

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
10Bureau Drive, Stop 8930
Gaithersburg, MD 20899 – 8930

123 Industrial Layout
Hosur Road, Koramangala
Bangalore 560 095
India
Tel.: +91 80 6657 5757
Fax: +91 80 6657 1404
www.boschindia.com

RE: Request for Comments on the Preliminary Cyber Security Framework.

Dear Mr. Adam,

It has been a pleasure to go through and review the 'Preliminary Cyber Security Framework'. The work at NIST is commendable in this regard. We have gone through the framework and have tried to provide as objective comments as possible.

The comments are provided in two separate sections.


- A. Overarching comments
- B. Specific comments (as per the 'note for reviewers' in the framework)

In addition to the comments, the following are included in the submission:


- 1) Methodology template is provided at the end of the section B.
- 2) A document with mapping of Appendix-A: framework core with ISO/IEC 27001:2013 controls (as a part of informative references)

We would be pleased to get associated with NIST in the process of development of this framework. We will look forward for a continued association in the journey towards enhancing Critical Infrastructure Cybersecurity.

Office of the Data Security Officer – Bosch India



Krishna Bhat 10.12.2013



Anitha R 10.12.2013



Santosh Krishna Putchala 10.12.2013

Preliminary Cybersecurity Framework – Comments

A. Overarching Comments:

1. As the private sector owns the vast majority of the Nation’s critical infrastructure and key resources – roughly 85 percent¹. It is beneficial if framework incorporates the following:
 - a. Harmonization with the standards (such as those from ANSI, ISO, IEC etc.) that the private sector has embraced, implemented and achieved maturity over years.
 - b. For the organizations to derive the most benefit from the developed framework, it is suggested that it be mapped with the long existing best practices (such as Generally Accepted Privacy Principles from AICPA for Privacy space).
 - c. Best practices and reference to the implementation in the Federal organizations² are indispensable. But in the current format, the framework may appear to the key audience as having a very thick government flavor.
 - d. The United States House Permanent Select Committee on Intelligence in October 2012 has reported³ significant security flaws back doors in products used for building Critical Information Infrastructures. It enunciates that equipment deployed in critical infrastructure is indispensable for national security. Testing and evaluation of such equipment is a key in building resilient Critical Information Infrastructure. It is strongly recommended that this point be emphasized in the framework.
2. The framework talks about securing the critical information infrastructure and the underlying building blocks. In addition to a cyclical process (Identify, protect, detect, respond and recover), it would be beneficial if the following are included in the framework:
 - a. Embedding security in the software / code, rather than defense-in-depth through the policy and enforcement framework.
 - b. Concept of ‘*Security by Design*’ needs to be emphasized, as retrofitting security will only add to complexity, not to mention the effort.

¹ Government Accountability Office, The Department of Homeland Security’s (DHS) Critical Infrastructure Protection Cost-Benefit Report, June 26, 2009. (Accessed, 9th December 2013)

² http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (Accessed, 9th December 2013)

³ <http://intelligence.house.gov/press-release/chairman-rogers-and-ranking-member-ruppersberger-warn-american-companies-doing> (Accessed, 9th December 2013)

- c. Inclusion of recommendations on implementing secure coding standards (for example, as those developed by FFRDCs such as Software Engineering Institute, CMU). This can further be bolstered by the Cybersecurity workforce development (as required by the EO13636) and the NICE initiative.
 - d. It is highly desired that inclusion of recommendations (without mentioning the names such as OWASP – Open Web Application Security Project) on usage of application security standards be present in the framework.
 - e. Concept of ‘*Privacy by Design*’ needs to be included. Privacy as an afterthought will be cumbersome.
 - f. It is suggested that key concepts regarding Cryptography be included in the framework.
 - g. References to the work of Federal and state government officials⁴ will only strengthen the basis for the adoption of the framework.
 - h. Integration into the Enterprise Architecture (as was the case with FISMA) needs to be presented. The respective views (technical, business etc.,) be mentioned and integrated into the preliminary framework. Also the alignment with FEAF (as a mapping) may please be introduced.
 - i. Introduction of a concept similar to PRISMA may help the ends meet and also would enable the framework to focus on incentives and outcomes.
3. In this framework, the concept of incentives and score cards as used in the FISMA implementation may also be discussed. This will:
- a. Enable the organizations to solve the ‘*business case for Information Security paradox*’.
 - b. Discussion on the ROSI (Return on Security Investment) may also be included.
4. With regards to Appendix A (From line # 457 to # 477):
- a. The reference (From line # 473 to #474) does not specify the version of the standard (either 2005 or 2013).
 - b. The reference to ISO/IEC 27001 (From line # 473 to #474) points to ISO/IEC 27001:2005 (http://www.iso.org/iso/catalogue_detail?csnumber=42103) has been withdrawn and replaced with ISO/IEC 27001:2013 (http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534)
 - c. Due to the reorganization and introduction of new control clauses and control objectives in ISO/IEC 27001:2013, the current mapping in the informative references column appears erroneous.

⁴ <http://oag.ca.gov/privacy> (Accessed, 9th December 2013)

- d. Due to the above three factors, the control information in the informative references column (with regards to ISO/IEC 27001) may have to be redone with the latest and active standard.
 - e. The COBIT version used for the mapping in the informative references column shall be included in the references (line # 472).
5. With regards to Appendix B (From line # 485 to # 492)
- a. Mapping with NIST SP 800-53 Rev. 4, Appendix J is commendable. But for the organizations that are not under the purview of FISMA, mapping (in informative references) with a more widely applicable standard or framework would be beneficial.
6. Miscellaneous:
- a. Inclusion of NIST RMF (if not, Deming cycle) in the framework so as to depict the section # 2.1 (From line # 238 to #280)
 - b. As there is a disclaimer (line # 32 to # 35) included in the framework, globally acceptable standards, principles and other frameworks may be included in the framework document.

B. Specific Comments (as per the 'note to reviewers', line # 2 to # 31):

1. Does the preliminary framework:
 - a. Adequately define outcomes that strengthen Cybersecurity and support business objectives?
 - A) The preliminary framework tries to provide a generic picture of the elements that should be present in the given context. But it has been felt that the framework does not adequately define the outcomes that strengthen Cybersecurity. It has also not adequately established the link between outcomes that strengthen Cybersecurity and support business objectives. The framework has followed a 20,000 feet view.
 - b. Enable cost-effective implementation?
 - A) Even though it is difficult to establish strong links between the implementation of Information Security & Privacy, and the investment, the framework does not include adequate information to answer this question. The preliminary framework does not answer this question and there is no specific guidance or direction that the framework envisages. It makes business sense to have a balanced approach for information security so that cost of measures implemented does not exceed the value of the asset being protected.

- c. Appropriately integrate Cybersecurity risk into business risk?
 - A) The contents and the processes mentioned in the framework are superficial to assist the executive to integrate cyber security risk into business risk. More specific processes, normative methodology and recommendations need to be included so as to achieve the stated objective.
- d. Provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?
 - A) It was felt that the preliminary framework will not be in a position to provide the senior executives and boards of directors with tools to understand risks and mitigations at the appropriate level of detail.
- e. Provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?
 - A) This preliminary framework is generic enough that it can aid business of all sizes. But, this framework in the current shape will not be able to provide sufficient guidance and resources.
- f. Provide the right level of specificity and guidance for mitigating the impact of Cybersecurity measures on privacy and civil liberties?
 - A) Appendix – B of this framework tries to define the methodology and it further provides informative references. However, the references are from NIST SP 800-53 Rev. 4. This mapping will be of great help to the organizations who are mandated by FISMA, as a part of e-government act or have currently adopted the SP 800 series. For the larger part of the audience, mapping with internationally and nationally recognized practices or principles will be beneficial.
- g. Express existing practices in a manner that allows for effective use?
 - A) It has to be agreed that the preliminary framework has incorporated some existing practices. But without a metrics and measurement mechanism discussed or defined, 'effective use' cannot be vouched for.

2. Will the Preliminary Framework, as presented:

- a. be inclusive of, and not disruptive to, effective Cybersecurity practices in use today, including widely-used voluntary consensus standards that are not yet final?
 - A) To our knowledge, the preliminary framework is not disruptive to the current Cybersecurity practices in use today. As the framework has followed a 20,000 feet view, it has become inclusive and non disruptive. But it may not be effective if the framework is too broad

(may be perceived as vague). The forthcoming versions of the framework should strike a right balance between being generic and being a beacon for assisting in adoption.

b. Enable organizations to incorporate threat information?

A) The preliminary framework will not enable the organizations to incorporate threat information. Further detailing needs to be added.

3. Is the Preliminary Framework:

a. Presented at the right level of specificity?

A) The preliminary framework may not be at the right level of specificity. As mentioned earlier, it depicts a 20,000 feet view.

b. Sufficiently clear on how the privacy and civil liberties methodology is integrated with the Framework Core?

A) The methodology presented in Appendix – B is elaborate. But it will be best received if the intricate procedure is represented via diagrammatic representation or illustration. Including a methodology template will greatly enable the adoption. A sample is provided below. This outline can be followed for each of the step in the methodology:

I. Purpose of the step

- a. statement defining the purpose of this step
- b. capturing the overall inputs, outputs and specifics
- c. outcome of the step
- d. resource Loading ~ # of FTEs (Full Time Equivalents) etc.,

II. Inputs to the step

- a. inputs to the current step
- b. specifics regarding the documents
- c. where to locate the documents
- d. points of contact

III. Outputs of the step

- a. outputs from the current step
- b. tangible outputs and intangibles
- c. linking step in the method
- d. specific documentation from this step

IV. Supporting standards and guidelines

- a. standards & guidelines to be referred

- b. links to the repository
 - c. specific exclusions if any
- V. Critical success factors for the step
 - a. CSF for initiation of this step
 - b. CSF for execution of this step
 - c. CSF for timely completion of this step
 - d. CSF for obtaining output & outcome
- VI. Considerations
 - a. things to watch for
 - b. probable issues that may arise
- VII. Support
 - a. support needed from stakeholders, including management
 - b. support needed from previous assignees
 - c. required supporting documentation
- VIII. Dependencies
 - a. dependencies of this step with other steps
 - b. relation with respect to other steps
- IX. Resources
 - a. specific skills & roles for the completion
 - b. budgeting of time & allocation of FTEs
 - c. artifacts & identifiers
- X. Tools and templates
 - a. tools and templates used in this step

For the ultimate successful adoption of the framework and to reap desired outcomes, it is suggested that the points in this document may please be addressed.

Appendix A: Framework Core

Function	Category	Sub category	Informative references	
			Existing	Replace with
IDENTIFY (ID)	Asset Management (AM):	ID.AM-1: Physical devices and systems within the organization are inventoried	ISO/IEC 27001 A.7.1.1, A.7.1.2	ISO/IEC 27001:2013 A.8.1.1, A8.1.2
		ID.AM-2: Software platforms and applications within the organization are inventoried	ISO/IEC 27001 A.7.1.1, A.7.1.2	ISO/IEC 27001:2013 A.8.1.1, A8.1.2
		ID.AM-3: The organizational communication and data flow is mapped	ISO/IEC 27001 A.7.1.1, A.7.1.2	ISO/IEC 27001:2013 A.8.1.1, A8.1.2
		ID.AM-4: External information systems are mapped and catalogued	None	None
		ID.AM-5: Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software	ISO/IEC 27001 A.7.2.1	ISO/IEC 27001:2013 A.8.2.1
		ID.AM-6: Workforce roles and responsibilities for business functions, including Cybersecurity, are established	ISO/IEC 27001 A.8.1.1	ISO/IEC 27001:2013 A.6.1.1
	Business Environment (BE):	ID.BE-1: The organization's role in the supply chain and is identified and communicated	ISO/IEC 27001 A.10.2	ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
		ID.BE-2: The organization's place in critical infrastructure and their industry ecosystem is identified and communicated	None	None
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established	None	None

Function	Category	Sub category	Informative references	
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	ISO/IEC 27001 9.2.2	ISO/IEC 27001:2013 A.11.2.2
		ID.BE-5: Resilience requirements to support delivery of critical services are established	None	None
	Governance (GV):	ID.GV-1: Organizational information security policy is established	ISO/IEC 27001 A.6.1.1	ISO/IEC 27001:2013 A.5.1.1
		ID.GV-2: Information security roles & responsibility are coordinated and aligned	ISO/IEC 27001 A.6.1.3	ISO/IEC 27001:2013 A.6.1.1
		ID.GV-3: Legal and regulatory requirements regarding Cybersecurity, including privacy and civil liberties obligations, are understood and managed	ISO/IEC 27001 A.15.1.1	ISO/IEC 27001:2013 A.18.1.1, A.18.1.4
		ID.GV-4: Governance and risk management processes address Cybersecurity risks	None	ISO/IEC 27001:2013 A.18.2.1, A.18.2.2, A.18.2.3
	Risk Assessment (RA):	ID.RA-1: Asset vulnerabilities are identified and documented	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.6.2.3	ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.14.2.5, A.14.2.7, A.14.2.8, A.14.2.9
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources.	ISO/IEC 27001 A.13.1.2	ISO/IEC 27001:2013 A.6.1.3, A.6.1.4, A.16.1.2, A.16.1.3
		ID.RA-3: Threats to organizational assets are identified and documented	None	None
		ID.RA-4: Potential impacts are analyzed	None	None
		ID.RA-5: Risk responses are identified.	None	None
	Risk Management Strategy (RM):	ID.RM-1: Risk management processes are managed and agreed to	None	None

Function	Category	Sub category	Informative references	
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	None	None
		ID.RM-3: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	None	None
PROTECT (PR)	Access Control (AC):	PR.AC-1: Identities and credentials are managed for authorized devices and users	ISO/IEC 27001 A.11	ISO/IEC 27001:2013 A.9
		PR.AC-2: Physical access to resources is managed and secured	ISO/IEC 27001 A.9.1, A.9.2, A.11.4, A.11.6	ISO/IEC 27001:2013 A.11.1, A.11.2
		PR.AC-3: Remote access is managed	ISO/IEC 27001 A.11.4, A.11.7	ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.2
		PR.AC-4: Access permissions are managed	ISO/IEC 27001 A.11.1.1	ISO/IEC 27001:2013 A.9.2
		PR.AC-5: Network integrity is protected	None	None
	Awareness and Training (AT):	PR.AT-1: General users are informed and trained	ISO/IEC 27001 A.8.2.2	ISO/IEC 27001:2013 A.7.2.2
		PR.AT-2: Privileged users understand roles & responsibilities	ISO/IEC 27001 A.8.2.2	ISO/IEC 27001:2013 A.7.2.2, A.9.2.3
		PR.AT-3: Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities	ISO/IEC 27001 A.8.2.2	ISO/IEC 27001:2013 A.7.2.2, A.15.1.1, A.15.1.2
		PR.AT-4: Senior executives understand roles & responsibilities	ISO/IEC 27001 A.8.2.2	ISO/IEC 27001:2013 A.6.1.1
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	ISO/IEC 27001 A.8.2.2	ISO/IEC 27001:2013 A.6.1.1
	Data Security (DS):	PR.DS-1: Data-at-rest is protected	ISO/IEC 27001 A.15.1.3, A.15.1.4	ISO/IEC 27001:2013 A.18.1.3, A.18.1.4

Function	Category	Sub category	Informative references	
		PR.DS-2: Data-in-motion is secured	ISO/IEC 27001 A.10.8.3	ISO/IEC 27001:2013 A.8.3.3, A.10.10.1
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	ISO/IEC 27001 A.9.2.7, A.10.7.2	ISO/IEC 27001:2013 A.8.1.2, A.8.1.4, A.8.3.2
		PR.DS-4: Adequate capacity to ensure availability is maintained.	ISO/IEC 27001 A.10.3.1	ISO/IEC 27001:2013 A.12.1.3
		PR.DS-5: There is protection against data leaks	ISO/IEC 27001 A.12.5.4	ISO/IEC 27001:2013 A.14.1.3
		PR.DS-6: Intellectual property is protected	None	ISO/IEC 27001:2013 A.18.1.2
		PR.DS-7: Unnecessary assets are eliminated	ISO/IEC 27001 A.10.1.3	ISO/IEC 27001:2013 A.8.1.1, A.8.2.3
		PR.DS-8: Separate testing environments are used in system development	ISO/IEC 27001 A.10.1.4	ISO/IEC 27001:2013 A.12.1.4, A.14.2.6
		PR.DS-9: Privacy of individuals and personally identifiable information (PII) is protected	ISO/IEC 27001 A.15.1.3	ISO/IEC 27001:2013 A.18.1.4
	Information Protection Processes and Procedures (IP):	PR.IP-1: A baseline configuration of information technology/operational technology systems is created	None	None
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	ISO/IEC 27001 A.12.5.5	ISO/IEC 27001:2013 A.14.2.2, A.14.2.6
		PR.IP-3: Configuration change control processes are in place	ISO/IEC 27001 A.10.1.2	ISO/IEC 27001:2013 A.12.1.2
		PR.IP-4: Backups of information are managed	ISO/IEC 27001 A.10.5.1	ISO/IEC 27001:2013 A.12.3.1
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets	ISO/IEC 27001 9.1.4	ISO/IEC 27001:2013 A.11.1, A.11.2

Function	Category	Sub category	Informative references	
		are met.		
		PR.IP-6: Information is destroyed according to policy and requirements	ISO/IEC 27001 9.2.6	ISO/IEC 27001:2013 A.11.2.7, A.8.2.1, A.8.2.3
		PR.IP-7: Protection processes are continuously improved	None	None
		PR.IP-8: Information sharing occurs with appropriate parties	ISO/IEC 27001 A.10	ISO/IEC 27001:2013 A.6.1.3, A.6.1.4, A.16.1.2, A.16.1.3, A.16.1.6
		PR.IP-9: Response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s)) are in place and managed	ISO/IEC 27001 A.14.1	ISO/IEC 27001:2013 A.17.1.1, A.17.1.2, A.17.1.3, A.16.1.1, A.16.1.4, A.16.1.5
		PR.IP-10: Response plans are exercised	None	ISO/IEC 27001:2013 A.16.1.5
		PR.IP-11: Cybersecurity is included in human resources practices (de-provisioning, personnel screening, etc.)	ISO/IEC 27001 8.2.3, 8.3.1	ISO/IEC 27001:2013 A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1
	Maintenance (MA):	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	ISO/IEC 27001:2013 A.11.2.4, A.12.4.1
		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.	ISO/IEC 27001 A.9.2.4, A.11.4.4	ISO/IEC 27001:2013 A.11.2.4
	Protective Technology (PT):	PR.PT-1: Audit and log records are stored in accordance with audit policy	ISO/IEC 27001 A.10.10.1, A.10.10.3, A.10.10.4, A.10.10.5,	ISO/IEC 27001:2013 A.12.4.2, A.12.4.3,

Function	Category	Sub category	Informative references	
			A.15.3.1	A.12.7.1
		PR.PT-2: Removable media are protected according to a specified policy	ISO/IEC 27001 A.10.7	ISO/IEC 27001:2013 A.8.3.1
		PR.PT-3: Access to systems and assets is appropriately controlled	None	ISO/IEC 27001:2013 A.9.1.1, A.9.2, A.9.4
		PR.PT-4: Communications networks are secured	ISO/IEC 27001 10.10.2	ISO/IEC 27001:2013 A.13.1
		PR.PT-5: Specialized systems are protected according to the risk analysis (SCADA, ICS, DLS)	None	ISO/IEC 27001:2013 A.12.2.1, A.11.1, A.11.2, A.12.6.1
DETECT (DE)	Anomalies and Events (AE):	DE.AE-1: A baseline of normal operations and procedures is identified and managed	None	ISO/IEC 27001:2013 A.5.1.1, A.12.1.1,
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	None	ISO/IEC 27001:2013 A.16.1.4, A.16.1.6
		DE.AE-3: Cybersecurity data are correlated from diverse information sources	None	ISO/IEC 27001:2013 A.6.1.4
		DE.AE-4: Impact of potential Cybersecurity events is determined.	None	ISO/IEC 27001:2013 A.17.1.1
		DE.AE-05: Incident alert thresholds are created	None	ISO/IEC 27001:2013 A.16.1.4
	Security Continuous Monitoring (CM):	DE.CM-1: The network is monitored to detect potential Cybersecurity events	ISO/IEC 27001 A.10.10.2, A.10.10.4, A.10.10.5	ISO/IEC 27001:2013 A.13.1.1, A.13.1.2, A.12.4.1
		DE.CM-2: The physical environment is monitored to detect potential Cybersecurity events	None	ISO/IEC 27001:2013 A.11.1.4
		DE.CM-3: Personnel activity is monitored to detect potential Cybersecurity events	None	ISO/IEC 27001:2013 A.8.1.3

Function	Category	Sub category	Informative references	
		DE.CM-4: Malicious code is detected	ISO/IEC 27001 A.10.4.1	ISO/IEC 27001:2013 A.12.2.1
		DE.CM-5: Unauthorized mobile code is detected	ISO/IEC 27001 A.10.4.2	ISO/IEC 27001:2013 A.12.6.2
		DE.CM-6: External service providers are monitored	ISO/IEC 27001 A.10.2.2	ISO/IEC 27001:2013 A.14.2.7, A.15.1, A.15.2
		DE.CM-7: Unauthorized resources are monitored	None	ISO/IEC 27001:2013 A.6.2.1, A.8.1.2, A.12.1.3
		DE.CM-8: Vulnerability assessments are performed	None	ISO/IEC 27001:2013 A.12.6.1, A.14.2.8, A.18.2.3
	Detection Processes (DP):	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	None	ISO/IEC 27001:2013 A.16.1.1, A.6.1.2
		DE.DP-2: Detection activities comply with all applicable requirements, including those related to privacy and civil liberties	None	None
		DE.DP-3: Detection processes are exercised to ensure readiness	None	None
		DE.DP-4: Event detection information is communicated to appropriate parties	None	None
		DE.DP-5: Detection processes are continuously improved	None	None
	RESPOND (RS)	Response Planning (RP):	RS.PL-1: Response plan is implemented during or after an event.	None
Communications (CO):		RS.CO-1: Personnel know their roles and order of operations when a response is needed	ISO/IEC 27001 A.13.2.1	ISO/IEC 27001:2013 A.16.1.1
		RS.CO-2: Events are reported consistent with established criteria	ISO/IEC 27001 A.13.1.1, A.13.1.2	ISO/IEC 27001:2013 A.16.1.2, A.16.1.3

Function	Category	Sub category	Informative references		
		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	ISO/IEC 27001:2013 A.16.1.5	
		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	ISO/IEC 27001:2013 A.7.1.2, A.7.2.1, A.16.1.1, A.6.1.3	
		RS.CO-5: Voluntary coordination occurs with external stakeholders (ex, business partners, information sharing and analysis centers, customers)	None	ISO/IEC 27001:2013 A.6.1.4, A.15.1.1	
		Analysis (AN):	RS.AN-1: Notifications from the detection system are investigated	ISO/IEC 27001 A.6.2.1	ISO/IEC 27001:2013 A.16.1.4, A.16.1.5
			RS.AN-2: Understand the impact of the incident	ISO/IEC 27001 A.6.2.1	ISO/IEC 27001:2013 A.16.1.5
	RS.AN-3: Forensics are performed		ISO/IEC 27001 A.13.2.2, A.13.2.3	ISO/IEC 27001:2013 A.16.1.6, A.6.1.7	
	RS.AN-4: Incidents are classified consistent with response plans		ISO/IEC 27001 A.13.2.2	ISO/IEC 27001:2013 A.16.1.1, A.16.1.4	
	Mitigation (MI):	RS.MI-1: Incidents are contained	ISO/IEC 27001 A.3.6, A.13.2.3	ISO/IEC 27001:2013 A.16.1.7	
		RS.MI-2: Incidents are eradicated	None	ISO/IEC 27001:2013 A.16.1.6	
	Improvements (IM):	RS.IM-1: Response plans incorporate lessons learned	ISO/IEC 27001 A.13.2.2	ISO/IEC 27001:2013 A.16.1.5, A.16.1.6	
		RS.IM-2: Response strategies are updated	None	ISO/IEC 27001:2013 A.16.1.1, A.16.1.6	
	RECOVER (RC)	Recovery Planning (RP):	RC.RP-1: Recovery plan is executed	ISO/IEC 27001 A.14.1.3, A.14.1.4, A.14.1.5	ISO/IEC 27001:2013 A.17.1.2, A.17.1.3
		Improvements (IM):	RC.IM-1: Plans are updated with	ISO/IEC 27001 13.2.2	ISO/IEC 27001:2013

Function	Category	Sub category	Informative references	
		lessons learned		A.17.1.3
		RC.IM-2: Recovery strategy is updated	None	None
	Communications (CO):	RC.CO-1: Public Relations are managed		ISO/IEC 27001:2013 A.6.1.3, A.6.1.4,
		RC.CO-2: Reputation after an event is repaired	None	None