From: Jackie Krzyzewski
Sent: Tuesday, December 19, 2017 4:32 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Submission on the Draft CSF Framework published in January 2017

Dear Sir/Madam,

Please find attached my submission on the draft CSF Framework which is offered for your consideration.

Best regards

Jackie Krzyzewski
Director
SAM for Compliance Ltd
www.samcompliance.co

[*Attachment copied below*]

NIST CYBER SECURITY FRAMEWORK SUBMISSION

I am a huge supporter of the NIST Cyber Security Framework. I have worked extensively with the CSF framework and I would like to propose changes to the Draft framework published on 10 January 2017 including the introduction of an additional function called MANAGE. This would fit in-between IDENTIFY and PROTECT.

MANAGE is utilised where appropriate levels of cybersecurity are maintained through good management practices, strong governance and establishment and implementation of effective processes and procedures as determined by the organisation.

PROTECT is utilised where the threat or vulnerability is outside of the control of the organisation and cannot be mitigated through acceptable use requirements and good management. The Function PROTECT requires the organization to implement appropriate technology (e.g., hardware, software and services) and effective configuration of systems and protection mechanisms in order to mitigate cybersecurity risk.

I propose the following for your consideration:

IDENTIFY

Asset Management

Subcategories AM.1-AM.5 are all well positioned within the function IDENTIFY and Category - Asset Management.

Subcategory AM.6 should be removed as this can easily be incorporated into an amended ID.GV.2. Cybersecurity roles and responsibilities are referred to in Asset Management, Detection Processes and Governance. It is good governance to ensure that the entire workforce have cybersecurity responsibilities established and it is good management to ensure that this is implemented through HR and awareness and training procedures and processes.

Business Environment

Subcategories BE.1-BE.5 are all well positioned within the function IDENTIFY and Category – Business Environment

Governance

Governance subcategories GV.1 – GV.4 should be moved to the new MANAGE function

Subcategory GV.2 should state that Information and cybersecurity roles and responsibilities are assigned for all staff and coordinated and aligned with internal roles and external partners.

Risk Assessment

Subcategories RA.1 – RA.6 are all well positioned within the function IDENTIFY and Category – Risk Assessment. RA.6 should include that Risk responses should be documented within the Response Plan.

Risk Management and Supply Chain Risk Management

The categories of Risk Management (RM.1 – RM.3) and Supply Chain Risk Management (SC.1 – SC.4) may be considered as management functions and be moved to MANAGE rather than IDENTIFY. These both relate to the management of the risk rather than the identification of the risk.

Supply Chain Sub Category SC.5 relates to response and recovery planning and should perhaps be removed from here and referenced in those function areas.

PROTECT

Access Control

Areas of access control that relate to user management – e.g., user registration/de-registration, user access provisioning, review of access rights, adjustment and removal of access rights, administrator rights management, restriction of access to information, network resources and services, program source code, utility programs, etc should be moved to the MANAGE function as it is the organisation that determines who, what, when and how users, systems and services access their system resources. Therefore Access Control Sub-categories AC.1 and AC.4 may be moved to the MANAGE area in a new category called Access Management

Access Control Sub-categories AC.2, AC.3, AC.5 and AC.6 all require systems, equipment or technology to facilitate, control and manage the access and therefore should remain within the PROTECT function within the category Access Control.

Awareness and Training

The category of Awareness and Training (AT.1 – AT.5) is a management activity and should therefore be moved to the function MANAGE. The organisation is responsible for this and should have programs in place which are managed and implemented to ensure users have the appropriate understanding of their cybersecurity responsibilities as stated in ID.GV.2.

Data Security

The Category description should remove the word managed and this should be replaced with protected so that it aligns with the function PROTECT.

As DS.1 – DS.8 all rely on some mechanism to enable the protection, e.g., encryption, classification mechanisms, USB control and management systems, information management systems, Integrity checking mechanisms, exfiltration identification mechanisms, content filtering systems, network segregation, capacity and bandwidth management systems. Therefore, I believe this Category is well positioned within the PROTECT function.

Information Protection Processes and Procedures

This whole Category including sub categories IP.1 – IP.8, IP11 and IP12 should be incorporated under the MANAGE function as it involves the establishment and implementation of policies, processes and procedures to support the effective management of systems, and infers the creation of documentation, the assignment of responsibilities and the implementation of procedure and processes so that systems are effectively maintained and managed in a manner that allows the organization business to run effectively and efficiently.

PR.IP.9 should be incorporated under Response and Recovery Planning.

PR.IP.10 should be incorporated under Response and Recovery planning

Note: It is confusing to have the development and testing of the plans in IP and the activity around respond and recover in their respective functions especially as Risk Management plan is in the Risk Management Category. This change gives the framework better consistency.

Maintenance

Regular maintenance carried out in accordance with policies and procedures may also be considered a MANAGE function. Preventative maintenance is good management practice to ensure that systems are not prone to downtime or degradation of performance. Therefore Maintenance, with Subcategories MA.1 and MA.2 should be moved to the function MANAGE.

Protective Technology

This whole Category (Subcategories PT.1 – PT.5) relates to the implementation and correct configuration of technology to ensure the security and resilience of systems and therefore is well positioned within the function PROTECT.

DETECT

Anomalies and Events

It could be argued that subcategory AE.1 may be better positioned within the IDENTIFY function as an organisation needs to identify and profile what its normal network operation and expected data flows are before it can understand what is an anomaly. Perhaps this could replace ID.AM.6

The wording for a new Subcategory AE.1 may be something along the lines that "Anomalous activity within systems is detected and recorded in logs. If the information is not first collected then it cannot be aggregated, correlated and analysed.

Subcategory AE.2 and AE.3 should be switched around. The information should first be collected (AE.1), then aggregated and correlated so that it can subsequently be effectively analysed (AE.3)

Subcategory AE.4 is OK here but it is close related to ID.RA.4.

Subcategory AE.5 should remain in this section but is closely related to ID.RA.6 which identifies and prioritizes risk responses. The trigger point(s) that determines when an identified anomaly becomes an incident or event should be included in the risk responses and in the Response Plan.

Continuous Monitoring

Subcategory CM.1 – CM.8 are well positioned within the DETECT function and Continuous Monitoring category.

Detection Processes

Subcategory DP.1 is able to be covered by ID.GV.2 so should be removed.

Subcategory DP.2 is a bit vague as to what the applicable requirements are. NIST SP 800-53 CA-2 refers to internal assessments so it could be construed that the applicable requirements could be derived from the security and privacy assessment plan, however SI-4 doesn't offer any clarity at all. It would be helpful if you could expand the description for this Subcategory.

Subcategories DP.3 – DP.5 are well positioned within the DETECT function and Detection Processes category

RESPOND

Response Planning

It would be helpful to have the first Subcategory RP.1 being that the organisation should have a documented response plan that can be executed if required and this should include supply chain partners where appropriate. Incorporate wording from PR.IP.9

An additional item RP.2 should state that Response plans are tested regularly to ensure that they will work if needed. This was PR.IP.10

Refer to my commentary in PROTECT, Information Protection Processes and Procedures.

Communications

Subcategory CO.1 should be moved into the Category Response Planning. Part of organizational planning should be to ensure that the organization has the personnel they need to respond and that these people have the knowledge and skills to be effective.

Subcategories CO.2 and CO.4 are well placed within the RESPOND Function and Communications category. It might be noted that CO.4 would include aspects of CO.5 as information would need to be shared in order to achieve a coordinated effort with external stakeholders.

Subcategories CO.3 and CO.5 should be combined as any requirement for voluntary sharing of information would also be documented within the response plan – e.g. CERT.

Analysis

Subcategory AN.1 should be clarified and perhaps state that: Detected events are investigated.

This is due to already stating that notifications are to be analysed in DE.AE.2

Subcategory AN.3 should perhaps be next and state that: Forensic analysis is performed on systems if necessary to gather in-depth information about the event and evidence if required for disciplinary or legal action

Subcategory AN.2 should be moved to here and clarified, perhaps stating that: Information gathered is analysed so that the scope and the scale of the event is understood together with its impact on organisational performance

Subcategory AN.4 should perhaps include: Incidents are categorized consistent with response plans and assigned the appropriate risk responses as documented in ID.RA.6.

Mitigation

Subcategory MI.1 – MI.3 are well positioned within the RESPOND function and Mitigation category.

Improvement

Subcategory IM.1 – IM.2 are well positioned within the RESPOND function and Improvements category

RECOVER

Recovery Planning

It would be helpful to have the first Subcategory RP.1 being that the organisation should have a documented recovery plan that can be executed if required. Incorporate wording from PR.IP.9

RP.2 should be derived from PR.IP.10 – Recovery Plans should be tested as and when appropriate

I believe a new sub-category should be included here RP.3 that states that: The organisation ensures that it has the resources available to effect an efficient recovery. This would include backups being available, alternative site if required, appropriate resources and appropriate technology and equipment.

Logically Communications RC.CO should come before Improvements RC.IM. in the structure as it does in Respond.

Communications

Subcategory CO.3 should perhaps be the first item and should include external stakeholders where required.

Subcategory CO.1 should perhaps include a reference to a Public relations communication strategy and should be combined with CO.2 as the public relations strategy would determine the communication requirements for repairing the organisation's reputation.

Improvements

Subcategories IM.1 – IM.2 are well positioned within the RECOVER function and improvements category.

PROPOSED STRUCTURE TOPOLOGY

SUMMARY OF IDENTIFY FUNCTION (Know and understand your environment)

Category AM – ID.AM.1 – ID.AM.6 with ID.AM.6 being the old DE.AE.1

Category BE – ID.BE.1 – ID.BE.5

Category RA – ID.RA.1- ID.RA.6

SUMMARY OF MANAGE FUNCTION (Effectively manage your environment)

Category AM* – MN.AM.1 and MN.AM.4 *New Access Management Category

Category AT – MN.AT.1 – MN.AT.5 – Awareness and Training

Category GV – MN.GV.1 – MN.GV.4 - Governance

Category IP – MN.IP.1 – MN.IP.8, MN.IP.11 – MN.IP.12 – Information Protection Processes and Procedures

Category MA – MN.MA.1 – MN.MA.2 - Maintenance

Category RM – MN.RM.1 – MN.RM.3 – Risk Management

Category SC – MN.SC.1 – MN.SC.4 – Supply Chain Risk Management

SUMMARY OF PROTECT FUNCTION (Protect your environment)

Category AC – PR.AC.2 – PR.AC.3, PR.AC.5 – PR.AC.6

Category DS – PR.DS.1 – PR.DS.8

Category PT – PR.PT.1 – PR.PT.5

SUMMARY OF DETECT FUNCTION (Detect anomalous activity within your environment)

Category AE – DE.AE.1 – DE.AE.5

Category CM – DE.CM.1 – DE.CM.8

Category DE – DE.DP.2 – DE.DP.5

SUMMARY OF RESPOND FUNCTION (Respond to anomalous activity within your environment)

Category RP – RS.RP.1 – RS.RP.3 which includes RP.1 (amended), RP.2 derived from IP.10 and CO.1.

Category CO – RS.CO.1 – RS.CO.3 which includes CO.2, CO.4 and a combined CO.3/CO.5

Category AN – RS.AN.1 – RS.AN.4

Category MI – RS.MI.1 – RS.MI.2

Category IM – RS.IM.1 – RS.IM.2

SUMMARY OF RECOVER FUNCTION (Recover from incidents and events)

Category RP – RC.RP.1 – RC.RP.3 which includes RP.1 (amended), RP.2 derived from IP.10 and a new RP3

Category CO – RC.CO.1 – RC.CO.2 – made up of CO.3 first then CO.1 and CO.2 combined.

Category IM – RC.IM.1 – RC.IM.2