Table of Contents

SUPPLEMENTARY INFORMATION:

The Cloud Security Alliance (CSA) is the world’s leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA’s activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

CSA operates the most popular cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, 3rd-party audit and continuous monitoring. CSA also manages the CSA Global Consulting Program, a professional program it developed that allows cloud users to work with a network of trusted security professionals and organizations that offer qualified professional services based on CSA best practices.

CSA’s comprehensive research program works in collaboration with industry, higher education and government on a global basis. CSA research prides itself on vendor neutrality, agility and integrity of results. CSA has a presence in every continent except Antarctica. With our own offices, partnerships, member organizations and chapters, there are always CSA experts near you. CSA holds dozens of high-quality educational events around the world and online. Please check out our events page for more information.

We applaud NIST and the CSF team for driving toward continual improvement and keeping the CSF relevant. With that said, CSA has reviewed the RFI and has made recommendations and comments that we feel will facilitate the revision of the CSF to include more cloud specific guidance and controls, thus closing a gap we feel needs to be addressed in the next revision.

CSA’s comments are in **bold** below

Contact Info

General inquiries: support@cloudsecurityalliance.org

Use of the NIST Cybersecurity Framework

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.

The cybersecurity framework allows you to mitigate risks both now and in the future. And following the NIST cybersecurity framework will make it easier for organizations to adopt new security procedures that use the CSF as a foundation when implemented in the future. We do believe however that cloud security risks have been left out or not addressed in a clear common controls perspective.

The CSA Cloud Control Matrix if added to the compendium will address this critical issue and may in fact identify opportunities to revise the five functions even further to address cloud security.

2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (*e.g.,* supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?

Again, we do not believe the framework goes far enough to address the risks in the cloud.

CSA has developed research and issued a report "Cloud Security Alliance Perspective on Cloud Risk Management Report That Identifies Cloud Computing Rapid Adoption Gaps and Risks"

The document lays out five questions to stimulate discussion and facilitate possible solutions:

- **Are the risk management methodologies currently available adequate to manage risks in the cloud?**
- **Are organizations aware of the shared responsibility model introduced by cloud computing, and are the responsibilities appropriately reflected in the risk management processes and programs?**
- **Are organizations aware of the concepts and implications of indirect/loss of control imposed by cloud computing and the challenges they pose to the design of risk mitigation procedures and their validation?**
- **Are organizations sufficiently aware of the impact that cloud computing has on the propagation of their supply chains and the difficulty in evaluating and monitoring the consolidated residual risk of third/fourth parties?**
- **Are the current governance practices adequate to effectively identify, evaluate and report the relevant cloud risks to relevant stakeholders?**

Risk management when applied to cloud operations plays a vital role in all of an organization's processes and is essential to its overall business improvement strategy. As such, it must be a top-level, enterprise-wide process rather than a siloed or departmental exercise. While the risk management approach is the same whether in the cloud or on-prem, there are significant differences in tactics and implementation that must be

addressed. An effective risk management program will address issues related to economic value, process improvement, compliance, information security, and privacy, including:

- **New operational security risks created by moving to the cloud**
- **Costs related to the failure to address cloud compliance**
- **Risks related to the cloud market growth**
- **Mitigation measures**

CSA's Perspective on Cloud Risk Management is a free document. Download it now.

3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (*e.g.,* resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

One big issue with the NIST framework, and an area we believe fast becoming obsolete, is cloud computing.

NIST currently approaches on-prem. The problem is that many companies today don't manage or understand the shared responsibility model when it comes to securing the cloud. In fact, many companies do not even secure their own cloud infrastructure. Instead, they outsource use of SaaS or PaaS offers in which they attempt to transfer the risk to third-party companies to take legal and operational responsibility for managing all parts of their cloud which could not be further from the truth. There are clear lines drawn between provider, customer and third-party responsibilities and these are not clearly defined or addressed.

The issue with this, is that NIST does not really deal with shared responsibility. The framework seems to assume a much more discreet way of working. Complying with NIST means that you are addressing the parts of your systems you manage yourself, but unfortunately, you may not have implemented any control over those parts that are managed remotely.

Why does this matter? This matters because companies who take cybersecurity seriously may lack the in-house resources to develop their own systems, so they are faced with contradictory solutions. Security is often the number one reason why big businesses look to the cloud but lack the understanding of shared responsibility.

The CSA Cloud Control Matrix breaks down the SSRM as well as Scope Applicability Mappings as well as Typical Control Applicability and Ownership. Adoption of such guidance would greatly improve the framework and fill what we see as a huge hole in the document.

Further, there is no accountability route. How do we know organizations are meeting the requirements? There is no path endorsed by NIST. The British Standards Institution

created this first certification path for the NIST CSF and was debated at three different NIST workshops prior to launch. This is in place, but certification; or any other route of accountability or proof of effectiveness is not endorsed or encouraged in the document.

4. Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.

See answer to number 3. Further, the Tiers need to be described as what they are…a maturity model. It is not acceptable to assume that there is no significant statement made by where an organization lies within the tiers.

Recommended additions to subcategories include

Asset Management - specific references to third-party, external, and cloud applications and services):

ID.AM-2: …including cloud services and third-party services of SaaS applications

ID.AM-3: …including data flows mapped to third-party and cloud supply chain

ID.AM-4: …including cloud IaaS, third-party use of cloud

Risk Assessment - subcategory for risk assessment frequency and cadence. e.g., procurement, post-procurement

Informative references: CSA CCM adds some context to these (mappings can be included in follow up)

5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.

Only impact would be transitioning to any significant change(s). This would require a transition period for adopters so as not to interrupt operations and allow for a systematic and organized transition.

6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.

More dedicated guidance on cloud security as well as a certification route.

Additional Informative References: CSA CCM (this reference also includes mappings to multiple regulations and frameworks)

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

CSA Comments: See our comments under Supply-Chain Risk as well

7. Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include:

- Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).
- Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.
- Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.

The CSF is a high level framework for quick risk assessments. Mapping the subcategories to 8286, IoT, and other frameworks allows for deeper and due diligent risk assessments.

8. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

NIST CSF categories are high-level enough to find commonality across multiple frameworks. However, expanded Subcategories (as shown in question 4) and additional Informative References are needed. CSA CCM can align most references to frameworks such as ISO/IEC 27000-series, NIST 800-53, AICPA TSP, and many more.

9. There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and

services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?

Helpful updates for international adaptations include adding data protection elements in the Identity category coverage of sovereign and privacy rights. The protection category may now need to include data-in-use protections.

Identity - Governance (ID.GV): ID.GV-3 includes privacy obligations but there is no subcategory covering sovereignty or data location.

Protect - Data Security (PR.DS): Data-in-use is protected

10. References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.

CSA Cloud Controls Matrix (CCM)/Consensus Assessment Initiative Questionnaire (CAIQ) are frameworks for cloud security specific controls and assessment questions. The CCM also maps cloud security controls to over 50 industry regulations/frameworks (including NIST 800-53, FedRAMP, and CSF) and is updated for auditability and implementation. These are part of the CSA Security, Trust, Assurance, and Risk (STAR) program for cloud vendor assessment.

Cybersecurity Supply Chain Risk Management

11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?

In addition to establishing a Software bill of materials (SBOM), a SaaSBOM for cloud services needs to be established. Part of the data flow for data identification and protection is knowing the cloud supply chain components of SaaS and other third-party applications. See CSA as a reference for SaaSBOM considerations.

12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (*e.g.* pieces of hardware or software assurance or assured services, or specific to

only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

CSA STAR/CCM/CAIQ and the CSA Enterprise Architecture (also referenced in NIST 500-292, 500-299 as TCI) assess the presence of security controls and capabilities in the cloud supply chain relevant to the security shared responsibility model (SSRM).

13. Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?

In addition to CSA CCM guidance for cloud, the CSA also developed the CSA IoT Controls Matrix for security controls in the IoT environment. Open-source software and cloud vulnerabilities are uniformly tracked in the Global Security Database

14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.

CSA Considerations/Recommendations

Overview of Risk Management considerations in providing guidance and framework modifications to the NIST Cybersecurity Framework for Critical Infrastructure:

1. The current framework, although targeted for critical infrastructure, provides no guidance or discussion of how to calibrate an organization's risk tolerance (def) or risk appetite (def) when applied to the named *critical infrastructure sectors* as opposed to the non-critical sectors. The inference of identifying *critical* sectors, from a risk perspective is that the organization's tolerance for risk is lower than non-critical, hence the strength of the security controls, policies and procedures should be elevated to minimize exposure and probability of breaches and successful attacks. This is crucial to organizations designing enterprise risk management programs, to ensure that the critical sectors of the enterprise appropriately deal with the need for strengthened controls to reduce the organization's risk tolerance.

2. The current NIST framework does not identify nor discuss the technology and other risks associated with the adoption and/or use of cloud-based services and platforms. It is imperative that such "inherent risks" be identified, measured, and included in the organization's risk register to ensure that relevant and appropriate controls, procedures and processes are built to effectively manage all cloud introduced risks.

3. The Matrix below is designed to identify and discuss many of the inherent risks associated with an organizations adoption of cloud computing. Implicit in this discussion is also a function of the scale, scope and validation of *all* cloud services and cloud service providers engaged by the organization.

Cloud Components	Risk Factors
Cloud Strategy	• Lack of a coherent cloud strategy or misalignment with other business strategies • Lack of an exit strategy for provider or customer/Concentration Risk • Ineffective organizational change management for cloud adoption • Lack of skills/experience to execute strategy
Shared Service Model (SRM)	• Subscribing to the services of a public cloud provider, will immediately expose a customer to a new management model, known as the SRM. This model allocates various roles and activities between the cloud customer and the cloud provider. However, the cloud customer is accountable for creating the practices and measures necessary to validate the proper performance of the cloud provider's performance. Further, service credits, fines and/or

	penalties for non-performance must be established by contract prior to execution thereof.
Loss of control and access to technology assets.	• In the cloud model except for private cloud deployments, the customer loses control over, and access to all physical technology assets. This can significantly decrease the customer’s ability to directly influence and impact the performance of relevant technology assets. Moreover, it directly impacts the concepts of assurance and continuous monitoring. Again these requirements are noted in the CSF, but additional guidance is warranted in cloud based environments subject to NIST requirements.
Cybersecurity	• Once launched, the cloud ecosystem immediately exposes the organization to unmeasurable threats and risks from threat actors around the globe. Risks on this scale were relatively non-existent when NIST CSF was originally published, certainly not with Cloud Services as the target.
Data Governance	• Data is the currency behind many cloud based products and services. Poorly designed practices and programs can lead to poor fiscal performance, compliance and regulatory fines and penalties and destruction of reputation and trust.
Operations	• Operational resilience and on line all of the time becomes an organizational necessity. Failure to conform, can lead to business failure.

	Business resilience and recovery becomes a crucial issue in a cloud based ecosystem, while the concepts are in the CSF; there is no guidance on how to achieve it and test it in a cloud based environment.
Compliance Configuration Risk	• Total compliance with all relevant customer regulations and laws is an expected service. Validation of continuous achievement is difficult to attain and maintain. Relevant guidance and requirements should be developed for any CSF update, especially for Supply Chain Risk, where compliance may require services from offshore CSPs for foreign regulations, laws and/or requirements. Gartner has estimated that thru 2025 0ver 99% of cloud failures will be related to customer misconfigurations and mismanagement. The NIST CSF updates present an ideal opportunity to enhance their framework to reduce these projected failure rates and develop guidance and guidelines that will enable customers to be more effective and efficient in managing their portfolio of cloud service providers.
Incident Response	• Developing an effective incident response (IR) and management program can be challenging and expensive when control and access to technology assets does not exist. The NIST incident management framework should be tightly integrated into the CSF. The preparation phase of the NIST program requires significant prework and coordination since ad hoc access to information and analysis to deal with potential breaches and remediation of real IR breaches may require significant investments in automation, monitoring and reporting. Some of which is being evaluated by various US and other regulatory agencies.

Vendor Selection and Monitoring	• This factor takes on significant importance in both scope, scale and execution, and in direct proportion to the migration away from legacy technology platforms to cloud based services. The ease of acquiring technology services combined with the potential difficulty of ensuring all cloud providers are properly vetted warrants the NIST CSF to increase the rigor required to manage this risk. This is especially critical for the management of cloud supply chains in critical infrastructure sectors. THIS AREA REQUIRES SIGNIFICANT ATTENTION IN ANY NIST updates
Performance Management	● Loss of direct control over, and access to, the assets/resources necessary for success introduces new and difficult to manage risks. ● The reliance upon contracts and supporting terms and conditions to manage outcomes and performance may require new skills and competencies for many organizations.
Employee Learning	• This will be a major challenge for many organizations to achieve and maintain success. The lack of experienced personnel, combined with the need to reskill and upskill current staff will introduce new risks to performance and quality of service.

What is the Shared Responsibility Model as applied to Cloud Computing?

In simple terms, the cloud (SRM) recognizes the joint and shared roles of both the cloud service provider (CSP) and the cloud customer. Namely, the CSP is responsible for the security *of* cloud,

while the customer is responsible for security in the cloud. This translates into the technology infrastructure, host operating system and virtualization software provided by the CSP as well the physical security of all related physical assets. The customer, on the other hand is responsible for application, network and data security usually through configuration settings and features available to them. Both parties are subsequently responsible for monitoring the integrity, availability and proper operations of all relevant features and settings upon the commencement of services.

12:2: Implications of the Shared Responsibility Model

It also creates new-found roles and responsibilities for both cloud provider and cloud customer that did not exist under traditional owned and operated technology resource provisioning. A major consideration for any new cloud customer, is the transfer of responsibility to the cloud provider for proper and continuous functioning of various compliance, security, operational and performance services as contracted.

Further, it is incumbent upon the customer to obtain appropriate assurances from the CSP that the services will be provided on a continuous basis, or that in the event of an operational failure, an appropriate resilience program has been established. Moreover, the customer should understand that regardless of the cause of CSP deficiencies, performance failures or service outages the customer remains fully accountable to its stakeholders, investors, employees and regulators. It is up to the customer to include these risks and their associated mitigation strategies in the organization's ERM Program.

Putting the SRM into action

To optimize the shared performance between customer and Cloud provider, best practice includes the establishment, measurement, monitoring and reporting of agreed upon key performance indicators (KPI's). This is usually accomplished thru the creation, management, monitoring and reporting of agreed upon Key Performance Indicators or KPIs and/or Service Level Agreements These are formalized between parties, through their inclusion in the only legally binding relationship between the two parties – the contract. They are normally documented as specific service level agreements (SLAS).