Microsoft Corporation
One Microsoft Way
[redacted]

[redacted]

Microsoft

March 17, 2023

Emailed to

National Institute of Standards and Technology
United States Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

Subject: Microsoft Comments on the NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

Introduction

Microsoft welcomes the opportunity to provide feedback to the National Institute of Standards and Technology (NIST) regarding the request for public comment for the NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework. Microsoft commends NIST on its commitment to public-private partnership and industry engagement while developing and updating the "Framework for Improving Critical Infrastructure Cybersecurity" ("Framework" or "CSF") versions 1.0, 1.1, and 2.0.

As a provider of technology products and services to more than one billion customers in the United States and worldwide, Microsoft recognizes the importance of and invests in developing, maturing, and promoting cybersecurity best practices, both internally and across the industry. Since the inception of the Framework development process in 2013, Microsoft has been a committed partner, sharing insights that we have acquired through our experiences and partnerships and that are relevant to the Framework's approach. Additionally, we have worked diligently to raise awareness and promote the implementation of the Framework. In recent comments to NIST regarding cybersecurity resources, among other recommendations, we underlined the importance of driving cohesion, interoperability, and simplicity and strengthening awareness and understanding across multiple audiences.

On CSF 2.0, Microsoft applauds NIST for its comprehensive review and analysis of industry comments as reflected by the breadth of proposed updates in the Concept Paper. This revision is critically important to the ongoing value of the Framework, but it is also complicated by heightened threats and an evolving regulatory landscape. NIST also faces the challenge of meeting the needs of a variety of Framework users, including critical infrastructure owners and operators; federal and state regulators; and small and medium-sized businesses. Moreover, in

this update, NIST is tackling complex issues like cybersecurity supply chain risk management amidst growing use of advanced, interconnected technologies while also seeking to retain the Framework's flexibility, strengthen its interoperability with NIST and global resources, and future proof its approach. This revision is a significant undertaking, and we welcome ongoing collaboration and partnership with NIST to help ensure CSF 2.0 is successful.

Given the challenges that NIST faces with this revision, we offer the following comments on the Concept Paper, conveying our perspective on four key areas: 1) the general approach of the Framework; 2) updates to the Framework's content, including across the Core and Implementation Tiers; 3) guidance, resources, and tools that can help drive adoption and effective implementation of the Framework; and 4) processes for strengthening the agility of and partnership on the Framework going forward.

I. The Framework approach: Maintaining broad applicability and simplicity and driving cohesion as a "framework" while also accounting for key communities and initiatives

Microsoft agrees that CSF 2.0 should remain a framework that provides context and connections to existing standards and resources. More specifically, NIST should retain the current level of detail in the framework, relate the CSF clearly to other NIST frameworks, leverage Cybersecurity and Privacy Reference Tool (CPRT) for an online CSF 2.0 Core, and use updatable, online informative references to provide more guidance to implement the CSF. However, responsiveness to key communities, such as critical infrastructure organizations, and initiatives, such as procurement requirements or regulatory developments, will help to ensure CSF 2.0 remains relevant to and integrated within a dynamic policy environment.

Providing context and connections to existing standards and resources

Microsoft agrees that NIST should keep other cybersecurity- and privacy related frameworks separate and distinct from CSF 2.0, providing dedicated guidance to each framework as it relates to the CSF. Mappings between frameworks and standards could be presented separately, ensuring CSF 2.0 retains its user friendliness and simplicity. In addition, a companion document that goes beyond 1:1 mappings could provide guidance on how to use all relevant frameworks (e.g., CSF 2.0, Software Secure Development Framework (SSDF v1.1), Risk Management Framework (RMF), Artificial Intelligence Framework (AI RMF 1.0), Privacy Framework) to manage organizational risk. NIST Interagency Report 8170 could serve as a model for such a document.

Microsoft supports NIST adopting online and updatable references and the development of the Cybersecurity and Privacy Reference Tool (CPRT) to support the Framework as a living document. The development of the CPRT is in its infancy, so NIST should allow for several rounds of industry feedback and engagement with the tool. NIST can provide education on the tool, demonstrating how it can be used to navigate and discover relationships and dependencies among the datasets and build profiles, overlays, baselines, and templates based on the NIST-referenced data in the CPRT.

Microsoft further supports NIST's efforts to grow and strengthen the inventory of informative references for use with CSF 2.0, not only helping users understand interrelationships across guidance documents and requirements but also helping to reinforce the role and profile of the Framework. Strengthening crosswalks to other international risk-based standards, such as ISO standards, both in the Core and more broadly in explaining how to use the Framework, promotes interoperability and innovation. To support strengthening the inventory of informative references, Microsoft welcomes the opportunity to provide resources such as the Microsoft Cloud Security Benchmark (formerly, Azure Security Benchmark) mapping to CSF 2.0 for cloud security guidance. In addition, Microsoft recently joined the Charter of Trust, a coalition of organizations working together to promote principles for a safer and more secure digital world. The Charter of Trust has developed 17 baseline requirements to guide organizations in developing a secure supplier program. These principles are founded on a risk-based cybersecurity approach and derived from international standards and best practices, including NIST CSFv1.1, ISO 27001, ISO 20243, and IEC 62443. We welcome the opportunity, in partnership with the Charter of Trust and NIST, to validate mapping to CSF 2.0 for broader use.

We encourage NIST to continue working closely with U.S. government partners, driving alignment across cybersecurity risk management efforts. We recommend NIST consider how to integrate or align CISA's Cross Sector Performance Goals (CPGs) with CSF 2.0, potentially as an informative reference; enabling use of the CPRT tool to understand the relationship between CSF 2.0 and CPGs could be particularly helpful for small and medium-sized businesses. Demonstrating alignment with the Cybersecurity Maturity Model Certification (CMMC) would also significantly benefit U.S. government contractors and help support approaches to security compliance grounded in cybersecurity risk management.

Recognizing the Framework's broad use and developing a profile for critical infrastructure

Microsoft supports continuing to broaden CSF 2.0 use across sectors and types and sizes of organizations globally, helping to provide a common language for discussing cybersecurity risk management. We understand NIST's efforts to widen the scope of CSF 2.0 to include organizations in government, industry, and academia.

However, Microsoft recommends that special attention be maintained for critical infrastructure as part of the NIST CSF 2.0 update process. Key strengths of the Framework v1.1 include the relevance of its cybersecurity risk management practices for protecting a nation's most critical systems and the consistent approach it facilitates across entities more often subject to regulation. Microsoft recommends NIST go further than the statement in the Concept Paper "that references to critical infrastructure in the CSF may be maintained as examples." NIST could facilitate ongoing use of the Framework for critical infrastructure cybersecurity risk management practices and regulatory developments by developing a "Critical Infrastructure Profile" of CSF 2.0. Such a profile could continue to be leveraged as an effective starting point for sector-

specific profiles, building on a roadmap specifically tailored toward reducing cybersecurity risk for owners and operators of critical infrastructure.

II. Updates to the Framework's content: Adding a Govern Function, integrating supply chain risk management, and clarifying and evolving Implementation Tiers

Microsoft supports the inclusion of a Govern Function in CSF 2.0 to strengthen alignment of an organization's security function to its business strategy, goals, missions, and objectives. The inclusion of a Govern Function will also drive alignment and interoperability with other NIST resources, such as the Privacy Framework and AI RMF. Furthermore, Microsoft reiterates its recommendation to integrate supply chain risk management across the entire Framework Core – including Functions, Categories and Subcategories – to allow for a cohesive and integrated approach. The increasing complexity of supply chains makes it imperative that an organization's governing body not only has oversight and responsibility of supply chain risk management as part of its broader cybersecurity risk management strategy but also visibility into implementation across risk management activities. We recommend that oversight of supply chain risk management is addressed through Categories or Subcategories in the Govern Function while further strengthening supply chain risk management outcomes throughout the rest of the five Functions. In addition, we support NIST's intention to provide more clarity and guidance on Tiers.

Emphasizing the importance of governance in CSF 2.0

In our April 2022 submission to NIST in response to the CSF 2.0 RFI, we recommended that NIST evaluate whether the existing Governance Category is sufficient to address an organization's overall security risk management or if there might be value in adding a Govern Function given ecosystem trends and opportunities to align with other resources. We commend NIST's efforts to explore the inclusion of a Govern Function in CSF 2.0 and appreciate the opportunity to contribute to the governance discussions during the February 2023 working sessions. Cybersecurity is a business enabler, and it is critical that practitioners have a clear understanding of how their security decisions fully align with an organization's business strategy, goals, mission, and objectives. Misalignment of cybersecurity and broader organizational decisions could result in serious business (including compliance and regulatory), operational, and security risks. Effective cybersecurity culture starts at the top, through the implementation of effective cybersecurity governance. Increasing interest from regulators on boards taking responsibility for cybersecurity, as well as increasingly complex supply chain interconnections and emerging threats and technology, require governance to be at the helm of cybersecurity risk management practices. As identified in the AI RMF, "attention to governance is a continual and intrinsic requirement for effective AI risk management over an AI system's lifespan and the organization's hierarchy." The same should apply to operational cybersecurity risk management. Similarly, the NIST Privacy Framework states: "The Govern-P Function is similarly foundational but focuses on organizational-level activities such as establishing organizational privacy values and policies,

identifying legal/regulatory requirements, and understanding organizational risk tolerance that enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs."

In developing a Govern Function in CSF 2.0, NIST should align with the Govern Function in the AI RMF and the Privacy Framework. Microsoft also recommends NIST reference the Cyber Risk Institute (CRI) Profile's Govern Function, which effectively identifies outcomes that should be achieved by a board or relevant governing body to manage the oversight of cyber risk. We further recommend that NIST includes supply chain risk management considerations in the Govern Function regardless of how it chooses to integrate supply chain risk management across the entire Framework (i.e., developing a Function for supply chain risk management vs. expanding the supply chain risk management Category vs. integrating supply chain risk management across the Framework Core). Below, we offer additional comments regarding the intersection of supply chain risk management and governance.

Using a holistic approach to integrate supply chain risk management into the Framework

Microsoft supports NIST's efforts to emphasize supply chain risk management in CSF 2.0. In our April 2022 comments to NIST, we recommended that supply chain risk should be considered across all appropriate Functions of the Framework, not just the Identify Function. Doing so shouldn't mean that supply chain risk management overwhelms the Framework; instead, it could result in a more holistic approach throughout the Framework Core.

We believe that the challenge of holistically incorporating supply chain risk management into the Framework lies in striking the right balance between elevating supply chain risk management at the governance level and addressing supply chain risk management across an organization's operational cybersecurity activities. Firstly, we recommend that supply chain risk management be a vital component of a cybersecurity risk management strategy – designated, approved, and monitored by an organization's governing processes (i.e., in the new Govern Function). Secondly, due to the pervasive nature of supply chains, it should be addressed across other Functions of the Framework, i.e., identify, assess, protect, respond, and recover.

As stated above, we support the inclusion of a Govern Function, within which oversight of supply chain risk management activities should be included. CSF 2.0 could build upon the approach in CSF v1.1 and the CRI Profile's Govern Function to address supply chain risk management oversight. For example, the CRI Profile's GV. RR states: "The organization has designated appropriate roles and responsibilities, including an individual responsible for cybersecurity for the organization." NIST CSF v1.1 ID.AM-6 likewise states: "Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established." The Govern Function or a Category within a CSF 2.0 Govern Function could integrate these approaches, stating: "The organization has designated appropriate roles and responsibilities, including an individual responsible for cybersecurity for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) for the organization." The same approach could be taken to address risk management, policy, programmatic roles, and responsibilities Categories developed in the Govern Function.

Supply chain risk management requires both governance and execution. The new Govern Function should stay focused on cyber risk oversight responsibility and not encroach on management and operations of cybersecurity. NIST should also integrate supply chain risk management across other Functions of the Framework. The integration of activities included in CSF v1.1's supply chain Category could also be revisited. For example:

- ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.
    - Recommendation: Move to the Govern function.
- ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.
    - Recommendation: Keep in Identify Function but move to the Asset Management Category.
- ID.SC-3- Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity programs and Cyber Supply Chain Risk Management Plan.
    - Recommendation: Keep in the Identify function.
- ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
    - Recommendation: Move to Detect Function's Monitoring Category.
- ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.
    - Recommendation: Move the response portion to the Respond Function and Response Planning subcategory and the recovery portion to the Recover Function and Recovery planning Category.

NIST can also help strengthen alignment across other NIST resources broader U.S. government supply chain security policy developments and references, such as the SSDF v1.1 and Executive Order 14028, to account for more organizations being both developers and consumers of software and other supply chain components and artifacts. To that end, we recommend that NIST include SSDF v1.1 as an informative reference for use with CSF 2.0. In addition, NIST should include the SSDF v1.1 in the introduction of the NIST CSF to increase awareness of the SSDF v1.1 as a resource for secure software development practices and help organizations understand how the resources are different but complementary.

In a previous submission to NIST, we shared that Microsoft, in collaboration with other companies, has joined with the Open Source Security Foundation (OpenSSF) to discover, construct, and suggest strategies to safeguard open source software and supply chains. We reiterate our recommendation that NIST considers the distinct supply chain risk management challenges for enterprises that consume (and produce) open source and provides recommendations regarding how to customize relevant supply chain risk management practices. We also recommend that NIST interacts with open source communities, such as via the

OpenSSF, to develop and get feedback on that guidance. Microsoft welcomes the opportunity to collaborate on such an effort with NIST and OpenSSF.

Strengthen and clarify Framework Tiers

Microsoft supports NIST's plan to provide more clarity and guidance on Tiers. We recommend that NIST updates the Tier definitions in the Framework to make them easier to implement and to help facilitate continuous improvement not only across but also within each Tier. The Current Profile and Target Profile definitions should be simplified to explicitly state that they are designated Implementation Tier levels, with more guidance provided to help organizations assess whether they are meeting Tier definitions.

Additionally, evolution of the current Tier levels may help foster measurement of continuous improvement, especially for organizations that use the Framework over an extended time. A new Tier 4, called 'Managed,' could describe cybersecurity risk management practices that address cybersecurity risk in a repeatable manner, i.e., Tier 1 (partial), Tier 2 (risk informed), Tier 3 (repeatable), Tier 4 (managed), and Tier 5 (adaptive). Adding an additional Tier raises the security bar for organizations, supports CSF 2.0's broad applicability, and reinforces continuous improvement over time. Not every organization's threat, legal and regulatory and business environment requires a target profile to be adaptive. A "Managed" Tier can set the appropriate cybersecurity risk management target for organizations managing cybersecurity risk proactively in a repeatable manner without extensive automation of cybersecurity practices while raising the bar for organizations targeting the "Adaptive" Tier. Ultimately, the overall goal should remain driving continuous improvement and assisting organizations in gaining a solid understanding of and confidence in what it takes to meet their Tier determinations.

III. Guidance, resources, and tools: Driving adoption and effective implementation with a CSF 2.0 ecosystem

Microsoft commends NIST's efforts to expand and improve guidance for implementing the CSF by adding notional examples in CSF 2.0. As a committed partner, we have attached a comprehensive list of implementation questions to serve as guidance or for inclusion as appropriate in the Framework. These questions can increase clarity and consistency for practitioners implementing outcomes in the Framework Categories. In addition, Microsoft has mapped CSF v1.1 to Microsoft Cloud Security Benchmark (MCSB v1) and welcomes the opportunity to include this resource in the National Online Informative References (OLIR) Program.

We also note that Profiles are an underutilized resource that could support further adoption of the Framework across diverse cybersecurity stakeholders, both domestic and international. We support NIST's efforts to broaden the applicability of CSF 2.0 and believe that Profiles can support and build on this effort. To increase the use and development of Profiles and other related extensions, we support NIST in creating clear guidance to foster the development of

Profiles to address sector-specific risks, technologies, and threat scenarios. As highlighted above, Microsoft recommends NIST develop a "Critical Infrastructure Profile" to support the Framework's transition from focusing on critical infrastructure to a broader audience. In addition, Microsoft welcomes the opportunity to work with industry and NIST to create a cloud profile extension, leveraging CRI's efforts to develop the CRI Profile Cloud Extension, which provides cloud-specific guidance for assessing security responsibilities and cyber risk.

Develop practical implementation guidance for the CSF 2.0

Microsoft supports NIST's efforts to provide implementation guidance to support practitioners in scoping and assessing their implementation of activities associated with the Framework's Core, including at the Subcategory level. Practical implementation guidance in the form of notional implementation examples or implementation questions can foster clarity, consistency, efficiency, compliance, and shared learning in implementing security outcomes described in the Framework Subcategories.

Microsoft supports developing notional implementation examples similar to the SSDF V1.1. In addition, we recommend that NIST explores the use of implementation questions for assessing Subcategories, using a people, process, and technology framework. The implementation questions should determine who is responsible for implementation, monitoring, and review. In addition, implementation questions should consider the process involved and whether it is documented, disseminated, and frequently updated. When technology is involved, implementation questions should capture whether the configuration meets the security objectives of the Subcategory and to what degree (i.e., autonomous vs manual). Specifically, the people, process, and technology framework could be applied to developing an implementation question that asks the following questions of each Subcategory:

- Responsibility: Who is responsible for implementing the Subcategory?
- Process: Are there processes and procedures in place and are they documented?
- Impact: Does the action meet the security outcome?
- Frequency: If there is a timing or frequency element of the security outcome, is it in place and is it documented?
- Review: Is the control being reviewed?

See Appendix for examples of implementation questions that could aid practitioners in achieving the security outcomes set out in CSF v1.1. These implementation examples could inform the development of notional implementation examples.

For each implementation example, answers corresponding to different CSF Tiers can be provided to support the user in considering how a process or control is implemented, along with an explanation of the level of implementation maturity corresponding to which CSF Tier.

Microsoft recommends notional implementation examples and implementation questions are provided in a companion document separate from CSF 2.0. Including detailed practical

implementation guidance in the body of CSF 2.0 could make it cumbersome and difficult to use.

Develop CSF Profile implementation guidance

Microsoft supports NIST's efforts to retain a technology- and vendor-neutral approach to CSF 2.0; additional guidance tailoring for specific technologies may be best accomplished by CSF profiles, mappings, and standards. We believe that a CSF Profile can be a powerful tool that builds on the Framework's flexibility to develop tailored guidance to specific scenarios, from sector-specific regulatory requirements to technologies to threat scenarios. Guidance on CSF Profiles can be developed to increase consistency, interoperability, and use of the Framework. Profile development and implementation guidance should address the following questions:

- Who can develop a Profile (i.e., an organization, a person, a group, etc.)?
- Is there a suggested Profile development methodology?
- Is there a process to approve the Profile by NIST? For example, there is a process via the OLIR program for approving informative references. Is there a similar process for Profiles?
- Is there a process for updating Profiles published on NIST's website?

Develop a cloud security extension to support consistency across sectoral profile development

In our April 2022 CSF 2.0 comments to NIST, we recommended the development of a cross-sector cloud profile to provide additional resources to support operational security of cloud deployments. Along with other cloud providers, Microsoft provided feedback to CRI on its development of the CRI Cloud Profile Extension. The Extension provides additional guidance to financial services organizations to strengthen existing cybersecurity systems or support the implementation of new cloud technologies and operations. The Extension particularly helps clarify the shared responsibility model of cloud deployments, leveraging the Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM) v4.0. While the CRI Cloud Profile Extension is developed for the financial services industry, a similar "Cross-Sector Cloud Extension" could support consistency across sectoral profile development efforts. A Cross-Sector Cloud Extension can be layered on existing or new sector-specific profiles to assess security responsibilities for deployment of cloud technologies. Microsoft welcomes the opportunity to work with NIST, industry bodies such as the IT Sector Coordinating Council (IT SCC), and standards bodies to develop a cloud extension to be used as an extension to sectoral profiles needing cloud guidance.

Our Microsoft NIST CSF success story

Microsoft is encouraged by NIST's efforts to place greater emphasis on success stories to demonstrate the benefits of the Framework and build global confidence in its use. We believe success stories can be a powerful tool for driving adoption of the Framework and share our story so others may gain insights for their own cybersecurity initiatives. We welcome inclusion of any of the content below for publication on the NIST CSF success stories webpage.

As a global technology company and recognized leader in cybersecurity, Microsoft is committed to helping to protect our interconnected digital systems by investing in and promoting safer and more secure computing environments and risk management practices. Since 2014, Microsoft has used the NIST Cybersecurity Framework to assess the company's security capability. We regularly conduct assessments, covering a broad mix of customer-facing and internal infrastructure services across the enterprise, and the assessments are the foundation for comprehensive, internal business discussions about security that extend from operational levels to senior leadership and the company's Board of Directors. The Cybersecurity Framework serves as a vehicle to enable such discussions about Microsoft's security profile across organizational silos and subcultures and to bring leaders together to talk about critical capability as well as aspirations and future investments in a risk-based format. The Cybersecurity Framework's interoperability and strong alignment with global best practices and reference points, including ISO/IEC 27103 and ISO/IEC 27001, also provide security benefits. Microsoft uses the Cybersecurity Framework to develop a unified view of security capability using an external standard and to reconcile multiple security approaches and compliance requirements. While maintaining strict alignment with the Cybersecurity Framework structure, Microsoft appreciates the Framework's flexibility to integrate with multiple informative references (e.g., ISO 27001) and global approaches (i.e., ISO/IEC 27103). Because of its flexibility and interoperability, Microsoft has been able to adopt and benefit from the Framework in a way that limits operational disruption and results in minimal duplication of efforts. Our investment in the Framework is tailored to existing operational approaches and focused on security capability. For example, we group services into self-defined pillars to enable aggregation and comparison, thus acknowledging and enabling differentiation between types of services. Microsoft also actively uses the NIST Cybersecurity Framework concept of a Target Profile. This allows for a focused measure of security capability and enables us to discuss priorities and track gaps as well as progress over time, thereby supporting a continuous improvement culture.

IV. An ongoing evolution: Future proofing the Framework through innovative public-private partnership

We commend NIST's approach to public-private partnership and encourage NIST to continue to work with industry to find new ways of future-proofing the Framework. Rapid technological advancement, the ever-evolving threat landscape, and the deepening complexity of supply chains will demand higher levels of agility, flexibility, and speed from the cybersecurity community. We applaud NIST for its openness to industry feedback and encourage NIST to retain this approach while seeking news ways of adapting CSF 2.0.

Fostering robust industry engagement with new mechanisms to achieve a continuous feedback loop

Microsoft appreciates NIST's public-private partnership approach to revising the Framework. Through the process of developing and evolving CSF 1.0 and 1.1, workshops were valuable to sharing perspectives and understanding NIST's direction. Going forward, we suggest that NIST continue to leverage mechanisms outside of the RFI process to receive industry feedback during

2.0's development. We welcome NIST's planned Fall 2023 workshop after the release of the draft CSF 2.0. As warranted based on ongoing NIST efforts and industry perspectives beyond that time frame, NIST could also host virtual listening sessions to engage with partners and receive feedback before the anticipated final release of CSF 2.0 (e. in Winter 2024).

The evolving and dynamic threat and technological landscape will also continue to make it challenging to keep the Framework relevant and up to date. Major revisions such as the ongoing CSF 2.0 development process are occasionally necessary but can be time-consuming and complex. To stay current and respond to threats and technological advancements, NIST could also consider ongoing approaches to more minor updates to the Framework. Currently, the Cybersecurity & Infrastructure Security Agency (CISA) is testing a novel mechanism for providing a continuous feedback loop through the Cross-Sector Cybersecurity Performance Goals (CPGs) GitHub page. The IT SCC may also provide a good forum for continuous engagement on CSF 2.0 adjustments. Microsoft recommends NIST experiments with approaches that might support iterative processes to complement extensive revisions.

In conclusion

Microsoft is grateful for the opportunity to reiterate its commitment to collaborating with industry and government stakeholders over the long term to develop, use, and understand the impact of cybersecurity risk management approaches. We believe that public-private partnerships, international standards, and best practices, like those integrated into the Framework, are indispensable for advancing cybersecurity risk management globally.
Respectfully submitted,

Respectfully submitted,

Patricia Ephraim Eke
Principal Security Strategist, Customer Security and Trust
Corporate, External & Legal Affairs
Microsoft Corporation

SubcatID	SubCatQnumber	Question
ID.AM-1	ID.AM-1.1	Is there a SOP for the tracking of physical assets for the organization?
ID.AM-1	ID.AM-1.2	How often is this documentation reviewed?
ID.AM-1	ID.AM-1.3	Does the team leverage tools to keep an inventory of all physical devices?
ID.AM-1	ID.AM-1.4	How often is the inventory of physical devices audited?
ID.AM-2	ID.AM-2.1	Is there an SOP for the creation/maintenance of software platforms and application assets for the organization?
ID.AM-2	ID.AM-2.2	How often is this documentation reviewed?
ID.AM-2	ID.AM-2.3	Does the team leverage tools to keep an inventory of all Software platforms and applications?
ID.AM-2	ID.AM-2.4	How often is the inventory of the Software Platforms and applications audited?
ID.AM-3	ID.AM-3.1	Does the team have a map of the flow of data between all services within the organization? (i.e. data flow diagram)
ID.AM-3	ID.AM-3.2	How often is the map of the flow of data (Data Flow Diagram) reviewed as part of the threat assessments?
ID.AM-4	ID.AM-4.1	Is there a mobile device management program/tool implemented to keep an inventory of mobile assets?
ID.AM-5	ID.AM-5.1	Does the organization implement a data classification policy?
ID.AM-6	ID.AM-6.1	Are the roles and responsibilities clearly documented for the entire workforce including third-party stakeholders? (Suppliers, customers, partners)
ID.BE-1	ID.BE-1.1	Does the service have a policy in place to document procedures followed for managing supplier relationships (SOP)?
ID.BE-2	ID.BE-2.1	Is the organization’s place in critical infrastructure and its industry sector is identified and communicated?
ID.BE-3	ID.BE-3.1	Does the team have documentation around organizational mission, objectives, and activities?
ID.BE-4	ID.BE-4.1	Are there external dependencies on other teams to support the objectives for delivery of critical functions?
ID.BE-4	ID.BE-4.2	Does the team have proper documentation for contacts/communication plan with external dependencies for Incident Response or BCDR purposes?
ID.BE-5	ID.BE-5.1	<PR.IP-9.1>: Does the service have a BCDR plan?
ID.BE-5	ID.BE-5.2	How often is the BCDR plan reviewed and revised?
ID.BE-5	ID.BE-5.3	How often is the BCDR plan tested?
ID.GV-1	ID.GV-1.1	Does the service maintain SOPs in a centralized location? (Some SOPs include: Logical/Physical Access control, Log Management, Configuration Management, BCDR, Incident Response, Patch Management, Asset Management)
ID.GV-1	ID.GV-1.2	How often are the documentation reviewed?
ID.GV-2	ID.GV-2.1	Does the team have documentation that states the roles and responsibilities of all team members?

ID.GV-3	ID.GV-3.1	Does the team have a dependency on legal to assist with all legal and regulatory requirements?
ID.GV-4	ID.GV-4.1	Does the team have a risk management process defined?
ID.GV-4	ID.GV-4.2	How often are risk assessments conducted?
ID.RA-1	ID.RA-1.1	Does the team have a defined vulnerability management process?
ID.RA-1	ID.RA-1.2	<DE.CM-8.1>: Does the service conduct vulnerability scanning using tools?
ID.RA-1	ID.RA-1.3	Does the team have a central management system for alerts generated by the vulnerability scanner?
ID.RA-2	ID.RA-2.1	Does the service leverage other threat intelligence services to gather threat intel?
ID.RA-2	ID.RA-2.2	Does the service leverage information sharing forums and other open source feeds to gain threat intel?
ID.RA-3	ID.RA-3.1	Does the service incorporate threat modelling during their SDLC?
ID.RA-4	ID.RA-4.1	<ID.GV-4.1>: Does the team have a risk management process defined?
ID.RA-5	ID.RA-5.1	<ID.GV-4.1>: Does the team have a risk management process defined?
ID.RA-6	ID.RA-6.1	Does the service follow the risk mitigation process provided by the risk management team?
ID.RM-1	ID.RM-1.1	<ID.GV-4.1>: Does the team have a risk management process defined?
ID.RM-2	ID.RM-2.1	Has the leadership team determined a risk tolerance level?
ID.RM-2	ID.RM-2.2	Is the risk tolerance level clearly documented (via reporting dashboard, risk reports, etc)?
ID.RM-3	ID.RM-3.1	<ID.RM-2.2>: Is the risk tolerance level clearly documented (via reporting dashboard, risk reports, etc.)?
ID. SC-1	ID. SC-1.1	During the risk assessment, have risks around supply chain management been addressed? Supply chain as defined above (ie procurement of media, devices, services).
ID. SC-2	ID. SC-2.1	Does the service have a documented process of vetting/selecting suppliers and partners of critical information systems, components, and services?
ID. SC-2	ID. SC-2.2	How often is this documentation reviewed?
ID. SC-3	ID. SC-3.1	After a supplier and/or third-party partner has been selected, does the service contract include SLAs and agreements to be compliant/align with <organization> security policies?
ID. SC-3	ID. SC-3.2	How often are the SLA's reviewed?
ID. SC-4	ID. SC-4.1	Does the supplier and/or third-party partner undergo audits or other forms of verifications to confirm that they are meeting contractual obligations?
ID. SC-5	ID. SC-5.1	Does the incident response plan include response plans for suppliers and third party providers?
ID. SC-5	ID. SC-5.2	Does the service involve the third party providers during Security Incident Response testing?

ID. SC-5	ID. SC-5.3	Does the BCDR plan include plans for suppliers and third-party providers?
ID. SC-5	ID. SC-5.4	Does the service involve the third-party providers during the BCDR testing?
PR.AC-1	PR.AC-1.1	Does the service leverage a cloud-based identity system to manage identities and credentials?
PR.AC-1	PR.AC-1.2	Does the service have the process and procedure for adding/removing accounts documented?
PR.AC-1	PR.AC-1.3	How often is the documentation reviewed?
PR.AC-1	PR.AC-1.4	Does the service audit the accounts (including privileged user accounts) within cloud-based identity system?
PR.AC-1	PR.AC-1.5	Does the service leverage a permissioning tool to restrict persistent admin accounts?
PR.AC-2	PR.AC-2.1	Does the service use physical security methods (i.e. badging, biometrics, physical keys) to access locations that contain sensitive data or valuable assets? (i.e. secrets, data centers, etc.)
PR.AC-2	PR.AC-2.2	Are physical security methods employed at locations storing high value assets? (i.e. ID badges/readers, mantraps, cameras, physical guards, physical keys, no drop tile ceiling, motion detectors, heat sensors)
PR.AC-2	PR.AC-2.3	Does the badge scanning mechanism keep auditable logs including timestamps and identification information?
PR.AC-2	PR.AC-2.4	Does the badge scanning system send alerts when unidentified or unauthorized personnel attempt to access physical asset?
PR.AC-2	PR.AC-2.5	Is there a list of personnel that have physical keys?
PR.AC-2	PR.AC-2.6	How often are the physical keys changed?
PR.AC-3	PR.AC-3.1	Is there a separate isolated management network for managing the systems that host the service?
PR.AC-3	PR.AC-3.2	Does the service use VPN to allow access to the management of network devices?
PR.AC-3	PR.AC-3.3	Is there MFA for logging into network devices for management?
PR.AC-3	PR.AC-3.4	Is remote access currently being monitoring by the security monitoring system?
PR.AC-3	PR.AC-3.5	Does the service use encryption mechanisms for remote access connections?
PR.AC-3	PR.AC-3.6	Does the remote connection automatically disconnect after an organization defined time period?
PR.AC-4	PR.AC-4.1	Does the service have a documented process for requesting access to physical and logical assets?
PR.AC-4	PR.AC-4.2	Are these requests (tickets) logged?
PR.AC-5	PR.AC-5.1	Does the service incorporate network segmentation via routing domains?

PR.AC-5	PR.AC-5.2	Does the service have any concurrent session controls implemented? (Note: Defining the maximum number of concurrent sessions for each account/account type through group policy)
PR.AC-5	PR.AC-5.3	Does the service utilize network monitoring systems?
PR.AC-5	PR.AC-5.4	Are the alerts/logs from the network monitoring systems tracked at a centralized location?
PR.AC-5	PR.AC-5.5	Does the team have a dedicated response team for alerts generated by the network monitoring system?
PR.AC-6	PR.AC-6.1	How often are the audits of logical access conducted?
PR.AC-7	PR.AC-7.1	Do all devices and assets utilize multi-factor authentication?
PR.AT-1	PR.AT-1.1	What percentage completion for security awareness training for all members of the team?
PR.AT-1	PR.AT-1.2	How often are the security awareness training conducted?
PR.AT-1	PR.AT-1.3	How are the security awareness training records tracked?
PR.AT-1	PR.AT-1.4	Are there other trainings (ie Brown bags) to train team members on security awareness/best practice?
PR.AT-2	PR.AT-2.1	Does the privileged user account holders have specific training to help understand roles and responsibilities?
PR.AT-2	PR.AT-2.2	Are the roles and responsibilities of privileged user accounts published in a documentation/wiki?
PR.AT-2	PR.AT-2.3	How often are the roles and responsibilities reviewed?
PR.AT-3	PR.AT-3.1	Are cybersecurity awareness training requirements included when selecting third party stakeholders?
PR.AT-4	PR.AT-4.1	<PR.AT-1.1>: What percentage completion for security awareness training for all members of the team?
PR.AT-5	PR.AT-5.1	<PR.AT-1.1>: What percentage completion for security awareness training for all members of the team?
PR.DS-1	PR.DS-1.1	If the service handles Personally Identifiable Information (PII), does the service follow GDPR Standards in Data Protection at rest and during transit?
PR.DS-1	PR.DS-1.2	For data that are classified as sensitive and above, are they protected with appropriate encryption methods?
PR.DS-2	PR.DS-2.1	Does the service employ cryptographic mechanism for communication of data between both internal and external networks?
PR.DS-3	PR.DS-3.1	Does the service have a documented data sanitization process?
PR.DS-3	PR.DS-3.2	Are assets formally managed throughout the removal, transfer, and disposition with auditable logs (i.e. chain of custody)?
PR.DS-4	PR.DS-4.1	Has the service undergone capacity planning to ensure availability of the service during high usage times (at or exceeding thresholds)? During contingency/disaster recovery?
PR.DS-4	PR.DS-4.2	Does the service leverage multiple/redundant data centers for capacity management?

PR.DS-4	PR.DS-4.3	Has the critical capacity threshold been established and documented with leadership approval?
PR.DS-4	PR.DS-4.4	Does the service receive alerts when capacity is reaching a critical capacity threshold?
PR.DS-5	PR.DS-5.1	Does the service leverage DLP tools?
PR.DS-5	PR.DS-5.2	Does the network monitoring service also provide monitoring for irregular activities that may potentially be data leakage?
PR.DS-6	PR.DS-6.1	Does the service have a documented process for integrity checking of software and hardware?
PR.DS-7	PR.DS-7.1	Does the service have a separate environment from the prod environment to develop and test new software, firmware, hardware?
PR.DS-8	PR.DS-8.1	<PR.DS-6.1>: Does the service have a documented process for integrity checking of software and hardware?
PR.IP-1	PR.IP-1.1	Does the service create a baseline configuration?
PR.IP-1	PR.IP-1.2	Are industry standards used when creating these baseline configurations (i.e. CIS Benchmarks)?
PR.IP-2	PR.IP-2.1	Does the service incorporate a system development life cycle to manage systems?
PR.IP-2	PR.IP-2.2	Does the service require a security requirements analysis for all systems development projects?
PR.IP-3	PR.IP-3.1	Does the service document configuration change requests?
PR.IP-3	PR.IP-3.2	Does the service have a documented Change and Release Management processes?
PR.IP-3	PR.IP-3.3	Does the service retain records of changes to configurations?
PR.IP-3	PR.IP-3.4	How long does the service maintain the configuration-controlled change records?
PR.IP-4	PR.IP-4.1	Does the service have a documented process for backing up information?
PR.IP-4	PR.IP-4.2	How often are backups performed?
PR.IP-4	PR.IP-4.3	Where are backups stored?
PR.IP-4	PR.IP-4.4	Are the backups encrypted?
PR.IP-4	PR.IP-4.5	How often are backups tested to ensure that they are working?
PR.IP-5	PR.IP-5.1	Does the service follow the Physical and Environmental Security Standard?
PR.IP-5	PR.IP-5.2	For all physical operating environments, does the service incorporate appropriate safety controls (fire suppressants, access control via badge control, etc)?
PR.IP-6	PR.IP-6.1	<PR.DS-3.2>: Are assets formally managed throughout the removal, transfer, and disposition with auditable logs (i.e. chain of custody)?
PR.IP-7	PR.IP-7.1	How often are the physical security policies reviewed?
PR.IP-7	PR.IP-7.2	Are there efforts outside of the dependency on other services to improve protection processes by the service team?

PR.IP-7	PR.IP-7.3	How often are the correspondence/status check-ins with dependent teams are conducted?
PR.IP-8	PR.IP-8	Does the service share/collaborate with other organizations around the effectiveness of protection technologies?
PR.IP-9	PR.IP-9.1	Does the service have a BCDR plan?
PR.IP-9	PR.IP-9.2	Has the service completed the Business Impact Analysis?
PR.IP-10	PR.IP-10.1	<ID.BE-5.3>: How often is this plan tested?
PR.IP-11	PR.IP-11.1	Does the HR policies and procedures incorporate cybersecurity practices such as deprovisioning, initial personnel screening, and policies/procedures for addressing personnel that needs to be escorted out of the building?
PR.IP-12	PR.IP-12.1	Does the service have a documented vulnerability management plan?
PR.IP-12	PR.IP-12.2	How often is the vulnerability management plan documentation reviewed?
PR.IP-12	PR.IP-12.3	How often are vulnerability scans conducted?
PR.IP-12	PR.IP-12.4	Which assets are scanned each month? (Operating System Scans, Database Scans, Web Application Scans)
PR.IP-12	PR.IP-12.5	Which environments are scanned as a part of the vulnerability scanning efforts? (Guest OS, Host OS, Native OS in the production as well as staging environment)
PR.IP-12	PR.IP-12.6	<DE.CM-8.2>: Does the service conduct external vulnerability assessments?
PR.IP-12	PR.IP-12.7	<DE.CM-8.3>: If the service does use external vulnerability assessments, how often are this assessments conducted?
PR.IP-12	PR.IP-12.8	Where are the external assessment reports stored?
PR.IP-12	PR.IP-12.9	<DE.CM-8.4>: How are the results of the vulnerability assessment addressed? (Lessons learned session, prioritize for immediate change management, maintain open risk item to mitigate for the detected vulnerability)
PR.MA-1	PR.MA-1.1	Does the service have a computerized maintenance management system to manage maintenance schedules and work order management?
PR.MA-1	PR.MA-1.2	Are the tickets/work order requests for maintenance tracked in a centralized tool?
PR.MA-2	PR.MA-2.1	Does the service require remote maintenance (i.e. providing maintenance service to remote data center locations), if so, does the service have a documented Request for Manufacturer's Assistance (RMA) Process?
PR.MA-2	PR.MA-2.2	If yes, are the tickets opened for the RMA Tool tracked in a central location within the service?
PR.PT-1	PR.PT-1.1	Does the service implement a SIEM Tool that maintains logs in a centralized location?
PR.PT-1	PR.PT-1.2	Are there documented procedures for maintaining audit/log records?
PR.PT-2	PR.PT-2.1	Are removeable media (i.e. USB) that are used also tracked in the asset inventory?

PR.PT-2	PR.PT-2.2	Is removable media used to transport sensitive information?
PR.PT-2	PR.PT-2.3	If yes, is the removable media encrypted?
PR.PT-3	PR.PT-3.1	Is the principle of least functionality incorporated at the systems level to provide only essential capabilities
PR.PT-4	PR.PT-4.1	<PR.AC-5.3>: Does the service utilize network monitoring systems?
PR.PT-5	PR.PT-5.1	Does the BCDR/ Incident Response plan include mechanisms for fail safe, load balancing, hot-swapping for resiliency?
DE.AE-1	DE.AE-1.1	Does the service employ detection capabilities for behavioral analytics, anomoly detection, IDS, and exceeding general performance thresholds? (i.e. Expected data flows, expected bandwidth to help monitor any anomalous activity.)
DE.AE-1	DE.AE-1.2	Does the detection systems generate alerts and are escalation procedures in place?
DE.AE-1	DE.AE-1.3	Are these alerts logged in a central log management system?
DE.AE-2	DE.AE-2.1	Does the service leverage threat analysis to understand the attack targets and the methods of attacks?
DE.AE-2	DE.AE-2.2	Does the service receive reports from outside dependencies that conduct analysis on these attacks?
DE.AE-2	DE.AE-2.3	How often are the reports analyzed and incorporated into the continuous monitoring system?
DE.AE-3	DE.AE-3.1	Are the event data (anomalous activity) aggregated and correlated from multiple sources and sensors?
DE.AE-4	DE.AE-4.1	Are the impacts of security events determined?
DE.AE-5	DE.AE-5.1	Has the service established a threshold for incident alerts before elevating the event to a higher severity?
DE.CM-1	DE.CM-1.1	<PR.AC-5.5>: Does the team have a dedicated response team for alerts generated by the network monitoring system?
DE.CM-1	DE.CM-1.2	Are the policies and procedures for the continuous network monitoring process documented?
DE.CM-1	DE.CM-1.3	<DE.AE-1.1> Does the service employ detection capabilities for behavioral analytics, anomoly detection, IDS, and exceeding general performance thresholds? (i.e. Expected data flows, expected bandwidth to help monitor any anomalous activity.)
DE.CM-1	DE.CM-1.4	How often are the detection values/rules for alerting reviewed?
DE.CM-2	DE.CM-2.1	Does the service have continuous monitoring of physical security?
DE.CM-2	DE.CM-2.2	Are the policies and procedures for the process of physical security monitoring documented?
DE.CM-2	DE.CM-2.3	How often are the physical assets used for the physical security tested to ensure that they are functioning properly? (i.e. testing for blind spots in cameras, ensuring ID badging system is functioning properly) (Should be incorporated into the incident response plan as well.)

DE.CM-3	DE.CM-3.1	Does the service utilize continuous monitoring of personnel activity? (i.e. insider threat protection via DLP monitoring of personal devices)
DE.CM-3	DE.CM-3.2	How many incorrect password logins does it take to trigger the alert/ Lock out?
DE.CM-4	DE.CM-4.1	Does the service utilize anti-malware software as part of the initial build on all systems (including the entry and exit points to the information system)?
DE.CM-4	DE.CM-4.2	Does the service update malicious code protection mechanisms for AV software including signature definitions?
DE.CM-4	DE.CM-4.3	How often do the servers check for updates to the signature files?
DE.CM-5	DE.CM-5.1	Does the service block unacceptable mobile code? (ex: blocking would be preventing the transmission of word processing files with embedded macros)
DE.CM-5	DE.CM-5.2	Does the detection of unacceptable mobile codes trigger an alert to administrators?
DE.CM-5	DE.CM-5.3	Does the service prevent automatic execution of mobile code?
DE.CM-6	DE.CM-6.1	Does the service utilize continuous monitoring of external service provider activity? (ie DLP monitoring of personal devices)
DE.CM-6	DE.CM-6.2	Does the contract with external services include an acceptable use policy?
DE.CM-6	DE.CM-6.3	Does the service have documented policies and procedures for addressing detected misuse of assets by external service providers?
DE.CM-6	DE.CM-6.4	Do all endpoints trigger alerts for suspicious network activity? (i.e. Massive transfer of data from hard drive to external device/network)
DE.CM-7	DE.CM-7.1	<DE.CM-3.1>: Does the service utilize continuous monitoring of personnel activity? (ie insider threat protection via DLP monitoring of personal devices)
DE.CM-8	DE.CM-8.1	Does the service conduct vulnerability scanning using tools?
DE.CM-8	DE.CM-8.2	Does the service conduct external vulnerability assessments?
DE.CM-8	DE.CM-8.3	If the service does use external vulnerability assessments, how often are these assessments conducted?
DE.CM-8	DE.CM-8.4	How are the results of the vulnerability assessment addressed? (Lessons learned session, prioritize for immediate change management, maintain open risk item to mitigate for the detected vulnerability)
DE.DP-1	DE.DP-1.1	Does the service have roles and responsibilities for the continuous monitoring team outlined in their SOP?
DE.DP-1	DE.DP-1.2	How often are these roles and responsibilities for the Continuous Monitoring team reviewed?
DE.DP-2	DE.DP-2.1	Does the service establish KPIs for continuous monitoring?
DE.DP-2	DE.DP-2.2	How often are these KPIs reviewed?

DE.DP-2	DE.DP-2.3	Has the service established a frequency for independent assessments to assess the continuous monitoring process?
DE.DP-3	DE.DP-3.1	Does the service engage in penetration testing?
DE.DP-3	DE.DP-3.2	How often are penetration tests conducted?
DE.DP-3	DE.DP-3.3	Are the lessons learned from the penetration test incorporated into the continuous monitoring process for improvement?
DE.DP-4	DE.DP-4.1	Does the continuous monitoring team have an established communication plan?
DE.DP-4	DE.DP-4.2	How often is the communication plan reviewed?
DE.DP-4	DE.DP-4.3	How often is the communication plan tested for efficiency?
DE.DP-5	DE.DP-5.1	Does the team incorporate lessons learned from detection tests and real incidents to improves the security monitoring process?
RS.RP-1	RS.RP-1.1	Does the service have a security incident response plan?
RS.RP-1	RS.RP-1.2	How often is the Security Incident Response Plan reviewed?
RS.RP-1	RS.RP-1.3	How often is the response to security incidents tested?
RS.RP-1	RS.RP-1.4	Have there been events where the response plan has been executed during or after the event?
RS.CO-1	RS.CO-1.1	Does the Security Incident Response Plan include roles and responsibilities?
RS.CO-1	RS.CO-1.2	<RS.RP-1.2>: How often is this plan reviewed?
RS.CO-2	RS.CO-2.1	Does the communication plan within the Security Incident Response Plan include an established criterion? (SEV1/SEV2/SEV3 alerts are transmitted to…)
RS.CO-3	RS.CO-3.1	Does the Security Incident Response Plan include a communication plan to share information during an incident?
RS.CO-3	RS.CO-3.2	Does the communication plan include a primary and secondary contact?
RS.CO-4	RS.CO-4.1	Does the communication plan within the Security Incident Response Plan include coordination with stakeholders?
RS.CO-5	RS.CO-5.1	Does the Security Incident Response Plan include instructions on sharing of information with external stakeholders in the event of an incident for situational awareness?
RS.AN-1	RS.AN-1.1	Are all alerts generated by detection systems investigated?
RS.AN-1	RS.AN-1.2	<RS.RP-1.1>: Does the service have a Security Incident Response plan?
RS.AN-2	RS.AN-2.1	Does the Security Incident Response Plan include guidance on determining the impact of an incident?
RS.AN-2	RS.AN-2.2	Does the service have a triaging process to determine the severity level of the security incident?
RS.AN-3	RS.AN-3.1	Does the incident response plan include a post-mortem forensics analysis of the security incident?
RS.AN-3	RS.AN-3.2	Are the results from this forensics analysis incorporated in a lesson learned to improve the Security Incident Response Plan?

RS.AN-4	RS.AN-4.1	<RS.AN-2.2>: Does the service have a triaging process to determine the severity level of the security incident?
RS.AN-5	RS.AN-5.1	Does the service have a vulnerability management program manager established?
RS.AN-5	RS.AN-5.2	Does the Vulnerability Management Program Manager conduct monthly calls with stakeholder to review updates based on the data provided by an advance notification service?
RS.AN-5	RS.AN-5.3	Does the service have management portals or a dedicated phone line to accommodate customers security incident reports?
RS.AN-5	RS.AN-5.4	Does the service subscribe to external security bulletins?
RS.AN-5	RS.AN-5.5	Does the service work with external parties such as law enforcement, ISPs, and other partners that can identify security issues?
RS.MI-1	RS.MI-1.1	Does the incident response plan include strategies for short term containment of a security incident?
RS.MI-1	RS.MI-1.2	Does the incident response plan include strategies for long term containment of a security incident?
RS.MI-1	RS.MI-1.3	Are these containment strategies tested with the Security Incident Response Plan testing?
RS.MI-2	RS.MI-2.1	Are incident mitigations tracked through tickets?
RS.MI-2	RS.MI-2.2	Does the Security Incident Response Plan include a mitigation process?
RS.MI-3	RS.MI-3.1	Is the incident response cycle incorporated into the risk management cycle?
RS.MI-3	RS.MI-3.2	Are new incidents documented as risks in the risk register?
RS.MI-3	RS.MI-3.3	Is the process of documenting new incidents documented within the incident response plan?
RS.IM-1	RS.IM-1.1	After each incident/ testing of the response plan, does the service conduct lessons learned session?
RS.IM-2	RS.IM-2.1	<RS.RP-1.2>: How often is this plan reviewed?
RC.RP-1	RC.RP-1.1	Which type of test on the BCDR plan was last conducted?
RC.RP-1	RC.RP-1.2	When was the last test of the BCDR plan conducted?
RC.RP-1	RC.RP-1.3	When was the BCDR plan last updated?
RC.IM-1	RC.IM-1.1	Following the test of the BCDR plan, was there a lessons learned/debrief session?
RC.IM-2	RC.IM-2.1	After lessons learned session, did the team review and update the disaster recovery plan with updated strategies?
RC.CO-1	RC.CO-1.1	Does the BCDR plan also indicate a specific PR contact to discuss the event?
RC.CO-2	RC.CO-2.1	After the previous live response, did the service engage the PR team to repair any reputational damage?
RC.CO-3	RC.CO-3.1	Does the BCDR plan outline a communication plan to the internal stakeholders and executive/management teams?