informative References	Suggested Additional References
PR.AT-5: Physical and information security personnel understand roles & responsibilities	**• ISA 99.02.01 4.3.2.4.2** **• COBIT APO07.03** **• ISO/IEC 27001 A.8.2.2** **• NIST SP 800-53 Rev. 4 AT-3** **• CCS CSC 9**	
PR.DS-1: Data-at-rest is protected	**• COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06** **• ISO/IEC 27001 A.15.1.3, A.15.1.4** **• CCS CSC 17** **• NIST SP 800-53 Rev 4 SC-28**	
PR.DS-2: Data-in-motion is secured	**• COBIT APO01.06, BAI02.01, BAI06.01, DSS06.06** **• ISO/IEC 27001 A.10.8.3** **• NIST SP 800-53 Rev. 4 SC-8** **• CCS CSC 17**	
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**• COBIT BAI09.03** **• ISO/IEC 27001 A.9.2.7, A.10.7.2** **• NIST SP 800-53 Rev 4 PE-16, MP-6, DM-2**	
PR.DS-4: Adequate capacity to ensure availability is maintained	**• COBIT APO13.01** **• ISO/IEC 27001 A.10.3.1** **• NIST SP 800-53 Rev 4 CP-2, SC-5**	
PR.DS-5: There is protection against data leaks	**• COBIT APO01.06** **• ISO/IEC 27001 A.12.5.4** **• CCS CSC 17** **• NIST SP 800-53 Rev 4 AC-4, PE-19, SC-13, SI-4, SC-7, SC-8, SC-31, AC-5, AC-6, PS-6**	
PR.DS-6: Intellectual property is protected	**• COBIT APO01.03, APO10.02, APO10.04, MEA03.01**	
PR.DS-7: Unnecessary assets are eliminated	**• COBIT BAI06.01, BAI01.10** **• ISO/IEC 27001 A.10.1.3** **• NIST SP 800-53 Rev. 4 AC-5, AC-6**	
PR.DS-8: Separate testing environments are used in system development	**• COBIT BAI07.04** **• ISO/IEC 27001 A.10.1.4** **• NIST SP 800-53 Rev. 4 CM-2**	
PR.DS-9: Privacy of individuals and personally identifiable information (PII) is protected	**• COBIT BAI07.04, DSS06.03, MEA03.01** **• ISO/IEC 27001 A.15.1.3** **• NIST SP 800-53 Rev 4, Appendix J**	
PR.IP-1: A baseline configuration of information technology/operational technology systems is created	**• ISA 99.02.01 4.3.4.3.2, 4.3.4.3.3** **• COBIT BAI10.01, BAI10.02, BAI10.03, BAI10.05** **• NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-7, CM-9, SA-10** **• CCS CSC 3, 10**	
PR.IP-2: A System Development Life Cycle to manage systems is implemented	**• ISA 99.02.01 4.3.4.3.3** **• COBIT APO13.01** **• ISO/IEC 27001 A.12.5.5** **• NIST SP 800-53 Rev 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-15, SA-17, PL-8** **• CCS CSC 6**	

Subcategory	Informative References	Suggested Additional References
PR.IP-3: Configuration change control processes are in place	• ISA 99.02.01 4.3.4.3.2, 4.3.4.3.3 • COBIT BAI06.01, BAI01.06 • ISO/IEC 27001 A.10.1.2 • NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10	
PR.IP-4: Backups of information are managed	• ISA 99.02.01 4.3.4.3.9 • COBIT APO13.01 • ISO/IEC 27001 A.10.5.1 • NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9	
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• COBIT DSS01.04, DSS05.05 • ISO/IEC 27001 9.1.4 • NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18	
PR.IP-6: Information is destroyed according to policy and requirements	• COBIT BAI09.03 • ISO/IEC 27001 9.2.6 • NIST SP 800-53 Rev 4 MP-6	
PR.IP-7: Protection processes are continuously improved	• COBIT APO11.06, DSS04.05 • NIST SP 800-53 Rev 4 PM-6, CA-2, CA-7, CP-2, IR-8, PL-2	
PR.IP-8: Information sharing occurs with appropriate parties	• ISO/IEC 27001 A.10 • NIST SP 800-53 Rev. 4 AC-21	
PR.IP-9: Response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s)) are in place and managed	• COBIT DSS04.03 • ISO/IEC 27001 A.14.1 • NIST SP 800-53 Rev. 4 CP-2, IR-8	
PR.IP-10: Response plans are exercised	• NIST SP 800-53 Rev.4 IR-3	
PR.IP-11: Cybersecurity is included in human resources practices (de-provisioning, personnel screening, etc.)	• COBIT APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • ISO/IEC 27001 8.2.3, 8.3.1 • NIST SP 800-53 Rev 4 PS Family	
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• ISO/IEC 27001 A.9.1.1, A.9.2.4, A.10.4.1 • NIST SP 800-53 Rev 4 MA-2, MA-3, MA-5	
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access and supports availability requirements for important operational and information systems	• COBIT 5 • ISO/IEC 27001 A.9.2.4, A.11.4.4 • NIST SP 800-53 Rev 4 MA-4	

Subcategory	Informative References	Suggested Additional References
PR.PT-1: Audit and log records are stored in accordance with audit policy	**• ISA 99.02.01 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4** **• COBIT APO11.04** **• ISO/IEC 27001 A.10.10.1, A.10.10.3, A.10.10.4, A.10.10.5, A.15.3.1** **• NIST SP 800-53 Rev. 4 AU Family** **• CCS CSC 14**	
PR.PT-2: Removable media are protected according to a specified policy	**• COBIT DSS05.02, APO13.01** **• ISO/IEC 27001 A.10.7** **• NIST SP 800-53 Rev. 4 AC-19, MP-2, MP-4, MP-5, MP-7**	
PR.PT-3: Access to systems and assets is appropriately controlled	**• CCS CSC 6** **• COBIT DSS05.02** **• NIST SP 800-53 Rev 4 CM-7**	
PR.PT-4: Communications networks are secured	**• COBIT DSS05.02, APO13.01** **• ISO/IEC 27001 10.10.2** **• NIST SP 800-53 Rev 4 AC-18** **• CCS CSC 7**	
PR.PT-5: Specialized systems are protected according to the risk analysis (SCADA, ICS, DLS)	**• COBIT APO13.01,** **• NIST SP 800-53 Rev 4**	
DE.AE-1: A baseline of normal operations and procedures is identified and managed	**• ISA 99.02.01 4.4.3.3** **• COBIT DSS03.01** **• NIST SP 800-53 Rev. 4 AC-2, SI-3, SI-4, AT-3, CM-2**	
DE.AE-2: Detected events are analyzed to understand attack targets and methods	**• NIST SP 800-53 Rev. 4 SI-4, IR-4**	
DE.AE-3: Cybersecurity data are correlated from diverse information sources	**• NIST SP 800-53 Rev. 4 SI-4**	
DE.AE-4: Impact of potential cybersecurity events is determined	**• NIST SP 800-53 Rev. 4 IR-4, SI -4**	
DE.AE-05: Incident alert thresholds are created	**• ISA 99.02.01 4.2.3.10** **• NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-9** **• NIST SP 800-61 Rev 2**	
DE.CM-1: The network is monitored to detect potential cybersecurity events	**• COBIT DSS05.07** **• ISO/IEC 27001 A.10.10.2, A.10.10.4, A.10.10.5** **• NIST SP 800-53 Rev. 4 CM-3, CA-7, AC-2, IR-5, SC-5, SI-4** **• CCS CSC 14, 16**	
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	**• NIST SP 800-53 Rev. 4 CM-3, CA-7, IR-5, PE-3, PE-6, PE-20**	
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**• NIST SP 800-53 Rev. 4 AC-2, CM-3, CA-7**	

Subcategory	Informative References	Suggested Additional References
DE.CM-4: Malicious code is detected	**• COBIT DSS05.01** **• ISO/IEC 27001 A.10.4.1** **• NIST SP 800-53 Rev 4 SI-3** **• CCS CSC 5**	
DE.CM-5: Unauthorized mobile code is detected	**• ISO/IEC 27001 A.10.4.2** **• NIST SP 800-53 Rev 4 SC-18**	
DE.CM-6: External service providers are monitored	**• ISO/IEC 27001 A.10.2.2** **• NIST SP 800-53 Rev 4 CA-7, PS-7, SI-4, SA-4, SA-9**	
DE.CM-7: Unauthorized resources are monitored	**• NIST SP 800-53 Rev. 4 CM-3, CA-7, PE-3, PE-6, PE-20, SI-4**	
DE.CM-8: Vulnerability assessments are performed	**• NIST SP 800-53 Rev. 4 CM-3, CA-7, CA-8, RA-5, SA-11, SA-12**	**OVAL (Rec. ITU-T X.1526 -- Open vulnerability and assessment language)**
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	**• ISA 99.02.01 4.4.3.1** **• COBIT DSS05.01** **• NIST SP 800-53 Rev 4 IR-2, IR-4, IR-8** **• CCS CSC 5**	
DE.DP-2: Detection activities comply with all applicable requirements, including those related to privacy and civil liberties	**• ISA 99.02.01 4.4.3.2** **• NIST SP 800-53 Rev 4 CA-2, CA-7**	
DE.DP-3: Detection processes are exercised to ensure readiness	**• ISA 99.02.01 4.4.3.2** **• NIST SP 800-53 Rev 4 PM-14**	
DE.DP-4: Event detection information is communicated to appropriate parties	**• NIST SP 800-53 Rev. 4 CP-2, IR-8**	
DE.DP-5: Detection processes are continuously improved	**• COBIT APO11.06, DSS04.05** **• NIST SP 800-53 Rev 4 PM-6, CA-2, CA-7, CP-2, IR-8, PL-2**	
RS.PL-1: Response plan is implemented during or after an event	**• ISA 99.02.01 4.3.4.5.1** **• NIST SP 800-53 Rev. 4 CP-10, IR-4** **• CCS CSC 18**	
RS.CO-1: Personnel know their roles and order of operations when a response is needed	**• ISO/IEC 27001 A.13.2.1** **• ISA 99.02.01 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4** **• NIST SP 800-53 Rev 4 CP-2, IR-8**	
RS.CO-2: Events are reported consistent with established criteria	**• ISO/IEC 27001 A.13.1.1, A.13.1.2** **• ISA 99.02.01 4.3.4.5.5** **• NIST SP 800-53 Rev 4 IR-6, IR-8**	
RS.CO-3: Detection/response information, such as breach reporting requirements, is shared consistent with response plans, including those related to privacy and civil liberties	**• ISO/IEC 27001 A.10**	

Subcategory	Informative References	Suggested Additional References
RS.CO-4: Coordination with stakeholders occurs consistent with response plans, including those related to privacy and civil liberties	• ISO/IEC 27001 A.8.1.1, A.6.1.2, A.6.1.6, A.10.8.2 • NIST SP 800-53 Rev. 4 CP-2, IR-8	
RS.CO-5: Voluntary coordination occurs with external stakeholders (ex, business partners, information sharing and analysis centers, customers)	• NIST SP 800-53 Rev. 4 PM-15, SI-5	
RS.AN-1: Notifications from the detection system are investigated	• ISO/IEC 27001 A.6.2.1 • NIST SP 800-53 Rev. 4 IR-4, IR-5, PE-6, SI-4, AU-13	
RS.AN-2: Understand the impact of the incident	• ISO/IEC 27001 A.6.2.1 • NIST SP 800-53 Rev. 4 CP-10, IR-4	
RS.AN-3: Forensics are performed	• ISO/IEC 27001 A.13.2.2, A.13.2.3 • NIST SP 800-53 Rev. 4 IR-4	
RS.AN-4: Incidents are classified consistent with response plans	• ISO/IEC 27001 A.13.2.2 • ISA 99.02.01 4.3.4.5.6 • NIST SP 800-53 Rev. 4 IR-4	
RS.MI-1: Incidents are contained	• ISO/IEC 27001 A.3.6, A.13.2.3 • ISA 99.02.01 4.3.4.5.6 • NIST SP 800-53 Rev. 4 IR-4	
RS.MI-2: Incidents are eradicated	• ISA 99.02.01 4.3.4.5.6, 4.3.4.5.10 • NIST SP 800-53 Rev. 4 IR-4	
RS.IM-1: Response plans incorporate lessons learned	• ISO/IEC 27001 A.13.2.2 • ISA 99.02.01 4.3.4.5.10, 4.4.3.4 • NIST SP 800-53 Rev. 4 CP-2, IR-8	
RS.IM-2: Response strategies are updated	• NIST SP 800-53 Rev. 4 CP-2, IR-8	
RC.RP-1: Recovery plan is executed	• COBIT DSS02.05, DSS03.04 • ISO/IEC 27001 A.14.1.3, A.14.1.4, A.14.1.5 • NIST SP 800-53 Rev. 4 CP-10, CP-2 • CCS CSC 8	
RC.IM-1: Plans are updated with lessons learned	• ISA 99.02.01 4.4.3.4 • COBIT BAI05.07 • ISO/IEC 27001 13.2.2 • NIST SP 800-53 Rev. 4 CP-2	
RC.IM-2: Recovery strategy is updated	• COBIT APO05.04, BAI07.08 • NIST SP 800-53 Rev. 4 CP-2	
RC.CO-1: Public Relations are managed	• COBIT MEA03.02 • NIST SP 800-53 Rev. 4 IR-4, IR-8	
RC.CO-2: Reputation after an event is repaired	• COBIT MEA03.02	