THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Cloud Computing: Cloud Computing Security Controls For NS/EP (Appendix E)

May 15, 2012

TABLE OF CONTENTS

1.0 CLOUD SECURITY ALLIANCE (CSA) CLOUD CONTROLS MATRIX

The Cloud Security Alliance (CSA) is a non-profit organization that promotes best practices for providing security assurance in cloud computing and consists of industry practitioners, corporations, associations (including its founding affiliate member the Information Systems Audit and Control Association [ISACA]) and other key stakeholders. This member-driven organization is comprised of regional chapters, both domestic and abroad, that focus on different areas of interest specific to a region and/or aspect of cloud computing.

CSA's Cloud Control Matrix (CCM) is a framework consisting of security control requirements built for the cloud and provides fundamental information security principles for cloud service owners and cloud service providers (CSP). The CSA CCM emphasizes business information security control requirements and identifies security threats and vulnerabilities in the cloud. The CCM also aligns with industry-accepted security standards and controls frameworks such as the International Organization for Standardization (ISO) 27001/27002[1], ISACA Control Objectives for Information and Related Technology (COBIT), payment card industry (PCI)[2], and the National Institute for Standards and Technology (NIST), among others, and received validation from an independent certification organization comprised of information security practitioners.

CCM consists of 100 controls developed around 13 control areas, or domains.[3] The President's National Telecommunications Advisory Committee (NSTAC) determined that certain control areas, such as control measurement or certification, were of limited relevance to informing the risk implications to the five key factors. Therefore, using relevancy to the five key factors and our professional judgment, the NSTAC reduced the number of controls to be assessed to 34. The NSTAC then analyzed those controls according to the general methodology previous discussed.

2.0 ISACA IT CONTROL OBJECTIVES FOR CLOUD COMPUTING: CONTROLS AND ASSURANCE IN THE CLOUD

ISACA is a non-profit, global association that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems.[4] ISACA has issued a number of information technology (IT) governance frameworks including its most widely recognized COBIT IT risk and controls framework, which was developed as a tool to map business requirements to IT controls for managing and securing information and information systems. COBIT consists of 210 controls developed around the lifecycle of a program. As such, this framework focuses on IT processes–not functions or applications – from the perspective of the process owners, who principally assumes the responsibility of the IT functions that support and

[1] ISO 27001: http://www.iso.org/iso/catalogue_detail?csnumber=42103 and ISO 27002 http://www.iso.org/iso/catalogue_detail?csnumber=50297
[2] https://cloudsecurityalliance.org/research/ccm/
[3] http://www.isaca.org/about-isaca/Pages/default.aspx
[4] ISACA's 95,000 membership includes auditors, chief executives (including CIOs), educators, information security and control professionals, business managers, students, and IT consultants spanning 160 countries.

enable the business processes under their purview. Leveraging the flexibility of the framework, ISACA created its IT Control Objectives for Cloud Computing, which extends the COBIT controls to the cloud computing environment. The ISACA IT Control Objectives for Cloud Computing also maps to other industry-accepted security standards, regulations, and controls frameworks such as NIST Special Publication 800-53, ISO 17799: Information Technology - Security Techniques - Code Of Practice For Information Security Management, and the Capability Maturity Model Integration (CMMI), among others.

The methodology the NSTAC used to review this framework is consistent with the one used for evaluating CSA's CCM; however, the NSTAC made necessary modifications to account for the differences in the constructs of the frameworks. As previously mentioned, the general COBIT framework, along with the IT Control Objectives for Cloud Computing, are structured around a life-cycle approach, therefore, it is not functions-based around specific IT (or cloud) domains like the CSA CCM. In reflecting this approach, the 210 control objectives are mapped to 34 IT processes, which fall under 4 larger domains: 1) plan and organize, 2) acquire and implement, 3) deliver and support, and 4) monitor and evaluate.[5] Similar to the CSA analysis, the NSTAC reduced the number of controls to include only those relevant to the cloud environment. ISACA self-designated the cloud-relevant controls, which reduced the number of controls to be evaluated from 210 controls down to 155. Taking into account the appropriate level of evaluation required for the report, and in order to preserve the life-cycle based construct of this framework, instead of further distilling the number of controls based on their relevance to the NS/EP context as done for the CSA CCM, the NSTAC performed our evaluation of the risks and NS/EP implications at the process-level. The NSTAC did, however, evaluate the five key factors and identify the responsible party at the control-level to provide context and support for the types of functions/controls that were classified under each of the five key factors and to determine the responsible parties for functions/processes and their associated risks.

3.0 FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FEDRAMP) SECURITY CONTROLS

As previously discussed, the Office of Management and Budget (OMB) established the Federal Risk Authorization and Management Program (FedRAMP) to provide a standard approach to assessing and authorizing cloud computing services and products. This approach leverages the existing processes based on NIST 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems Processes* and the NIST 800-53 *Recommended Security Controls for Federal Information Systems and Organizations* and adapts them for cloud computing. FedRAMP is intended to enable multiple agencies to gain from the benefit and insight of the FedRAMP's authorization, including access to service provider's security documentation packages. FedRAMP's 168 security controls and enhancements were selected from NIST 800-53 Revision 3 for systems designated at the low and moderate impact levels as defined by Federal Information Processing Standards (FIPS) 199. Consistent with the rationale for analyzing the ISACA framework, the NSTAC performed our evaluation of the risks and national security and emergency preparedness

[5] http://www.isaca.org/COBIT/Pages/COBIT-Request.aspx

(NS/EP) implications at the higher domain (i.e. "family") level, totaling 17 families. The NSTAC also evaluated the five key factors at the individual control level to provide context and support for the types of functions/controls that were classified under each of the five factors. Finally, since FedRAMP will identify responsible parties for the each of the controls in forthcoming guidance, the NSTAC did not identify them during our review.

4.0 EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA) CLOUD COMPUTING: BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY

The European Network and Information Security Agency (ENISA) is a European Union agency that provides expertise in network and information security issues. The NSTAC evaluated ENISA's Cloud Computing: Benefits, Risks and Recommendations for Information Security to understand the broader, holistic perspective of assessing risks for cloud services for government functions. The document enumerates risks in the following domain areas: policy and organizational, technical, legal, and risks not specific to the cloud. The NSTAC reviewed the 35 individual risk factors that were categorized into the domains identified above and mapped them to the affected security controls in the CSA and ISACA frameworks. In so doing, the NSTAC identified a baseline set of controls from the CSA and ISACA frameworks that can be used to address the risks highlighted in the ENISA framework.

5.0 THE NSTAC NS/EP CLOUD CONTROL FRAMEWORKS

5.1 CSA Cloud Controls Matrix

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Data	Data Governance Ownership / Stewardship/ Classification	All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated. Data, and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligation for retention and prevention of unauthorized disclosure or misuse.	R.1. Lock-in; R.2 Loss of governance; R.20 Conflict between customer hardening procedures and cloud environment; R.21 Subpoena and e-discovery; R.21 Subpoena and e-discovery; R.23 Data protection risks; R.30 Loss or compromise of operational logs	X	X	X	An incomplete and/or inaccurate inventory of assets (such as data), improper designation of appropriate risk level (to the data), and misallocation of the appropriate roles and responsibilities to data owners (commensurate with the risk level) can result in unauthorized access, use, disclosure, modification, and/or destruction.	In an NS/EP event, many different users will need access to systems, data and services. It will be critical for NS/EP owners to maintain (and automate where possible) data classification. While certain types of data will require immediate access, specialized handling, and/or distribution can lead to liability concerns when the data is managed in a manner not explicitly defined by or consistent with its original intent (i.e. audit trail or no audit trail.) Additionally, as data is being generated from an event, its classification could change and NS/EP service owners will need SLAs that will enable the rapid movement to a classified platform and guarantee wiping of data.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Data	Data Governance - Retention Policy	Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of disk or tape backups must be implemented at planned intervals.	R.1 Lock-in; R.2 Loss of governance; R.23 Data protection risks; R.30 Loss or compromise of operational logs		X	X	Loss of data or prolonged inability to access critical data can have significant impact on operations. Cloud services should implement redundant data storage as well as thorough data backup procedures allowing for recovery of historical data for a set period of time. At the same time, if the service owner or the provider are required to comply with regulatory or legal requirements to preserve certain types of data (e.g. access logs) for set periods of time, loss of said data can result in penalties and/or impede forensic / LE activities.	The key characteristics of the cloud, including distributed computing base, geo-redundancy, scalability, and ability to rapidly deploy new services makes cloud services a promising environment for NS/EP applications. NS/EP owners will need to set clear requirements for data retention in the cloud. NS/EP owners will need to determine specific policies related to data retention, including not just how long but where the data is being retained (e.g., user devices, cloud, or back inside of government enterprises). For example, in response to national disasters, does the NS/EP data generated in a collaborative cloud model have specific time-to-live? Are there specific Government policies for retention or is up to the service owners and stake holders to establish this?

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Data	Data Governance - Secure Disposal	Policies and procedures shall be established and mechanisms implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	R.1 Lock-in; R.2 Loss of governance; R.14 Insecure or ineffective deletion of data; R.23 Data protection risks; R.30 Loss or compromise of operational logs		X	X	The redundant nature of cloud storage and its built-in backup mechanisms could present a challenge in ensuring complete erasure of information. Most commercial cloud providers do not truly erase data. In many cases it is simply marked as erased, and then portions of the disk space allocated to the data are erased prior to reuse by other customers.	In dealing with sensitive information, complete and secure removal of data must be supported and access to the functionality needs to be effectively controlled. Depending on the cloud service model, the responsibility may reside with application owner, the service provider, or jointly with both. Additionally, NS/EP owners may need to have the ability to wipe devices once an event is over and this may require building permissions and management systems into non-government owned/managed devices.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Data	Data Governance - Information Leakage	Security mechanisms shall be implemented to prevent data leakage.	R.1 Lock-in; R.2 Loss of governance; R.12 Intercepting data in transit; R.13 Data leakage on up/download, intra-cloud; R.23 Data protection risks	X	X	X	In addition to presenting the same data leakage risks as most in-house and/or outsourced IT environments, cloud computing may introduce additional leakage channels due to multi-tenancy or insider threat. The most serious information leakage risk in cloud computing at this point seems to lie with out-of-policy cloud migration projects that expose organization data to the cloud without proper risk assessment. Finally, cloud-based service may provide improved protection of data by allowing ubiquitous access without the need for local storage of the data on mobile devices (currently one of the most significant sources of data leakage).	Ensuring controlled access to sensitive information is essential to NS/EP applications. Depending on the service model and architecture the responsibility of the area may reside with some or all of the actors (user, owner, provider). At the same time, properly architected and implemented cloud applications can significantly reduce data leakage due to some of the most common channels such as device loss or theft.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Data	Information Security - Acceptable Use	Policies and procedures shall be established for the acceptable use of information assets.	R.10 Cloud provider malicious insider-abuse of high privilege roles; R.12 Intercepting data in transit; R.28 Privilege escalation	X	X	X	Policies and procedures should clearly define activities that qualify as both authorized and unauthorized uses of information assets, infrastructure components, and services/technologies.	NS/EP users may not be fully aware of acceptable use of information assets and compliance requirements. Acceptable use exception scenarios along with risk implications need to be anticipated and planned for.
Data	Information Security - Asset Returns	Employees, contractors and third party users must return all assets owned by the organization within a defined and documented time frame once the employment, contract or agreement has been terminated.	R.2 Loss of governance; R.6 Cloud Provider Acquisition; R.7 Supply Chain Failure; R.34 Computer Theft	X	X	X	A complete inventory of all assets (including asset classification) and designation of owners accountable for managing the asset and updating the inventory is essential to ensure adequate asset management, including returns.	In an NS/EP event, assets can be lost, damaged, stolen, or otherwise unaccounted for, which can result in its inappropriate use, mishandling, or destruction. NS/EP owners need to consider whether data can (temporarily) reside on a device during an event and also put mechanisms in place to wipe the data upon return.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Data	Security Architecture - Data Integrity	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data.	R.7 Supply Chain Failure; R.10 Cloud provider malicious insider-abuse of high privilege roles; R.28 Privilege escalation; R.30 Loss or compromise of operational logs		X	X	Failure to ensure data integrity at application interfaces and databases leave data vulnerable to alteration, exploitation, or corruption.	With vast amounts of data flowing and no reliable mechanism by which to ascertain a user's identity, particularly in the context of P2P and government-citizen data sharing via social media sites, the security and integrity of the data can be compromised by a user to intentionally mislead or convey wrong information. Potential need for a process to snap shot data so that in case it was corrupted, it could be readily recovered.
Policy/Legal	Information Security - Baseline Requirements	Baseline security requirements shall be established and applied to the design and implementation of (developed or purchased) applications, databases, systems, and network infrastructure and information processing that comply with policies, standards and applicable regulatory requirements.	R.10 Cloud provider malicious insider-abuse of high privilege roles; R.11 Management interface compromise; R.15 DDoS; R.20 Conflict between customer hardening procedures and		X	X	Lack of compliance with baseline security standards without compensating controls is likely to leave significant gaps in protection of the cloud infrastructure or application putting the service and data at risk.	Compliance with security baseline requirements identified for the specific service is essential in ensuring security of the service and the data. In NS/EP applications, compliance with the NS/EP specific baseline standards must be evaluated.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		Compliance with security baseline requirements must be reassessed at least annually or upon significant changes.	cloud environment; R.25 Network breaks; R.26 Network management; R.28 Privilege escalation					
Policy/Legal	Information Security - User Access Policy and Configuration	User access policies and procedures shall be documented, approved and implemented for granting and revoking normal and privileged access to applications, databases, and server and network infrastructure in accordance with business, security, compliance and service level agreement (SLA) requirements. Normal and privileged user access to	R.2 Loss of governance; R.10 Cloud provider malicious insider-abuse of high privilege roles; R.20 Conflict between customer hardening procedures and cloud environment; R.23 Data protection risks; R.27 Modifying		X	X	Ineffective access policies and controls can lead to data leakage and/or service compromise by untrusted parties.	Effective access controls are essential in the NS/EP environment, which deals with sensitive information and where the availability of the service is essential. In a crisis situation, dynamic management of credentials and modifying access policies to facilitate response activities is essential. The Access Control policy and system must support this for NS/EP applications. NS/EP owners will need to think about access policies and configurations that will enable rapidly granting access to new users and

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		applications, systems, databases, network configurations, and sensitive data and functions shall be restricted and approved by management prior to access granted. Timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data shall be implemented upon any change in status of employees, contractors, customers, business partners or third parties. Any change in status is intended to include termination of employment, contract or agreement, change of employment or transfer within the organization.	network traffic; R.28 Privilege escalation					determining what authentication methods it will use to make it easy and safe. NS/EP owners should also consider whether they want to establish a set of role-based access requirements that are not tied to unique people but rather functions.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Infrastructure	Information Security - Encryption	Policies and procedures shall be established and mechanisms implemented for encrypting sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging).	R.12 Intercepting data in transit; R.13 Data leakage on up/download, intra-cloud; R.17 Loss of encryption keys; R.23 Data protection risks; R.27 Modifying network traffic		X	X	Unencrypted data at rest or in transit makes it easier for an adversary to intercept information. Compensating / defense-in-depth controls can be provided to protect information from unauthorized disclosure within the cloud environment / data center. When data is processed in an unattended manner managing security of the at-rest encryption keys becomes a significant challenge in the cloud environment.	NS/EP applications can impose stringent encryption requirements based on the sensitivity of the data and/or classified data handling standards. However, NS/EP users may want to determine whether they need encryption for NS users and functions and no encryption for the emergency response side.
Infrastructure	Information Security - Audit Tools Access	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	R.22 Risks from changes of jurisdiction; R.28 Privilege escalation; R.30 Loss or compromise of operational logs; R.31 Loss or compromise of security logs		X	X	Appropriately segmenting and limiting access to and use of audit tools can reduce the risk that the user/owner of the system being audited has privileged access to that system and corrupts the audit log.	Audit logs that can be used to support investigations or post-incident analysis can be inadvertently or intentionally compromised or destroyed by users that have acquired privileged access to the log data.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Infrastructure	Information Security - Diagnostic / Configuration Ports Access and Utility Programs Access	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications. Utility programs capable of potentially overriding system, object, network, virtual machine and application controls shall be restricted.	R.26 Network management; R.28 Privilege escalation			X	Lack of proper user and application access rights can allow unauthorized access to diagnostic tools, configuration ports and utility programs that sit in the cloud service network or infrastructure management layer. Access to this management layer allows for configuration changes or the potential for insertion of malicious code that could ultimately undermine the underpinnings of the cloud infrastructure or virtual infrastructure including virtualized partitions.	NS/EP owners who are operating a collaborative platform may have the ability to run their own diagnostics or tools to determine if there is a security issue or understand a problem in the system and resolve it. There could be an instance where such tools are needed to conduct an investigation into breaches, misuse of data, or system compromise.
Infrastructure	Information Security - Network / Infrastructure Services and Third Party Agreements	Network and infrastructure service level agreements (in-house or outsourced) shall clearly document security controls, capacity and service levels, and business or customer requirements. Additionally, third party agreements that directly, or indirectly,	R.2 Loss of governance; R.8 Resource Exhaustion (under or over provisioning); R.7 Supply Chain Failure; R.12 Intercepting data in transit;		X	X	Service Level Agreements are key to ensuring that the owners' requirements for security controls (including non-standard controls), capacity and service levels, and other business requirements are completely spelled out and agreed to. Lack of clear documentation of these requirements	Specific, well-spelled out agreements must be documented and signed by all parties to ensure that the most critical functions are able to persist during an NS/EP event. Failure of such can result in a security breach, data leak or service interruption.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		impact an organization's information assets or data are required to include explicit coverage of all relevant security requirements. For network, infrastructure and third party SLAs, this includes agreements involving processing, accessing, communicating, hosting or managing the organization's information assets, or adding or terminating services or products to existing information. Assets agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	R.13 Data leakage on up/download, intra-cloud; R.17 Loss of encryption keys; R.20 Conflict between customer hardening procedures and cloud environment; R.26 Network management; R.27 Modifying network traffic; R.28 Privilege escalation				and mutual agreements can potentially lead to reliability issues due to misalignment of expectations and requirements.	

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Infrastructure	Information Security - Portable / Mobile Devices	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	R.12 Intercepting data in transit; R.17 Loss of encryption keys; R.23 Data protection risks	X	X	X	A lost or stolen portable device without the proper encryption protections can potentially put an organization's data in unauthorized hands and lead to compromise. Properly configured mobile devices can provide the necessary security protections for the device itself and the data residing or transmitting to/from the device. An additional risk comes from the use of consumer / low-end enterprise systems that automatically back up data to a cloud provider, which might not be configured appropriately for NS/EP purposes, and could lead to data leakage.	A properly encrypted and secured mobile/portable device may be a great tool during an NS/EP incident, particularly for emergency response. For instance, a mobile device can be used as a thin client to access and download required information during an NS/EP incident. Owners also need to ensure that authentication and authorization checks are in place. Also, in this low-bandwidth environment, users will need to be able to share data in a peer-to-peer situation. For NS/EP uses, policy should be established whereby mobile devices (laptops, tablets, cellphones, etc.) are managed, and can be remotely tracked, wiped or decommissioned.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Infrastructure	Information Security - Source Code Access Restriction	Access to application, program or object source code shall be restricted to authorized personnel on a need to know basis. Records shall be maintained regarding the individual granted access, reason for access and version of source code exposed.	R.2 Loss of governance; R.10 Cloud provider malicious insider-abuse of high privilege roles; R.20 Conflict between customer hardening procedures and cloud environment; R.28 Privilege escalation		X	X	Unauthorized access to source code could lead to the ability to insert malicious code or compromise existing code.	NS/EP owners need to particularly concerned about unauthorized access to source code because of the sensitivity of the issues that are being supported by their services. Also, it is important to note that code in the cloud can be refreshed (sometimes) on a biweekly basis and during the midst of a crisis.
Resiliency	Operations Management - Capacity / Resource Planning	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with regulatory, contractual and business requirements. Projections of future capacity requirements shall be made to	R.2 Loss of governance; R.8 Resource exhaustion; R.9 Isolation failure		X	X	Poor capacity management, planning, and requirements can lead to denial of service due to lack of available capacity when demand spikes.	NS/EP owners need to be especially concerned about instances where they may be sharing resources with other government agencies and they both are responding to competing incidents. Example, natural disaster in the U.S. and military issue abroad.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		mitigate the risk of system overload.						
Resiliency	Risk Management - Third Party Access	The identification, assessment, and prioritization of risks posed by business processes requiring third party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	R.2 Loss of governance; R.7 Supply Chain failure; R12. Intercepting data in transit; R.17 Loss of encryption keys; R.20 Conflict between customer hardening procedures and cloud environment; R.27 Modifying network traffic; R.28 Privilege escalation		X	X	Using cloud services is likely to involve a number of applications (app) providers. Understanding the interdependency and risk between and among app providers, CSP, and service owner is complex but essential.	NS/EP owners who are operating collaborative platforms and services will need to ensure that the NS/EP SLA requirements are extended to app providers. They should ensure that these providers comply with security and personnel requirements and have audit logs for code changes. Moreover, cycles for updates and changes to cloud services and applications are continuous, which raises concerns about the level of third-party access to the data and how to protect it (e.g. encryption considerations).

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Policy/Legal	Release Management - New Development / Acquisition	Policies and procedures shall be established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.	R.6 Cloud provider acquisition; R.11 Management interface compromise; R.13 Data leakage on up/download, intra-cloud; R.15 DDoS		X	X	The owner's risk does not include any of the risk to hardware acquisition or facilities. By virtue of deployment and development mechanisms for cloud software (especially in a PaaS environment), the risks associated with new software are reduced since it should be sufficiently tested in the cloud environment.	Due to the high impact of NS/EP services, cloud applications need to be developed with a lifecycle approach to security. For example, a DISA STIG can be used for implementing the proper controls for an NS/EP application. The owner should realize that they have a primary responsibility in all of the three possible service models. The development and testing of new software should be demonstrated by the Owner (in the PaaS or IaaS model) or by the Provider (in the SaaS model), if the Provider or a third-party is the creator of the software. All hardware infrastructure and facilities are the responsibilities of the Provider.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Infrastructure	Release Management - Production Changes	Changes to the production environment shall be documented, tested and approved prior to implementation. Production software and hardware changes may include applications, systems, databases and network devices requiring patches, service packs, and other updates and modifications.	R.7 Supply chain failure; R.26 Network management; R.27 Modifying network traffic		X	X	The unique characteristic here is the separation of the environments for cloud service provider and service owner. The provider will have primary responsibility for supporting a portion of the technology stack (varying by service model and CSP), some elements will be assigned joint responsibility, while others will be the sole responsibility of the service owner.	The owner and provider have shared responsibilities in this control area. The owner who uses the software has responsibility of ensuring the quality and provenance of the data; the provider has the responsibility to ensure that the production level software quality assured. In the PaaS service model, the owner has a greater role in the security and assurance of the software since they are the authors of that software and have deployed it in the cloud environment. In the IaaS service model, the owner is responsible for the software, creation of the virtual machines (VMs) and associated service updates for those VMs. In addition the owner needs to be able to block updates to the cloud resources that they are using to guarantee availability. It is possible in all three service models for changes to occur, initiated by the provider, that can impact availability.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Infrastructure	Security Architecture - Equipment Identification	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	R.2 Loss of governance			X	Failure to automatically identify and authenticate equipment connections could result in unknown equipment having "insider like" access to network resources, performing unauthorized activities.	In an NS/EP event, assets can be lost, damaged, stolen, or otherwise unaccounted for, which can result in its inappropriate use, mishandling, or destruction. NS/EP owners also need to determine whether unauthenticated equipment can be granted temporary access to network resources, determine the level of access to be granted, and implement sanitization/return procedures.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Infrastructure	Security Architecture - Audit Logging / Intrusion Detection	Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel.	R.2 Loss of governance; R.26 Network management; R.27 Modifying network traffic; R.28 Privilege escalation; R.30 Loss or compromise of operational logs; R.31 Loss or compromise of security logs; R.33 Unauthorized access to premises		X	X	Failure to enable, retain, and control access to appropriate audit logs, at least daily review of audit logs, coupled with file integrity and intrusion prevention systems allow unauthorized activity to exist without detection and severely limits root cause analysis capabilities. In addition, there may be availability issues if an IPS incorrectly flags activity as an intrusion attempt, and denies legitimate access to a system. This could have disastrous consequences in EP scenarios.	Poor audit logging and intrusion detection/prevention can lead to services that do not perform as expected when needed for an NS/EP incident. NS/EP owners need to be especially concerned about instances where they may be sharing resources with other government agencies and both are responding to competing incidents which could lead to denial of service due to lack of available capacity to handle demand spikes in the midst of an NS/EP incident. Additionally, in an NS/EP event where there is an application in the cloud supporting many users, the owner may want to have increased security monitoring to prevent the application from being unavailable or the target of an attack. SLAs need to provide enough resources and support for extra monitoring of the architecture.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Infrastructure Data Policy	Security Architecture - Customer Access Requirements	Prior to granting customers access to data, assets and information systems, all identified security, contractual and regulatory requirements for customer access shall be addressed and remediated.	R.2 Loss of governance; R.20 Conflict between customer hardening procedures and cloud environment; R.28 Privilege escalation; R.11 Management interface compromise		X	X	Failure to address security, contractual, and regulatory requirements prior to granting customer access creates substantial unmitigated risks for the owner. In most cases, the risks would be too high to begin operation. Requirements must be developed that allow privileges to only those who have been properly authorized to access certain data, applications, systems, etc.	NS/EP situations will require well developed designs and plans to ensure that security, contractual, and regulatory requirements continue to be met in all scenarios. Rapid provisioning of access to data, applications, devices, systems, etc. need to be accounted for, particularly in cross-jurisdictional scenarios.
Policy/Legal Data Interdependency	Security Architecture - Data Security	Policies and procedures shall be established and mechanisms implemented to ensure security (e.g., encryption, access controls, and leakage prevention) and integrity of data exchanged between one or more system interfaces, jurisdictions, or with a third party shared	R.2 Loss of governance; R.9 Isolation failure; R.12 Intercepting data in transit; R.13 Data leakage on up/download, intra-cloud; R.17 Loss of		X	X	Failure to protect data exchanged between systems, jurisdictions, or data using shared third party services could result in improper disclosure, alteration, or destruction of data.	Data exchange crosses many jurisdictional boundaries, particularly between federal, state, local, and private sector entities, which can lead to loss of data control. Additionally, the different tagging of data (e.g. FOUO, classified, etc.) can create concerns over compliance with data handling/management.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		services provider to prevent improper disclosure, alteration or destruction complying with legislative, regulatory, and contractual requirements.	encryption keys; R.22 Risks from changes of jurisdiction; R.23 Data protection risks; R.28 Privilege escalation					
Policy/Legal	Security Architecture - Application Security	Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and complies with applicable regulatory and business requirements.	R.3 Compliance challenges; R.11 Management interface compromise		X	X	Failure to incorporate appropriate security controls into applications could result in compromise of systems, applications, and data.	Due to the high impact of NS/EP services, cloud applications need to be developed with a lifecycle approach to security. For example, a DISA STIG can be used for implementing the proper controls for an NS/EP application. NS/EP owners who are operating collaborative platforms and services will need to ensure that the NS/EP SLA requirements are extended to app providers. They should ensure that these providers comply with security and personnel requirements and have audit logs for code changes. Moreover, cycles for updates and changes to cloud services

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
								and applications are continuous, which raises concerns about the level of 3rd party access to the data and how to protect it (e.g. encryption considerations). In the case of the use of COTS or open source software in cloud solutions, there needs to be a supply chain process put in place that guarantees the integrity of the solution being deployed.
Interdependency	Security Architecture - Shared Networks	Access to systems with shared network infrastructure shall be restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations.	R.2 Loss of governance: cross cloud applications creating hidden dependency; R.7 Supply chain failure; R.8 Resource exhaustion; R.9 Isolation failure; R.20 Conflict between customer hardening procedures and			X	Failure to appropriately restrict and document authorized personnel access to shared network infrastructure and implement compensating controls to separate network traffic between organizations could result in the unintended disclosure of information to untrusted parties.	CSPs that rely on third-party services or products as part of their cloud offerings may offer different levels of assurances or be supporting many other critical functions. Additionally, impacts to the underlying (telecommunications) infrastructure supporting cloud services can make cloud resources unavailable.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
			cloud environment; R.26 Network management; R.27 Modifying network traffic; R.28 Privilege escalation					
Interdependency Infrastructure Resiliency	Security Architecture - Network Security	Network environments shall be designed and configured to restrict connections between trusted and untrusted networks and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure. Network architecture diagrams must clearly identify high-risk environments and	R.2 Loss of governance: cross cloud applications creating hidden dependency; R.15 DDoS; R.16 Economic Denial of Service; R.17 Loss of encryption keys; R.18 Undertaking malicious probes or scans; R.26 Network management; R.27 Modifying		X	X	Failure to adequately separate trusted and untrusted networks could result in unintended access to the network and the devices connected to the network as well as disclosure of information (potentially classified or sensitive) to untrusted parties.	In an NS/EP event, managing an ad hoc user base and the devices they own and operate calls for policies that extend beyond the infrastructure itself and to the end points that are connected to the network. As the network will likely be stressed during an NS/EP event, it is important to consider the need for increased security monitoring to prevent key applications from being unavailable or the target of an attack.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		data flows that may have regulatory compliance impacts.	network traffic; R.28 Privilege escalation					
All	Information Security - Management Program	An Information Security Management Program (ISMP) has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management	R.2 Loss of governance; R.20 Conflict between customer hardening procedures and cloud environment; R.23 Data protection risks; R.33 Unauthorized access to premises; R.34 Theft of computer equipment		X	X	Poor ISMP by the owner or provider can have swift and broadly felt implications for both parties. For owners, it could enable staff to move unauthorized data into cloud for processing without management knowledge. Moreover, without an information security policy that is calibrated for the cloud, organizations can suffer data loss, misuse, unauthorized access, disclosure, alteration, and destruction.	Because of the broad spectrum of NS/EP users, building and maintaining an effective ISMP program that can address existing services, as well as, cloud services requires cross government collaboration, clear SLA's with CSP (including agencies), and oversight and enforcement mechanisms. This complexity is further heightened for two additional reasons. First, most NS/EP users are leveraging assets and services in response to emergencies and the infrequent use can hinder user compliance. Second, CSPs may have to rapidly scale resources to meet a surge in demand and the NS/EP service owner will need to ensure that all future capabilities can come

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		• Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance						online instantly and meet ISMP compliance requirements.
Resiliency	Information Security - Vulnerability / Patch Management/ Anti-virus/ Malicious software	Policies and procedures shall be established and mechanism implemented for	R.2 Loss of governance; R.10 Cloud provider		X	X	Development and implementation of an effective patch management policy and procedures are an	Unpatched devices, systems, or networks during an NS/EP event can result in the malfunction of assets and processes

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.	malicious insider-abuse of high privilege roles; R.26 Network management; R.27 Modifying network traffic; R.28 Privilege escalation; R.29 Social engineering attacks				important component in mitigating the risks associated with software vulnerabilities and overall network configuration management. Patches must be prioritized, tested, and deployed in a timely manner to prevent successful exploitation of and mitigate threats to devices, systems, and networks. When applicable, work arounds and/or mitigating controls should be applied immediately for issues that pose a high risk to the environment in order to provide protections while patches are being deployed. In addition to centralized automated signature updates and malicious code protection mechanisms (e.g. integrity scans), controls must be in place to prevent non-privileged users from circumventing these	which can impede communications and/or the flow of data. As such, patches must be up-to-date for all data, devices, applications, and systems classified as critical. Additionally, in an NS/EP event when processes will likely be highly distributed/decentralized, removable media or user-installed software can introduce malicious code into the system, device, network without user awareness. NS/EP owners may want to require that users/devices are up to date with current browsers, AV and applications to reduce the chance of security issues being introduced into services.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
							mechanisms.	
Resiliency	Information Security - Incident Management and Reporting	Policy, process and procedures shall be established to triage security related events and ensure timely and thorough incident management. Contractors, employees and third party users shall be made aware of their responsibility to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a prompt and expedient manner in compliance with statutory, regulatory and contractual requirements.	R.8 Resource exhaustion; R.10 Cloud provider malicious insider; R.16 Economic Denial of Service; R.28 Privilege escalation; R.29 Social engineering attacks	X	X	X	Incident management policies, processes, and procedures must be kept up-to-date to ensure an efficient, effective, and orderly incident response capability, including identification, detection, containment/eradication, and recovery processes. Incident severity categories should also be in place to appropriately respond to and resource the incident. The accountability to and execution of these roles must be clearly defined.	NS/EP users, NS/EP service owners, and CSPs will require a high level of collaboration during an event. Users and owners should already be familiar with the technology/service/process prior to the outbreak of an event to prevent any bottlenecks in getting the right data to the right people. Owners and CSPs also need to manage the large amounts of (uncontrollable) data flow and ensure dissemination of the most relevant and critical data. The capability to appropriately handle an incident can also be compromised if adequate resources are strained or not appropriately accounted for. CSPs also need to provide a reliable and resilient infrastructure and rapid scalability of capacity to prevent oversaturation of

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
								the network. Prompt reporting of suspected or actual incidents to the right entities/authorities can be stymied with vast amounts of data being disseminated and competing priorities during an NS/EP event. The capability to sufficiently resource the handling of a reported incident can also be compromised.
All	Risk Management - Program	Organizations shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level.	R.23 Data protection risks; R.27 Modifying network traffic		X		Migrating a series of operations to the cloud can change the risk profile-based on how the services are going to be used.	In a traditional NS/EP context, the NS/EP owner had defined risk management issues delineating their responsibilities and their carrier's responsibilities. In the cloud environment, an overarching NS/EP risk management plan is required that considers the risks introduced and assumed by multiple stakeholders, including the carrier, cloud provider, application provider, and user. The Owner is the primary responsible party in this scenario. As with all IT organizations, the

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
								infrastructure, software, data & services should be operated and maintained in a method appropriate to the level of acceptable (low/med/high) risk program. It is their duty to ensure that the Provider has also made the necessary efforts and security controls as well.
Resiliency	Risk Management - Assessments/Mitigation/ Acceptance	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory	R.2 Loss of governance; R.23 Data protection risks; R.30 Loss or compromise of operational logs		X	X	Each cloud architecture relies on a highly specialized platform, the service engine that sits above the physical hardware resources and manages customer resources at different levels of abstraction. For example, in IaaS clouds this software component can be the hypervisor. The service engine is developed and supported by cloud platform vendors and the open source community in some cases. It can be further customized by the cloud computing providers. Like any other software layer, the service engine	The NS/EP owner will need carefully evaluate the overall functional risk of the service they are supplying (via the provider) and then ensure that those risks are mitigated by the platform chosen and thru the specific actions of the CSP. Additionally, because of the high consequences of NS/EP communications failures, the NS/EP owner will need to perform some due diligence stress tests and exercises to ensure readiness.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		compliance).					code can have vulnerabilities and is prone to attacks or unexpected failure. An attacker can compromise the service engine by hacking it from inside a virtual machine (IaaS clouds), the runtime environment (PaaS clouds), the application pool (SaaS clouds), or through its APIs. Hacking the service engine may be useful to escape the isolation between different customer environments (jailbreak) and gain access to the data contained inside them, to monitor and modify the information inside them in a transparent way (without direct interaction with the application inside the customer environment), or to reduce the resources assigned to them, causing a denial of service.	

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
Resiliency	Resiliency - Management Program	Policy, process and procedures defining business continuity and disaster recovery shall be put in place to minimize the impact of a realized risk event on the organization to an acceptable level and facilitate recovery of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) through a combination of preventive and recovery controls, in accordance with regulatory, statutory, contractual, and business requirements and consistent with industry standards. This Resiliency management program shall be communicated to all organizational participants with a	R.15 Distributed Denial of Service; R.25 Network breaks; R.26 Network management; R.35 Network disasters		X	X	To deploy enterprise solutions in the cloud, off-premise solutions must be architected differently than on-premise solutions. The focus in this instance should be on architecture. You don't buy security, compliance, failover, resiliency....you build it.	The NS/EP risk would be to view the cloud as having the same "traditional" factors that are considered when developing the program. Omission by definition equals risk. The provider has the primary responsibility for delivering on the resiliency (i.e., uptime/failover), and they need a plan that they develop, distribute and implement as it relates to their own infrastructure, but the owner can has a secondary responsibility to ensure that their particular needs are met by defining what their parameters will be prior to entering into a cloud services agreement.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		need to know basis prior to adoption and shall also be published, hosted, stored, recorded and disseminated to multiple facilities which must be accessible in the event of an incident.						
Resiliency	Resiliency - Impact Analysis	There shall be a defined and documented method for determining the impact of any disruption to the organization which must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners and third party service providers	R.2- Cross cloud applications creating hidden dependency; R.3 Compliance challenges; R.8 Resource exhaustion; R.9 Isolation failure; R.12 Intercepting data in transit; R.20 Conflicts between customer hardening procedures and cloud environment;		X	X	Needs to encompass both risk and impact to ensure resiliency. The risk if it does is that they are addressing two different focus areas and are commonly confused – A risk assessment determines what could cause an outage; a business impact analysis shows the effects if one did occur.	The issue lies in the resulting consequences of interruptions of varying durations, regardless of the causation. The downstream affects lead to mistakes such as: a. Considering the impact of interrupted applications, not business functions b. Considering applications in isolation c. While business users may know which applications they rely on, they do not often know which other applications or infrastructure those

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		• Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the	R.22 Risk from changes of jurisdiction; R.23 Data protection risks					applications rely on d. Failing to distinguish enterprise applications e. Failing to recognize data center applications f. Some applications do not have business users g. These applications include the operating systems, database management systems and data center tools that enable business applications. It is easy to say that all of the infrastructure must be recovered before all applications, but should the operating system on an obscure server that performs analysis really be recovered before the mission systems? h. Confusing risk acceptance with an impact analysis

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		resources required for resumption						i. If a business manager is willing to take the risk of an application's unavailability that does not mean it's not necessary to determine the impact.
Resiliency	Resiliency - Business Continuity Planning	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing and maintenance and information security requirements. Requirements for business continuity	R.32 Backups lost, stolen		X	X	The cloud provider's plan will be an extension of the organizational BCP that in many cases already developed. This is a major risk area b/c of the interdependencies that will occur and may not be fully understood and/or recognized up front prior to moving to the cloud. Many people view "cloud computing" as the solution for BCP and that is also a risk. The cloud is not the	The NS/EP owner needs to think about the BCP of both the application and cloud service provider. For example, if an application has to be patched or changed in a crisis situation, will the provider be able to meet your SLAs for that function? Additionally, when considering the global nature of the cloud environment, what are the implications of the different deployment models on BCP? For example, in a

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update and approval • Defined lines of communication, roles and responsibilities • Detailed recovery procedures, manual work-around and reference					panacea for poor planning.	public cloud model, data centers reside all over world and data can rapidly move between data centers. However, in a private cloud model, only two data centers may be involved, which can limit redundancy capabilities, and result in a different BCP process than for a public cloud model.

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
		information • Method for plan invocation						
Resiliency	Resiliency - Equipment Location/ Power Failures	To reduce the risks from environmental threats, hazards and opportunities for unauthorized access equipment shall be located away from locations subject to high probability environmental risks and supplemented by redundant equipment located a reasonable distance.	R.5 Cloud service termination or failure; R.8 Resource exhaustion; R.21 Subpoena and e-discovery; R.25 Network breaks; R.26 Network management; R.33 Unauthorized access to premises; R.34 Theft of computer			X	The cloud provider's plan will be an extension of the organizational BCP that in many cases already developed. This is a major risk area b/c of the interdependencies that will occur and may not be fully understood and/or recognized up front prior to moving to the cloud. Many people view "cloud computing" as the solution for BCP and that is also a risk. The cloud is not the panacea for poor planning.	Equipment power failures are, in almost all NS/EP situations, region-specific with minimal likelihood that such a failure would occur at the national level. Owners need a well-planned redundancy process in place to ensure that back-up facilities/equipment will perform and provide the necessary capacity and functions. Additionally, in an NS/EP app scenario, can an owner take the app and port it to another CSP rapidly because of the CSP's greater redundancy capability? Or would certain P2P capabilities be built in the application to overcome

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
			equipment; R.35 Network disasters					this scenario?
Resiliency	Resiliency - Power / Telecommunications	Telecommunications equipment, cabling and relays transceiving data or supporting services shall be protected from interception or damage and designed with redundancies, alternative power source and alternative routing.	R.5 Cloud service termination or failure; R.8 Resource exhaustion			X	The cloud provider's telecommunications continuity plan must support the service owner's organizational BCP. The service owner must also have a telecommunications continuity plan for the telecomm links within its scope of responsibility. This is a major risk area b/c of the interdependencies that will occur and may not be fully understood and/or recognized up front prior to moving to the cloud.	Specific NS/EP / CI Telecomm resilience needs must be clearly articulated as requirements to the Telecomm Provider. Resilience needs of and failure scenarios for many NS/EP services may cover areas not normally addressed under the Telecomm Provider's business continuity / resiliency planning of a general-purpose service. NS/EP SLAs must be adopted. Another consideration is how to negotiate priority access to 4G networks with the carriers in order to access and leverage the

Primary NSTAC Concerns	Control Area	Control Specification	ENISA Mapping R.35 Natural Disasters applicable to all	Responsible Party			Unique Characteristic or Risk	Potential NS/EP Implications
				User	Owner	Provider		
								capabilities of the cloud.

5.2 ISACA IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
Policy/Legal	PO1.1 IT Value Management Work with the business to ensure that the enterprise portfolio of IT-enabled investments contains programmes that have solid business cases. Recognise that there are mandatory, sustaining and discretionary investments that differ in complexity and degree of freedom in allocating funds. IT processes should provide effective and efficient delivery of the IT components of programmes and early warning of any deviations from plan, including cost, schedule or functionality, that might impact the expected outcomes of the programmes. IT services should be executed against equitable and enforceable SLAs. Accountability for achieving the benefits and controlling the costs should be clearly assigned and monitored. Establish fair, transparent,		x	x	IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resources requirements and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise	R.2 Loss of governance	An IT plan and processes around it are required to define details in non-NS/EP scenarios for optimum efficiency, performance, governance, risk and compliance; additional details, plans and processes must be identified to maximize efficiency and minimize chaos for NS/EP scenarios. Given that no specific standards for GRC are currently in place for the Cloud, existing IT standards should be observed with additional cloud best practices included. These standards and best practices should be coordinated between owner and provider as well. Additionally, it should be noted that there are emerging cloud	The user community is not involved in the strategic or tactical planning of the owner and thereby their requirements are not met by the owner or the provider, regardless of how good their individual planning may be. IT strategic planning for NS/EP incidents needs to be coordinated between owner and provider and an SLA in place to ensure that this planning is followed in the case of an NS/EP incident.

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	repeatable and comparable evaluation of business cases, including financial worth, the risk of not delivering a capability and the risk of not realising the expected benefits.				objectives, action plans and tasks that are understood and accepted by both business and IT.		standards, which can pose a new risk in that use of existing standards may require rework when cloud-specific standards emerge.	
Policy/Legal	PO1.3 Assessment of Current Capability and Performance Assess the current capability and performance of solution and service delivery to establish a baseline against which future requirements can be compared. Define performance in terms of IT's contribution to business objectives, functionality, stability, complexity, costs, strengths and weaknesses. Comment: The current capability and performance can be used to evaluate the decision to utilise a cloud solution and the requirements of the CSP to satisfy the customer's requirements.		x	x				
Interdependency	PO1.5 IT Tactical Plans Create a portfolio of tactical IT plans that are derived from the IT strategic plan. The		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	tactical plans should address IT-enabled programme investments, IT services and IT assets. The tactical plans should describe required IT initiatives, resource requirements, and how the use of resources and achievement of benefits will be monitored and managed. The tactical plans should be sufficiently detailed to allow the definition of project plans. Actively manage the set of tactical IT plans and initiatives through analysis of project and service portfolios.							
Policy/Legal	PO1.6 Portfolio Management Actively manage with the business the portfolio of IT-enabled investment programmes required to achieve specific strategic business objectives by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling programmes. This should include clarifying desired business outcomes, ensuring that programme objectives support achievement of the outcomes,		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	understanding the full scope of effort required to achieve the outcomes, assigning clear accountability with supporting measures, defining projects within the programme, allocating resources and funding, delegating authority, and commissioning required projects at programme launch.							
Data	PO2.2 Enterprise Data Dictionary and Data Syntax Rules Maintain an enterprise data dictionary that incorporates the organisation's data syntax rules. This dictionary should enable thesharing of data elements amongst applications and systems, promote a common understanding of data amongst IT and business users, and prevent incompatible data elements from being created. Comment: This would apply to customizable processes within SaaS and with systems developed in PaaS.		x		PO2 Define the Information Architecture The information systems function creates and regularly updates a business information model and defines the appropriate systems to optimise the use of this information. This encompasses the development of a corporate data dictionary with the organisation's data syntax rules, data classification scheme and security levels. This process improves the quality of management decision making by making sure that reliable	R.20 Conflicts between customer hardening procedures and cloud environment	This would require a considerable upfront investment by the business owners to develop and deploy a data dictionary that covers all of their enterprise applications. Generally, there is no upper management appreciation of the value of this need and no budget to perform it. Today, there is no way to easily assess the security proposition of an individual cloud service. Additionally, without a formal data classification scheme exposed by the	Lack of a sound data dictionary can cause problems within and across organizations. Organizations may call the same data element by different names or they may call different data elements by the same name across an enterprise. As a result, an organization may not collect all of the information it needs or it may

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
Data	PO2.3 Data Classification Scheme Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption.		x		and secure information is provided, and it enables rationalising information systems resources to appropriately match business strategies. This IT process isalso needed to increase accountability for the integrity and security of data and to enhance theeffectiveness and control of sharing information across applications and entities.		provider, organizations tend to play it safe adopting the cloud for only those tasks that present the most minimal risk. Also, since the sensitivity of data can be subjective, it's all about context and that's tough to measure. Even if it were easy, the prospect of declaring a data classification and grading accordingly is a scary one since it begs the question – "now what"? Are we willing to modify existing business applications and processes to segregate data and unify protection metrics around each tier of classification? More importantly, can it be done (i.e. time/budget). Worse still, the whole thing is a moving target with more types of data coming under the regulatory spotlight every day. In the context of	be unable to combine or map data across systems because the definitions are not identical. A worse possibility is that an organization may combine data elements it believes to be equivalent and draws incorrect inferences from the invalid data. Multiple users entering data may have different definitions or perceptions of what goes into a data field, thereby confounding the data and making it useless. How does the cloud provider manage this in a NS/EP environment that is large, diverse, and rapidly changing?

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
							adoption of cloud computing for NS/EP purposes, FIPS 199 would apply, and an assessment of risk to data assets would need to be conducted to determine whether they are low or medium impact, and the associated FedRAMP controls also need to be considered.While many adopters of cloud computing may choose perceived low-risk applications and data, without actually doing an inventory of data assets they are introducing risk.	
Infrastructure	PO3.1 Technological Direction Planning Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Also identify in the plan which technologies have the potential to create business opportunities. The		x	x	PO3 Determine Technological Direction The information services function determines the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages	R.5 Cloud service termination R.6 Cloud provider acquisition R.7 Supply chain failure	There is no standardized capability maturity model developed for use when it comes to Cloud Computing for use in technological planning. Since there are no standardized processes to deploy cloud-services; instead, ad hoc and isolated	Any changes to technological direction that affect the provider must be communicated immediately to the provider from the owner to ensure that all systems are working most

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.				clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. The plan is regularly updated and encompasses aspects such as systems architecture, technological direction, acquisition plans, standards, migration strategies and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems staffing and investments, as well as improved interoperability of platforms and applications.		approaches are used that tend to be applied on an individual or case-by-case basis. It is a reactive and operationally focused approach to providing cloud services. Technology directions are driven by the often contradictory product evolution plans of hardware, systems software and applications software vendors rather than the needs of the owners/users. Also, communication of the potential impact of technology changes, not in the owner/provider's control is inconsistent.	efficiently are in sync. Regularly updating the plan to account for changes (e.g. lessons learned, technological upgrades) in the NS/EP environment can help to achieve responsiveness and preparedness during the outbreak of an event. An impact arising from the change in technological direction is likely minimized when using IaaS, rising with PaaS, and is likely the greatest when using SaaS. This should be considered when evaluating cloud-based solutions.
Infrastructure	PO3.2 Technology Infrastructure Plan Create and maintain a technology infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan should be based on the technological direction and include contingency arrangements and direction for acquisition of technology resources. It should consider changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications. Comment: The infrastructure plan will be limited to CSP capabilities vs. customer needs and customer interfaces to the CSP provided technology (IaaS) or software (SaaS).		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
Interdependency	PO4.5 IT Organisational Structure Establish an internal and external IT organisational structure that reflects business needs. In addition, put a process in place for periodically reviewing the IT organizational structure to adjust staffing requirements and sourcing strategies to meet expected business objectives and changing circumstances. Comment: The organisational structure will transition from an operational to a management focused group of processes.		x	x	PO4 Define the IT Processes, Organisation and Relationships An IT organisation is defined by considering requirements for staff, skills, functions, accountability,authority, roles and responsibilities, and supervision. This organisation is embedded into an IT process framework that ensures transparency and control as well as the involvement of senior executives and business management. A strategy committee ensures board oversight of IT, and one or more steering committees in which business and IT participate determine the prioritisation of IT resources in line with business needs. Processes, administrative policies and procedures arein place for all functions, with specific attention to control, quality	R.2 Loss of governance R.4 Loss of business reputation due to co-tenant activities R.10 Cloud provider malicious insider-abuse of high privilege role R.11 Management interface compromise (manipulation, availability of infrastructure) R.12 Intercepting data in transit R.13 Data leakage on up/download, intra-cloud R.14 Insecure of ineffective deletion of data R.20 Conflicts between customer hardening procedures and cloud environment R.22 Risk from	Whether the size of a given enterprise's IT staff will need to change as it ascends into the cloud depends on current staffing and business needs. However, there is no question that two types of staffing shifts will take place: individuals who are working in IT today will need to learn new skills, and certain jobs will shift from the enterprise to the cloud service provider. Enterprises will continue to need individuals who understand the company's software applications and how the applications relate to the business. Also, service owners will still need project managers, business analysts and network administrators as cloud-based systems will not manage themselves. Cloud computing, today, is replacing the	It is critical that policies and procedures pertaining to personnel security, such as access rights/controls, user privileges, etc., are both known and adhered to by ad hoc users. However, this can be a challenge during an NS/EP event where first responders from other jurisdictions are needed for reinforcement and require immediate access to specific services/application. Service owners need to implement a process that provides flexibility while maintaining security.
Interdependency	PO4.6 Establishment of Roles and Responsibilities Establish and communicate roles and responsibilities for IT personnel and end users that delineate between IT personnel and end-user authority, responsibilities and accountability for meeting the organisation's needs. Comment: The organisational structure will transition from		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	an operational to a management focused group of processes.				assurance, risk management, information security, data and systems ownership, and segregation of duties. To ensure timely support of business requirements, IT is to be involved in relevant decision processes.	changes of jurisdiction R.23 Data protection risks R.28 Privilege escalation R.29 Social engineering attack (IE, impersonation)	datacenter. There is some, but not measurable, adoption of virtual desktop infrastructure in the cloud. That means that an IT department focused on desktop maintenance will still be required. Some servers will likely never move to the cloud, including those supporting Tier-1 applications that are not cloud-ready. Existing IT staff required to manage applications and operating systems on servers will need to be retained if IaaS is used.	
Data	PO4.9 Data and System Ownership Provide the business with procedures and tools, enabling it to address its responsibilities for ownership of data and information systems. Owners should make decisions about classifying information and systems and protecting them in line with this classification.		x					
Policy/Legal	PO4.11 Segregation of Duties Implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. Make sure that personnel are performing only authorised duties relevant to their respective jobs and positions.		x	x				
Resiliency	PO4.12 IT Staffing Evaluate staffing requirements on a regular basis or upon major changes		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	to the business, operational or IT environments to ensure that the IT function has sufficient resources to adequately and appropriately support the business goals and objectives. Comment: IT staffing requirements will change as the operational staff move to a more strategic, business focused and monitoring role in a production cloud environment.							
Resiliency	PO4.13 Key IT Personnel Define and identify key IT personnel (e.g., replacements/backup personnel), and minimise reliance on a single individual performing a critical job function. Comment: See PO4.12		x	x				
Policy/Legal	PO4.14 Contracted Staff Policies and Procedures Ensure that consultants and contract personnel who support the IT function know and comply with the organisation's policies for the		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	protection of the organisation's information assets such that they meet agreed-upon contractual requirements. Comment: No difference to any outsourcing arrangement.							
Interdependency	PO4.15 Relationships Establish and maintain an optimal coordination, communication and liaison structure between the IT function and various other interests inside and outside the IT function, such as the board, executives, business units, individual users, suppliers, security officers, risk managers, the corporate compliance group, outsourcers and offsite management. Comment: No difference to any outsourcing arrangement.		x	x				
Policy/Legal	PO6.2 Enterprise IT Risk and Control Framework Develop and maintain a framework that defines the enterprise's overall approach to IT risk and control and that		x	x	PO6 Communicate Management Aims and Direction Management develops an enterprise IT control framework and defines	R.1-R.35 (all risks are applicable)	Depending upon the standards and best practices that the owner decides to implement, compliance reporting run on a regular basis	There has yet to be "regulation" around NS/EP policy and reporting requirements.

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	aligns with the IT policy andcontrol environment and the enterprise risk and control framework. Comment: ERM must be updated to reflect specific risks introducedthrough cloud computing.				and communicates policies. An ongoing communication programme is implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management. The communication supports achievement of IT objectives and ensures awareness and understanding of business and IT risks, objectives and direction. The process ensures compliance with relevant laws and regulations.		and provides insurance that all processes and plans are being properly implemented across environments. If there are any SLA agreements with providers that they also follow specific standards or best practices, reporting back from them also provides assurance that the provider is in compliance with the agreed upon standards and best practices.	
Policy/Legal	PO6.3 IT Policies Management Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly. Comment: Policies directly affecting cloud should be aligned with the CSP contract and the SLAs.		x	x				
Policy/Legal	PO7.1 Personnel Recruitment and Retention Maintain IT personnel recruitment processes in line with the overall		x	x	PO7 Manage IT Human Resources A competent workforce is acquired and maintained for the	R.10 Cloud provider malicious insider-abuse of high privilege role R.28 Privilege	One of the most fundamental issues, deciding who is actually part of the acquisition workforce, is a bit of a	Service agreements are often made by people whose principal skills are

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	organisation's personnel policies and procedures (e.g., hiring, positive work environment, orienting). Implement processes to ensure that the organisation has an appropriately deployed IT workforce with the skills necessary to achieve organisational goals. Comment: Personnel needs will change. IaaS and SaaS platforms will require a focus on personnel who can manage the CSP relationship. Many IT tasks will move to the business units.				creation and delivery of IT services to the business. This is achieved by following defined and agreed-upon practices supporting recruiting, training, evaluating performance, promoting and terminating. This process is critical, as people are important assets, and governance and the internal control environment are heavily dependent on the motivation and competence of personnel.	escalation R.29 Social engineering attack (IE, impersonation) R.30 Loss or compromise of operational logs R.31 Loss or compromise of security logs (Manipulation of forensic investigation) R.32 Backups lost, stolen R.33 Unauthorized access to premises (including physical access to machines and other facilities)	challenge. Depending upon who you talk to in DoD or FAI they categorize them differently. The FAI model doesn't account for the engineers, logisticians, and finance people that are all an important part of the PM team. DoD considers them part of the acquisition workforce, where FAI does not. Another problem we're facing is that many people are in project management type jobs, even though they aren't "coded" for that position.	often not in acquisitions.
Policy/Legal	PO7.2 Personnel Competencies Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Define core IT competency requirements and verify that they are being maintained, using qualification and certification programmes where appropriate. Comment: IT competencies change as described in		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	PO7.1.							
Policy/Legal	PO7.3 Staffing of Roles Define, monitor and supervise roles, responsibilities and compensation frameworks for personnel, including the requirement to adhere to management policies and procedures, the code of ethics, and professional practices. The level of supervision should be in line with the sensitivity of the position and extent of responsibilities assigned. Comment: See PO7.1		x	x				
Interdependency	PO7.4 Personnel Training Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organisational goals. Comment: Objective remains in place, however, some responsible organisations will		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	move into the business.							
Interdependency	PO7.5 Dependence Upon Individuals Minimise the exposure to critical dependency on key individuals through knowledge capture (documentation), knowledge sharing, succession planning and staff backup. Comment: Non-cloud specific process, but required. The transfer of responsibility to the business units may result in single points of failure.		x	x				
Policy/Legal	PO8.3 Development and Acquisition Standards Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schemaand data dictionary design standards; user		x		PO8 Manage Quality A quality management system (QMS) is developed and maintained that includes proven development and acquisition processes and standards. This is enabled by planning, implementing and maintaining the QMS by providing clear quality requirements, procedures and policies.	R.1 Lock-in R.3. Compliance challenges R.5 Cloud service termination or failure R.6 Cloud provider acquisition R.7 Supply chain failure R.9 Resource acquisition (under or	As an organization moves to a cloud environment, it is important that they establish an articulate quality bar for development, processes and standards so as to ensure that the new cloud environment maintains or exceeds their previously determined quality bar.	A differing set of quality standards and processes may be necessary during an NS/EP incident. This quality bar must be clearly articulated, documented, communicated and signed off via an SLA so that both owner and

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans;and unit, regression and integration testing. Comment: The management focus must be on approval of acquisitionsand support for business cases and cost/benefits.				Quality requirements are stated and communicated in quantifiable and achievable indicators. Continuous improvement is achieved by ongoing monitoring, analysis and acting upon deviations, and communicating results to stakeholders. Quality management is essential to ensure that IT isdelivering value to the business, continuous improvement and transparency for stakeholders.	over provisioning)		provider understand the quality bar required during NS/EP incidents.
Resiliency	PO9.3 Event Identification Identify events (an important realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects. Determine the nature of the impact and maintain this information.		X	X	PO9 Assess and Manage IT Risks A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified,	R.1-R.35 (all risks are applicable)	The organization's Risk appetite and Risk management framework must be well defined. Risks and mitigations must be defined in a way that can be measured and monitored and meaningful to the stakeholders.	The unique NS/EP risk scenarios must be identified in the RMF and mitigations must crafted with NS/EP scenarios in mind. Agreements with Providers must be established to define the provider's role in

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	Record and maintain relevant risks in a risk registry. Comment: Address new risks that apply only to cloud.				analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.			NS/EP mitigations.
Resiliency	PO9.4 Risk Assessment Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis. Comment: See PO9.3		X	X				
Resiliency	PO9.5 Risk Response Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels.		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	Comment: See PO9.3							
All	PO10.1 Program Management Framework Maintain the programme of projects, related to the portfolio of IT-enabled investment programmes, by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling projects. Ensure that the projects support the programme's objectives. Coordinate the activities and interdependencies of multiple projects, manage the contribution of all the projects within the programme to expected outcomes, and resolve resource requirements and conflicts.		X		PO10 Manage Projects A programme and project management framework for the management of all IT projects isestablished. The framework ensures the correct prioritisation and co-ordination of all projects. The framework includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, QA, a formal test plan, and testing and post-implementationreview after installation to ensure project risk management and value delivery to the business. This approach reduces the risk of unexpected costs and project cancellations, improves communications to and involvement of business and end users, ensures the value and quality ofproject deliverables,	N/A	The organization must have a holistic enterprise view when integrating external services such as cloud computing. The complexity of building solutions based in-part on externally provided Cloud services requires agreements between service owners & providers detailing responsibilities of each party for ensuring comprehensive project management.	NS/EP service owners must establish SLAs with service providers that clearly identify NS/EP scenarios, the plan of action and the responsibilities of each party to ensure the preparedness of people, processes, and technologies during an event. BCP also needs to be considered. For instance, when considering the global nature of the cloud environment, what are the implications of different deployment models on BCP?
All	PO10.2 Project Management Framework Establish and maintain a project management framework that defines the scope and boundaries of managing projects, as well as the method to be adopted and applied to each project undertaken. The framework		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	and supporting method should be integrated with the programme management processes. Comment: IaaS and SaaS would relate to the conversion; PaaS would be ongoing for each project.				and maximises their contribution to IT-enabled investment programmes.			
All	PO10.3 Project Management Approach Establish a project management approach commensurate with the size, complexity and regulatory requirements of each project. The project governance structure can include the roles, responsibilities and accountabilities of the programme sponsor, project sponsors, steering committee, project office and project manager, and the mechanisms through which they can meet those responsibilities (such as reporting and stage reviews). Make sure all IT projects have sponsors with sufficient authority to own the execution of the project within the overall strategic programme.		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	Comment: IaaS and SaaS would relate to the conversion; PaaS would be ongoing for each project.							
All	PO10.5 Project Scope Statement Define and document the nature and scope of the project to confirm and develop amongst stakeholders a common understanding of project scope and how it relates to other projects within the overall IT-enabled investment programme. The definition should be formally approved by the programme and project sponsors before project initiation.		X					
All	PO10.6 Project Phase Initiation Approve the initiation of each major project phase and communicate it to all stakeholders. Base the approval of the initial phase on programme governance decisions. Approval of subsequent phases should be based on review and acceptance of the deliverables of the previous		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	phase, and approval of an updated business case at the next major review of the programme. In the event of overlapping project phases, an approval point should be established by programme and project sponsors to authorise project progression.							
All	PO10.7 Integrated Project Plan Establish a formal, approved integrated project plan (covering business and information systems resources) to guide project execution and control throughout the life of the project. The activities and interdependencies of multiple projects within a programme should be understood and documented. The project plan should be maintained throughout the life of the project. The project plan, and changes to it, should be approved in line with the programme and project governance framework.		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
All	PO10.8 Project Resources Define the responsibilities, relationships, authorities and performance criteria of project team members, and specify the basis for acquiring and assigning competent staff members and/or contractors to the project. The procurement of products and services required for each project should be planned and managed to achieve project objectives using the organisation's procurement practices.		X					
Resiliency	PO10.9 Project Risk Management Eliminate or minimise specific risks associated with individual projects through a systematic process of planning, identifying, analysing, responding to, monitoring and controlling the areas or events that have the potential to cause unwanted change. Risks faced by the project management process and the project deliverable should be established and centrally recorded.		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
All	PO10.10 Project Quality Plan Prepare a quality management plan that describes the project quality system and how it will be implemented. The plan should be formally reviewed and agreed to by all parties concerned and then incorporated into the integrated project plan.		X					
All	PO10.11 Project Change Control Establish a change control system for each project, so all changes to the project baseline (e.g., cost, schedule, scope, quality) are appropriately reviewed, approved and incorporated into the integrated project plan in line with the programme and project governance framework.		X	X				
All	PO10.12 Project Planning of Assurance Methods Identify assurance tasks required to support the accreditation of new or modified systems during project planning, and include		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	them in the integrated project plan. The tasks should provide assurance that internal controls and security features meet the defined requirements.							
All	PO10.13 Project Performance Measurement, Reporting and Monitoring Measure project performance against key project performance scope, schedule, quality, cost and risk criteria. Identify any deviations from the plan. Assess the impact of deviations on the project and overall programme, and report results to key stakeholders. Recommend, implement and monitor remedial action, when required, in line with the programme and project governance framework.		X	X				
All	PO10.14 Project Closure Require that, at the end of each project, stakeholders ascertain whether the project delivered the planned results and benefits. Identify and communicate any outstanding activities required to achieve		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	the planned results of the project and the benefits of the programme, and identify and document lessons learned for use on future projects and programmes.							
All	AI1.1 Definition and Maintenance of Business Functional and Technical Requirements Identify, prioritise, specify and agree on business functional and technical requirements covering the full scope of all initiatives required to achieve the expected outcomes of the IT enabled investment programme. Comment: This is not a cloud specific step. However, it should be required prior to considering a cloud computing solution.		X		AI1 Identify Automated Solutions The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach. This process covers the definition of the needs, consideration of alternative sources, review of technological and economic feasibility, execution of a risk analysis and cost-benefit analysis, and conclusion of a final decision to 'make' or 'buy'. All these steps enable organisations to minimisethe cost to acquire and implement solutions whilst ensuring	R.6 Cloud provider acquisition R.7 Supply chain failure R.8 Resource exhaustion (under or over provisioning) R.9 Isolation failure R.20 Conflicts between customer hardening procedures and cloud environment R.22 Risk from changes of jurisdiction R.23 Data protection risks	Service owners must clearly identify business and technical requirements followed by risk analysis and feasibility studies prior to making a solution decision. The cost of cloud computing services is compelling but a thorough analysis may identify unforeseen risks and costs. Additionally, a distinction between new automated solutions vs. migration of existing solutions to cloud platforms (especially relevant for IaaS) should be made. At the end of hardware lifecycles, the decision might be made to move to a cloud platform to save capital expenditure, and shift	NS/EP owners have unique requirements and must have appropriate assurance that cloud services will perform as required in specified NS/EP scenarios. For example, automated updates to devices and applications raise concerns with regard to the level of 3rd party access to (sensitive) data. Additionally, owners needs to prioritize which applications would (not) be continuously
All	AI1.2 Risk Analysis Report Identify, document and analyse risks associated with the business requirements and solution design as part of the organisation's process for the development of		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	requirements. Comment: This would be required for all projects. Cloud computing poses new risks requiring consideration.				that they enable the business to achieve its objectives.		to operational expenditure, yet no new automated solutions are actually acquired.	monitored in low bandwidth situations.
All	AI1.3 Feasibility Study and Formulation of Alternative Courses of Action Develop a feasibility study that examines the possibility of implementing the requirements. Business management, supported by the IT function, should assess the feasibility and alternative courses of action and make a recommendation to the business sponsor. Comment: This is a standard step in all feasibility studies. Cloud computing is one alternative, with its own set of risks and rewards.		X					
All	AI1.4 Requirements and Feasibility Decision and Approval Verify that the process requires the business sponsor to approve and sign off on business functional and		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	technical requirements and feasibility study reports at predetermined key stages. The business sponsor should make the final decision with respect to the choice of solution and acquisition approach. Comment: IaaS and PaaS requires IT involvement, a process with which most IT organisations are familiar. SaaS decisions are often made outside the IT organisation. Focus should be on the business unit's evaluation of the proposal and alternative solutions.							
All	AI2.1 High-level Design Translate business requirements into a high-level design specification for software acquisition, taking into account the organisation's technological direction and information architecture. Have the design specifications approved by management to ensure that the high level design responds to the requirements. Reassess when significant technical or logical		X	X	AI2 Acquire and Maintain Application Software Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This allows	R.2 Loss of governance R.5 Cloud service termination or failure R.6 Cloud provider acquisition R.7 Supply chain failure R.8 Resource exhaustion (under or over provisioning)	Solutions built using cloud computing services must adhere to the same lifecycle processes as non-cloud solutions. In cloud computing a portion of these lifecycle processes will be the responsibility of the cloud service provider, making visibility into their processes essential for the service owner. SLAs between	NS/EP owners must adhere to lifecycle best practices including accommodation of specific NS/EP scenarios in all phases of the lifecycle. Additionally, cycles for updates to applications (and cloud services)

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	discrepancies occur during development or maintenance. Comment: IaaS high level design addresses the infrastructure requirements and whether the CSP can provide the technology and configurations necessary to host the applications. PaaS high-level design is the same as an internally developed design. SaaS design is limited, unless customisation is planned. However, entity interfaces and other internal customisations may be required.				organisations to properly support business operations with the correct automated applications.	R.19 Compromise service engine R.23 Data protection risks R.24 Licensing risks	provider and owner must stipulate the degree of visibility and mechanisms for communication and reporting.	are continuous, which raises concerns about the level of 3rd party access to the data and how to protect it. Owners also need to consider the resiliency of application providers since devices and applications add a new dimension to resiliency.
All	AI2.2 Detailed Design Prepare detailed design and technical software application requirements. Define the criteria for acceptance of the requirements. Have the requirements approved to ensure that they correspond to the high-level design. Perform reassessment when significant technical or logical discrepancies occur during development or maintenance. Comment: Same as AI2.1, but		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	focusing on detail design.							
All	AI2.3 Application Control and Auditability Implement business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorised and auditable. Comment: IaaS will address operational functional processes and automated controls, and SaaS will address the user interfaces with the CSP's application.		X	X				
All	AI2.4 Application Security and Availability Address application security and availability requirements in response to identified risks and in line with the organisation's data classification, information architecture, information security architecture and risk tolerance. Comment: The scope is the same as AI2.3, but the focus		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	is on security and availability.							
All	AI2.5 Configuration and Implementation of Acquired Application Software Configure and implement acquired application software to meet business objectives. Comment: Since the software is 'effectively leased', standard configuration objectives would be consistent with any acquired software.		X	X				
All	AI2.6 Major Upgrades to Existing Systems In the event of major changes to existing systems that result in significant change in current designs and/or functionality, follow a similar development process as that used for the development of new systems. Comment: Ensure that the CSP provides adequate lead time and details of changes prior to deployment.		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
All	AI2.7 Development of Application Software Ensure that automated functionality is developed in accordance with design specifications, development and documentation standards, QA requirements, and approval standards. Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties. Comment: PaaS would address typical system development controls. SaaS control objectives would focus on customisations, and rights and obligations of both parties.		X	X				
All	AI2.8 Software Quality Assurance Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation's quality policies and procedures. Comment: Establish appropriate metrics to be		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	used along with SLAs to ensure the quality of CSP delivery.							
All	AI2.9 Applications Requirements Management Track the status of individual requirements (including all rejected requirements) during the design, development and implementation, and approve changes to requirements through an established change management process.		X	X				
All	AI2.10 Application Software Maintenance Develop a strategy and plan for the maintenance of software applications. Comment: Ensure that the customer and the CSP has a notification process to provide sufficient notification of application software changes to allow the customer to modify any interfacing applications.		X	X				
Infrastructure	AI3.1 Technological Infrastructure Acquisition Plan Produce a plan for the		X	X	AI3 Acquire and Maintain Technology Infrastructure	R.1 Lock-in R.2 Loss of	Technology infrastructure solutions built using cloud	NS/EP owners must stipulate requirements for

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	acquisition, implementation and maintenance of the technological infrastructure that meets established businessfunctional and technical requirements and is in accord with the organisation's technology direction. Comment: IaaS is the primary focus, but PaaS may require supportingtechnology during development and as a precondition of implementation.				Organisations have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development andtest environments. This ensures that there is ongoing technological support for business applications.	governance R.5 Cloud service termination or failure R.6 Cloud provider acquisition R.7 Supply chain failure R.8 Resource exhaustion (under or over provisioning) R.9 Isolation failure R.11 Management interface compromise (manipulation, availability of infrastructure) R.19 Compromise service engine R.22 Risk from changes of jurisdiction R.23 Data protection risks	computing services must adhere to established processes for acquisition, protection, maintenance and testing. In cloud computing, a portion of these processes will be the responsibility of the cloud service provider, making visibility into their processes essential for the service owner. SLAs between provider and owner must stipulate the degree of visibility and mechanisms for communication and reporting.	acquisition, protection, maintenance and testing of the infrastructure for specified NS/EP scenarios, such as supporting a broader community of ad-hoc users (e.g. first responders) or increased monitoring during an event to prevent an application from being unavailable or the target of an attack.
Infrastructure	AI3.2 Infrastructure Resource Protection and Availability Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	evaluated. Comment: Private and hybrid delivery models require the customer to consider these control objectives. The CSP is solely responsible for public delivery of IaaS, PaaS and all SaaS.							
Infrastructure	AI3.3 Infrastructure Maintenance Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organisation's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements. Comment: In a private or hybrid delivery model, maintenance is the partial responsibility of the customer and a major focus of the CSP.		X	X				
Infrastructure	AI3.4 Feasibility Test Environment		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	Establish development and test environments to support effective and efficient feasibility and integration testing of infrastructure components. Comment: Since PaaS is a development platform, this is necessary. IaaS is limited to hardware configuration issues.							
Infrastructure	AI4.1 Planning for Operational Solutions Develop a plan to identify and document all technical, operational and usage aspects such that all those who will operate, use and maintain the automated solutions can exercise their responsibility. Comment: PaaS is excluded here because it is a development platform not designed for operations processing.		X		AI4 Enable Operation and Use Knowledge about new systems is made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure the proper use and operation of applications and infrastructure.	R.20 Conflicts between customer hardening procedures and cloud environment	End users and support staff can intentionally or unintentionally introduce vulnerabilities or overwrite/fail to comply with existing controls established by policy. Enforcement mechanisms need to be in place to ensure acceptable use practices are not being violated. Inadequate training, lack of sufficient personnel with resident knowledge, and lack of senior-level stakeholder involvement can lead to inadequate knowledge transfer.	It is critical that first responders have sufficient knowledge of how to use NS/EP devices and applications and the process for trouble shooting prior to the occurrence of an event. Owners also need to ensure that any lessons learned are incorporated into procedural and policy updates, including SLAs, device/application
Interdependency	AI4.2 Knowledge Transfer to Business Management Transfer knowledge to business management to		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	allow those individuals to take ownership of the system and data, and exercise responsibility for service delivery and quality, internal control, and application administration.							upgrades, etc.
Interdependency	AI4.3 Knowledge Transfer to End Users Transfer knowledge and skills to allow end users to effectively and efficiently use the system in support of business processes. Comment: IaaS is included because, by definition, infrastructure can be provisioned by the user.		X					
Interdependency	AI4.4 Knowledge Transfer to Operations and Support Staff Transfer knowledge and skills to enable operations and technical support staff to effectively and efficiently deliver, support and maintain the system and associated infrastructure.		X					
Policy/Legal	AI5.1 Procurement Control Develop and follow a set of		X		AI5 Procure IT Resources	R.2 Loss of governance	NS/EP service owners need to ensure that	Due to the high impact of NS/EP

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	procedures and standards that is consistent with the business organisation's overall procurement process and acquisition strategy to acquire IT related infrastructure, facilities, hardware, software and services needed by the business.				IT resources, including people, hardware, software and services, need to be procured. This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup of contractual arrangements, and the acquisition itself. Doing so ensures that the organisation has all required IT resources in a timely and cost effective manner.	R.6 Cloud provider acquisition R.7 Supply chain failure R.8 Resource exhaustion R.20 Conflicts between customer hardening procedures and cloud environment	their unique requirements are clearly defined and that they understand the distinctions in the capabilities provided among various CSPs to discern which CSPs can best meet those needs. Procurement decisions must be made with security in mind, and not bolted on after the fact.	services, cloud applications need to be developed with a lifecycle approach to security. For example, a DISA STIG can be used for implementing the proper controls for an NS/EP application.
Policy/Legal	AI5.2 Supplier Contract Management Set up a procedure for establishing, modifying and terminating contracts for all suppliers. The procedure should cover, at a minimum, legal, financial, organisational, documentary, performance, security, intellectual property, and termination responsibilities and liabilities (including penalty clauses). All contracts and contract changes should be reviewed by legal advisors. Comment: Cloud contract must be explicit in its definition of rights and obligations, and SLAs.		X					
Policy/Legal	AI5.3 Supplier Selection		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimised with input from potential suppliers.							
Policy/Legal	AI5.4 IT Resources Acquisition Protect and enforce the organisation's interests in all acquisition contractual agreements, including the rights and obligations of all parties in the contractual terms for the acquisition of software, development resources, infrastructure and services. Comment: Refer to AI5.2		X					
Policy/Legal	AI6.1 Change Standards and Procedures Set up formal change management procedures to handle in a standardized manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the		X		AI6 Manage Changes All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures,	R.22 Risk from changes of jurisdiction R.27 Modifying network traffic R.3 Compliance challenges	Effective change management requires careful coordination of policy and technical requirements and synchronization among responsible staff, otherwise, it can result in conflicting changes or trouble shooting challenges. In the	An NS/EP event may require immediate changes that bypass a formally established process. Certain risks may need to be accepted in order to provision urgent

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	underlying platforms. Comment: This would be applicable to SaaS if the customer has implemented any customisation to the applications or manages interfaces to internal applications.				processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.		cloud environment, there may be challenges in aligning business process changes with standardized cloud service options.	capabilities to first responders.
Interdependency	AI6.2 Impact Assessment, Prioritisation and Authorisation Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorised, prioritised and authorised. Comment: See AI6.1		X					
Interdependency	AI6.3 Emergency Changes Establish a process for defining, raising, testing, documenting, assessing and authorising emergency changes that do not follow the established change process. Comment: See AI6.1		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
Interdependency	AI6.4 Change Status Tracking and Reporting Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned. Comment: Even though the CSP is providing much of the infrastructure and applications, it is critical that the customer maintains control over tracking and reporting. This will be useful in evaluating compliance with SLAs.		X					
Interdependency	AI6.5 Change Closure and Documentation Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.		X					
Interdependency	AI7.1 Training Train the staff members of the affected user departments		X		AI7 Install and Accredit Solutions and Changes New systems need to be	R.25 Network breaks R.26 Network management (IE,	The process for installing and accrediting solutions	Cycles for updates and patched to

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	and the operations group of the IT function in accordance with the defined training and implementation plan and associated materials, as part of every information systems development, implementation or modification project.				made operational once development is complete. This requires propertesting in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post implementation review. This assures that operational systems are in line with the agreed upon expectations and outcomes.	network congestion/mis-connection/non-optimal use) R.30 Loss or compromise of operational logs R.31 Loss or compromise of security logs (manipulation of forensic investigation)	may vary based on the technology, application, accreditor, organizational processes, and possibly even regulatory requirements. The length of time required can also vary and often times lag.	applications (and cloud services) are continuous. An NS/EP situation may not allow time for the testing of changes/ remediation of errors before implementation into the operational environment, which can reduce device/application performance to suboptimal levels.
Interdependency	AI7.2 Test Plan Establish a test plan based on organisation-wide standards that define roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.		X	X				
Interdependency	AI7.3 Implementation Plan Establish an implementation and fallback/back out plan. Obtain approval from relevant parties.		X	X				
Infrastructure	AI7.4 Test Environment Define and establish a secure test environment representative of the planned operations environment relative to security, internal controls, operational practices, data quality and privacy requirements, and		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	workloads. Comment: The customer should be encouraged to provision its own test environment as required.							
Infrastructure	AI7.5 System and Data Conversion Plan data conversion and infrastructure migration as part of the organisation's development methods, including audit trails, rollbacks and fallbacks.		X	X				
Infrastructure	AI7.6 Testing of Changes Test changes independently in accordance with the defined test plan prior to migration to the operational environment. Ensure that the plan considers security and performance.		X	X				
Infrastructure	AI7.7 Final Acceptance Test Ensure that business process owners and IT stakeholders evaluate the outcome of the testing process as determined by the test plan. Remediate significant errors identified in the testing process, having		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	completed the suite of tests identified in the test plan and any necessary regression tests. Following evaluation, approve promotion to production.							
Infrastructure	AI7.8 Promotion to Production Following testing, control the handover of the changed system to operations, keeping it in line with the implementation plan. Obtain approval of the key stakeholders, such as users, system owner and operational management. Where appropriate, run the system in parallel with the old system for a while, and compare behaviour and results. Comment: SaaS will focus on changes and their effect on the functionality. PaaS will relate to standard development considerations.		X	X				
Infrastructure	AI7.9 Post-implementation Review Establish procedures in line with the organisational change management standards to require a post-		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	implementation review as set out in the implementation plan.							
Policy/Legal	DS1.1 Service Level Management Framework Define a framework that provides a formalised service level management process between the customer and service provider. The framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding between the customer and provider(s). The framework should include processes for creating service requirements, service definitions, SLAs, OLAs and funding sources. These attributes should be organised in a service catalogue. The framework should define the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers. Comment: Service levels are key to the effective		X		DS1 Define and Manage Service Levels Effective communication between IT management and business customers regarding services requiredis enabled by a documented definition of an agreement on IT services and service levels. This processalso includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements.	R.1 Lock-in R.2 Loss of governance R.3 Compliance challenges R.4 Loss of business reputation due to co-tenant activities R.5 Cloud service termination or failure R.6 Cloud Provider Acquisition R.7 Supply chain failure R.8 Resource exhaustion (under or over provisioning) R.9 Isolation failure R.20 Conflict between customer hardening procedures and cloud environment R.22 Risk from	The unique risk here is this type of purchasing activity is relatively new. Standardized NS/EP requirements for CSPs are currently not in place, leading to individual (and perhaps inconsistent) sets of requirements pushed out by the different service owners.	NS/EP service owners need to drive SLAs that address capacity planning issues, particularly in a shared environment.

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	administration of the contract and maintaining mutual expectations.					changes of jurisdiction R.23 Data protection risks		
Infrastructure	DS1.2 Definition of Services Base definitions of IT services on service characteristics and business requirements. Ensure that they are organised and stored centrally via the implementation of a service catalogue portfolio approach. Comment: The contract should define the business requirements and services explicitly, with metrics to facilitate SLA monitoring.		X					
Infrastructure	DS1.3 Service Level Agreements Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities. This should cover customer commitments; service support requirements; quantitative and qualitative metrics for measuring the service signed off on by the stakeholders;		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	funding and commercial arrangements, if applicable; and roles and responsibilities, including oversight of the SLA. Consider items such as availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints. Comment: SLAs must be part of the contract, be measurable, and monitored by the customer.							
Infrastructure	DS1.4 Operating Level Agreements Define OLAs that explain how the services will be technically delivered to support the SLA(s) in an optimal manner. The OLAs should specify the technical processes in terms meaningful to the provider and may support several SLAs.		X					
Infrastructure	DS1.5 Monitoring and Reporting of Service Level Achievements Continuously monitor specified service level performance criteria. Reports		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	on achievement of service levels should be provided in a format that is meaningful to the stakeholders. The monitoring statistics should be analysed and acted upon to identify negative and positive trends for individual services as well as for services overall. Comment: The CSP should report SLA metrics on a timely basis; the customer should maintain its own version of the SLA attainment for the purposes of comparison.							
Infrastructure	DS1.6 Review of Service Level Agreements and Contracts Regularly review SLAs and underpinning contracts with internal and external service providers to ensure that they are effective and up to date and that changes in requirements have been taken into account.		X	X				
Infrastructure	DS2.1 Identification of All Supplier Relationships Identify all supplier services, and categorise them according to supplier type,		X	X	DS2 Manage Third-party Services The need to assure that services provided by third parties (suppliers,	R.7 Supply chain failure R.23 Data protection risks	Using cloud services is likely to also involve a number of applications (app) providers. Understanding the	NS/EP owners who are operating collaborative platforms and services will need

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	significance and criticality. Maintain formal documentation of technical and organisational relationships covering the roles andresponsibilities, goals, expected deliverables, and credentials of representatives of these suppliers.				vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers.		interdependency and risk between and among app providers, CSP, and service owner is complex but essential. An additional risk is the dependency on vendors and contractors by cloud providers to supplement full-time employees. Will NS/EP users have access to those personnel for background checks, etc.? Will contractual obligations passed to cloud provider be passed down to their contractors and vendors?	to ensure that the NS/EP SLA requirements are extended to the app providers. They should ensure that these providers comply with security and personnel requirements and have audit log for code changes. Moreover, cycles for updates and changes to cloud services and applications are continuous, which raises concerns about the level of third-party access to the data and how to protect it (e.g. encryption considerations).
Policy/Legal	DS2.2 Supplier Relationship Management Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).		X	X				
Infrastructure	DS2.3 Supplier Risk Management Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.							
Infrastructure	DS2.4 Supplier Performance Monitoring Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.		X	X				
Resiliency	DS3.1 Performance and Capacity Planning Establish a planning process for the review of performance and capacity of IT resources to ensure that cost-justifiable capacity and performance are available to process the agreed-upon workloads as determined by		X	X	DS3 Manage Performance and Capacity The need to manage performance and capacity of IT resources requires a process to periodically review current performance and	R.5 Cloud service termination or failure R.8 Resource exhaustion (under or over provisioning) R.9 Isolation failure R.26 Network management (IE,	Close attention must be paid to monitoring and predicting capacity and performance to ensure that resiliency is maintained in every given situation. Dependencies and contingencies must also be clearly defined	Lack of performance and capacity planning could lead to a service outage should demand suddenly spike during an NS/EP incident. Depending on the

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	the SLAs. Capacity and performance plans should leverage appropriate modeling techniques to produce a model of the current and forecasted performance, capacity and throughput of the IT resources. Comment: Users must continue future capacity needs with respect to future requirements, e.g., acquisition. The time frame necessary to address additional capacity is much shorter in a cloud environment. Focus will be on the purchase of more licenses.				capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.	network congestion/mis-connection/non-optimal use) R.30 Loss or compromise of operational logs R.31 Loss or compromise of security logs (manipulation of forensic investigation)	that trigger capacity demand to ensure that the appropriate levels are continually available on demand. Capacity and performance analysis and forecasts must be documented and well-communicated to the CSP on a timely and regular basis.	service, it could cause a catastrophic outage. Also, a spike in use might not come from NS/EP users, but from other users of the cloud provider's services, especially if that includes social media or communications services (e.g. email). This is especially true for consumers in the geographical area impacted by the NS/EP event, and their families and friends trying to communicate with them. Of course, such use of social media and communications services might help NS/EP missions, if data belonging to, and use of service, is
Resiliency	DS3.2 Current Performance and Capacity Assess current performance and capacity of IT resources to determine if sufficient capacity and performance exist to deliver against agreed upon service levels. Comment: This objective changes focus—customer wants to be sure that internal resources exist to handle		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	service levels. The CSP is responsible for addressing the infrastructure and processing needs.							mined and analyzed.
Resiliency	DS3.3 Future Performance and Capacity Conduct performance and capacity forecasting of IT resources at regular intervals to minimise the risk of service disruptions due to insufficient capacity or performance degradation, and identify excess capacity for possible redeployment. Identify workload trends and determine forecasts to be input to performance and capacity plans. Comment: See DS3.2		X	X				
Resiliency	DS3.5 Monitoring and Reporting Continuously monitor the performance and capacity of IT resources. Data gathered should serve two purposes: • To maintain and tune current performance within IT and address such		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	issues as resilience, contingency, current and projected workloads, storage plans, and resource acquisition • To report delivered service availability to the business, as required by the SLAs. Accompany all exception reports with recommendations for corrective action. Comment: Monitoring and reporting focuses on internal performance/ capacity, and CSP's attainment of SLAs.							
Resiliency	DS4.1 IT Continuity Framework Develop a framework for IT continuity to support enterprise-wide business continuity management using a consistent process. The objective of the framework should be to assist in determining therequired resilience of the infrastructure and to drive the developmentof disaster recovery and IT contingency		X		DS4 Ensure Continuous Service The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilising offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimises the probability and impact of	R.25 Network breaks R.26 Network management (IE, network congestion, mis-connection, non-optimal use) R.32 Backups lost, stolen	Ensuring that a plan and framework is in place to ensure service continuity is maintained in non-NS/EP times is the basis for a plan and framework during NS/EP incidents.	A plan and framework for continuous service during NS/EP incidents must take into consideration offsite backup and contingency concerns that include the complete failure of the entire site infrastructure.

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	plans. The framework should address the organisational structure for continuity management, covering the roles, tasks and responsibilities of internal and externalservice providers, their management and their customers, and theplanning processes that create the rules and structures to document,test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of criticalresources, noting key dependencies, the monitoring and reporting ofthe availability of critical resources, alternative processing, and the principles of backup and recovery. Comment: Customer needs to address the internal IT continuity framework, which supports the CSP interface. Work station and network considerations would address this issue.				a major IT serviceinterruption on key business functions and processes.			The ability to have appropriate access to important data during an NS/EP incident must also take into consideration that the systems continue to function for whatever sort of device the data request is coming. (smartphones, tablets, etc.)

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
Resiliency	DS4.2 IT Continuity Plans Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach. Comment: Same as DS4.1		X	X				
Policy/Legal	DS4.3 Critical IT Resources Focus attention on items specified as most critical in the IT continuity plan to build in resilience and establish priorities in recovery situations. Avoid the distraction of recovering less-critical items and ensure response and recovery in line with prioritised business		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	needs, while ensuring that costs are kept at an acceptable level and complying with regulatory and contractual requirements. Consider resilience, response and recovery requirements for different tiers, e.g., one to four hours, four to 24 hours, more than 24 hours and critical business operational periods. Comment: Customers must define their critical internal IT resources, and processes to address the need for continuous service. This may include interfaces and internal automated processes. Alternate processing approaches may need to be considered if the servicer is incapable of restoring CSP in a timely manner. CSP is responsible for providing infrastructure to assure continuous service.							
Policy/Legal	DS4.4 Maintenance of the IT Continuity Plan Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	kept up to date and continually reflects actual business requirements. Communicate changes in procedures and responsibilities clearly and in a timely manner.							
Interdependency	DS4.5 Testing of the IT Continuity Plan Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.		X	X				
Policy/Legal	DS4.6 IT Continuity Plan Training Provide all concerned parties with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	disaster. Verify and enhance training according to the results of the contingency tests.							
Interdependency	DS4.7 Distribution of the IT Continuity Plan Determine that a defined and managed distribution strategy exists to ensure that plans are properly and securely distributed and available to appropriately authorised interested parties when and where needed. Attention should be paid to making the plans accessible under all disaster scenarios.		X	X				
Resiliency	DS4.8 IT Services Recovery and Resumption Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	business recovery and resumption needs. Comment: The CSP is responsible for processing and infrastructure. The customer retains ultimate responsibility for interfaces and interim processing during outages.							
Policy/Legal	DS4.9 Offsite Backup Storage Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data, and		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	periodically test and refresh archived data. Comment: The customer must contractually mandate appropriate backup storage policies and where possible, obtain physical control over copies of customer backup storage.							
Interdependency	DS4.10 Post-resumption Review Determine whether IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster, and update the plan accordingly. Comment: The post-resumption review needs to analyse the effectiveness of the CSP and customer staff and processes. In addition, it has to evaluate whether the CSP has the ability and resources to manage the customer's data and recovery needs.		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
Policy/Legal	DS5.1 Management of IT Security Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements. Comment: The customer's security focus must address those processesto which the customer is responsible: policy, standards and guidelines. In addition, the customer must focus on the CSP's IT security management specific to the platform and delivery method.		X		DS5 Ensure Systems Security The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security rolesand responsibilities, policies, standards, and procedures. Security management also includesperforming security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.	R.2 Loss of governance R.7 Supply chain failure R.10 Cloud provider malicious insider-abuse of high privilege roles R.11 Management interface compromise (manipulation, availability of infrastructure) R.14 Insecure or ineffective deletion of data R.15 DDOS R.16 Economic DDOS R.17 Loss of encryption keys R.20 Conflicts between customer hardening procedures and cloud environment R.23 Data protection	A holistic, clearly spelled out security framework with a robust set of controls must be in place to ensure full end-to-end systems security. Minimizing vulnerabilities and incidents in non-NS/EP times will be a strong base for ensuring security is maintained during NS/EP incidents.	Management approach to security in cloud computing requires careful attention as some considerations, threats and mitigation techniques work identically as in legacy environments, but some work differently or are not applicable. NS/EP cloud-based identity factors are most needed when dealing with opportunistic or event-generated criteria for mission collaboration across multiple organizations, levels of government, and private industries. Additionally, while multiple federation systems/
Policy/Legal	DS5.2 IT Security Plan Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	security policies and procedures to stakeholders and users. Comment: The customer must evaluate the risk associated with cloud computing against compliance and business risks. The security plan would be limited to the boundaries within the customer's site and administrative scope.					risks R.25 Network breaks R.26 Network management R.27 Modifying network traffic R.28 Privilege escalation R.29 Social engineering attacks (IE, impersonation) R.30 Loss or compromise of operational logs R.31 Loss or compromise of security logs R.32 Backups lost, stolen R.33 Unauthorized access to premises (including physical access to machines and other facilities) R. 34 Theft of		protocols currently coexist for online identity management, none has been broadly accepted as the standard.
Policy/Legal	DS5.3 Identity Management Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights. Comment: Customer responsibility in an IaaS model would be the definition of and scope of access to the authorisation system. Whether the customer could specify the identity management features and processes would depend on the contract and infrastructure functional capabilities. In the PaaS model, the design of security within the application is the responsibility of the customer, the CSP would be responsible for access to CSP applicable libraries, etc. In the SaaS model, the customer would be responsible for access privileges, access controls,					computer equipment		

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	etc., but the CSP would be responsible for the IT management within the application and architecture delivering the application functions. Access to customer application programs and data through super user privileges is highly restricted and monitored.							
Policy/Legal	DS5.4 User Account Management Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges. Comment: The customer retains responsibility for user access provisioning. CSP personnel should be excluded from the user account management process. If any CSP personnel are permitted access, their activities should be monitored through logging and management review processes.							
Policy/Legal	DS5.5 Security Testing, Surveillance and Monitoring Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed. Comment: Detection and prevention are the primary responsibilities of the CSP, but the customer should have processes in place to test and monitor the detection and prevention activities.							
Policy/Legal	DS5.6 Security Incident Definition Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process. Comment: Customers must maintain their own security incident definition processes to assure CSP compliance and follow through of identified security incidents. The contract must require the CSP to report every		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	customer-relevant incidence to the customer in detail and in a timely fashion.							
Policy/Legal	DS5.8 Cryptographic Key Management Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure. Comment: The customer is responsible for key management to maintain the integrity and privacy of data. Where appropriate, key management can be shared between the customer and CSP, provided advanced key management procedures are in place.		X	x				
Policy/Legal	DS5.10 Network Security Use security techniques and related management procedures (e.g., firewalls,		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	security appliances, network segmentation, intrusion detection) to authorise access and control information flows from and to networks. Comment: When provisioning under IaaS, the customer is responsible to ensure that appropriate network security devices are in place. For PaaS and SaaS, the customer is responsible for the customer's internal network.							
Infrastructure	DS5.11 Exchange of Sensitive Data Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin. Comment: Same as DS5.10, but the regulators and compliance authorities would hold the customer responsible for data leakage. Any actions between the parties as a		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	result of noncompliance would be based upon contractual agreements and penalties.							
Policy/Legal	DS6.1 Definition of Services Identify all IT costs, and map them to IT services to support a transparentcost model. IT services should be linked to business processes such thatthe business can identify associated service billing levels. Comment: Definition of services is a customer internal matter.		X	X				
Policy/Legal	DS6.2 IT Accounting Capture and allocate actual costs according to the enterprise cost model. Variances between forecasts and actual costs should be analysed and reported on, in compliance with the enterprise's financial measurement systems. Comment: The CSP must provide a detailed report of resources used.		X		DS6 Identify and Allocate Costs The need for a fair and equitable system of allocating IT costs to the business requires accuratemeasurement of IT costs and agreement with business users on fair allocation. This process includes building and operating a system to capture, allocate and	R.6 Cloud provider acquisition R.7 Supply chain failure	Data and service portability can be financially cost-prohibitive. SLAs need to explicitly discuss such lock-in issues. Licensing conditions, such as per-seat agreements, and online licensing checks may become unworkable in a cloud environment. For example, if software is charged on a per instance basis	A robust system that captures, allocates and reports on IT costs can better predict the cost of an NS/EP incident when paired with a robust disaster recovery plan.

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
Interdependency	DS6.3 Cost Modelling and Charging Establish and use an IT costing model based on the service definitions that support the calculation of chargeback rates per service. The IT cost model should ensure that charging for services is identifiable, measurable and predictable by users to encourage proper use of resources. Comment: The CSP will provide billing based upon usage; the customer is responsible for defining and managing cost allocations and chargebacks.		X	X	report IT costs to the usersof services. A fair system of allocation enables the business to make more informed decisionsregarding the use of IT services.		every time a new machine is instantiated then the cloud customer's licensing costs may increase exponentially even though they are using the same number of machine instances for the same duration. In the case of PaaS and IaaS, there is the possibility for creating original work in the cloud (new applications, software etc). As with all intellectual property, if not protected by the appropriate contractual clauses (see ANNEX I – Cloud computing – Key legal issues , Intellectual Property), this original work may be at risk.	
Policy/Legal	DS6.4 Cost Model Maintenance Regularly review and benchmark the appropriateness of the cost/recharge model to maintain its relevance and appropriateness to the evolving business and IT activities.		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	Comment: See DS6.3							
Policy/Legal	DS7.1 Identification of Education and Training Needs Establish and regularly update a curriculum for each target group of employees considering: • Current and future business needs and strategy • Value of information as an asset • Corporate values (ethical values, control and security culture, etc.) • Implementation of new IT infrastructure and software (i.e., packages, applications) • Current and future skills, competence profiles, and certification and/or credentialing needs as well as required		X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	reaccreditation • Delivery methods (e.g., classroom, web-based), target group size, accessibility and timing Comment: Ensure that training is updated to reflect the CSP's functionality and technology.							
Policy/Legal	DS7.2 Delivery of Training and Education Based on the identified education and training needs, identify target groups and their members, efficient delivery mechanisms, teachers, trainers, and mentors. Appoint trainers and organise timely training sessions. Record registration (including prerequisites), attendance and training session performance evaluations.	X	X		DS7 Educate and Train Users Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group. In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results. An effective training programme increases effective use of technology by reducing user errors, increasing productivity and increasing compliance with key	N/A	A well-educated and trained set of users will create a heightened awareness of security and compliance and minimizes risk in the everyday workplace systems. Additional training around emergency procedures that go into place in the case of an NS/EP incident provide some assurance that a speedy response can happen during these times.	Training and education of users as to appropriate protocol and procedures during an NS/EP incident are a first step to assuring continuity of systems access and resiliency of systems. It is also critical to train end users of systems deployed to the cloud, as this will be a big consideration, especially if moving from a traditional, on-
Policy/Legal	DS7.3 Evaluation of Training Received Evaluate education and training content delivery upon completion for	X	X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	relevance, quality, effectiveness, the retention of knowledge, cost and value. The results of this evaluation should serve as input for future curriculum definition and the delivery of training sessions.				controls, such as user security measures.			premise solution.
Policy/Legal	DS8.2 Registration of Customer Queries Establish a function and system to allow logging and tracking of calls, incidents, service requests and information needs. It should work closely with such processes as incident management, problem management, change management, capacity management and availability management. Incidents should be classified according to a business and service priority and routed to the appropriate problem management team, where necessary. Customers should be kept informed of the status of their queries. Comment: The service desk would generally be the	X	X					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	responsibility of the CSP. However, the customer must register customer issues. This will be used as the primary record to reconcile customer requests to the CSP's problem reporting system, to ensure that all requests are addressed in a timely manner and according to the SLAs.							
Interdependency	DS8.3 Incident Escalation Establish service desk procedures, so incidents that cannot be resolved immediately are appropriately escalated according to limits defined in the SLA and, if appropriate, workarounds are provided. Ensure that incident ownership and life cycle monitoring remain with the service desk for user-based incidents, regardless which IT group is working on resolution activities.		X	X	DS8 Manage Service Desk and Incidents Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the	N/A	Managed service desks can be a vector for launching social engineering attacks and will require training for the service owner and user community to discern legitimate calls and requests from the managed service desks. Additionally, incident management procedures need to be clearly defined in the SLAs to understand the shared and unique roles of the service owner and CSP with regard to incident management reporting, auditing, etc. Presumably, in times of	Well-documented incidents with timely resolution ensures that these incidents don't get in the way of assuring continuity of systems access and resiliency of systems. Personnel planning for sufficient and timely support of the service desk during an NS/EP event needs to be accounted for. It is also important to consider whether support staff, including
Interdependency	DS8.4 Incident Closure Establish procedures for the timely monitoring of clearance of customer queries. When the incident		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	has been resolved, ensure that the service desk records the resolution steps, and confirm that the action taken has been agreed to by the customer. Also record and report unresolved incidents (known errors and workarounds) to provide information for proper problem management.				business can address root causes (such as poor user training) through effective reporting.		NS/EP incidents, timely access to relevant and accurate data may be more important than security of the data. There is always the risk that the service desk is in the geographical area impacted by the NS/EP event, or that service desk personnel have family and/or friends in the impacted geographical areas. This should be factored in, especially with regard to data leakage prevention.	service desk personnel, should be geographically distributed, or have an alternate site with staff, to avoid problems when staff are in the area impacted by the NS/EP event.
Interdependency	DS8.5 Reporting and Trend Analysis Produce reports of service desk activity to enable management to measure service performance and service response times and to identify trends or recurring problems, so service can be continually improved. Comment: The customer must develop an internal service desk summary based upon the CSP's metrics.		X	X				
Interdependency	DS10.1 Identification and Classification of Problems Implement processes to report and classify problems that have been identified as		X	X				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	part of incident management. The steps involved inproblem classification are similar to the steps in classifying incidents; they are to determine category, impact, urgency and priority. Categorise problems as appropriate into related groups or domains (e.g., hardware, software, support software). These groups may match the organisational responsibilities of the user and customer base, and should be the basis for allocating problems to support staff. Comment: The process must refer to the SLA and/or contract.							
Policy/Legal	DS10.2 Problem Tracking and Resolution Ensure that the problem management system provides for adequate audit trail facilities that allow tracking, analysing and determining the root cause of all reported problems considering: • All associated configuration items		x	x	DS10 Manage Problems Effective problem management requires the identification and classification of problems, rootcause analysis and resolution of problems. The problem management process also includes the formulation of recommendations for	N/A	Incident management policies, processes, and procedures must be kept up-to-date to ensure an efficient, effective, and orderly incident response capability, including identification, detection, containment/eradication , and recovery processes. Incident severity categories	NS/EP users, NS/EP service owners, and CSPs will require a high level of collaboration during an event. Users and owners should already be familiar with the technology/ service/process

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	• Outstanding problems and incidents • Known and suspected errors • Tracking of problem trends Identify and initiate sustainable solutions addressing the root cause, raising change requests via the established change management process. Throughout the resolution process, problem management should obtain regular reports from change management on progress in resolving problems and errors. Problem management should monitor the continuing impact of problems and known errors on user services. In the event that this impact becomes severe, problem management should escalate the problem, perhaps referring it to an appropriate board to increase the priority of the request for change (RFC) or to implement an urgent change as appropriate.				improvement, maintenance of problem records and reviewof the status of corrective actions. An effective problem management process maximises systemavailability, improves service levels, reduces costs, and improves customer convenience andsatisfaction.		should also be in place to appropriately respond to and resource the incident. The accountability to and execution of these roles must be clearly defined.	prior to the outbreak of an event to prevent any bottlenecks in getting the right data to the right people. Owners and CSPs also need to manage the large amounts of (uncontrollable) data flow and ensure dissemination of the most relevant and critical data. The capability to appropriately handle an incident can also be compromised if adequate resources are strained or not appropriately accounted for. CSPs also need to provide a reliable and resilient infrastructure and rapid scalability of capacity to prevent oversaturation of

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	Monitor the progress of problem resolution against SLAs.							the network. Prompt reporting of suspected or actual incidents to the right entities/authorities can be stymied with the vast amount of data dissemination and competing priorities during an NS/EP event. The capability to sufficiently resource the handling of a reported incident can also be compromised.
Interdependency	DS10.3 Problem Closure Put in place a procedure to close problem records either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.		x	x				
Interdependency	DS10.4 Integration of Configuration, Incident and Problem Management Integrate the related processes of configuration, incident and problem management to ensure effective management of problems and enable improvements. Comment: No or minimal configuration management		x					
Interdependency	DS11.1 Business Requirements for Data Management Verify that all data expected for processing are received and processed completely,		x					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	accurately and in a timely manner, and all output is delivered in accordance with business requirements. Support restart and reprocessing needs. Comment: The customer must establish SLAs defining expectations and requirements. The customer must establish data management policy and procedures for interfacing data that remains within the confines of the customer's IT infrastructure. The customer may also need to establish transaction control mechanisms to ensure completeness of processing.							
Data	DS11.4 Disposal Define and implement procedures to ensure that business requirements for protection of sensitive data and software are met when data and hardware are disposed or transferred. Comment: The CSP will physically destroy any remaining data upon the expiration/termination of the		x	x	DS11 Manage Data Effective data management requires identifying data requirements. The data management process also includes the establishment of effective procedures to manage the media library, backup and recovery of data, and	R.2 Loss of governance R.12 Intercepting data in transit R.13 Data leakage on up/download, intra-cloud R.14 Insecure or ineffective deletion of data	Business requirements for data in transit and at rest require a clear designation of responsibilities that are unique vs. shared between the service owner and CSP. Loss of data or prolonged inability to access critical data can have significant impact on operations. Cloud	In an NS/EP event, many different users will need access to systems, data and services. It will be critical for NS/EP owners to maintain (and automate where possible) data classification. While certain

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	contract.				proper disposal of media. Effective data management helps ensure the quality, timeliness and availability of business data.	R.21 Subpoena and e-discovery R.22 Risk from changes of jurisdiction R.23 Data protection risks R.30 Loss or compromise of operational logs R.31 Loss or compromise of security logs R.32 Backups lost, stolen R.33 Unauthorized access to premises R.34 Theft of computer equipment	services should implement redundant data storage as well as thorough data backup procedures allowing for recovery of historical data for a set period of time. At the same time, if the service owner or the provider are required to comply with regulatory or legal requirements to preserve certain types of data (e.g. access logs) for set periods of time, loss of said data can result in penalties and/or impede forensic / LE activities. In dealing with sensitive information complete and secure removal of data must be supported and access to the functionality needs to be effectively controlled. Depending on the cloud service model, the responsibility may reside with application owner, the service	types of data will require immediate access, specialized handling and/or distribution can lead to liability concerns when the data is managed in a manner not explicitly defined by or consistent with its original intent.(i.e. audit trail or no audit trail.) Additionally, as data is being generated from the event the classification could change and NS/EP service owners will need SLA that would enable the rapid movement to a classified platform and guarantee wiping of data. The key characteristics of the cloud, including
Data	DS11.5 Backup and Restoration Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan. Comment: A contract must define SLAs relevant to the backup and restoration of data.		x	x				
Data	DS11.6 Security Requirements for Data Management Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	output of data to meet business objectives, the organisation's security policy and regulatory requirements. Comment: See DS11.1						provider, or jointly with both. Additionally, NS/EP Owners may need to have the ability to wipe devices once an event is over and this may require building permissions and management system into non-government owned/managed devices.	distributed computing base, geo-redundancy, scalability, and ability to rapidly deploy new services makes cloud services a promising environment for NS/EP applications. NS/EP owners will need to set clear requirements for data retention in the cloud. NS/EP owners will need to determine specific policies related to data retention, including not just how long but where the data is being retained (e.g., user devices, cloud, or back inside of government enterprises). For example, in response to national
Data	DS12.1 Site Selection and LayoutDefine and select the physical sites for IT equipment to support thetechnology strategy linked to the business strategy. The selection anddesign of the layout of a site should take into account the risk associatedwith natural and man-made disasters, whilst considering relevant lawsand regulations, such as occupational health and safety regulations.Comment: Contract requirements should specify whether the customermust comply with regulations or statutes on geographiclocation of data. This requirement may impact the CSP'ssite selection, or its ability to meet		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	customer processingrequirements.							disasters, does the NS/EP data generated in a collaborative cloud model have specific time-to-live? Are there specific government policies for retention or is up to the service owners and stake holders to establish this. In dealing with sensitive information complete and secure removal of data must be supported and access to the functionality needs to be effectively controlled. Depending on the cloud service model, the responsibility may reside with application owner, the

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
								service provider, or jointly with both. Additionally, NS/EP Owners may need to have the ability to wipe devices once an event is over and this may require building permissions and management system into non-government owned/managed devices.
Infrastructure	DS12.2 Physical Security Measures Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.		x	x	DS12 Manage the Physical Environment Protection for computer equipment and personnel requires well-designed and well-managedphysical facilities. The process of managing the physical environment includes defining thephysical site requirements, selecting appropriate facilities, and designing effective processesfor monitoring environmental factors	R.22 Risk from changes of jurisdiction R.23 Data protection risks R.30 Loss or compromise of operational logs R.31 Loss or compromise of security logs R.32 Backups lost, stolen R.33 Unauthorized	Physical security measures can present two different types of risk: 1) physical security controls applied to individuals can prevent unauthorized personnel from accessing systems and modifying, corrupting, mishandling, and/or deleting data and 2) the physical location of the data (center) and compliance considerations associated with housing	Contract requirements should specify whether the customer must comply with regulations or statutes on geographic location of data. This requirement may impact the CSP's site selection, or its ability to meet customer processing

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	Comment: The CSP is responsible for physical security based upon contract provisions.				and managing physical access. Effective managementof the physical environment reduces business interruptions from damage to computer equipmentand personnel.	access to premises R.34 Theft of computer equipment	data in a particular jurisdiction.	requirements. Equipment power failures are, in almost all NS/EP situations, region-specific with minimal likelihood that such a failure would occur at the national level. Owners need a well-planned redundancy process in place to ensure that back-up facilities/equipment will perform and provide the necessary capacity and functions.
Infrastructure	ME1.1 Monitoring Approach Establish a general monitoring framework and approach to define the scope, methodology and process to be followed for measuring IT's solution and service delivery, and monitor IT's contribution to the business. Integrate the framework with the corporate performance management system.		x	x				
Policy/Legal	ME1.2 Definition and Collection of Monitoring Data Work with the business to define a balanced set of performance targets and have them approved by the business and other relevant stakeholders. Define benchmarks with which to compare the targets, and identify available data to		x	x	ME1 Monitor and Evaluate IT Performance Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of	R.3 Compliance challenges R.26 Network management (i.e. network congestion, misconnection, non-optimal use)	SLAs need to effectively represent the performance requirements of the NS/EP owner and user, including which party will bear the liability for diminished or failed performance of specific functions and under what circumstances,	In an NS/EP event, where there is an application in the cloud supporting many users, the owner may want to have increased security monitoring to prevent the

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	be collected to measure the targets. Establish processes to collect timely and accurate data to report on progress against targets.				performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.		priority access/bandwidth requirements for specific applications or types of data, etc. Continuous monitoring and evaluation of data can indicate deviations from performance requirements and data usage patterns.	application from being unavailable or the target of an attack. The SLAs need to provide enough resources and support for extra monitoring of the architecture.
Interdependency	ME1.3 Monitoring Method Deploy a performance monitoring method (e.g., balanced scorecard) that records targets; captures measurements; provides a succinct, all-around view of IT performance; and fits within the enterprise monitoring system.	x	x	x				
Policy/Legal	ME1.4 Performance Assessment Periodically review performance against targets, analyse the cause of any deviations, and initiate remedial action to address the underlying causes. At appropriate times, perform root cause analysis across deviations. Comment: Analyse actual performance against SLA requirements.		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
Infrastructure	ME1.5 Board and Executive Reporting Develop senior management reports on IT's contribution to the business, specifically in terms of the performance of the enterprise's portfolio, IT-enabled investment programmes, and the solution and service deliverable performance of individual programmes. Include in status reports the extent to which planned objectives have been achieved, budgeted resources used, set performance targets met and identified risks mitigated. Anticipate senior management's review by suggesting remedial actions for major deviations. Provide the report to senior management, and solicit feedback from management's review. Comment: This will depend upon the investment and the overall significance to the organisation.		x	x				
Interdependency	ME1.6 Remedial Actions Identify and initiate remedial actions based on performance		x					

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	monitoring, assessment and reporting. This includes follow-up of all monitoring, reporting and assessments through: • Review, negotiation and establishment of management responses • Assignment of responsibility for remediation • Tracking of the results of actions committed Comment: This is a monitoring of the CSP's performance as well as the interface processes that are the responsibility of the customer.							
Policy/Legal	ME3.1 Identification of External Legal, Regulatory and Contractual Compliance Requirements Identify, on a continuous basis, local and international laws, regulations, and other external requirements that must be complied with for incorporation into the		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	organisation's IT policies, standards, procedures and methodologies. Comment: When considering the monitoring of compliance requirements, the customer must recognise that it is responsible for compliance with external regulations regardless of the CSP's actions or inactions							
Policy/Legal	ME3.2 Optimisation of Response to External Requirements Review and adjust IT policies, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.		x	x	ME3 Ensure Compliance With External Requirements Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimising and evaluating the response, obtaining assurance that the requirements have been complied with and,	R.3 Compliance challenges R.7 Supply chain failure R.21 Subpoena and e-discovery R.22 Risk from changes of jurisdiction R.23 Data protection risks R.24 Licensing risks	Competing jurisdictional requirements (e.g. local, state, national) can result in challenges to comply with laws, regulations, and contracts. For example, states with different laws on data breach requirements can create difficulties in developing an internal policy for handling data breach incidents for both the NS/EP owner and CSP. Additionally, in the absence of a validation body that accredits/ authorizes specific third	In a crisis event that: 1) affects a broad range of jurisdictions 2) involves a multi-cloud environment, who determines the requirements related to data retention, storage, and sanitization among the key players involved, including but not limited to, the service owner, local/state/federal Government
Policy/Legal	ME3.3 Evaluation of Compliance With External Requirements Confirm compliance of IT policies, standards, procedures and methodologies with legal and regulatory requirements.		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
Policy/Legal	ME3.4 Positive Assurance of Compliance Obtain and report assurance of compliance and adherence to all internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner. Comment: Refer to third party review or customer auditing of CSP processes.		x	x	finally, integrating IT's compliance reporting with the rest of the business.		party audit organizations for cloud computing, the audit methodology and rigor with which it is applied can create inconsistent or unreliable mechanisms by which audits are performed. The potential for cybersecurity regulation, as well as preemptive federal breach notification legislation, to help (or hinder) NS/EP missions and their compliance obligations cannot be underestimated.	agency, CSP, law enforcement, etc.? Additionally, in a post-event situation, which of these entities owns the data? Specific Federal preemptive legislation in the areas of privacy, cybersecurity, critical infrastructure and breach notification, all tailored to NS/EP purposes, may be required.
Policy/Legal	ME4.5 Risk Management Work with the board to define the enterprise's appetite for IT risk, and obtain reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite. Embed risk management responsibilities into the organisation, ensuring that the business and IT regularly assess and report IT-related risks and their impact and that		x	x				

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	the enterprise's IT risk position is transparent to all stakeholders. Comment: Ensure that the C-suite is apprised of the risk associated with the adoption of cloud computing for critical functions.							
Resiliency	ME4.6 Performance Measurement Confirm that agreed-upon IT objectives have been met or exceeded, or that progress toward IT goals meets expectations. Where agreed-upon objectives have been missed or progress is not as expected, review management's remedial action. Report to the board relevant portfolios, programme and IT performance, supported by reports to enable senior management to review the enterprise's progress toward identified goals. Comment: The SLA metrics will provide the basis for performance measurement and will include both CSP and		x		ME4 Provide IT Governance Establishing an effective governance framework includes defining organisational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.	R.1-R.35 (all risks are applicable)	Service owners need to determine the risk of placing low, moderate, and high risk functions in the cloud and determine whether they can implement controls to mitigate those risks, delegate the risk to a third party or the CSP, or accept the risk. Migrating a series of operations to the cloud can change the risk profile based on how the services are going to be used.	Currently, organizations are moving low to moderate risk functions to the cloud. When critical NS/EP functions begin migrating to the cloud, the NS/EP owner needs an overarching NS/EP risk management plan that considers the risks introduced and assumed by multiple stakeholders, including the carrier, cloud provider, application provider, and

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	ENISA Risk (R.35 Natural Disasters applicable to all)	Unique Characteristic or Risk	NS/EP Implication
		User	Owner	Provider				
	customer internal SLAs.							user.
Policy/Legal	ME4.7 Independent Assurance Obtain independent assurance (internal or external) about the conformance of IT with relevant laws and regulations; the organisation's policies, standards and procedures; generally accepted practices; and the effective and efficient performance of IT. Comment: Independent assurance will be limited to third-party reviews or internal audits within the contractual rightsand obligations.		x					

5.3 FedRAMP Security Controls

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	1.1. Access Control (AC)			The basis of trust which the cloud sponsor (i.e., Government) must have with the cloud provider in order to accomplish the overall goals for this control. The Cloud Consumer must be able to transfer the relevant identity credentials to the cloud provider safely & securely using the appropriate ID management processes and technologies; policies governing access controls need to balance providing the right level of access to the right end user as the situation requires while safeguarding the program/ application/data from unauthorized access or use.	The overall NS/EP implication is one of complete system access denial if the end user is prevented either by accidental or malicious intent at the time of need. Authentication of users need to be rapidly provisioned (or de-provision), particularly in a BYOD scenario. AC-14 Permitted actions without authentication and authorization need to be carefully considered based upon mission function/criticality, end user need, and data classification level. There are a couple of considerations. The first is that the cloud provider will provision their own user accounts for their staff and vendors, and then the NS/EP customer will likely provision accounts for their users. These accounts will likely be managed differently, and to different standards, even if the same controls are required. The second consideration is that NS/EP users will likely need HSPD-12 support, and it is not guaranteed that every cloud provider can support HSPD-12, and that HSPD-12 will work in some NS/EP scenarios where identity and management systems not under the control of the cloud provider
	AC-1	Access Control Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.		
	AC-2	Account Management	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges;		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts at least annually.		might be unavailable.
	AC-2 (1)	Account Management	The organization employs automated mechanisms to support the management of information system accounts.		
	AC-2 (2)	Account Management	The information system automatically terminates temporary and emergency accounts after no more than ninety days for temporary and emergency		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			account types.		
	AC-2 (3)	Account Management	The information system automatically disables inactive accounts after ninety days for user accounts. Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB.		
	AC-2 (4)	Account Management	The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.		
	AC-2 (7)	Account Management	The organization: a. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and b. Tracks and monitors privileged role assignments.		
	AC-3	Access Enforcement	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AC-3 (3)	Access Enforcement	The information system enforces role-based access control over all users and resources where the policy rule set for each policy specifies: a. Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and b. Required relationships among the access control information to permit access. Requirement: The service provider: a. Assigns user accounts and authenticators in accordance within service provider's role-based access control policies; b. Configures the information system to request user ID and authenticator prior to system access; and c. Configures the databases containing federal information in accordance with service provider's security administration guide to provide role-based access controls enforcing assigned privileges and permissions at the file, table, row, column, or cell level, as appropriate.		
	AC-4	Information Flow Enforcement	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AC-5	Separation of Duties	The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion; b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations.		
	AC-6	Least Privilege	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.		
	AC-6 (1)	Least Privilege	The organization explicitly authorizes access to - See additional requirements and guidance. Requirement: The service provider defines the list of security functions. The list of functions is approved and accepted by the JAB.		
	AC-6 (2)	Least Privilege	The organization requires that users of information system accounts, or roles, with access to all security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions. Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.		
	AC-7	Unsuccessful Login Attempts	The information system: a. Enforces a limit of not more than three consecutive invalid login attempts by a user during a fifteen minute period; and b. Automatically locks the account/node for thirty minutes when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AC-8	System Use Notification	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system. Requirement: The service provider shall determine		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB. Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB. Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided. Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB.		
	AC-10	Concurrent Session Control	The information system limits the number of concurrent sessions for each system account to one session.		
	AC-	Session Lock	The information system:		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	11		a. Prevents further access to the system by initiating a session lock after fifteen minutes of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.		
	AC-11 (1)	Session Lock	The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen. Guidance: For IaaS and PaaS.		
	AC-14	Permitted Actions Without Identification/ Authentication	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.		
	AC-14 (1)	Permitted Actions Without Identification/ Authentication	The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AC-16	Security Attributes	The information system supports and maintains the binding of [See additional requirements and guidance] to information in storage, in process, and in transmission. Requirement: If the service provider offers the capability of defining security attributes, then the security attributes need to be approved and accepted by JAB.		
	AC-17	Remote Access	The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system.		
	AC-17 (1)	Remote Access	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.		
	AC-17 (2)	Remote Access	The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AC-17 (3)	Remote Access	The information system routes all remote accesses through a limited number of managed access control points.		
	AC-17 (4)	Remote Access	The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.		
	AC-17 (5)	Remote Access	The organization monitors for unauthorized remote connections to the information system continuously, real time, and takes appropriate action if an unauthorized connection is discovered.		
	AC-17 (7)	Remote Access	The organization ensures that remote sessions for accessing [See additional requirements and guidance] employ [See additional requirements and guidance] and are audited. Requirement: The service provider defines the list of security functions and security relevant information. Security functions and the implementation of such functions are approved and accepted by the JAB. Guidance: Security functions include but are not limited to: establishing system accounts; configuring access authorizations; performing system administration functions; and auditing system events or accessing event logs; SSH, and VPN.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AC-17 (8)	Remote Access	The organization disables tftp, (trivial ftp); X-Windows, Sun Open Windows; FTP; TELNET; IPX/SPX; NETBIOS; Bluetooth; RPC-services, like NIS or NFS; rlogin, rsh, rexec; SMTP (Simple Mail Transfer Protocol); RIP (Routing Information Protocol); DNS (Domain Name Services); UUCP (Unix-Unix Copy Protocol); NNTP (Network News Transfer Protocol); NTP (Network Time Protocol); Peer-to-Peer except for explicitly identified components in support of specific operational requirements. Requirement: Networking protocols implemented by the service provider are approved and accepted by JAB. Guidance: Exceptions to restricted networking protocols are granted for explicitly identified information system components in support of specific operational requirements.		
	AC-18	Wireless Access	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system.		
	AC-18	Wireless Access	The information system protects wireless access		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	(1)		to the system using authentication and encryption.		
	AC-18 (2)	Wireless Access	The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points at least quarterly, and takes appropriate action if an unauthorized connection is discovered.		
	AC-19	Access Control for Mobile Devices	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies [See additional requirements and guidance] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures. Requirement: The service provider defines inspection and preventative measures. The measures are approved and accepted by JAB.		
	AC-19 (1)	Access Control for Mobile Devices	The organization restricts the use of writable, removable media in organizational information systems.		
	AC-19 (2)	Access Control for Mobile Devices	The organization prohibits the use of personally owned, removable media in organizational information systems.		
	AC-19 (3)	Access Control for Mobile Devices	The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.		
	AC-20	Use of External Information Systems	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AC-20 (1)	Use of External Information Systems	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: a. Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or b. Has approved information system connection or processing agreements with the organizational entity hosting the external information system.		
	AC-20 (2)	Use of External Information Systems	The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.		
	AC-22	Publicly Accessible Content	The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			d. Reviews the content on the publicly accessible organizational information system for nonpublic information at least quarterly; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.		
	1.2. Awareness and Training (AT)			The unique risk in this set of controls is having cloud sponsors and end users be unaware of or inadequately trained in the additional cloud computing security risks/rules of behavior/compliance requirements, in addition to the "normal/traditional" IT security risks.	The overall NS/EP implication here relates to the users' knowledge of and compliance with the additional security considerations/requirements of the cloud system and its operations. The cloud also has additional risk factors that are not found in a normal IT environment. Awareness and training addressing those specific risks need to be effectively implemented in order to minimize security breaches resulting from poor end user (intentional or inadvertent) habits. There will need to be training for the Cloud Provider's staff and for the NS/EP users. This training needs to be tailored for each audience.
	AT-1	Security Awareness and Training Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.		
	AT-2	Security Awareness	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and at least annually thereafter.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AT-3	Security Training	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) at least every three years thereafter.		
	AT-4	Security Training Records	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for at least three years.		
	1.3. Audit and Accountability (AU)			A third party auditor who operates on behalf of the USG or CSP can perform a review of the cloud system and associated processes in order to verify the documented polices/SLAs are performed against as intended. Processes employed by the Cloud Auditor may allow inadvertent release of sensitive information. Additionally, the sufficiency of expertise in the cloud audit community is still developing/nascent.	A full understanding of interfaces and processes used by the Cloud Auditor must also be understood in order to mitigate risk of sensitive information being mishandled or not properly secured. The NS/EP customer can likely dictate who the third party auditor is, which can negate this implication. The continuous monitoring requirement in FedRAMP should not be ignored. What should be monitored needs to be defined, but it will be against NIST SP 800-53.
	AU-1	Audit and Accountability Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			accountability controls.		
	AU -2	Auditable Events	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes; b. Coordinates the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			information and ongoing assessment of risk, that the following events are to be audited within the information system: [See additional requirements and guidance] continually. Requirement: The service provider defines the subset of auditable events from AU-2a to be audited. The events to be audited are approved and accepted by JAB.		
	AU -2 (3)	Auditable Events	The organization reviews and updates the list of auditable events annually or whenever there is a change in the threat environment. Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB.		
	AU -2 (4)	Auditable Events	The organization includes execution of privileged functions in the list of events to be audited by the information system. Requirement: The service provider configures the auditing features of operating systems, databases, and applications to record security-related events, to include logon/logoff and all failed access attempts.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AU -3	Content of Audit Records	The information system produces audit records that contain sufficient information to, at aminimum, establish what type of event occurred, when (date and time) the event occurred, wherethe event occurred, the source of the event, the outcome (success or failure) of the event, and theidentity of any user/subject associated with the event.		
	AU -3 (1)	Content of Audit Records	The information system includes session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon in the audit records for audit events identified by type, location, or subject. Requirement: The service provider defines audit record types. The audit record types are approved and accepted by the JAB. Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.		
	AU -4	Audit Storage Capacity	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.		
	AU -5	Response to Audit Processing Failures	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: low-impact: overwrite oldest audit records;		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			moderate-impact: shut down.		
	AU-6	Audit Review, Analysis, and Reporting	The organization: a. Reviews and analyzes information system audit records at least weekly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.		
	AU-6 (1)	Audit Review, Analysis, and Reporting	The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.		
	AU-6 (3)	Audit Review, Analysis, and Reporting	The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.		
	AU-7	Audit Reduction and Report Generation	The information system provides an audit reduction and report generation capability.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AU-7 (1)	Audit Reduction and Report Generation	The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.		
	AU-8	Time Stamps	The information system uses internal system clocks to generate time stamps for audit records.		
	AU-8 (1)	Time Stamps	The information system synchronizes internal information system clocks at least hourly with http://tf.nist.gov/tf-cgi/servers.cgi. Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server. Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server. Guidance: Synchronization of system clocks improves the accuracy of log analysis.		
	AU-9	Protection of Audit Information	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.		
	AU-9 (2)	Protection of Audit Information	The information system backs up audit records at least weekly onto a different system or media than the system being audited.		
	AU-10	Non-Repudiation	The information system protects against an individual falsely denying having performed a particular action.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	AU-10 (5)	Non-Repudiation	The organization employs [See additional requirements and guidance] cryptography to implement digital signatures. Requirement: The service provider implements FIPS-140-2 validated cryptography (e.g., DOD PKI Class 3 or 4 tokens) for service offerings that include Software-as-a-Service (SaaS) with email.		
	AU-11	Audit Record Retention	The organization retains audit records for at least ninety days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements.		
	AU-12	Audit Generation	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at all information system components where audit capability is deployed; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	1.4. Assessment and Authorization (CA)			The unique characteristic here is the presence of FedRAMP for Federal Cloud Systems. At this time, there is no FedRAMP related materials for data which classified as high-risk. FedRAMP fulfills the goals of procuring cloud services for low & moderate risk systems.	The overall security of the system is now a "shared" responsibility between Cloud Consumer & Cloud Provider and that is also based on the service deployment & service model employed. Again, this risk should be carefully measured before a cloud deployment is initiated. There are different levels of responsibility for both the provider and consumer depending on the service model (IaaS, PaaS or SaaS). That might be a factor in deciding whether or not to move to the cloud.
	CA -1	Security Assessment and Authorization Policies and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.		
	CA -2	Security Assessments	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system at least annually to		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.		
	CA -2 (1)	Security Assessments	The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.		
	CA -3	Information System Connections	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	CA-5	Plan of Action and Milestones	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones at least quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.		
	CA-6	Security Authorization	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization at least every three years or when a significant change occurs. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would require a reauthorization of the information system. The		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			types of changes are approved and accepted by the JAB.		
	CA-7	Continuous Monitoring	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials monthly.		
	CA-7 (2)	Continuous Monitoring	The organization plans, schedules, and conducts assessments annually, unannounced, penetration testing, in-depth monitoring to ensure compliance		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			with all vulnerability mitigation procedures.		
	1.5. Configuration Management (CM)			The cloud sponsor does not have direct access to or knowledge of the hardware in a cloud environment. Therefore, configuration management must be performed in a cloud sense only as the underlying hardware is unknown. The sponsor interacts with the cloud through one of the three service models and interfaces and is only aware of that environment & any should have input on configuration management. These layers run on top of a middleware layer that interacts directly with the hardware. Therefore changes to the hardware may occur without any knowledge of the cloud sponsor. Interoperability & portability of services and data must be ensured such that configuration changes occur smoothly and with fidelity. This risk can be minimized through contract negotiations. A NS/EP will likely source a private cloud, and the cloud provider can detail the equipment that will be used. The equipment specifications are typically shared anyway, as part of FISMA.	The resulting implications for NS/EP are vendor lock-in as well as an uncertainty of the hardware which in some cases might relate in uncertain performance of services. The SLA will document the performance requirements, so the selection of hardware is largely immaterial as long as the SLA is met. A potentially greater concern is the sourcing of hardware from a nation state which is implicated in a NS/EP event, and where there is reasonable suspicion that the supply chain integrity has been compromised and equipment is being used that has "back doors" or "Trojan horses".
	CM-1	Configuration Management Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.		
	CM-2	Baseline Configuration	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.		
	CM-2 (1)	Baseline Configuration	The organization reviews and updates the baseline configuration of the information system: a. Annually; b. When required due to a significant change; and c. As an integral part of information system component installations and upgrades. Guidance: Significant change is defined in NIST		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would require a review and update of the baseline configuration. The types of changes are approved and accepted by the JAB.		
	CM -2 (3)	Baseline Configuration	The organization retains older versions of baseline configurations as deemed necessary to support rollback.		
	CM -2 (5)	Baseline Configuration	The organization: a. Develops and maintains [See additional requirements and guidance]; and b. Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system. Requirement: The service provider defines and maintains a list of software programs authorized to execute on the information system. The list of authorized programs is approved and accepted by the JAB.		
	CM -3	Configuration Change Control	The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through [See additional requirements and guidance] that convenes [See additional requirements and guidance]; [See additional requirements and guidance]. Requirement: The service provider defines the configuration change control element and the frequency or conditions under which it is convened. The change control element and frequency/conditions of use are approved and accepted by the JAB. Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			communication are approved and accepted by the JAB.		
	CM -3 (2)	Configuration Change Control	The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.		
	CM -4	Security Impact Analysis	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.		
	CM -5	Access Restrictions for Change	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.		
	CM -5 (1)	Access Restrictions for Change	The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.		
	CM -5 (5)	Access Restrictions for Change	The organization: a. Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and b. Reviews and reevaluates information system developer/integrator privileges at least quarterly.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	CM-6	Configuration Settings	The organization:a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;b. Implements the configuration settings;c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; andd. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.		
	CM-6 (1)	Configuration Settings	The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.		
	CM-6 (3)	Configuration Settings	The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.		
	CM-7	Least Functionality			
	CM-7 (1)	Least Functionality	The organization reviews the information system at least quarterly to identify and eliminate unnecessary functions, ports, protocols, and/or services.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	CM-8	Information System Component Inventory	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [See additional requirements and guidance]; and e. Is available for review and audit by designated organizational officials. Requirement: The service provider defines information deemed necessary to achieve effective property accountability. Property accountability information are approved and accepted by the JAB. Guidance: Information deemed necessary to achieve effective property accountability may include hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			networked component/device, the machine name and network address.		
	CM-8 (1)	Information System Component Inventory	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.		
	CM-8 (3)	Information System Component Inventory	The organization: a. Employs automated mechanisms Continuously, using automated mechanisms with a maximum five-minute delay in detection to detect the addition of unauthorized components/devices into the information system; and b. Disables network access by such components/devices or notifies designated organizational officials.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	CM-8 (5)	Information System Component Inventory	The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.		
	CM-9	Configuration Management Plan	The organization develops, documents, and implements a configuration management plan for the information system that:a. Addresses roles, responsibilities, and configuration management processes and procedures;b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; andc. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.		
	1.6.	Contingency Planning (CP)		Traditionally the organization is responsible for the contingency planning and execution because they control the enterprise and/or	1. NS/EP owners will take on the bulk of the upfront cost to build robust cloud services that meet their

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Resiliency	CP-1	Contingency Planning Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	environment that they are using from end-to-end. However, Cloud Computing in the FedRAMP model takes the execution out of the hands of the organization and puts the onus on owner/operator to implement. The owner operator will have to account for multiple contingencies that may or may not be relevant to their operations, but are only relevant to the organization(s) that they are supporting. The owner/operator has increased risk in this model and will have to account for that risk by building/planning not to the mean, but rather to the maximum.	unique CP requirements; 2. Commercial providers may not wish to comply with the unique CP requirements of the NS/EP environment; 3. NS/EP CP requirements will not translate to the commercial marketplace and therefore the value of using a shared service is never realized; and 4. Leveraging existing certification and accreditation models authorized under FedRAMP may not fully address NS/EP CP requirements as they are not the same across the

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Resiliency	CP-2	Contingency Plan	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to		community and change dynamically.

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			[See additional requirements and guidance]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system at least annually; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [See additional requirements and guidance]. CP-2b. Requirement: The service provider defines a list of key contingency personnel (identified by name and/or by role) and organizational elements. The contingency list includes designated FedRAMP personnel. CP-2f. Requirement: The service provider defines a list of key contingency personnel (identified by name and/or by role) and organizational elements. The contingency list includes designated FedRAMP personnel.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	CP-2 (1)	Contingency Plan	The organization coordinates contingency plan development with organizational elements responsible for related plans.		
	CP-2 (2)	Contingency Plan	The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.		
Resiliency	CP-3	Contingency Training	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training at least annually.		
Resiliency	CP-4	Contingency Plan Testing and Exercises	The organization: a. Tests and/or exercises the contingency plan for the information system at least annually for moderate impact systems; at least every three years for low impact systems using functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions. CP-4a. Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			approved and accepted by the JAB.		
	CP-4 (1)	Contingency Plan Testing and Exercises	The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.		
Resiliency	CP-6	Alternate Storage Site	The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.		
	CP-6 (1)	Alternate Storage Site	The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.		
	CP-6 (3)	Alternate Storage Site	The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Resiliency	CP-7	Alternate Processing Site	The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [See additional requirements and guidance] when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption. CP-7a. Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis. The time period is approved and accepted by the JAB.		
	CP-7 (1)	Alternate Processing Site	The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.		
	CP-7 (2)	Alternate Processing Site	The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	CP-7 (3)	Alternate Processing Site	The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.		
	CP-7 (5)	Alternate Processing Site	The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.		
Resiliency	CP-8	Telecommunications Services	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [See additional requirements and guidance] when the primary telecommunications capabilities are unavailable. CP-8 Requirement: The service provider defines a time period consistent with the business impact analysis. The time period is approved and accepted by the JAB.		
	CP-8 (1)	Telecommunications Services	The organization: a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			telecommunications services are provided by a common carrier.		
	CP-8 (2)	Telecommunications Services	The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Resiliency	CP-9	Information System Backup	The organization: a. Conducts backups of user-level information contained in the information system daily incremental; weekly full; b. Conducts backups of system-level information contained in the information system daily incremental; weekly full; c. Conducts backups of information system documentation including security-related documentation daily incremental; weekly full; and d. Protects the confidentiality and integrity of backup information at the storage location. CP-9 Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control. The cloud environment elements requiring Information System Backup are approved and accepted by the JAB. Requirement: The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check. The verification and periodicity of the Information System Backup are approved and accepted by the JAB.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			CP-9a. Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB. CP-9b. Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB. CP-9c. Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.		
	CP-9 (1)	Information System Backup	The organization tests backup information at least annually to verify media reliability and information integrity.		
	CP-9 (3)	Information System Backup	The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware,		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.		
Resiliency	CP-10	Information System Recovery and Reconstitution	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.		
	CP-10 (2)	Information System Recovery and Reconstitution	The information system implements transaction recovery for systems that are transaction-based.		
	CP-10 (3)	Information System Recovery and Reconstitution	The organization provides compensating security controls for [See additional requirements and guidance]. CP-10 (3) Requirement: The service provider defines circumstances that can inhibit recovery and reconstitution to a known state in accordance with the contingency plan for the information system and business impact analysis.		
	1.7. Identification and Authentication (IA)			Organizations must extend their existing Identity and Access Management Strategies into the Cloud. New IAM solutions for the cloud simply will not scale; rather the cloud must be seen as part of the "extended" enterprise, whereas existing privacy concerns, compliance issues, and processes and controls are dealt with within the cloud using strategies and solutions already built and utilized within the enterprise.The	1) NS/EP IAM systems are not integrated and or compatible with cloud services (i.e. TMR is not integrated with authentication methodologies used to access the cloud); 2) Priority access and control is needed in a NS/EP environment and the FedRAMP IAM controls do not account for them; 3) Mobile devices are the main medium for connectivity to data for the NS/EP community, but within the FedRAMP control IA-5(1)a such devices are exempt from the complexity control
Infrastructure	IA-1	Identification and Authentication Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			authentication policy and associated identification and authentication controls.	FedRAMP model of "Certify Once, Use Many" must take this point into consideration. If they do not they will be adding in complexity that is unnecessary and likely to fail due to the following reasons: User Experience; • Separate systems increases user frustration; • Users having more than a single credential can be problematic; • Users have to deal with two separate processes for identity creation; • Users may potentially become confused with enterprise vs. cloud issues and or policies. Manageability • Administration of identities requires double the amount of administration; • User attributes are not automatically populated in cloud-based systems. Compliance and Risk	thereby increasing risk for misuse, unauthorized access, etc.
Infrastructure	IA-2	Identification and Authentication (Organizational Users)	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).		
	IA-2 (1)	Identification and Authentication (Organizational Users)	The information system uses multifactor authentication for network access to privileged accounts.		
	IA-2 (2)	Identification and Authentication (Organizational Users)	The information system uses multifactor authentication for network access to non-privileged accounts.		
	IA-2 (3)	Identification and Authentication (Organizational Users)	The information system uses multifactor authentication for local access to privileged accounts.		
	IA-2 (8)	Identification and Authentication (Organizational Users)	The information system uses [See additional requirements and guidance] for network access to privileged accounts. IA-2 (8) Requirement: The service provider defines replay-resistant authentication mechanisms. The mechanisms are approved and accepted by the JAB.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	IA-3	Device Identification and Authentication	The information system uniquely identifies and authenticates [See additional requirements and guidance] before establishing a connection. IA-3 Requirement: The service provider defines a list a specific devices and/or types of devices. The list of devices and/or device types is approved and accepted by the JAB.	• Cloud-based systems must adhere to regulatory requirements for identity provisioning; • Cloud-based systems can easily be overlooked when changes are made to enterprise User's identities and privileges; • Cloud-based systems may be susceptible to internet breach.	
Infrastructure	IA-4	Identifier Management	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for at least two years; and e. Disabling the user identifier after ninety days for user identifiers [See additional requirements and guidance]. IA-4e. Requirement: The service provider defines time period of inactivity for device identifiers. The time		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			period is approved and accepted by JAB.		
	IA-4 (4)	Identifier Management	The organization manages user identifiers by uniquely identifying the user as contractors; foreign nationals.		
Infrastructure	IA-5	Authenticator Management	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators sixty days; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.		
	IA-5 (1)	Authenticator Management	The information system, for password-based authentication: a. Enforces minimum password complexity of case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters; b. Enforces at least a at least one or as determined by the information system (where possible) when new passwords are created; c. Encrypts passwords in storage and in transmission; d. Enforces password minimum and maximum lifetime restrictions of one day minimum, sixty day maximum; and		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			e. Prohibits password reuse for twenty four generations. IA-5 (1) (a) Guidance: Mobile devices are excluded from the password complexity requirement.		
	IA-5 (2)	Authenticator Management	The information system, for PKI-based authentication: a. Validates certificates by constructing a certification path with status information to an accepted trust anchor; b. Enforces authorized access to the corresponding private key; and c. Maps the authenticated identity to the user account.		
	IA-5 (3)	Authenticator Management	The organization requires that the registration process to receive HSPD12 smart cards be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).		
	IA-5 (6)	Authenticator Management	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	IA-5 (7)	Authenticator Management	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.		
Infrastructure	IA-6	Authenticator Feedback	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.		
Infrastructure	IA-7	Cryptographic Module Authentication	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.		
Infrastructure	IA-8	Identification and Authentication (Non-Organizational Users)	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).		
	1.8. Incident Response (IR)			1. Incident response plans are required to be JAB certified unlike traditional plans that were a necessary "exercise" but not reviewed/certified by a third-party. 2. The "certification" of an incident response plan that does not take in consideration all factors could possibly bind the provider or the organization to a process	1) Latency and visibility issues - by not controlling this function an enterprise/organization may find themselves "blind" in a time of crisis. Another consideration is that cloud provider IR plans are focused at responding to security incidents at the cloud provider, where are the NS/EP IR plans are focused at the national /international level. Additionally, the NS/EP IR plan might be involved due to an issue with the Internet or Cloud Computing in general, yet its cloud
Resiliency	IR-1	Incident Response Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			policy and associated incident response controls.	that is not robust enough to respond to a threat or an event. 3. Maintenance is largely irrelevant as long as negotiated SLAs surrounding uptime/availability are met.	provider(s) are unavailable as they are part of the event.
Resiliency	IR-2	Incident Response Training	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training at least annually.		
Resiliency	IR-3	Incident Response Testing and Exercises	The organization tests and/or exercises the incident response capability for the information system annually using [See additional requirements and guidance] to determine the incident response effectiveness and documents the results. IR-3 Requirement: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). Requirement: The service provider provides test plans to FedRAMP annually. Test plans are approved and accepted by the JAB prior to test commencing.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Resiliency	IR-4	Incident Handling	The organization:a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;b. Coordinates incident handling activities with contingency planning activities; andc. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.IR-4Requirement: The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.		
	IR-4 (1)	Incident Handling	The organization employs automated mechanisms to support the incident handling process.		
Resiliency	IR-5	Incident Monitoring	The organization tracks and documents information system security incidents.		
Resiliency	IR-6	Incident Reporting	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended); and b. Reports security incident information to designated authorities.		
	IR-	Incident Reporting	The organization employs automated mechanisms		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	6 (1)		to assist in the reporting of security incidents.		
Resiliency	IR-7	Incident Response Assistance	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.		
	IR-7 (1)	Incident Response Assistance	The organization employs automated mechanisms to increase the availability of incident response-related information and support.		
	IR-7 (2)	Incident Response Assistance	The organization: a. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and b. Identifies organizational incident response team members to the external providers.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Resiliency	IR-8	Incident Response Plan	The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response		

Primary NSTAC Concern	Control Number and Name	Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
		plan to [See additional requirements and guidance]; c. Reviews the incident response plan at least annually; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [See additional requirements and guidance]. IR-8b. Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel. IR-8e. Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.		
	1.9. Maintenance (MA)		1. The organization does not have	1. 1) Maintenance windows will need

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	MA -1	System Maintenance Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	the requisite expertise to be able to identify the appropriate maintenance procedures for the information system or hardware for the architecture being used (i.e. the lack of visibility into the cloud architecture from an end-to-end perspective). 2. The frequency of an audit interval for the maintenance plan operational processes could be too long and thereby problematic 3. Providers will plan/bid to the mean or lowest requirement to be certified by the JAB	to be coordinated so that access to the cloud, cloud services, or data is not impacted. 2. The MP may be inadequate for the NS/EP system requirements. 3. There may be two maintenance plans that need to be crafted. For IaaS and PaaS-based cloud solutions the NS/EP cloud consumer will need to create a maintenance plan and ensure it is coordinated with cloud providers' maintenance plans. SaaS NS/EP consumers will likely not need their own maintenance plans.
Infrastructure	MA -2	Controlled Maintenance	The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			organizational facilities for off-site maintenance or repairs; and e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.		
	MA-2 (1)	Controlled Maintenance	The organization maintains maintenance records for the information system that include: a. Date and time of maintenance; b. Name of the individual performing the maintenance; c. Name of escort, if necessary; d. A description of the maintenance performed; and e. A list of equipment removed or replaced (including identification numbers, if applicable).		
Infrastructure	MA-3	Maintenance Tools	The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.		
	MA-3 (1)	Maintenance Tools	The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	MA-3 (2)	Maintenance Tools	The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.		
	MA-3 (3)	Maintenance Tools	The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.		
Infrastructure	MA-4	Non-Local Maintenance	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; ande. Terminates all sessions and network connections when non-local maintenance is completed.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	MA-4 (1)	Non-Local Maintenance	The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.		
	MA-4 (2)	Non-Local Maintenance	The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.		
Infrastructure	MA-5	Maintenance Personnel	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	MA-6	Timely Maintenance	The organization obtains maintenance support and/or spare parts for [See additional requirements and guidance] within [See additional requirements and guidance] of failure. MA-6 Requirement: The service provider defines a list of security-critical information system components and/or key information technology components. The list of components is approved and accepted by the JAB. Requirement: The service provider defines a time period to obtain maintenance and spare parts in accordance with the contingency plan for the information system and business impact analysis. The time period is approved and accepted by the JAB.		
	1.10. Media Protection (MP)			1. Controls do not address anything above a low/medium classification; 2. The SP defines the types of media to be used and certified by the JAB, rather than the organization	1. Media and access to data to create media is out of the organization's control, which increases the possibility of loss of data or lapse in process control. 2. How does the organization sanitize the system media (MP-6a) when the system provider controls it? This appears to violate the MP-6a control that it must be sanitized prior to it being released out of the organizations control.
Infrastructure	MP-1	Media Protection Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	MP-2	Media Access	The organization restricts access to [See additional requirements and guidance] to [See additional requirements and guidance] using [See additional requirements and guidance]. MP-2 Requirement: The service provider defines types of digital and non-digital media. The media types are approved and accepted by the JAB. Requirement: The service provider defines a list of individuals with authorized access to defined media types. The list of authorized individuals is approved and accepted by the JAB. Requirement: The service provider defines the types of security measures to be used in protecting defined media types. The security measures are approved and accepted by the JAB.		
	MP-2 (1)	Media Access	The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.		
Infrastructure	MP-3	Media Marking	The organization: a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts no removable media types from marking as long as the exempted items		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			remain within not applicable.		
Infrastructure	MP-4	Media Storage	The organization: a. Physically controls and securely stores magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks within [See additional requirements and guidance] using for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secure storage in locked cabinets or safes; b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. MP-4a. Requirement: The service provider defines controlled areas within facilities where the information and information system reside.		
	MP-4 (1)	Media Storage	The organization employs cryptographic mechanisms to protect information in storage.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	MP-5	Media Transport	The organization: a. Protects and controls magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks during transport outside of controlled areas using for digital media, encryption using a FIPS 140-2 validated encryption module; b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel. MP-5a. Requirement: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB.		
	MP-5 (2)	Media Transport	The organization documents activities associated with the transport of information system media.		
	MP-5 (4)	Media Transport	The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	MP-6	Media Sanitization	The organization: a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.		
	MP-6 (4)	Media Sanitization	The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies.		
	1.11. Physical and Environmental Protection (PE)			Failure to protect the physical data center facilities could result in an unstable operating environment or unauthorized physical access to equipment.	Physical and environmental controls are intended to maintain the integrity of the physical environment in all situations, including following an NS/EP event. This protection is essential for all Critical Infrastructure Key Resources (CI/KR).
Policy/Legal	PE-1	Physical and environmental protection policy and procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	PE-2	Physical Access Authorizations	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials at least annually, removing from the access list personnel no longer requiring access.		
Infrastructure	PE-3	Physical Access Control	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices at least annually; and g. Changes combinations and keys at least annually and when keys are lost, combinations are compromised, or individuals are transferred or terminated.		
Infrastructure	PE-4	Access Control for Transmission Medium	The organization controls physical access to information system distribution and transmission lines within organizational facilities.		
Infrastructure	PE-5	Access Control for Output Devices	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.		
Infrastructure	PE-6	Monitoring Physical Access	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs at least semi-annually; and c. Coordinates results of reviews and investigations with the organization's incident response capability.		
	PE-6	Monitoring Physical Access	The organization monitors real-time physical intrusion alarms and surveillance equipment.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	(1)				
Infrastructure	PE-7	Visitor Control	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.		
	PE-7 (1)	Visitor Control	The organization escorts visitors and monitors visitor activity, when required.		
Infrastructure	PE-8	Access Records	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Reviews visitor access records at least monthly.		
Infrastructure	PE-9	Power Equipment and Power Cabling	The organization protects power equipment and power cabling for the information system from damage and destruction.		
Infrastructure	PE-10	Emergency Shutoff	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [See additional requirements and guidance] to facilitate safe and easy access for		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			personnel; and c. Protects emergency power shutoff capability from unauthorized activation. PE-10b. Requirement: The service provider defines emergency shutoff switch locations. The locations are approved and accepted by the JAB.		
Infrastructure	PE-11	Emergency Power	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.		
Infrastructure	PE-12	Emergency Lighting	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.		
Infrastructure	PE-13	Fire Protection	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.		
	PE-13 (1)	Fire Protection	The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.		
	PE-13 (2)	Fire Protection	The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			the organization and emergency responders.		
	PE-13 (3)	Fire Protection	The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.		
Infrastructure	PE-14	Temperature and Humidity Controls	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments; and b. Monitors temperature and humidity levels continuously. PE-14a. Requirements: The service provider measures temperature at server inlets and humidity levels by dew point.		
Infrastructure	PE-15	Water Damage Protection	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.		
Infrastructure	PE-16	Delivery and Removal	The organization authorizes, monitors, and controls all information systems entering and exiting the facility and maintains records of those		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			items.		
Resiliency	PE-17	Alternate Work Site	The organization: a. Employs [See additional requirements and guidance] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems. PE-17a. Requirement: The service provider defines management, operational, and technical information system security controls for alternate work sites. The security controls are approved and accepted by the JAB.		
Infrastructure	PE-18	Location of Information System Components	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.		
	1.12. Planning (PL)			Security-related planning activities	With an ad hoc user base during an

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	PL-1	Security Planning Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	can help cloud sponsors to consider policies, practices, and procedures affecting the information system, information, and the user. This upfront planning adopts a systems lifecycle approach, which incorporates holistic risk considerations from system planning through retirement.	NS/EP event, it may be challenging to achieve compliance with rules of behavior requirements. Therefore, upfront planning, instead of reactive response during an incident, can help address the risks associated with a "rogue" user. Privacy concerns also present a unique challenge with use of the new technologies. For instance, if a first responder takes a photo or a video clip of an incident that becomes used in a LE investigation, what are the privacy rights of the innocent bystanders caught in the shot? Who "owns" that medium?
	PL-2	System Security Plan	The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of missions and business processes; - Provides the security categorization of the information system including supporting rationale;		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			- Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system at least annually; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	PL-4	Rules of Behavior	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.		
	PL-5	Privacy Impact Assessment	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.		
	PL-6	Security-Related Activity Planning	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.		
	1.13. Personnel Security (PS)			Failure to implement personnel security controls could lead to personnel with unknown backgrounds and affiliations having physical access to equipment and increasing the risk of compromise by insiders.	Personnel Security controls are intended to maintain the consistent standards for personnel across organizations in all situations, including following an NS/EP event. This protection is essential for all Critical Infrastructure Key Resources (CI/KR).
Policy/Legal	PS-1	Personnel Security Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.		
Infrastructure	PS-2	Position Categorization	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations at least every three years.		
Infrastructure	PS-3	Personnel Screening	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to for national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	PS-4	Personnel Termination	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.		
Infrastructure	PS-5	Personnel Transfer	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [See additional requirements and guidance] within five days. PS-5 Requirement: The service provider defines transfer or reassignment actions. Transfer or reassignment actions are approved and accepted by the JAB.		
Infrastructure	PS-6	Access Agreements	The organization: a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements at		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			least annually.		
Interdependency	PS-7	Third-Party Personnel Security	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.		
Infrastructure	PS-8	Personnel Sanctions	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.		
	1.14. Risk Assessment (RA)			Failure to categorize, assess risk and scan for vulnerabilities could result in the existence of an unknown or unacceptable level of risk.	Risk Assessment controls are intended to categorize sensitivity of data, identify risk including likelihood and magnitude of harm, proactively scan for vulnerabilities to the systems, applications and databases to maintain a known and acceptable level of risk for the environment in all situations, including following an NS/EP event. This protection is essential for all Critical Infrastructure Key Resources (CI/KR).
Policy/Legal	RA-1	Risk Assessment Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	RA -2	Security Categorization	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.		
Infrastructure	RA -3	Risk Assessment	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in security assessment report; c. Reviews risk assessment results at least every three years or when a significant change occurs; and d. Updates the risk assessment at least every three years or when a significant change		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			occurs or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. RA-3c. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. RA-3d. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.		
Infrastructure	RA-5	Vulnerability Scanning	The organization: a. Scans for vulnerabilities in the information system and hosted applications quarterly operating system, web application, and database scans (as applicable) and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities high-risk vulnerabilities mitigated within thirty days; moderate risk vulnerabilities mitigated within ninety days in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).		
	RA-5 (1)	Vulnerability Scanning	The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.		
	RA-5 (2)	Vulnerability Scanning	The organization updates the list of information system vulnerabilities scanned continuously, before each scan or when new vulnerabilities are		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			identified and reported.		
	RA-5 (3)	Vulnerability Scanning	The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).		
	RA-5 (6)	Vulnerability Scanning	The organization attempts to discern what information about the information system is discoverable by adversaries.		
	RA-5 (9)	Vulnerability Scanning	The organization includes privileged access authorization to [Assignment: organization-identified information system components] for selected vulnerability scanning activities to facilitate more thorough scanning.		
	1.15. System and Services Acquisition (SA)			Failure to implement acquisition controls could lead to the realization of any or all of the following risks: insufficient funding for security, acquisition of inadequately secure components, usage of inappropriate software, acquisition of inadequately secure external services, developer environments that do not properly manage & track change, test for security effectiveness or properly consider supply chain risks.	System and Services Acquisition controls are intended to ensure security requirements are identified and included with all other requirements in the Acquisition process. Additionally governance of User Installed Software, External Information Services, Security Testing of Developer Environments & a comprehensive approach to Supply Chain Protection as part of a defense-in-breadth information security strategy throughout the acquisition process, including following an NS/EP event. This protection is essential for all Critical Infrastructure Key Resources (CI/KR). Supply chain concerns (see earlier comment) will likely be paramount. It is not clear to me if it would be possible to use a public cloud
Policy/Legal	SA-1	System and Services Acquisition Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	SA-2	Allocation of Resources	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.		offering for NS/EP purposes, as the NS/EP customer will likely have no control of this set of controls. Even private cloud deployments could be problematic.
Infrastructure	SA-3	Life Cycle Support	The organization: a. Manages the information system using a system development life cycle methodology that includes information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.		
Infrastructure	SA-4	Acquisitions	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			standards: a. Security functional requirements/ specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements. SA-4 Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred. See http://www.niap-ccevs.org/vpl or http://www.commoncriteriaportal.org/products.html .		
	SA-4 (1)	Acquisitions	The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.		
	SA-4 (4)	Acquisitions	The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	SA-4 (7)	Acquisitions	The organization: a. Limits the use of commercially provided information technology products to those products that have been successfully evaluated against a validated U.S. Government Protection Profile for a specific technology type, if such a profile exists; and b. Requires, if no U.S. Government Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, then the cryptographic module is FIPS-validated.		
Infrastructure	SA-5	Information System Documentation	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			available to authorized personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and - User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.		
	SA-5 (1)	Information System Documentation	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	SA-5 (3)	Information System Documentation	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.		
Infrastructure	SA-6	Software Usage Restrictions	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		
Infrastructure	SA-7	User-Installed Software	The organization enforces explicit rules governing the installation of software by users.		
Infrastructure	SA-8	Security Engineering Principles	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Interdependency	SA-9	External Information System Services	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.		
	SA-9 (1)	External Information System Services	The organization: a. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by Joint Authorization Board (JAB). SA-9 (1) Requirement: The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. Future, planned outsourced services are		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			approved and accepted by the JAB.		
Infrastructure	SA-10	Developer Configuration Management	The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes; d. Document approved changes to the information system; and e. Track security flaws and flaw resolution.		
Infrastructure	SA-11	Developer Security Testing	The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan;		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes.		
	SA-11 (1)	Developer Security Testing	The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis. SA-11 (1) Requirement: The service provider submits a code analysis report as part of the authorization package and updates the report in any reauthorization actions. Requirement: The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.		
Interdependency	SA-12	Supply Chain Protection	The organization protects against supply chain threats by employing: [See additional requirements and guidance] as part of a comprehensive, defense-in-breadth information security strategy. SA-12 Requirement: The service provider defines a list of measures to protect against supply chain threats. The list of protective measures is approved and accepted by JAB.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	1.16. System and Communications Protection (SC)			Failure to implement system and communications protection could lead to exposure of sensitive information, unauthorized alteration of data or unavailability of data.	System and Communication Protections controls are intended to ensure Confidentiality, Integrity and Availability of the processing transmission and storage of data in all situations, including following an NS/EP event. This protection is essential for all Critical Infrastructure Key Resources (CI/KR).
Policy/Legal	SC -1	System and Communications Protection Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.		
Infrastructure	SC -2	Application Partitioning	The information system separates user functionality (including user interface services) from information system management functionality.		
Data	SC -4	Information in Shared Resources	The information system prevents unauthorized and unintended information transfer via shared system resources.		
Infrastructure	SC -5	Denial of Service Protection	The information system protects against or limits the effects of the following types of denial of service attacks: [See additional requirements and guidance]. SC-5 Requirement: The service provider defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			attacks) or provides a reference to source for current list. The list of denial of service attack types is approved and accepted by JAB.		
Infrastructure	SC -6	Resource Priority	The information system limits the use of resources by priority.		
Infrastructure	SC -7	Boundary Protection	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.		
	SC -7 (1)	Boundary Protection	The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces. SC-7 (1) Requirement: The service provider and service consumer ensure that federal information (other than unrestricted information) being transmitted from federal government entities to external entities using information systems providing cloud services is inspected by TIC processes.		
	SC -7 (2)	Boundary Protection	The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			employing boundary protection devices.		
	SC-7 (3)	Boundary Protection	The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.		
	SC-7 (4)	Boundary Protection	The organization: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; e. Reviews exceptions to the traffic flow policy at least annually; and f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.		
	SC-7 (5)	Boundary Protection	The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	SC-7 (7)	Boundary Protection	The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.		
	SC-7 (8)	Boundary Protection	The information system routes [See additional requirements and guidance] to [See additional requirements and guidance] through authenticated proxy servers within the managed interfaces of boundary protection devices. SC-7 (8) Requirements: The service provider defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing. The internal communications traffic and external networks are approved and accepted by JAB.		
	SC-7 (12)	Boundary Protection	The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.		
	SC-7 (13)	Boundary Protection	The organization isolates [See additional requirements and guidance] from other internal information system components via physically separate subnets with managed interfaces to other portions of the system. SC-7 (13) Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools,		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			mechanisms, and support components from other internal information system components via physically or logically separate subnets.		
	SC-7 (18)	Boundary Protection	The information system fails securely in the event of an operational failure of a boundary protection device.		
Data	SC-8	Transmission Integrity	The information system protects the integrity of transmitted information.		
	SC-8 (1)	Transmission Integrity	The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.		
Data	SC-9	Transmission Confidentiality	The information system protects the confidentiality of transmitted information.		
	SC-9 (1)	Transmission Confidentiality	The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by [See additional requirements and guidance]. SC-9 (1) Requirement: The service provider must implement a hardened or alarmed carrier Protective Distribution System (PDS) when transmission confidentiality cannot be achieved		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			through cryptographic mechanisms.		
Infrastructure	SC-10	Network Disconnect	The information system terminates the network connection associated with a communications session at the end of the session or after thirty minutes for all RAS-based sessions; thirty to sixty minutes for non-interactive users of inactivity. SC-10 Guidance: Long running batch jobs and other operations are not subject to this time limit.		
Infrastructure	SC-11	Trusted Path	The information system establishes a trusted communications path between the user and the following security functions of the system: [See additional requirements and guidance]. SC-11 Requirement: The service provider defines the security functions that require a trusted path, including but not limited to system authentication, re-authentication, and provisioning or de-provisioning of services (i.e. allocating additional bandwidth to a cloud user). The list of security functions requiring a trusted path is approved and accepted by JAB.		
Infrastructure	SC-12	Cryptographic Key Establishment and Management	The organization establishes and manages cryptographic keys for required cryptography employed within the information system.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	SC-12 (2)	Cryptographic Key Establishment and Management	The organization produces, controls, and distributes symmetric cryptographic keys using NIST-approved key management technology and processes.		
	SC-12 (5)	Cryptographic Key Establishment and Management	The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key. SC-12(5) Requirement: The service provider supports the capability to produce, control, and distribute asymmetric cryptographic keys.		
Infrastructure	SC-13	Use of Cryptography	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.		
	SC-13 (1)	Use of Cryptography	The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.		
Data	SC-14	Public Access Protections	The information system protects the integrity and availability of publicly available information and applications.		
Infrastructure	SC-15	Collaborative Computing Devices	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: no exceptions; and		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			b. Provides an explicit indication of use to users physically present at the devices.		
Infrastructure	SC-17	Public Key Infrastructure Certificates	The organization issues public key certificates under an [See additional requirements and guidance] or obtains public key certificates under an appropriate certificate policy from an approved service provider. SC-17 Requirement: The service provider defines the public key infrastructure certificate policy. The certificate policy is approved and accepted by the JAB.		
Infrastructure	SC-18	Mobile Code	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.		
Infrastructure	SC-19	Voice Over Internet Protocol	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.		
Infrastructure	SC-20	Secure Name /Address Resolution Service (Authoritative Source)	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.		
	SC-20 (1)	Secure Name /Address Resolution Service (Authoritative Source)	The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.		
Infrastructure	SC-21	Secure Name/ Address Resolution Service (Recursive or Caching Resolver)	The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.		
Infrastructure	SC-22	Architecture and Provisioning for Name/Address Resolution Service	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.		
Infrastructure	SC-23	Session Authenticity	The information system provides mechanisms to protect the authenticity of communications sessions.		
Data	SC-28	Protection of Information at Rest	The information system protects the confidentiality and integrity of information at rest. Requirement: The organization supports the		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			capability to use cryptographic mechanisms to protect information at rest		
Infrastructure	SC-30	Virtualization Techniques	The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.		
Infrastructure	SC-32	Information System Partitioning	The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.		
	1.17. System and Information Integrity (SI)			Failure to implement system and integrity controls could lead to malicious code infestation and compromise or exfiltration of data.	System and Information Integrity controls are intended to ensure the Integrity of Systems, Applications and Information in all situations, including following an NS/EP event. This protection is essential for all Critical Infrastructure Key Resources (CI/KR).
Policy/Legal	SI-1	System and Information Integrity Policy and Procedures	The organization develops, disseminates, and reviews/updates at least annually: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.		
Infrastructure	SI-2	Flaw Remediation	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.		
	SI-2 (2)	Flaw Remediation	The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation.		
Infrastructure	SI-3	Malicious Code Protection	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			mechanisms to: - Perform periodic scans of the information system at least weekly and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and -Block or quarantine malicious code, send alert to administrator, send alert to FedRAMP in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.		
	SI-3 (1)	Malicious Code Protection	The organization centrally manages malicious code protection mechanisms.		
	SI-3 (2)	Malicious Code Protection	The information system automatically updates malicious code protection mechanisms (including signature definitions).		
	SI-3 (3)	Malicious Code Protection	The information system prevents non-privileged users from circumventing malicious code protection capabilities.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	SI-4	Information System Monitoring	The organization: a. Monitors events on the information system in accordance with ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.		
	SI-4 (2)	Information System Monitoring	The organization employs automated tools to support near real-time analysis of events.		
	SI-4 (4)	Information System Monitoring	The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	SI-4 (5)	Information System Monitoring	The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: protected information system files or directories have been modified without notification from the appropriate change/configuration management channels; information system performance indicates resource consumption that is inconsistent with expected operating conditions; auditing functionality has been disabled or modified to reduce audit visibility; audit or log records have been deleted or modified without explanation; information system is raising alerts or faults in a manner that indicates the presence of an abnormal condition; resource or service requests are initiated from clients that are outside of the expected client membership set; information system reports failed logins or password changes for administrative or key service accounts; processes and services are running that are outside of the baseline system profile; utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose. SI-4(5) Requirement: The service provider defines additional compromise indicators as needed. Guidance: Alerts may be generated from a variety of sources including but not limited to malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.		
	SI-4	Information System Monitoring	The information system prevents non-privileged users from circumventing intrusion detection and		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
	(6)		prevention capabilities.		
Infrastructure	SI-5	Security Alerts, Advisories, and Directives	The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to all staff with system administration, monitoring, and/or security responsibilities including but not limited to FedRAMP; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. SI-5c. Requirement: The service provider defines a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives. The list also includes designated FedRAMP personnel.		
Infrastructure	SI-6	Security Functionality verification	The information system verifies the correct operation of security functions upon system startup and/or restart and periodically every ninety		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
			days and notifies system administrator when anomalies are discovered.		
Infrastructure	SI-7	Software and Information Integrity	The information system detects unauthorized changes to software and information.		
	SI-7 (1)	Software and Information Integrity	The organization reassesses the integrity of software and information by performing at least monthly integrity scans of the information system.		
Infrastructure	SI-8	Spam Protection	The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.		
Infrastructure	SI-9	Information Input Restrictions	The organization restricts the capability to input information to the information system to authorized personnel.		
Data	SI-10	Information Input Validation	The information system checks the validity of information inputs.		

Primary NSTAC Concern	Control Number and Name		Control Description (from NIST 800-53)	Unique Characteristic or Risk	NS/EP Implication
Infrastructure	SI-11	Error Handling	The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing user name and password combinations; attributes used to validate a password reset request (e.g. security questions); personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record); biometric data or personal characteristics used to authenticate identity; sensitive financial records (e.g. account numbers, access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes and settings) in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel.		
Data	SI-12	Information Output Handling and Retention	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.		