A CENTER FOR DIGITAL GOVERNMENT REPORT

Best Practice Guide for Cloud and As-A-Service Procurements

CENTER FOR DIGITAL GOVERNMENT | DIGITAL COMMUNITIES

Executive Summary

The Center for Digital Government (CDG) Best Practice Guide for Cloud and As-a-Service Procurements was first published in 2014 and updated in 2016. The guide was created to provide government and industry with consensus-based advice and terms and conditions for cloud solution procurement models. For nearly a decade, the guide has been viewed as the standard for many state and local government cloud contracting efforts.

In 2014, as private companies were rapidly moving systems and applications to the cloud, public agencies were lagging far behind — struggling to adopt managed, hosted services that could save their jurisdictions money, enhance security and provide better value.

Old rules clashed with the new way of doing business, making it difficult or even impossible for cloud service providers to submit a bid for a state or local government information technology (IT) procurement opportunity. All too often, government agencies and industry weren't on the same page, or even speaking the same language, when it came to the secure acquisition and deployment of IT solutions.

Our approach to bridging that gap was straightforward: put some of the nation's most progressive state and local government jurisdictions in the same room with some of the industry's top cloud service providers to look for common ground. The result was a mutually acceptable package of definitions, contracting terms and related information designed for the rapidly emerging as-a-service environment.

The 2016 update included critical information about how public agencies and their technology vendors could work together to effectively manage cloud and hybrid cloud deployments while incorporating best practices for classifying and encrypting data, methods for safeguarding information on mobile devices and advice on how to approach security audits of service providers.

The 2016 guide proved useful to many jurisdictions as they migrated to or built new applications on cloud-based platforms. But over the past few years we've seen significant changes in the public sector marketplace related to cybersecurity, risk management, and data protection and privacy.

This new version of the guide offers information, options and examples designed to strengthen cloud service cybersecurity assurance and resiliency. It lays out a strategy for employing consistent baseline security and privacy controls and integrating cloud service risk and authorization management practices into cloud governance and procurement policies.

Opportunity for Public Agency and Service Provider Alignment: *A whole of government approach to cloud and as-a-service procurement*

Today, cloud-based solutions are the platform of choice for an ever-growing number of technology-enabled government programs and services. But knowing how to select the right cloud service solution with appropriate security, privacy and data protection remains challenging.

While the pace of state and local government procurement still leaves room for improvement, contract vehicles are being established to support everything from replacing data centers (e.g., computing, network and data storage environments) and jurisdictionwide enterprise resource planning (ERP) systems (e.g., finance and budget, procurement, human resources and payroll, etc.) to discrete software-as-a-service (SaaS) solutions designed to support program specific needs and requirements (e.g., permitting and licensing, campground reservations, veteran's home loans, etc.).

The COVID-19 pandemic created even more demand for cloud-based solutions that could be rapidly acquired and deployed. Expectations for streamlined access to contracts for a growing range of cloud services will continue as state and local governments ride a wave of post-pandemic investments in secure technology improvements.

As the shift to cloud-based platforms accelerates, cybersecurity concerns are top of mind for business and IT leaders at all levels of government. In addition, privacy and supply chain risks have joined cybersecurity as concerns that must be addressed for on-premises and cloud service solutions alike.

NIST Special Publication (SP) 800-53 security and privacy controls, developed by experts from industry and government, are mandated for federal agencies to address risks in cloud service contracts and are becoming the consensus standard for state and local governments across the nation. For state and local governments, adopting and using these same NIST SP 800-53 controls is far more prudent and practical than developing their own. This approach is also more likely to be accepted by service providers, especially those that serve local, state and federal government organizations.

In the past few years, a growing number of state and local governments have integrated risk and authorization management programs (RAMP) into their contracting processes to assess, audit, manage, and continuously monitor cybersecurity risk and compliance of cloud services.

Jurisdictions can greatly reduce cyber risk by having qualified, independent third-party audit and assessment organizations (3PAOs) review and authorize cloud service offerings for compliance with NIST SP 800-53 security and privacy controls. 3PAOs should also continuously monitor cloud services to ensure compliance throughout the life of the contract.

Now, some states and local governments are accepting the U.S. General Service Administration's FedRAMP marketplace designations for specific cloud service offerings. Others rely on some form of self-attestation or third-party attestation (e.g., the Cloud Security Alliance's Security Trust Assurance and Risk (STAR) program). Two states, Arizona (voluntarily) and Texas (directed by legislation) took on the herculean task to build and operationalize their own RAMPs based on NIST SP 800-53. In 2020, StateRAMP, a non-profit entity, launched a RAMP service based on NIST SP 800-53 and modeled after FedRAMP to provide a common, shared approach for RAMP services that state and local governments could leverage and rely upon.

Unfortunately, piecemeal security policies that vary from one government jurisdiction to another still make

contract compliance challenging for many service providers. Uneven approaches to cloud cybersecurity, privacy and supply chain risk management by government entities unnecessarily inhibits and complicates the cloud service contracting process. Service provider resistance to unique and widely varied terms, conditions and requirements may prolong the negotiation process — which is inefficient and costly for all concerned — or lead to disqualification of proposals altogether.

It doesn't have to be that way. We are at an inflection point where public agency and service provider alignment is possible if we take a whole of government approach to cloud and as-a-service procurements. Why not leverage the latest version of NIST SP 800-53 controls for more secure cloud service contracts and integrate risk and authorization management practices to continuously monitor and manage more secure and competitive cloud service solutions? Procuring cloud and as-a-service solutions would be more consistent, standardized and competitive across the nation if state and local governments align with one another and their federal government counterparts on this issue — the common adoption of a single set of security and privacy controls (NIST SP 800-53) as a baseline — and require service providers to ensure their cloud service offerings comply with those common controls.

What Now?

The material presented on these pages supplies a backdrop and options for change, but change won't occur without action. If state and local governments want to enjoy the benefits of secure cloud-based solutions, an array of leaders must get involved. Modernizing rules, oversight and risk management processes that impede rapid, effective and secure cloud contracting requires leadership and help from policymakers, finance directors, IT and security leaders, risk management professionals, auditors, procurement officers, attorneys and ultimately elected officials.

We offer these suggestions for getting started:

- Use model terms and conditions in this guide to frame new relationships with service providers.
- Adopt NIST SP 800-53 (most current version) as baseline controls for cloud services and avoid customization and one-off controls.
- Harmonize procurement terms and conditions, solicitation language and security policies, standards, and controls to eliminate conflicts and redundancies.
- Incorporate a RAMP or RAMP service in cloud service acquisition and management. Use the RAMP checklist as a roadmap.
- Change procurement infrastructure and acquisition policies and processes to align with cloud service governance and risk authorization and management practices.
- Pilot and implement continuous monitoring by qualified auditors for cloud service control compliance to protect the public interest and enable the secure use of as-a-service solutions.

State and local governments can't ignore trends sweeping society and the technology marketplace. Cloud-based services are commercially proven, and they support a level of innovation and value that public agencies desperately need. It's time for governments to embrace this change and benefit from it.

Introduction

Although the specific paths to cloud and as-a-service procurement may vary from state to state, the Center for Digital Government (CDG) believes there are common practices and terms and conditions that state and local governments can use to streamline cloud solution contracting; strengthen cloud security, privacy and data protection; and lower supply chain risk.

This updated guide, like its predecessors, is the product of an ongoing discussion among government IT and security leaders, risk management and procurement professionals, legal counsel and cloud service providers. Representatives from six states and four local governments who are in the process of adopting a risk and authorization management program (RAMP) for cloud procurement worked from May 2022 to December 2022 to produce this latest version. CDG also recognizes the vital role that cloud service providers have in this discussion. Effective contracting requires viable actions and obligations that can be achieved by all parties to a contract. While cloud solutions must meet government requirements, policies and statutes, the contracting practices and terms and conditions for these solutions must also be viable for competitive service providers to perform.

To that end, the CDG senior fellows leading this project met with four representative cloud service providers to obtain and consider their best practice advice and comments on draft revisions to the guide. Those revisions include updates to guide sections related to data, breach notification, security and audits. This guide also includes new appendices focused on the development and use of RAMPs (i.e., a RAMP checklist) and procurement approaches that align with RAMP.

This guide has been a collaborative effort and contains the contributions and collective views of several authors representing various companies, governmental agencies or themselves. Each contributor is responsible for his/her own views and opinions which may or may not be expressed in this guide. Such opinions are not necessarily those of e.Republic or of any of the other contributors. This guide contains general information only and should not be considered as professional advice or services of any nature, and it is not intended as a substitute for any such advice or services.

Specific Cloud Models and Understanding Cloud Procurement

Service Models

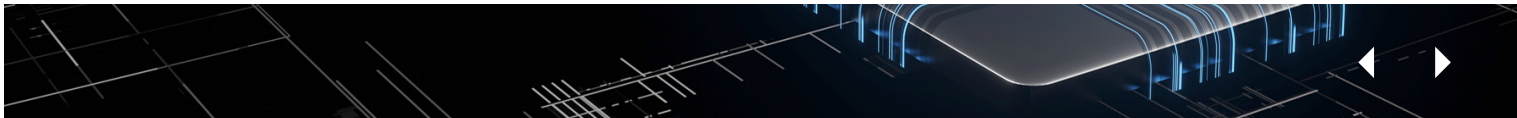
The National Insitute of Standards and Technology (NIST) defines **Software-as-a-Service (SaaS)** as the "capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

In this model, as shown in Table 1, the service provider owns and operates all software and hardware needed to provide the service. Only limited controls are available to the public jurisdiction. The model is suited for full-service applications accessed by end users within an organization. It requires a minimal level of support by the jurisdiction. Applications range from email and collaboration tools to office productivity tools/ suites to integrated enterprise resource planning systems.

NIST defines Platform-as-a-Service (PaaS) as "the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications

Table 1: SaaS Technology Stack Controls[1]

Service Provider	Technology Stack	Public Jurisdiction
Administrative Control	Application (e.g., mail)	Limited Admin Control User Level Control
Total Control	Middleware (e.g., java)	No Control
Total Control	Operating System	No Control
Total Control	Hardware	No Control



using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations."

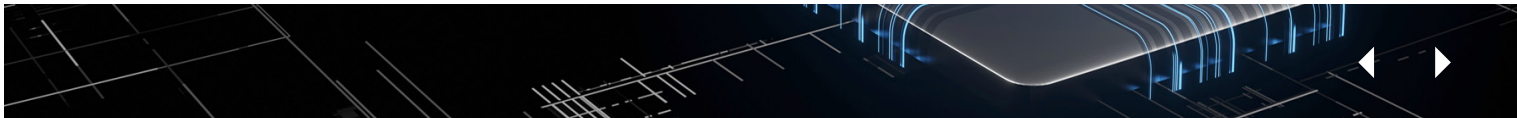
With this service model, the public jurisdiction has complete control over its application software and program control over middleware. The service is suited for public jurisdictions that want to use the PaaS provider's tools to develop, deploy and administer applications to its end-user customers.

NIST defines Infrastructure-as-a-Service (IaaS) as "the capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage and deployed applications, and possibly limited control of select networking components (e.g., host firewalls)."

The service provider maintains control over the hardware and administrative control over the hypervisor that uses the hardware to synthesize one or more virtual machines. The public jurisdiction maintains control over the operation of the guest operating system and all the software layers above it. In this model, the consumer may make requests to create and manage new virtual machines. The public jurisdiction assumes the greatest operational control responsibility. This model is suited to a public jurisdiction where systems administrators need quick access to virtual computing and storage capacity.

Table 2: PaaS Technology Stack Controls[2]

Service Provider	Technology Stack	Public Jurisdiction
No Control	Application (e.g., mail)	Admin Control
Admin Control	Middleware (e.g., java)	Program Control
Total Control	Operating System	No Control



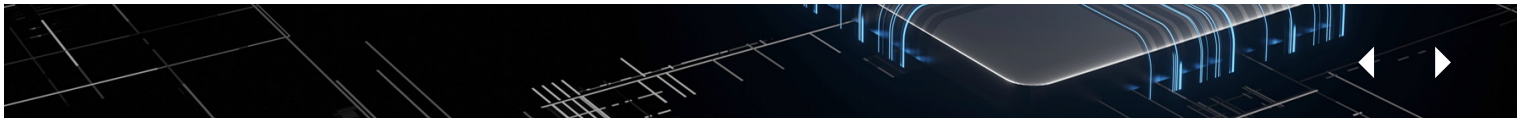
Different Terms and Conditions

The service models do not always work the same way. As a result, the three model terms and conditions presented in this guide share many common clauses, but those dealing with operational responsibilities (e.g., data protection, security incident or breach notification, breach responsibilities, access to security logs and reports, and encryption of data at rest) vary. For example, a SaaS provider is responsible for most of the technology stack and for these clauses; therefore, the service provider has more and broader responsibility for protecting data and reporting.

On the other hand, an IaaS service provider is essentially leasing infrastructure to the public jurisdiction, so the public jurisdiction is responsible for its own data protection, encryption and reporting. Termination and suspension of a service are also managed differently for SaaS contracts than for PaaS and IaaS. SaaS contracts specifically require a service provider to maintain data for up to 10 days after a contract expires in accordance with the termination timelines. Finally, clauses dealing with compliance for application accessibility standards and requiring web services are simply not applicable to IaaS contracts.

Table 3: IaaS Technology Stack Controls[3]

Service Provider	Technology Stack	Public Jurisdiction
No Control	Application (e.g., mail)	Total Control
No Control	Middleware (e.g., java)	Total Control
No Control	Guest Operating System	Total Control
Administrative Control	Hypervisor	Make Requests
Total Control	Hardware	No Control



Data

Public jurisdictions must work with their service providers to determine responsibilities for data management and protection. They should start by implementing and enforcing data protection policies to reduce the potential impact of data leakage and data loss. Public jurisdictions should discover, inventory and classify the data they manage, store and use. They must decide what data needs to be protected, how much protection to apply, and who controls any data sharing requests and manages access for the service provider. Data at rest and in transit should be encrypted to prevent data leaks and unauthorized access. Jurisdictions should conduct regular and frequent testing of back-ups — separating resources to avoid inadvertent leaks, managing account access and monitoring the cloud region.

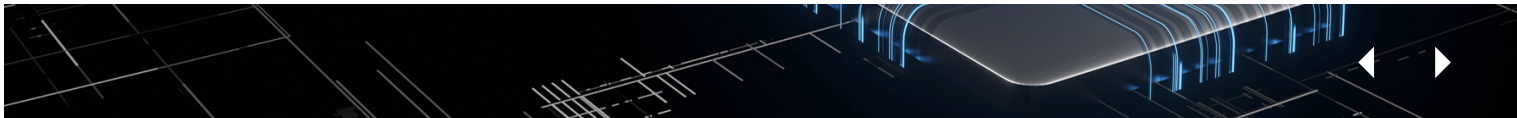
The public jurisdiction should establish with service providers three attributes for government data: ownership rights, privacy requirements and the physical location(s) where the data resides. Then data access needs to be protected with modern identity management techniques. Finally, parameters should be set for data movement to and from the contracted service provider and the public jurisdiction's on-premises site(s), outsourced site(s) and/or other cloud environments.

Ownership of Data

Governments have a fundamental responsibility to limit access to non-public information and to protect the privacy, confidentiality and integrity of their data. A critical step for a public jurisdiction and the service provider is to affirm the jurisdiction's ownership of its data and how to manage that data. This is typically a mandatory provision for public jurisdictions. Key public jurisdiction concerns that should be addressed in a data ownership clause include the following:

- Public jurisdictions must protect the privacy of certain constituent information. To protect privacy, the public jurisdiction must control and continuously own the data, including personally identifiable information (PII) and protected health information (PHI). Personal data is defined in **Clause 1 Definitions** to cover both PII and PHI. Regardless of the type of service selected to process and manage the data, the public jurisdiction still has a duty as an owner to comply with state and federal laws requiring the protection of PII and PHI. Protection of data in an XaaS contract is often a shared responsibility. Specific roles and responsibilities should be clearly identified within the service level agreement (SLA).
- Data must not be accessed for any purposes except those authorized by the public jurisdiction. Establishing ownership and prohibiting the provider from accessing the data or user accounts for any purpose not authorized by the government limits access to the minimum level needed to perform the services of the contact. **Clause 2 Data Ownership** affirms data ownership, restricts access to the data to use within the provider's data center or disaster recovery site (and then only for the intended purposes of the contract) and prevents access to the data for any other purpose except as authorized by the jurisdiction in writing.

** Clauses can be found in Appendix 1.*



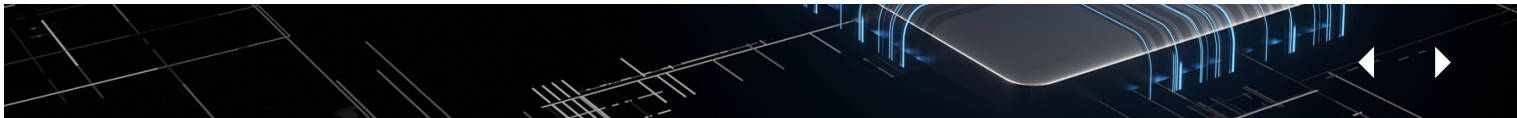
- **Clause 3 Data Protection** requires the service provider to protect the confidentiality and integrity of a public jurisdiction's data. The service provider must encrypt both personal data and non-public data. Non-public data is defined in **Clause 1 Definitions** to cover all data deemed sensitive by the jurisdiction that requires some level of protection. This is typically information that is exempt from public records requests. Service providers are prohibited from using the data for any purpose not intended under the contract or explicitly authorized by the public jurisdiction. This includes copying, disclosing or otherwise using the data or any information collected under the contract for purposes not required as part of the services under the contract or authorized by the government.
- The treatment of data, including the treatment of sensitive data, is a key cost factor for service providers. Unique data requirements create both constraints and costs. To manage costs and constraints, a thorough understanding of the data controlled and managed by the XaaS provider is essential for both the public jurisdiction and the service provider.
- Some IaaS providers may not access data at all with their relatively self-serve offering; therefore, the Center for Digital Government (CDG) recommends that the public jurisdiction adjust the last sentence of the **Clause 2 Data Ownership** to read: "The service provider shall not access public jurisdiction user accounts or public jurisdiction data" to further strengthen this requirement.
- Public jurisdictions can protect the security and integrity of data through encryption. Depending on

Governments have a fundamental responsibility to limit access to non-public information and to protect the integrity of their data.

the type of service received under the contract, identity and access management and encryption could be a public jurisdiction responsibility, provider responsibility or a joint responsibility. The service level agreement (SLA) must include a clear delineation of responsibilities based on the nature of the relationship. **Clause 3 Data Protection** makes it the service provider's responsibility to encrypt and otherwise protect personal data and non-public data for SaaS. However, in an IaaS model, the public jurisdiction is responsible for the encryption and protection of its data. Public jurisdictions must understand the integration of data architectures between their on-premises systems and those of the service providers, the roles and responsibilities for software and system control, and data flow. Each party may have responsibilities that cannot be performed by the other. These responsibilities must be understood and identified in the SLA and contract. NIST provides an excellent reference framework in its Cloud Computing Reference Architecture (SP 500-292).

Data Privacy

With the advent of commercial data mining, public jurisdictions have extended their data privacy provisions to include data derived from a citizen's access of



government data, such as a user's location data when accessing a government online service. To ensure there is no misunderstanding about the extent public jurisdictions want to protect information tied to government citizen services, **Clause 4 Data Privacy**:

- Prevents service providers, including service provider contractors or affiliates, from mining any government data for any purpose other than security analysis that is not explicitly authorized by the public jurisdiction
- Prevents service providers from selling any government data to any third party, including service provider affiliates, without permission from the public jurisdiction
- Prevents service providers from transferring any government data to any third party, including service provider affiliates, without permission from the public jurisdiction

Location of Data

Public jurisdictions want services provided from and their data maintained in data centers located within the United States. Data and services provided outside the United States are subject to the laws of the country where the data is physically stored. By requiring services to be provided from data centers within the United States, public jurisdictions can be certain about the laws impacting their data. Public jurisdictions retain ownership, control and should assert responsibility for replication of their data in primary and secondary locations. **Clause 5 Data Location** requires the service provider to:

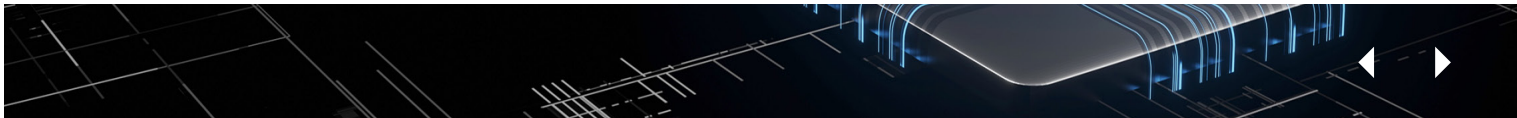
- Provide services only from data centers located within the United States
- Prevent service provider employees or subcontractors from storing public jurisdiction data on portable devices except as used in data centers within the United States
- Permits use of Follow the Sun technical support concept when needed for 24/7 end-user support (Note: this is often not permitted if sensitive data is being accessed)

Data Access

Stringent identity management techniques, such as multi-factor authentication, need to be used to ensure that service provider access to public jurisdiction systems and data are tightly controlled. Public jurisdictions want no offshore access by service provider personnel and contractors. Foreign nationals operating outside the United States are subject to the laws of the country where they reside. By requiring service provider employees and contractors to operate from within the United States, public jurisdictions can be certain about laws impacting their data.

Clause 6 Data Access requires service providers to:

- Use, at a minimum, multi-factor authentication as the access mechanism for all their personnel and contractors to access any system and data management tool which is used to act upon any public jurisdiction data
- Prevent service provider employees and contractors from working outside the United States on any system accessing the public jurisdiction's data, unless explicitly authorized by the public jurisdiction for Follow the Sun technical support under the contract
- Maintain government data and allow downloading for a minimum period of 90 days after the termination of



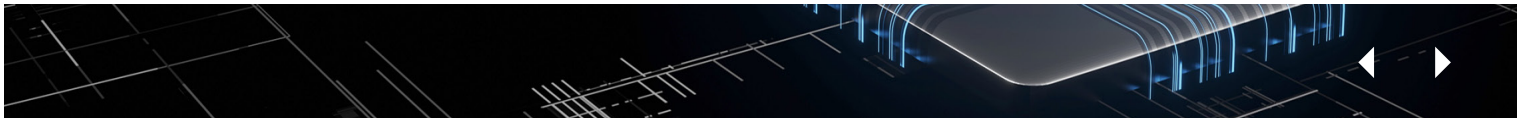
the agreement between the public jurisdiction and the service provider. After this period, the service provider will destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/deletion to the public jurisdiction.

Data Movement: Import and Export

Public cloud XaaS models are attractive to public jurisdictions in part because they allow rapid provisioning of applications using the public jurisdiction's data. This may mean moving data and applications between service providers. Also, public jurisdictions need the ability to move government data between different systems, which may be located within the public jurisdiction's own computing environment or in other service provider environments. Often public jurisdictions need this data movement to occur every few minutes. As cloud-driven service models proliferate, government agencies should be prepared for smooth disengagement and reengagement between service providers.

Clause 7 Import and Export of Data affirms the public jurisdiction's ability to import and/or export its data:

- In whole or in part at the public jurisdiction's sole discretion with the cooperation of the service provider
- At intervals as frequent as the public jurisdiction requires



Breach Notification

Security Incident and Breach Notification

All public jurisdictions are critically concerned about protecting personally identifiable information (PII) and other sensitive data. In the event of an incident, a public jurisdiction must act both internally and through service providers to monitor and investigate. Of course, not all incidents result in a security breach. Prompt notice of an incident gives a public jurisdiction more time to take any actions needed to address the incident. It also allows the public jurisdiction to understand what actions the service provider is taking to protect personal data and non-public data.

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have security breach notification laws that require businesses or governments to notify consumers or constituents if their personal information is breached.[4] NIST defines PII as, "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."[5]

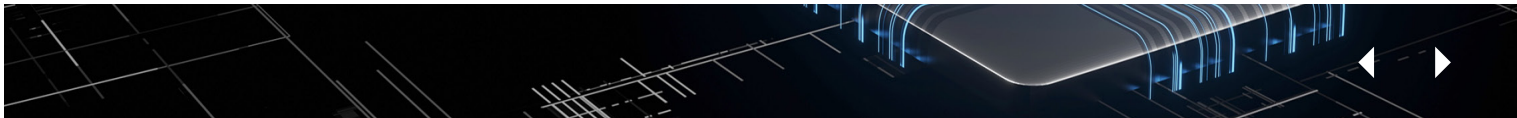
A Congressional Research Service report described state security breach notification laws as generally following a similar framework and characterized by similar elements, including:

- Identifying who must comply with the law
- Defining the terms "personal information" and "breach of security"
- Establishing elements of harm that must occur, if any, for notice to be triggered
- Adopting requirements for notice
- Creating exemptions and safe harbors
- Clarifying preemptions and relationships to federal laws
- Creating penalties, enforcement authorities and remedies

According to the National Conference of State Legislatures, the most common legislative trends in 2022 included proposals that would:

- Establish or shorten the timeframe within which an entity must report a breach
- Require state or local government entities to report data breaches
- Provide an affirmative defense for entities that had reasonable security practices in place at the time of a breach
- Expand definitions of personal information to include biometric information, health information, etc.

In addition to state laws covering PII, there are federal laws to protect health information. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), covered entities holding protected health information (PHI) must comply with privacy rules, including the HIPAA Breach Notification Rule, 45 CFR



164.400. Service providers that have contracts with entities covered under HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) typically have security procedures in place to protect PII and PHI data. Their breach notification procedures must be designed to comply with these federal requirements. Security policies adopted by state and local governments guide the security of the technology systems they operate. These policies also guide compliance with state and federal laws. When contracting for a cloud service, it is important to understand the elements of the security policies that apply to the contracted service model. Not all policies will make sense or should be applied, but the requirements set by law must be addressed.

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have security breach notification laws that require businesses or governments to notify consumers or constituents if their personal information is breached.

To effectively protect personal data, the service provider and public jurisdiction must understand what constitutes a breach and under what conditions and timeframes a breach must be reported. Contract terms must align with state laws to require service providers to detect data breaches and notify the public jurisdiction in a timely way to enable the public jurisdiction to comply with its obligations under law.

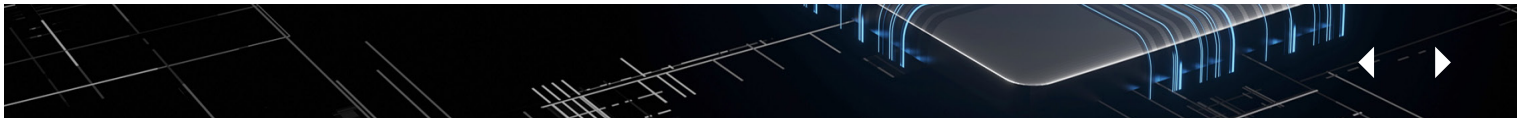
Breach Notification Checklist:

☐ **Event Trigger.** When the service provider confirms a breach affecting any public jurisdiction data that contains personal information.

☐ **Know the law in your state:** All 50 states have enacted security breach disclosure laws. The National Conference of State Legislatures offers a compilation of security breach notification legislation and laws online. State and local governments must know and follow the laws in their states.

☐ **Notify law enforcement:** Public jurisdiction contracts or service level agreements (SLAs) with service providers must include provisions requiring service providers to notify the public jurisdiction of a breach so it can appropriately advise public safety organizations or local law enforcement agencies and report the potential risk for identity theft in accordance with state or federal law. The sooner law enforcement learns about the possible breach, the more effective it can be. Contact the local office of the FBI or U.S. Secret Service as deemed appropriate.

☐ **HIPAA Breach Notification:** Rule 45 CFR §§ 164.400-414 requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured PII. Similar breach notification provisions implemented and enforced by the Federal Trade Commission apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.



☐ **Timing:** Without undue delay but at the latest within 24 hours. Timely notice requirements in service provider contracts can vary with providers typically willing to agree to provide notice of a breach within 24, 48 or 72 hours. The public jurisdiction must ensure that timely notice requirements in the contract or SLA meet the public jurisdiction's needs.

☐ **Information Provided:** Descriptions of the breach and reasonably anticipated consequences, the service provider's response and, where possible, the types of personal information affected.

☐ **Governing Principles:** All notifications shall be consistent with state and federal laws concerning the disclosure of PII, such as the Payment Card Industry Data Security Standard (PCI DSS), Cloud Security Technical Reference Architecture (TRA), California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), and NIST SP 800-53 (current version). Notifications shall also be consistent with international standards, such as the European Union General Data Protection Regulation (GDPR).

☐ **General Statement of Responsibility:** Service providers shall provide guidelines and services that prevent, detect, respond to and remediate breach incidents in cooperation with public jurisdiction personnel. Public jurisdictions shall be responsible for security and potential breach risks within their hosted application and any specified dependencies that may exist with other applications. Internal security standards for shared services shall be clearly identified and have passed the public jurisdiction's internal security reviews consistent with NIST SP 800-53 (current version).

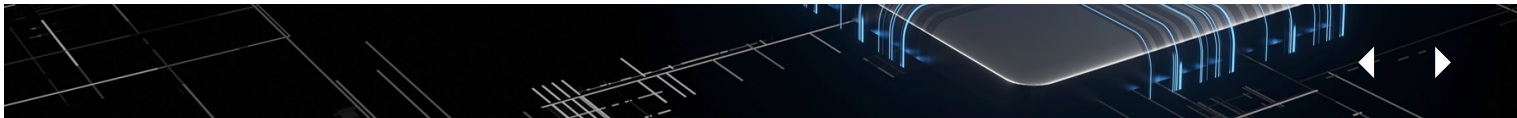
☐ **Multi-Jurisdictional Government Deployments:** Identify the governing authority for breach and incident notification policies covering multi-jurisdictional deployments.

☐ **Hosted Services Interactions:** Identify service dependency interactions with other systems and services and any associated security risks and vulnerabilities (e.g., directory services, payment services, etc.)

☐ **SaaS Applications**: All SaaS applications shall undergo a security review prior to deployment, with documentation of any known breach vulnerabilities that may impact personal information. Service dependencies with other hosted services will also be documented.

Definitions. The Federal Information Security Management Act (FISMA) defines an incident as "an occurrence that (a) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system; or (b) constitutes a violation or imminent threat of violation of law, security policies, security procedures or acceptable use policies." The terms "security incident" and "information security incident" are also used interchangeably with "incident" within the body of the law.

After a service provider obtains a FedRAMP or StateRAMP Agency Authorization To Operate (ATO) or Provisional Authorization To Operate (P-ATO) for its service offering, it enters the continuous monitoring (ConMon) phase. Clear and timely incident communication to relevant stakeholders is a key aspect of ConMon to ensure all incident handling is transparent and all stakeholders are aware of the status and remediation efforts.



FedRAMP and StateRAMP require service providers to report any suspected or confirmed incident that results in the actual or potential loss of confidentiality, integrity or availability of the cloud service or the data/metadata that it stores, processes or transmits. Reporting real and suspected incidents lets agencies and other affected customers take steps to protect important data, maintain a normal level of efficiency and resolve the incident in a timely manner.

Reporting incidents or suspected incidents — as well as responses to emergency directives to the appropriate stakeholders — does not result in punitive actions against the service provider. However, failure to report incidents will result in escalation actions against a service provider, as defined in the FedRAMP and StateRAMP continuous monitoring guides. A collaborative approach between service providers and stakeholders to reporting incidents complies with NIST standards and guidance. With respect to incidents, the FedRAMP Continuous Monitoring Performance Management Guide follows NIST Special Publication 800-61 Rev 2, CISA guidance and the US-CERT Federal Incident Notifications Guidelines. In accordance with these standards and guidance, additional program-specific guidance and procedures are provided to aid all stakeholders in reporting incidents. This allows stakeholders to understand and manage the risk associated with an incident and to classify and resolve suspected incidents.

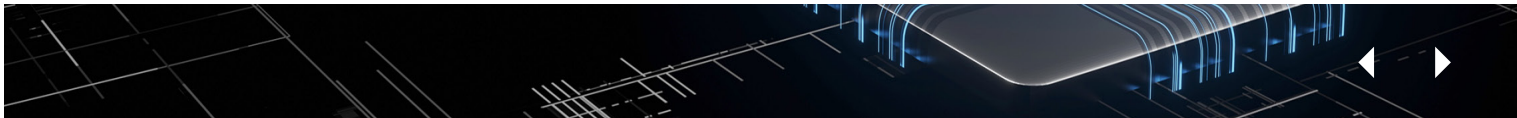
Clause 8 Security Incident or Data Breach Notification requires a service provider to notify the public jurisdiction of a data breach. The clause further defines the service provider's responsibilities for incident response and security incident and data breach reporting. A data breach is defined in **Clause 1 Definitions** as the unauthorized access by non-authorized person(s) that results in the use, disclosure or theft of a public jurisdiction's unencrypted personal data. Personal data is defined to include PII or PHI, but the clause allows for individual state definitions to take precedence over any other definition of PII. Data breach notification requires the service provider to notify the public jurisdiction's designated contact person within 24, 48 or 72 hours of the time the service provider has actual knowledge of a confirmed breach of personal data, unless applicable law requires a faster notification. Timely notice requirements in service provider contracts can vary. The public jurisdiction must ensure that timely notice requirements in the contract or SLA meet the public jurisdiction's needs.

A breach involving non-public data typically does not have the same legal requirements for reporting as PII. A potential loss, theft or unauthorized access to unencrypted non-public data or personal data must be reported immediately as a security incident to the designated contact person. A public jurisdiction must clarify what is meant by "immediately" and outline other reporting requirements in the SLA.

Breach Responsibilities

One of the most difficult contract terms to define and agree on is the service provider's liability. It's hard for either party in a contract to define the risk and potential cost involved in a situation where the clause is triggered.

Service providers have a fiduciary duty to shareholders and legal reporting requirements under Sarbanes-Oxley (SOX). Under section 302 of SOX, service provider

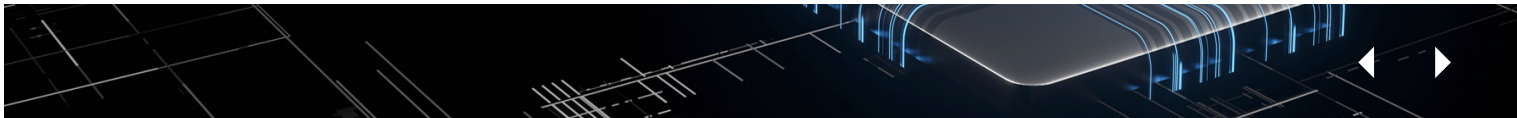


management must have systems in place to identify material information that must be disclosed to investors and other third parties who rely on financial statements of publicly traded companies.[6] This makes it difficult for a service provider to agree to unlimited liability in a contract of significant size. It's difficult for service providers to enter agreements where they cannot quantify their potential liabilities.

Some states have addressed the issue of unlimited liability in more traditional IT contracts by creating a liability cap calculated as a multiplier of the total contract value (i.e., 2x contract value). **Clause 9 Breach Responsibilities** uses a similar method to create a known liability amount when the service provider is the cause of a breach. It creates a definitive amount that is understood by both parties. This answers the service provider's question of what the quantifiable exposure is if a data breach occurs. It also answers the question of what the public jurisdiction will receive in the event of a breach. This approach seems to be a fair and reasonable way to apportion risk and mitigate damages in the event of a breach.

- The liability recommended in **Clause 9 Breach Responsibilities** for a data breach caused by the service provider is based on studies conducted annually by the Ponemon Institute. The average cost of a data breach in the public sector was $2.07 million (USD) across the 17 countries and regions involved in the institute's 2022 Cost of a Data Breach study. Across all sectors, the study estimated the average total cost of a breach in the United States was $9.44 million (USD), the highest of any country involved in the study.[7] Further, the 2022 study indicated that 83% of organizations surveyed have experienced more than one data breach; 45% of breaches were cloud based; and the average reported time to identify and contain a breach was 277 days. The Ponemon samples do not specifically benchmark U.S. public sector data breaches, but they provide a starting point for quantifying data breach mitigation costs.
- **Clause 9 Breach Responsibilities** requires the service provider to pay the cost of the breach investigation, resolution, notification, credit monitoring and call center support up to a set amount per record/per person if the service provider is responsible for the data breach. The service provider will take corrective action to mitigate the breach based on a root cause analysis.

Finally, public jurisdictions must pay attention to the last sentence of **Clause 9 Breach Responsibilities**. It limits the service provider's collective obligations and liabilities to all corrective actions "... as reasonably determined by service provider based on root cause ... subject to this contract's limitation of liability."



Personnel

Background Checks of Personnel

One of the biggest threats to data security can be internal. Public jurisdictions have a duty to protect their data no matter where it is and who is handling it. A prudent practice in contracting for services is to make sure the service provider's team has a background that is free of dishonesty, fraud or other offenses that could jeopardize the security of data.

Clause 10 Background Checks requires the service provider to conduct criminal background checks on its employees and subcontractors. Service providers may not use staff that fail the background check. The clause further makes it a duty of the service provider to promote and maintain the awareness and importance of securing the public jurisdiction's information.

Separation of Duties and Non-Disclosure

One way public jurisdictions protect their information is to limit the number of staff with access to their data. With sensitive and PII data, reducing the exposure of the information to others reduces the risk of breach and loss of privacy. Service providers with a wide variety of clients are sensitive to this concern and typically have procedures to limit the knowledge of customer data to essential staff, as well as require staff to sign non-disclosure agreements (NDAs).

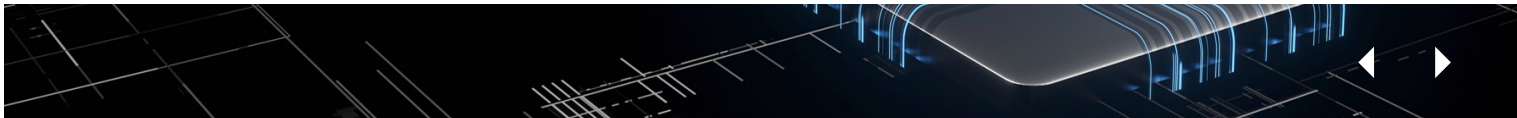
Clause 11 Non-Disclosure and Separation of Duties requires the service provider to enforce separation of job duties and limit staff knowledge of customer data to staff that absolutely need the knowledge to perform their job duties. Commercially reasonable NDAs are required of service provider staff handling this data.

A prudent practice in contracting for services is to make sure the service provider's team has a background that is free of dishonesty, fraud or other offenses that could jeopardize the security of data.

Right to Remove Personnel

An effective working relationship between the service provider and the public jurisdiction is critical to the success of a service relationship. The public jurisdiction can ensure the working relationship remains positive and productive by maintaining the right to require the service provider to remove any service provider representative who is detrimental to that relationship. This ability can also provide recourse to the public jurisdiction when a service provider representative compromises the security of the jurisdiction's data.

Clause 12 Right to Remove Individuals establishes the right of public jurisdictions to require the removal of service provider representatives and sets out conditions for their removal. A representative can be staff or subcontractor personnel. In the event of a potential security violation, the removal must be immediate.



Security

A public jurisdiction is obligated to protect the integrity and security, privacy, and confidentiality of the public's data. To uphold the public's trust, a public jurisdiction entering XaaS contracts must perform due diligence on the service provider and its second-tier subcontractors, including determining whether the service provider has sufficient and adequate security processes to protect and safeguard the data.

Any assessment should include a review of the service provider's technical security procedures to ensure security is commensurate with the classification level of data to be stored and managed by the provider. To obtain a complete assessment of the security chain, the service provider and the jurisdiction must understand their roles and responsibility for data security. A framework for assessment can be found in ISO 27001 and NIST SP 800-53. StateRAMP- or FedRAMP-certified third-party assessment organizations (3PAOs) can make the due diligence of security assessments much easier. A third-party security report from the service provider that includes an independently audited AICPA Service Organization Control (SOC) 2 report can also support security due diligence requirements. Although useful, it is important to note that these SOC 2 reports are point-in-time assessments (typically annual) that may or may not consistently include all required security controls. The Center for Digital Government (CDG) recomments more frequent monthly assessments, if not continuous monitoring, of cloud provider compliance with required security controls by approved 3PAOs.

For more information, AICPA SOC 2 Type 2 audits are based on Trust Services Criteria (and associated controls) for Security, Availability, Processing Integrity, Confidentiality and Privacy. The Trust Services Criteria (TSC) Mappings to various frameworks, including ISO 27001, the NIST Cybersecurity Framework and NIST SP 800-53 can be found here.

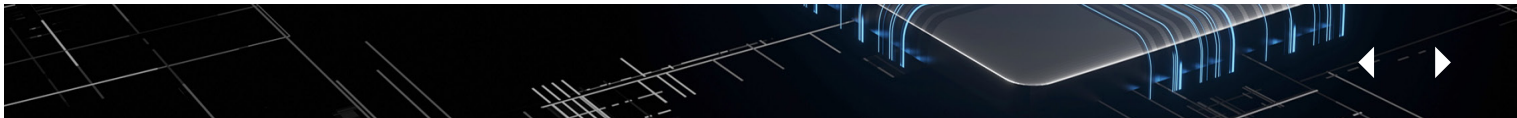
It is important to note that the TSC Mappings only provide specific implementations for 42 out of 325 NIST SP 800-53 Rev 4 controls for SOC 2 audits. Both FedRAMP and StateRAMP provide specific implementations for all 325 NIST SP 800-53 controls (see Audits section).

Clause 13 Security requires the service provider to disclose its non-proprietary security protocols, processes and any technical limitations. It requires a joint understanding of respective roles and responsibilities by each party that must be documented within a service level agreement (SLA).

Security Logs and Reports

Security officers in public jurisdictions use security logs when investigating an incident to determine if data was lost or compromised. However, sharing technical information such as security logs can create vulnerabilities for service providers and they believe their unique reports are difficult for public jurisdictions to decipher in any meaningful way. To address this issue, service providers are typically willing to pledge their cooperation to assist a customer in the event of an incident.

Public jurisdictions need meaningful and relevant reports, statistics, access information, and security log information to understand vulnerabilities and threats to their data



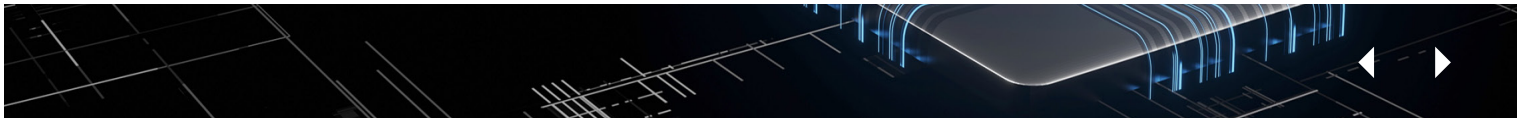
and systems when linked to the service provider. Service providers must share access information with their clients to assist them in assessing their vulnerabilities and responding to threats and attacks. At the same time, service providers have a duty to all their clients not to disclose information that creates vulnerabilities.

Because logs contain records of system and network security, they need to be protected, and the availability, integrity and confidentiality of these sensitive records must be maintained at all times. In addition, logs that are secured improperly in storage or transit might also be susceptible to intentional or unintentional alteration or destruction. Security logs and reports must be securely retained and available to the service provider and the jurisdiction for a period of time agreed to within the SLA. Procedures for authorized access to log management systems or log data and reports must also be agreed to within the SLA.

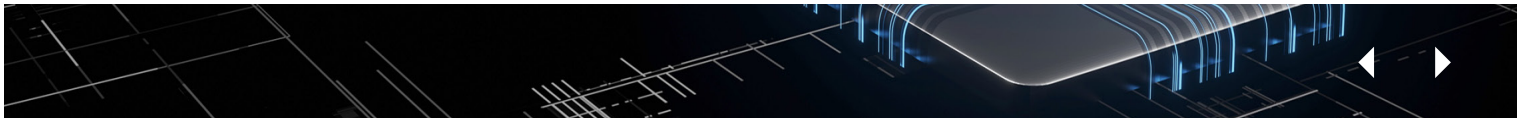
To meet data retention requirements, copies of log files may need to be kept for a longer period of time than the original log sources can support, which will necessitate the establishment of log archival processes. In addition, a process must be put in place to provide for log preservation (i.e., legal hold) requirements to prevent the alteration or destruction of log records and reports. Finally, storage of excessive cloud logs can be expensive and transferring log data out of cloud platforms into an on-premises security information and event management (SIEM) or standalone log management tool can be costly. Jurisdictions need to budget for these expenses within the cloud solution cost estimate/total cost of ownership. Public jurisdictions should assess the capability, suitability and cost associated with the use of native cloud service provider SIEM/log management tools as part of their cloud solution procurement evaluation process. From a business model perspective, the service provider cannot create expensive and unique services that are not included in the SLA, or in the case of public cloud offerings, consistent with the general service offering. Clear expectations and responsibilities must be spelled out and agreed to in the SLA.

Clause 14 Access to Security Logs and Reports requires the service provider to provide security logs and reports that include latency statistics, data and time stamps, user access IP addresses, source and destination IP addresses, system events, log-on/authentication attempts (failed and successful), user access history, account changes (e.g., account creation and deletion, account privilege assignment, etc.), security policy changes, system configuration changes, usage information (e.g., number of transactions occurring in a certain period of time), transaction size (e.g., email message size, file transfer size, etc.), and security logs for the data covered under the contract. The clause requires the methods and conditions for authorized access to logs/reports and the format for the logs/reports to be specified and agreed upon by both parties in the SLA.

Clause 15 Retention, Preservation and Archival of Security Logs and Reports requires the service provider to retain



security logs and reports in a usable format for a minimum of _____ (days, months, years) and a maximum retention/archival of _____ (days, months, years or for a specific time beyond the termination of the contract). The clause requires the methods and timeframes for the retention, preservation (i.e., legal hold), and archival for the logs/reports to be specified and agreed upon by both parties in the SLA.



Encryption

Encryption of Data at Rest (Mobile Devices)

Some of the most notorious public data breaches involve data at rest. Data at rest typically refers to any data that is not transiting through a network via email, wireless transmission or other electronic interchange. It is data that resides in a database, file system, hard drive, portable storage device, memory or any other structured storage method. Data at rest, particularly in mobile devices (flash drives, laptops, tablets, etc.), is highly vulnerable to theft or loss. Data at rest in file servers and other structured data management systems is also at risk of attack.

Jurisdictions that classify their information and data can select the appropriate level of protection based on that data classification. Data that contains personally identifiable information (PII) is critical to protect and typically has the highest data classification level. Public data is at the lower end of the classification scale. It is available to the public upon request and is often readily available on the public jurisdiction's portal. Since it has the lowest level of classification, it may not require special security treatment. Non-public data is sensitive information that is typically classified in the middle.

The primary security controls for restricting access to sensitive data such as PII and non-public data stored on end-user devices are encryption and authentication.[8] The specific level of protection or strength of encryption depends on the sensitivity of the data and the classification level set by the public jurisdiction. Service providers typically encrypt data in transit and at rest within their network. Jurisdictions must understand the level of encryption required and affirm that it is the appropriate level for the classification of its data.

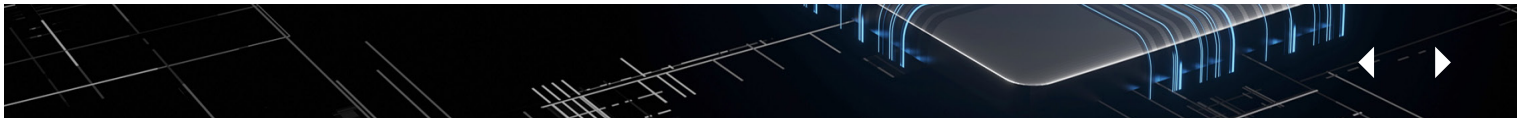
Clause 16 Encryption of Data at Rest requires the service provider to prevent its employees and subcontractors from storing personal data on portable devices, except within data centers located in the United States. If personal data must be stored on portable devices to accomplish work, the service provider must use hard drive encryption in accordance with cryptography standards referenced in FIPS 140-2, Security Requirements for Cryptographic Modules.

Tips and Best Practices for Encryption in the Cloud

Knowing data is protected can help relieve reluctance, anxiety and uncertainty for governments wanting to move applications and data to the cloud. Understanding what data needs to be encrypted; which mandates or regulations apply; what encryption techniques to use; and who owns, stores and has access to the encryption keys can help make a jurisdiction's journey to the cloud a safe one.

- **Encrypt only what you need to or what is required**

It is important to only encrypt what you need to or what is required by law, regulation or mandate. Some data may be public information and likely does not need to be



encrypted. For this reason, jurisdictions should classify data before moving it to the cloud. Lastly, jurisdictions should only store data they need to store and purge old data.

- **Consider special data encryption conditions**
  In some cases, encryption standards are dictated by the type of data being stored, in transit or in use.

  Some special encryption conditions and considerations include:
  - **IRS 1075** — For using and storing income tax data
  - **Payment Card Industry Data Security Standard (PCI DSS)** — For using and storing credit cardholder data
  - **Criminal Justice Information System (CJIS)** — A division of the FBI that establishes minimum security requirements to protect and secure various types of criminal justice information
  - **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** — Data privacy and security provisions for safeguarding medical information
  - **Other confidential information** — Data classified or protected by regulations, mandates, etc.

- **Conduct a security review before moving to the cloud**
  Before moving any applications and data to the cloud, all information should undergo a security review and require signoff from the data owner.

  Data governance and classification are critical to successfully move information from an internal data center to a cloud provider. If you do not know what you have, you cannot apply the appropriate protections to sensitive data.

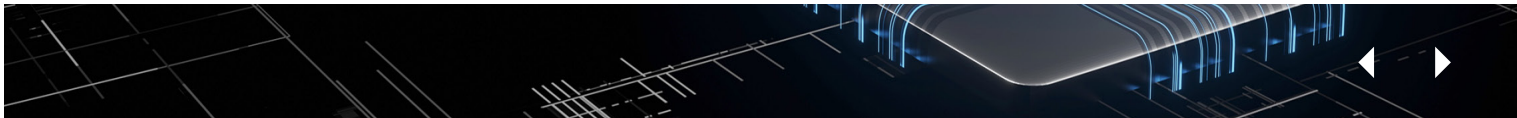
It is important to only encrypt only what you need to or what is required to encrypt by law, regulation or mandate. Some data may be public information and likely does not need to be encrypted.

Identify each data owner and have them designate data as public, sensitive or internal only. Also, know that special types of data (HIPAA, PCI and CJIS) have mandates that describe how data may be used and protected. After it has been classified, decide which components of data will be moved to the cloud and what protections are required.

- **Know where your sensitive data resides — at rest, in transit or in use**
  If you do not know what kind of data you have and where that data is located, you cannot protect it.

  - **Data at rest**
    It seems like a simple concept, but at any given time your structured and unstructured data may be stored or archived in a database, storage media, file server, application server, network, etc. Encrypting where your data resides is often referred to as encrypting data at rest. Define where your data is located and what data your organization needs to encrypt at rest.

  - **Data in transit**
    Data doesn't sit still. It's often in transit from server to server or one location to another. Jurisdictions must



understand how their data is being encrypted in transit across networks and servers.

› **Data in use**
Most of the time, data is in use by applications. Data may be processed, modified, deleted, updated or viewed through a server or end-user device at any time in the process. Where is your data in use and how is it being encrypted?

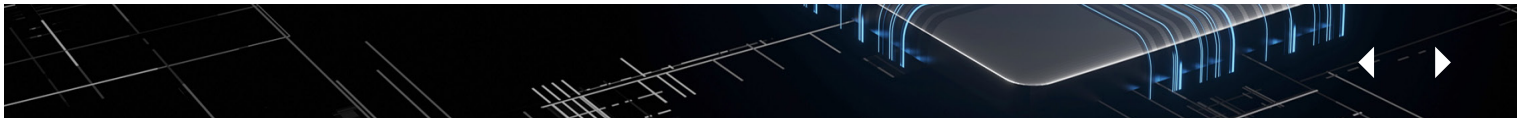
- **Encrypt to the strictest regulations required to protect your data**
A common standard for encryption is the 256-bit Advanced Encryption Standard (AES). 256-bit AES encryption seems to be a viable encryption method offered by all major vendors and with little performance constraints. Data sets that only encrypt partial sensitive data run the risk of leaving sensitive data unencrypted. Therefore, CDG recommends encrypting the entire data set.

- **Identify who manages and stores encryption keys**
Jurisdictions must decide if encryption keys will be managed by themselves or a vendor. A common best practice is for encryption keys to remain with the owners of the data. Keeping the encrypted keys with the data owner is an important safeguard and helps alleviate the owner's fear of storing and protecting data in the cloud. Options for vendor managed keys could include key escrow, key storage, controls, etc.

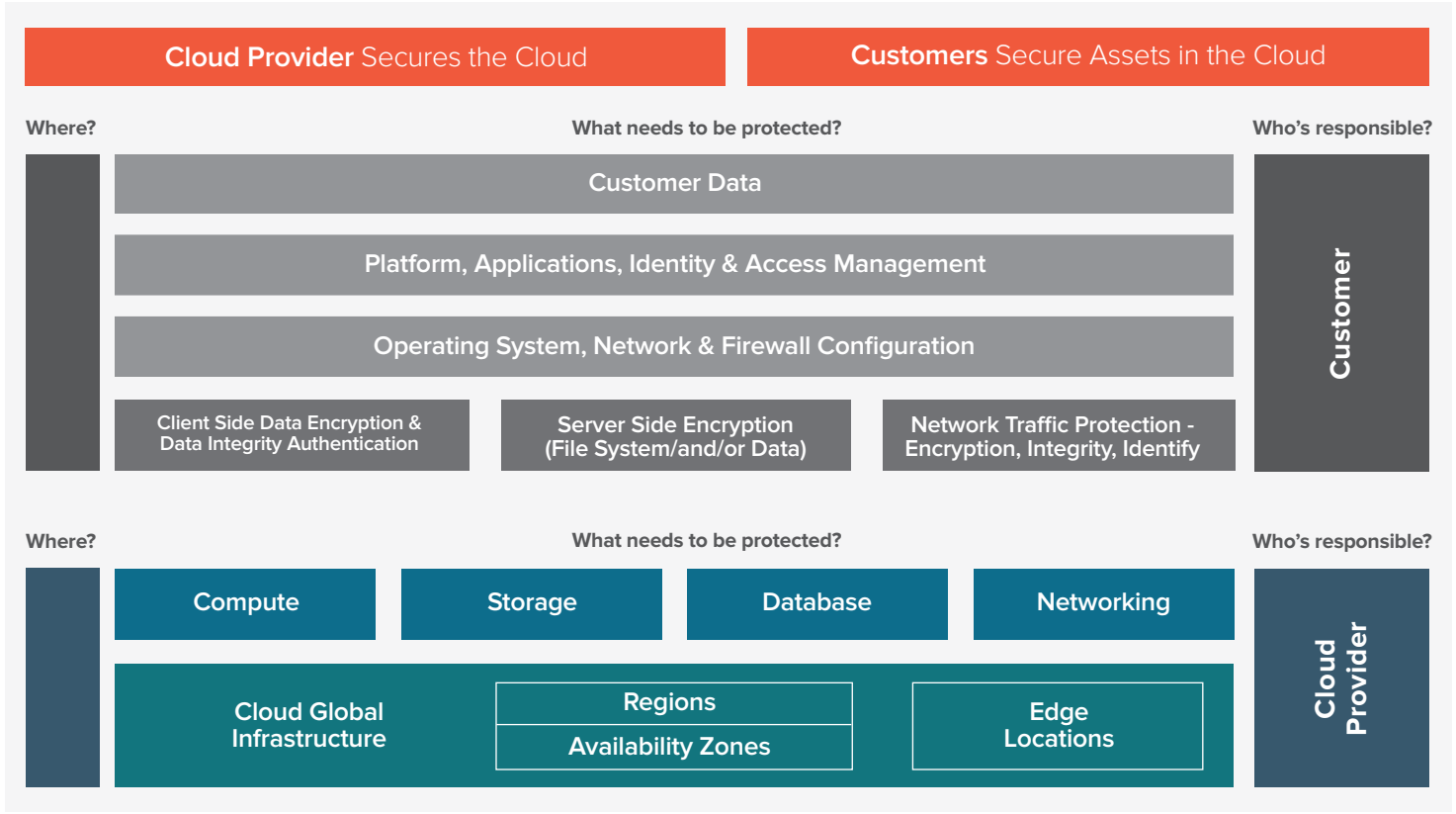
- **Don't forget the human factor**
Often it is easier for hackers or cybercriminals to go after your credentials rather than trying to compromise the encryption. Educate your organization on protecting your credentials, otherwise all the encryption in the world won't prevent your data from being compromised.

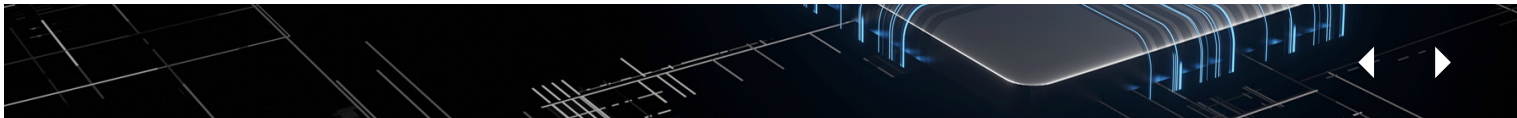
- **Get help if you need it**
Make sure your data is encrypted properly in the cloud and get help if you need it. Data encryption is a critical aspect of protecting your data in the cloud. Don't be afraid to ask for help from your vendors and other security professionals.

Resources and Useful External Links
NIST — http://csrc.nist.gov/publications/PubsSPs.html
FBI CJIS — https://www.fbi.gov/services/cjis
IRS 1075 — www.irs.gov/pub/irs-pdf/p1075.pdf



Who is responsible for protecting your data when it is moved to the cloud?





Audits, Third Party Assessments and Continuous Monitoring

In addition to the normal oversight and contract management, independent security audits are needed to confirm the public's interests are protected. With XaaS-based service contracts, audits typically cover the following areas:

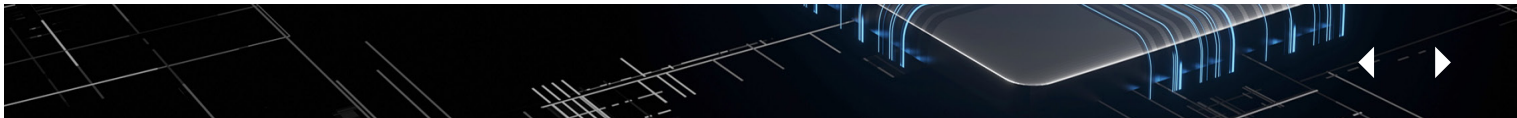
- **Contract Compliance** — Is the jurisdiction getting what is required by the contract? This is usually limited to determining if the parties to a contract are meeting their obligations under the contract and identifying any gaps in the performance of the contract. Contracts with clear performance expectations simplify audits.
- **Financial Compliance** — Are the payments consistent with the terms of the contract? Are financial penalties or service credits being applied consistent with the terms of the contract or service level agreement (SLA)? When the contracted service supports financial reporting, the audits may examine the integrity of the information and data upon which reports depend.
- **Security Compliance** — Are appropriate security controls and protections in place to ensure the availability and integrity of systems and data per the SLA, protect the data from unauthorized access, and keep it private and confidential?

Cloud service models are changing how public jurisdictions ensure security and how privacy controls protect the public's interest. Jurisdictions must understand how using XaaS impacts their risk by understanding their service provider's security controls.

To assess and manage overall risk, effective use of XaaS-based contracts should start with a clear understanding of the jurisdiction's business objectives and the classification levels of the information systems and data involved in the procurement. Next, jurisdictions should assess potential security threats to the objectives, systems and data. Risks should be prioritized according to severity and likelihood. Prioritized risks should then be removed/transferred, controlled/mitigated or accepted. The resulting set of risk-based controls can then serve as the template for the controls expected of the service provider. NIST SP 800-53 (current version) should be used to guide the selection and assessment of necessary security controls.

The jurisdiction must establish methods for monitoring obligations for all aspects of the contract, including security and privacy requirements, to ensure they are being met throughout the term of the contract. Someone (an individual or team) representing the public jurisdiction must be identified and responsible to track and ensure the overall performance expectations set out in the contract are met. If information deemed confidential or proprietary must be reviewed during the course of a contract compliance audit, either party may request the execution of a non-disclosure agreement (NDA), to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.

Regarding financial compliance, the public jurisdiction must establish clear standards and expectations for the

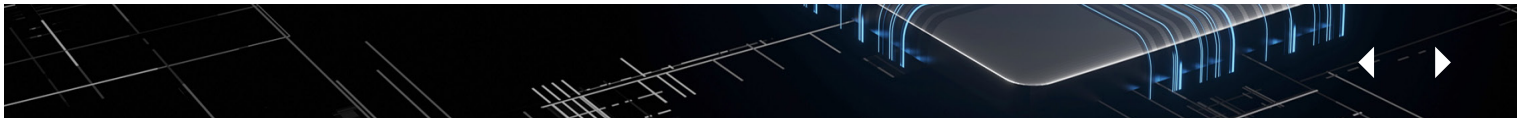


delivery and review of discrete deliverables, submission and review of invoices and processing of payments, and ongoing performance standards for delivered services within the contract (e.g., deliverables expectations document, deliverables and payment schedule, etc.) and an associated SLA, including financial penalties or service credits for non-performance (i.e., failure to meet performance targets/levels agreed to by both parties within the SLA). Procedures should be in place for the review and processing of service provider invoices and for the review and processing of payments that ensure continued compliance with contract terms and conditions. Procedures should also be in place for deliverables and SLA performance review and for remediation and resolution of performance/compliance issues. Someone (an individual or team) representing the jurisdiction must be identified and responsible to track and ensure the overall financial performance expectations set out in the contract are met.

To economically meet the security compliance and audit needs of multiple customers, service providers will typically contract with an independent audit firm. If the product or service offering has achieved StateRAMP or FedRAMP authorization, then the provider is required to have an annual audit that is standardized and specifically designed to measure compliance with NIST SP 800-53 (current version).

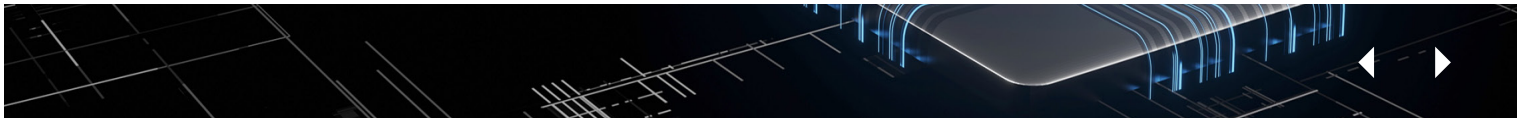
To assess and manage overall risk, effective use of XaaS-based contracts should start with a clear understanding of the jurisdiction's business objectives and the classification levels of the information systems and data involved in the cloud and as-a-service procurement.

In previous versions of this guide, Service Organization Controls (SOC) 2 audit reports were featured as the primary type of security audit that public jurisdictions should request from their service providers. At the time, there were no viable alternative audits to provide public jurisdictions with higher levels of security assurance. StateRAMP and FedRAMP now require initial audits and continuous monitoring audits by third-party assessment organizations (3PAOs) based on NIST SP 800-53 (current version) controls. Although public jurisdictions may continue to request and accept SOC 2 audits from their service providers, CDG now recommends RAMP audits based on NIST SP 800-53 that include continuous monitoring.



A brief comparison of a SOC 2 and a StateRAMP or FedRAMP audit is provided in the tables, charts and graphics below.

SOC 2 Audit	StateRAMP or FedRAMP Audit
A SOC 2 audit is a measurement against self-established security controls, procedures and policies. It is a framework designed by financial experts of the American Institute of CPAs and "is intended to meet the needs of a broad range of users." It provides specific implementation requirements for 42 out of 325 NIST SP 800-53 Rev. 4 controls.	StateRAMP compliance is a measurement against a standard set of security controls, procedures and policies established by the StateRAMP committees. FedRAMP compliance is a measurement against a standard set of security controls, procedures, and policies adopted by U.S. General Services Administration (GSA) and its committees. StateRAMP requirements are designed by cybersecurity professionals specifically to measure compliance with NIST SP 800-53 for state and local government. FedRAMP requirements are designed specifically to measure compliance with NIST SP 800-53 for federal government agencies and to protect federal information. StateRAMP and FedRAMP audits provide specific implementation requirements for 325 out of 325 NIST SP 800-53 Rev. 4 controls.

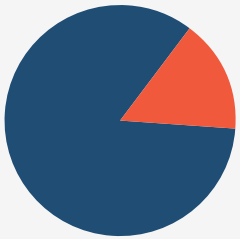


StateRAMP v. SOC 2 Audits for Cloud Security Compliance of NIST SP 800-53

As an example, the charts below provide a comparison of the NIST SP 800-53 controls required within a StateRAMP and a SOC 2 Audit.

Low Impact:
StateRAMP v. SOC 2 Audits

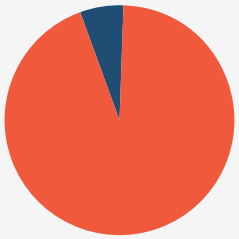
SOC 2 NIST 800-53 Low Impact Compliance



16.8% SOC 2

**Assumes audited CSP selects all 21 Low Impact NIST Controls for audit*

StateRAMP NIST 800-53 Low Impact Compliance

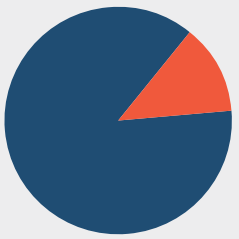


94% of low impact controls are required in StateRAMP audit

**StateRAMP audits are the same every time. StateRAMP does not require controls that are federal specific.*

Moderate Impact:
StateRAMP v. SOC 2 Audits

SOC 2 NIST 800-53 Moderate Impact Compliance



13% SOC 2

**Assumes audited CSP selects all 42 Low Impact NIST Controls for audit*

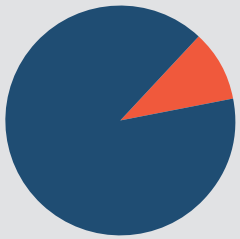
StateRAMP NIST 800-53 Moderate Impact Compliance

96% of moderate impact controls are required in StateRAMP audit

**StateRAMP audits are the same every time. StateRAMP does not require controls that are federal specific.*

High Impact:
StateRAMP v. SOC 2 Audits

SOC 2 NIST 800-53 High Impact Compliance



10% SOC 2

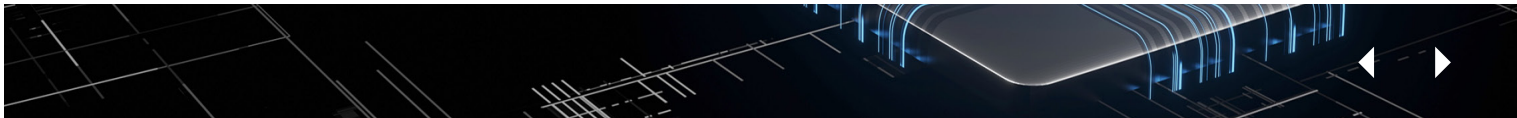
**Assumes audited CSP selects all 42 Low Impact NIST Controls for audit*

StateRAMP NIST 800-53 High Impact Compliance

100% of high impact controls are required in StateRAMP audit

**StateRAMP audits are the same every time. StateRAMP recognizes FedRAMP high impact requirements.*

*StateRAMP audits are the same every time. Control requirements vary only by impact level.

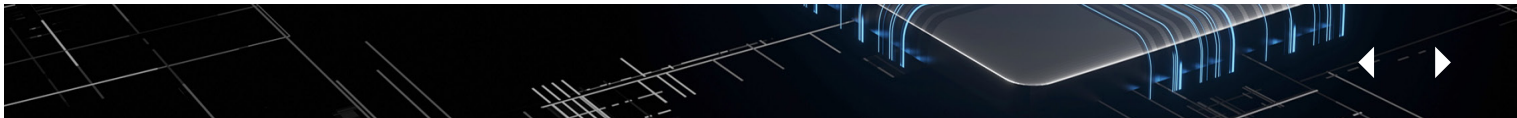


SOC 2 is a framework, not a control catalog. As such, its controls are not descriptive and allow interpretation of implementation.

- StateRAMP and FedRAMP have specific requirements and implementations for NIST SP 800-53 controls.
- The gap in SOC 2 coverage of NIST SP 800-53 controls is due to the lack of implementation requirements.
- SOC 2 has only 42 specific implementation requirements out of the 325 NIST SP 800-53 controls for the Moderate and High impact categories.

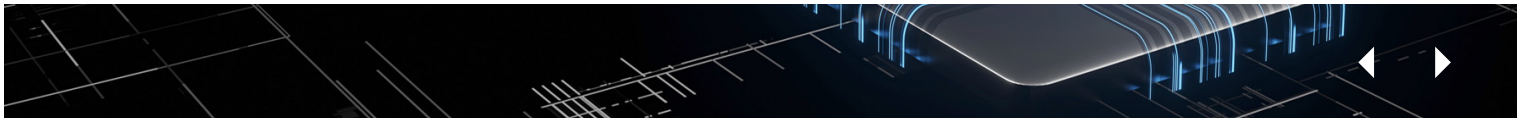
Example of Differences in Audit Requirements and Impact

- SOC 2 requires self-definition. StateRAMP and FedRAMP require specific NIST SP 800-53 compliance. For example, SOC 2 password requirements simply state that "Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian."



This chart illustrates the difference in password compliance for audits.

Requirement	StateRAMP & FedRAMP/NIST	SOC 2
Defined number of characters	12	None
Required upper case letters	At least one	None
Required lower case letters	At least one	None
Required numbers	At least one	None
Required special characters	At least one	None
Requires new password to not be the same as old password	Yes	No
Password transmission must be encrypted	Yes	No
Minimum age of password	One day	None
Maximum age of password	60 days	None
Prohibit password re-use	24 generations	None



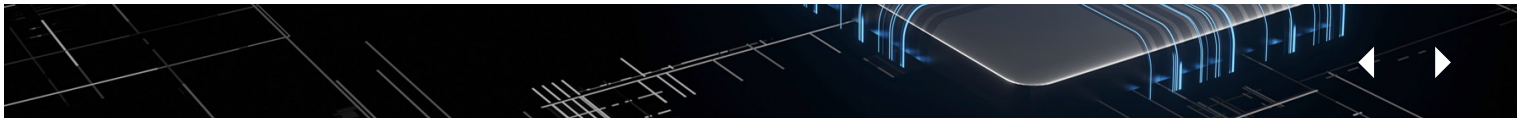
In this example, password compliance differs significantly.

Requirement	StateRAMP & FedRAMP Password Compliance
Compliant IF: Define a password as being four numbers **Requirement self-defined**	Compliant IF: Password has "minimum of 12 characters, and at least one each of upper-case letters, lower-case letters, numbers and special characters, one character change with each password change, only transmit passwords encrypted, require lifetime restriction of one-day minimum and 60-day maximum, and prevent reuse of the previous 24 passwords" **Requirement set by NIST SP 800-53**

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1K years	12K years	202K years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1b years
16	5 hours	3K years	173m years	3b years	92b years
17	2 days	69k years	9b years	179b years	7t years
18	3 weeks	2m years	467b years	11t years	438t years

Time it Takes a Hacker to Brute Force Your Password in 2022

SOC 2 Password Risk	StateRAMP & FedRAMP Password Risk
Four-digit password could be cracked instantly with brute force	**Password adhering to the NIST requirements would take 3,000 years**



Additional Background

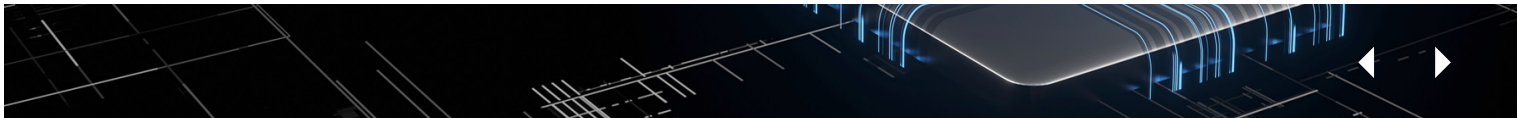
Both FedRAMP and StateRAMP were founded to provide a standardized approach to cybersecurity in government cloud service contracts using NIST SP 800-53 controls.

FedRAMP, administered through the General Services Administration (GSA), was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government, with an emphasis on security and protection of federal information.[9] FedRAMP is governed by federal executive branch entities that develop, manage and operate the program. The Joint Authorization Board (JAB), the primary governance and decision-making body for FedRAMP, consists of the chief information officers from the Department of Defense (DoD), Department of Homeland Security (DHS) and GSA.[10] FedRAMP standardizes security requirements for the authorization and ongoing cybersecurity of cloud services in accordance with the Federal Information Security Modernization Act (FISMA), Office of Management and Budget Circular A-130, and FedRAMP policy. FedRAMP leverages NIST standards and guidelines to provide standardized security requirements for cloud services, a conformity assessment program, standardized authorization packages and contract language, and a repository for authorization packages.[11]

Although FedRAMP is focused on federal government agencies and the protection of federal information, state and local governments have generally accepted a service provider's achievement of FedRAMP Marketplace designations (e.g., Ready, In-Process and Authorized) for specific impact levels (e.g., Low, Moderate or High) as a verification of the cybersecurity posture of the service provider and its offering(s). Prior to achieving a FedRAMP authorized designation, a cloud service provider's offering(s) must, among other requirements, be audited (initially and via continuous monitoring) by an authorized third party assessment organization (3PAO) and be in use by a federal agency. However, not all cloud service providers operate in the federal government marketplace and instead focus their cloud service offerings on the state and local government and education (SLED) marketplace. In addition, the readiness and security assessment reports, 3PAO audit and continuous monitoring reports, authorization packages, and other foundational documentation generated within the FedRAMP program may contain federal data and would require redaction prior to authorization to share with any non-federal entity.

More information on specific FedRAMP requirements, documents and resources can be found here.

StateRAMP, established in 2020 as an independent non-profit organization, is modeled in part after FedRAMP, and like FedRAMP, relies on FedRAMP Authorized 3PAOs and, more recently, StateRAMP registered 3PAOs to conduct assessments. StateRAMP offers RAMP services designed specifically for state and local government, public education institutions and special districts. StateRAMP's Standards and Technical Committee, comprising government and cloud service provider members, makes recommendations to the StateRAMP Board of Directors regarding verification policies,



security standards, best practices, and audit and assessment processes to create common standards that are acceptable to state and local governments and service providers. To be verified, service providers must meet minimum security requirements and provide an independent audit conducted by an approved 3PAO. StateRAMP recognizes three verified statuses (e.g., Ready, Provisional and Authorized). To ensure ongoing security compliance and risk mitigation, service providers must comply with continuous monitoring requirements to maintain a verified security status. Verified cloud service offerings on the StateRAMP Authorized Product List (APL) can be found here.

StateRAMP's requirements were established by the StateRAMP Steering Committee, adopted by the Board of Directors, and are updated annually by the StateRAMP Standards and Technical Committee. The requirements are based on NIST SP 800-53. More information can be found here.

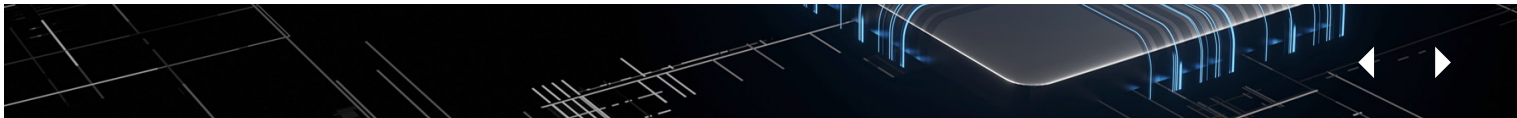
The SOC 2 report was established by the leading standards organization for accountants, the American Institute of Certified Public Accountants (AICPA). Its purpose is to enable data security and other trust principles to be reviewed and verified by the same independent accounting and auditing firms trusted by clients to vouch for the financial integrity of companies. The AICPA Web page introducing SOC 2 reports for relying entities is here.

Additional information can be found here. Included on the page is a link to ISACA's helpful "SOC 2 User Guide."

Public jurisdictions can obtain some level of assurance that their service providers have established an acceptable cybersecurity posture and are meeting security controls required within the contract through SOC 2 Type 2 audits. However, these types of audits are typically conducted on an annual basis, may not be readily available to the public jurisdiction during the RFP evaluation period and may not be conducted for up to a year following contract execution. Further, SOC 2 Type 2 audits may only assess a limited subset of security controls required under the contract by the public jurisdiction. That may be acceptable for some cloud solutions involving low-risk public jurisdiction data and systems, but cloud solutions involving medium and high-risk data and systems may require a higher and more frequent (perhaps continuous) level of security monitoring and assurance.

AICPA SOC 2 Type 2 audits are based on Trust Services Criteria (and associated controls) for Security, Availability, Processing Integrity, Confidentiality and Privacy. The Trust Services Criteria (TSC) Mappings to various frameworks, including the NIST Cybersecurity Framework and NIST SP 800-53, can be found here.

Note: The Trust Services Criteria (TSC) Mappings only provide specific implementations for 42 out of 325 NIST 800-53 Rev. 4 controls for SOC 2 Audits. Both FedRAMP and StateRAMP provide specific implementations for all 325 controls.



Third-Party Assessments and Continuous Monitoring

Source – NIST SP 800-53, Rev 5.1, FedRAMP & StateRAMP

Public jurisdictions have multiple options to gain assurance that their service provider has required security and privacy controls in place. The basic options include some combination of a) reliance on StateRAMP authorization, b) reliance on FedRAMP authorization, c) review of control documentation by internal staff or third-party assessment organization, d) acceptance of the service provider's third-party attestation (e.g. SOC 2 Type 2 audit) or e) self-assessment by the service provider.

The responsibility for this basic due diligence decision ultimately rests with the public jurisdiction. However, jurisdictions should objectively assess whether and to what extent they can rely on internal staff to perform control documentation reviews or related audits. They may not have enough internal staff with sufficient knowledge and experience to effectively perform security and privacy control reviews or audits.

Third-party assessments help to ensure that service providers meet information security and privacy requirements, identify weaknesses and deficiencies that require mitigation or correction, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures.

Third-party assessment organizations (3PAOs) play a critical role in FedRAMP and StateRAMP security assessment process by providing an independent assessment of a service provider's security controls. FedRAMP requires 3PAOs be accredited through the FedRAMP 3PAO program. The accreditation ensures 3PAOs have demonstrated independence and the technical competence required to test security implementations and collect representative evidence.[12]

Leveraging the marketplace and standards FedRAMP has created, StateRAMP also requires 3PAOs be accredited through the FedRAMP 3PAO program. A listing of accredited 3PAOs can be found here.[13]

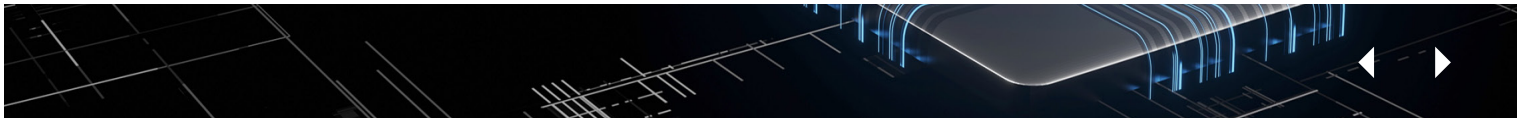
3PAOs participating in the FedRAMP program must:

- Plan and perform initial and periodic assessments of cloud systems based on federal security requirements
- Review security package artifacts in accordance with FedRAMP requirements

During FedRAMP assessments, 3PAOs produce a readiness assessment report, which is required for the joint authorization board authorization process and is optional but highly recommended for the federal agency authorization process, and/or a security assessment plan and security assessment report that is submitted for authorization to a federal government authorizing official.[14]

3PAOs participating in the StateRAMP program must:[15]

- Plan and perform security assessments of provider systems
    - StateRAMP Security Assessment Plan Template
    - StateRAMP Security Readiness Assessment



Report Template
- StateRAMP Security Assessment Report Template

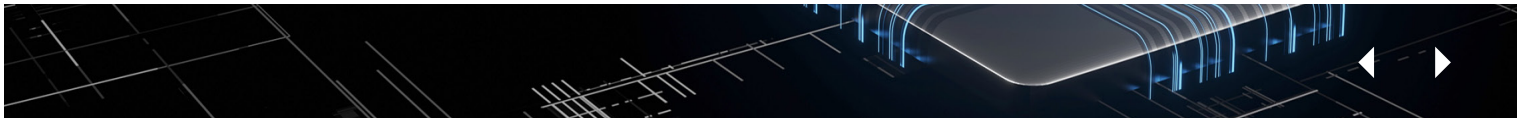
- Review security package artifacts in accordance with StateRAMP requirements

The StateRAMP Readiness Assessment Report (SR-RAR) and StateRAMP Security Assessment Report (SR-SAR) created by the 3PAO are key deliverables for consideration of a StateRAMP Ready or StateRAMP Authorized status. The SR-RAR and SR-SAR provide consistency in security audits upon which verification status is granted by StateRAMP. This repeatable model establishes confidence in authorizations that can be reciprocated and recognized by other public jurisdictions across the country. Although public jurisdictions and service providers can use non-FedRAMP certified 3PAOs as independent assessors at their discretion, use of an independent assessor may not be recognized by StateRAMP.[16]

Continuous monitoring and reporting facilitate ongoing awareness of the cloud solution's security and privacy posture to support risk management decisions. The terms continuous and ongoing imply that relevant controls and risks are assessed and monitored at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives public jurisdiction officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions.[17]

Monitoring security and privacy controls is part of the overall risk management framework for information security. Performing ongoing security assessments determines whether the set of deployed security controls in a cloud information system remains effective considering new exploits and attacks and planned and unplanned changes that occur in the system and its environment over time. Security control assessments performed periodically and on an ongoing basis validate whether stated security controls are implemented correctly, operating as intended and meet baseline requirements set by the public jurisdiction as part of the cloud service contract. Security status reporting provides public jurisdiction officials with the information necessary to make risk-based decisions and provides assurance regarding the security and privacy posture of the cloud information system.[18]

Public jurisdictions should require their service providers to monitor their security controls, assess them on a regular basis and demonstrate that the security posture of their cloud service offering is continuously acceptable to the public jurisdiction client throughout the life of the contract.[19] It is recommended that public jurisdictions require the use of independent 3PAOs for initial and continuous monitoring, especially where medium and high-risk information systems and data are concerned.



StateRAMP Fast Track for Cloud Service Offerings with FedRAMP Designations

StateRAMP and FedRAMP have similar requirements based on NIST SP 800-53, and both rely on independent audits and continuous monitoring by approved 3PAOs. Recognizing these shared best practices, StateRAMP has developed a Fast Track process for cloud service provider offerings that have achieved FedRAMP Marketplace designations (e.g., Ready, In-Process or Authorized) for specific impact levels (e.g., Low, Moderate or High).

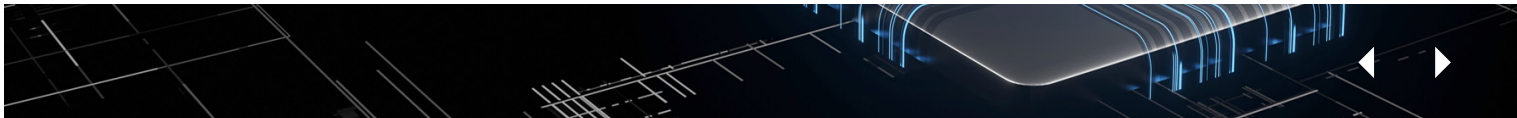
The Fast Track process allows cloud service provider offerings with designations of FedRAMP Ready, Authorization-to-Operate from a federal agency, or a Provisional Authorization-to-Operate from the FedRAMP Joint Authorization Board to leverage their FedRAMP audit reports and associated documentation to become StateRAMP Ready or Authorized. The service provider does not have to complete a new audit for StateRAMP and may use FedRAMP templates for ease of compliance. The StateRAMP Security Team, operating within the StateRAMP Program Management Office, works with service providers to validate and authenticate relevant security packages and reviews recent continuous monitoring audits and reports. Ongoing, cloud service providers participating in the Fast Track process can utilize the same reporting they provide FedRAMP for StateRAMP.

Clause 17 Contract Audit requires the service provider to cooperate with public jurisdiction audit of conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction. If information deemed confidential or proprietary must be reviewed during the course of a contract compliance audit, either party may request the execution of a non-disclosure agreement (NDA), to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.

Clause 18 Data Center Audit requires the service provider to have an independent audit performed of its data centers annually. Some governments may accept an independent SOC 2 Type 2 audit annually for all relevant data centers at the service provider's expense. Access to the audit must be provided to the jurisdiction if requested under unilateral NDA or after being redacted. If the public jurisdiction requires

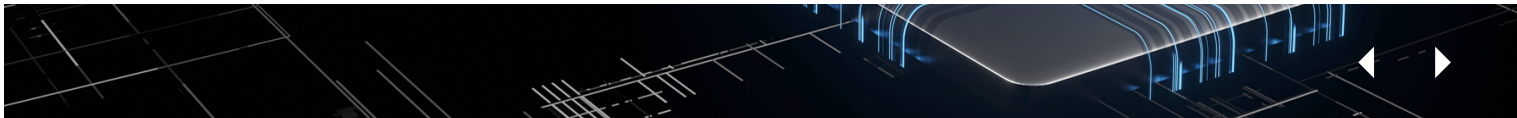
StateRAMP or FedRAMP authorization (recommended) an annual audit as required by StateRAMP and/or FedRAMP shall be performed for all relevant data centers associated with provision of the cloud service at the data center provider's expense. Providers must grant the government's information security office access to view the audit and artifacts through StateRAMP, if applicable.

Clause 19 Continuous Monitoring requires the service provider to demonstrate that the security posture of its cloud service offering is continuously acceptable to the



public jurisdiction throughout the life of the contract. Continuous monitoring shall be conducted at the service provider's expense using 3PAO's and methods approved by the public jurisdiction. Continuous monitoring reports shall be provided to the public jurisdiction under mutual NDA. Alternative - Continuous monitoring reports shall be provided to the public jurisdiction and the 3PAO for the appropriate impact category under which the cloud service offering is authorized by StateRAMP or FedRAMP.

State and local governments can improve government service delivery through responsible development of XaaS contracts. However, traditional control models — designed to protect and safeguard the public's interest — may prevent some public jurisdictions from taking advantage of new service models. Government policymakers beyond procurement officials and CIOs must identify and eliminate barriers to the adoption of these service models. Appropriate oversight and control are critical parts of any public expenditure, but both must be tailored to meet business needs and work effectively with the service model. Without this alignment, business needs cannot be fully met and the full benefit of the service will not be received.



Operations

Operations Responsibility and Uptime Guarantee

System performance and service reliability are important to the business of public jurisdictions. CIOs know how little tolerance end users have for service outages — no matter the cause. Establishing clear service expectations in the terms and conditions is essential for XaaS contracting. Jurisdictions should conduct market research before the procurement to know what to expect in the market and to make sure applications selected for XaaS contracts are well suited to expected operational reliability.

The service provider and the public jurisdiction must agree to the specific details of service performance measure and maintenance downtime schedules in the SLA.

Clause 20 Responsibilities and Uptime Guarantee makes the service provider responsible for all of the plant, capacity, hardware, software and personnel needed to provide the service and commits the service provider to service 24/7.

Changes and Maintenance

Today's XaaS providers are providing performance through a service. For XaaS business models to achieve economies of scale, providers must use "one line code" for all. Upgrades and changes are rolled out to all customers, not to individual users.

Even though the service is more seamless than on-premises systems of the past, public jurisdictions still need to keep their users apprised of any changes that could impact the performance of the system and their use of the services.

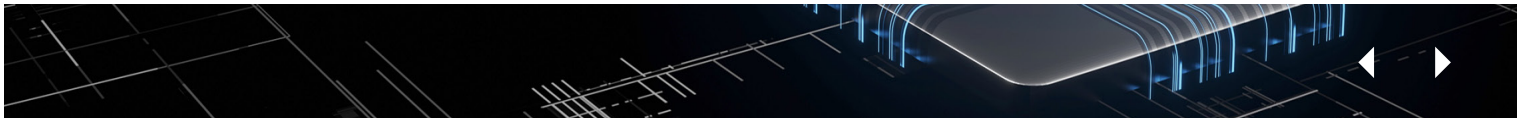
CIOs know how little tolerance end users have for service outages — no matter the cause. Establishing clear service expectations in the terms and conditions is essential for XaaS contracting.

Clause 21 Change Control and Advance Notice requires the service provider to give advanced notice of upgrades or system changes that may impact the public jurisdiction's performance.

Subcontractors

The nature of new cloud-based business models results in service providers relying on a variety of partners, subcontractors or other third parties to provide services to their customers. Public jurisdictions must identify the prime contractor and the various third-party providers and their relationship with the service provider. Ideally, a public jurisdiction will seek this information as a part of its pre-contracting due diligence.

Clause 22 Subcontractor Disclosure requires the service provider to identify all strategic business partners, subcontractors, and other entities and individuals who will be involved with the public jurisdiction's applications and data in the performance of the contract.



Operations Business Continuity and Disaster Recovery
For any application that supports business operations and business continuity, disaster recovery plans are critical to address potential public jurisdiction business disruptions and how the elements of the business will be returned to service. For any XaaS business application, the contract recovery objectives should be aligned with the public jurisdiction's overall business continuity plan.

Clause 23 Business Continuity and Disaster Recovery requires a business continuity plan and disaster recovery plan for the service provider's operations. It specifically requires the service provider to recover the public jurisdiction's data within time objectives agreed upon by both parties. The details of the recovery time must be negotiated between the service provider and the public jurisdiction and should be specific in the terms and conditions and SLA.

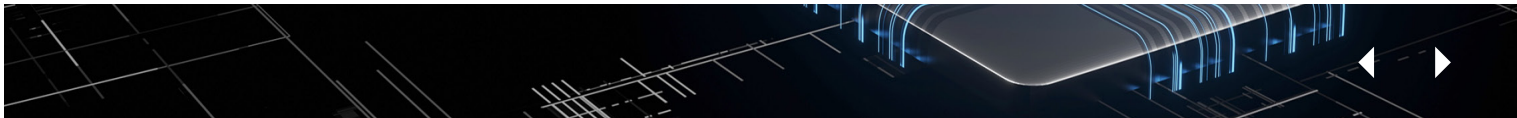
Hybrid Cloud Environments

Hybrid cloud is a cloud computing environment that uses a mixture of on-premises, private cloud and third-party cloud services with orchestration between these platforms. Hybrid cloud environments require management and governance models that encompass all the environments used in any particular deployment. A hybrid application may be as simple as a single application running in multiple hosted computing environments that leverages the strengths of each.

Management

Data center technicians need to track workload locations, ensure device connections are clean and monitor performance. The management of heterogeneous hybrid environments will be as varied as the combinations imaginable. However, there may be solutions available to provide some central management so that visibility and control can be maintained across the entirety of the environment(s). Data centers already struggle with multiple control environments (servers, storage systems, network devices, specialized appliances, database platforms, etc.). The hybrid cloud adds complexity to the control environment. Operational management visibility requirements expand the already complex array of components to link new disparate sets of devices. Clear agreements are needed across each area to determine what source of measures is authoritative. These agreements need to be negotiated between the customer and the service provider.

Terms and conditions associated with hybrid cloud management must accommodate the increased system complexity. There is currently no genuine "single pane of glass" that will work in all hybrid environments, but administrators require visibility across public and private clouds that minimizes the the need to bounce between management applications and attempt to correlate the



results. Further, the authoritative source of diagnostic data must be agreed upon.

Governance

Governance is a mix of terms and conditions and best practices. External cloud governance is the system by which the provision and use of cloud services is controlled. In this case, many components of the hybrid cloud computing environment are likely already operating under SLAs that will form the basis of the governance for each environment. Internal cloud governance focuses on the application of run-time policies to ensure that cloud services are designed, implemented and delivered according to specified expectations.

Public clouds are, by definition, vastly shared resources built for only the most standard of uses. They do not permit unusual customizations. This requires jurisdictions to articulate potential conflicts and interdependencies in SLAs across different hybrid cloud service components for each application.

Customizations or supplementary agreements may be needed to address specific service management gaps, objectives or concerns. Jurisdictions should perform a gap analysis of the differing service agreements and harmonize new and existing policies. Organizational SLAs need to be as close to a standard as possible to ensure easy comparison and understanding of the “net” performance results of multiple SLAs.

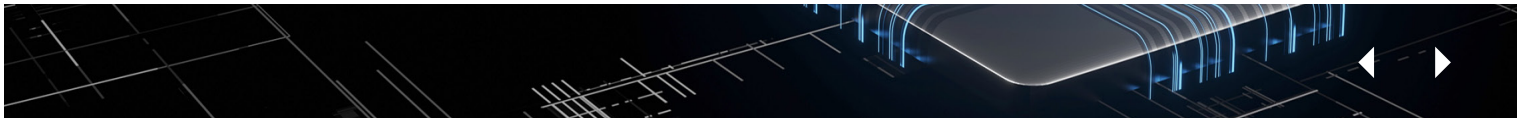
As hybrid and multiple clouds consist of different subsystems which could be sourced from different providers, jurisdictions must understand how these components interact.

In terms of vendor selection, hybrid cloud environments require a governance model that encompasses all the environments used in any particular deployment. The extent to which a service provider participates in governance related activities can be used as a differentiator when choosing between providers for particular workloads.

SLA governance (management) for hybrid cloud computing environments should take into account multiple communication touch points, change management cycles, responsibility hand-offs and even time zones.

The overarching governance for a specific hybrid environment is impacted by each included service and system, which may have its own architecture and governance model. These need to be considered when planning the whole and can change with new application considerations.

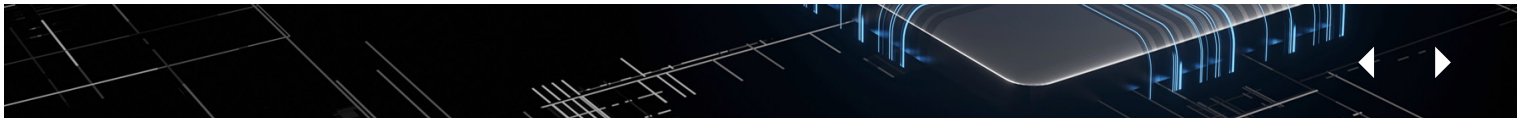
The multiple integrations and touch points between hybrid components may make it difficult to determine what or who is responsible for an outage or incident, and vendor contracts may limit resolution of customer disputes.



Therefore, decisions on what workload may be run on what portion of a hybrid cloud need to consider the remedies for outages and incidents.

Opportunity

Even though complexity increases with hybrid cloud deployments, they provide a unique opportunity for government customers to leverage industry best practices. They also provide access to more capable technology stacks and massively scalable environments. In addition, hybrid cloud implementations let government customers leverage and reuse common infrastructure components as externally managed services, such as database and load balancing environments. This can provide significant cost savings as well as improved access to highly specialized cloud provider staff resources.



Preparation for Migrating Workloads to the Cloud

Governments looking at leveraging cloud opportunities with existing application portfolios face a number of considerations. First, what are the alternatives?

- Continue to strengthen on-premises services and maintain current investment and staffing patterns.
- Begin leveraging cloud services for PaaS and SaaS opportunities with familiar government cloud contract providers.
- Consider migrating to IaaS for critical government infrastructure services.
- Begin developing and rewriting existing agency applications so they are optimized for leveraging cloud services stacks.

Cloud Preparedness Considerations

Migrating to cloud platforms while preserving and improving existing data center services — in whole or in part — requires a great deal of planning and sensitivity to changing customer needs. Government IT organizations need to transform and perform simultaneously. A number of perspectives and areas of focus need to be considered including:

1. **Business** focuses on identifying, measuring and creating business value using technology services.

2. **Product** considers what services agencies are providing to customers and looks at why, what, how, who, where and when services are provided. This perspective considers how services are meeting customer needs and their uniqueness within government.

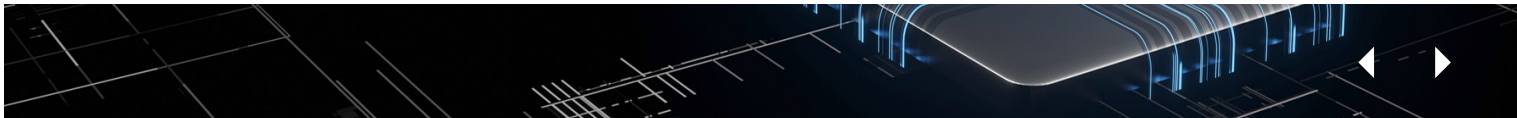
3. **Cost** considers careful analysis of the existing real costs of doing business. What kind of budgetary room for change is possible within the organization and with key stakeholders?

4. **Value** considers what added intangible values might be available if an organization deployed services differently but maintained and improved usability and reliability.

5. **People** considers organizational capacity, capability and change management functions required to implement change throughout the organization. This perspective provides opportunities to define capability and skill requirements, assess current organizational effectiveness, and acquire necessary skills.

6. **Maturity** identifies the target state of an organization's capabilities, measuring maturity and ability to optimize resources. A maturity perspective can help assess the organization's ability to prioritize and sequence initiatives to develop execution roadmaps.

7. **Platform** focuses on describing the structure and relationship of technology elements and services in complex IT environments. This perspective can help develop conceptual and functional models of the IT environment.



8. **Process** looks at processes for managing portfolios, programs and projects to deliver expected business outcomes on time and within budget, while managing risks at acceptable levels.

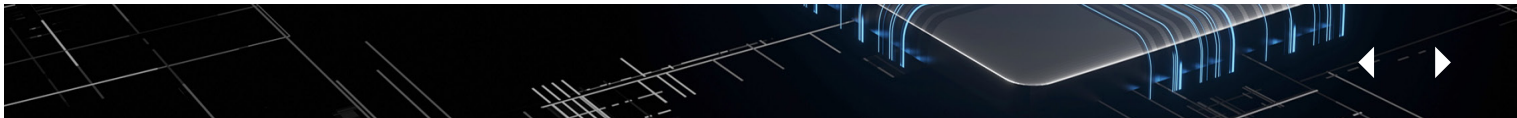
9. **Operations** focuses on the ongoing operation of IT environments, operating procedures, service management, change management and recovery.

10. **Security** emphasizes the methods for governments to achieve risk management and compliance goals with rigorous methods to describe structure of security and compliance processes, systems and personnel.

Government organizations have struggled to simplify infrastructure management, speed up deployment, improve agility, accelerate innovation and lower costs. Customer and stakeholder expectations are rising, necessitating changes in the way government IT does business.

Cloud services stacks from major cloud providers can deliver mature services designed to meet unique security, compliance, privacy and governance requirements of agency and government IT organizations. Professional services can provide deep assistance for planning and migration projects.

Cloud platforms are exceeding security, reliability and scalability requirements associated with government mission-critical and strategic services. Cloud services contracts present an opportunity for governments to move toward new approaches for adding value to customers.



Conclusion

Many governments still try to buy XaaS through traditional procurement methods and standard contract terms and conditions, even though what they are buying is fundamentally different from traditional IT. This approach is not working.

Procurement processes that require strict conformance to prescribed specifications and unique terms and conditions are ineffective in the current technological environment. They were developed to acquire products, not services. Effective procurement achieves timely results and good outcomes, while protecting the public's interest. That is all possible through a more flexible, services-centric approach. Over-reliance on traditional state and local procurement policies, rules or statutes impedes effective procurement of technology services and unnecessarily inflates a project's cost and delivery schedule.

The XaaS model relies on standardization and consistency in code, process, security and, ultimately, a business model supporting the delivery of service over the Internet. XaaS delivers value and benefit for its users because services are not unique to each purchaser. This creates tremendous efficiency and economy of scale. It may, however, require significant changes in government business practices.

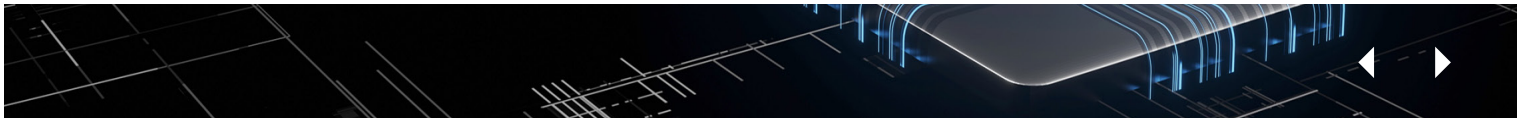
If state and local governments want to take advantage of this service model, policymakers — finance directors, auditors, procurement officers, attorneys and elected officials — must reconsider and modernize controls and processes that create barriers to accessing these services. New ways to provide transparency and accountability must be identified and used to both protect the public interest and enable the purchase of XaaS technology when appropriate.

What Now?

The material presented on these pages supplies a backdrop and options for change, but change won't occur without action. If state and local governments want to enjoy the benefits of secure cloud-based solutions, a wide array of leaders must get involved. Modernizing the rules, oversight and risk management processes that impede rapid, effective and secure cloud contracting requires leadership and help from policymakers, finance directors, IT and security leaders, risk management professionals, auditors, procurement officers, attorneys and ultimately elected officials.

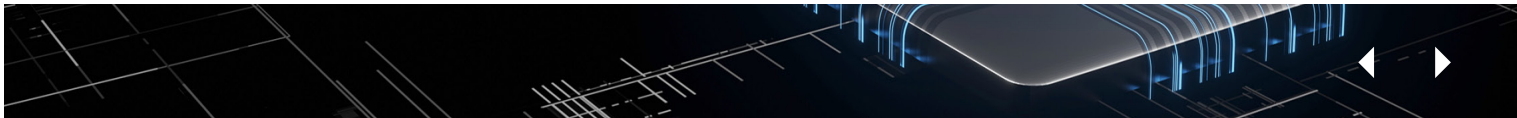
We offer these suggestions for getting started:

- Use model terms and conditions in this guide to frame new relationships with cloud service providers.
- Adopt NIST SP 800-53 (most current version) as baseline controls for cloud services and avoid customization and one- off controls.
- Harmonize procurement terms and conditions, solicitation language and security policies, standards, and controls to eliminate conflicts and redundancies.
- Incorporate a RAMP or RAMP service in cloud service acquisition and management. Use the RAMP checklist as a roadmap.
- Change the procurement infrastructure and acquisition policies and processes to align with cloud service governance and risk authorization and management practices.



- Pilot and implement continuous monitoring by qualified auditors for cloud service control compliance to protect the public interest and enable the secure use of as-a-service solutions.

The rapid proliferation of these service offerings is profoundly changing how the world does business. State and local governments must not isolate themselves from that change, but rather position themselves to embrace and benefit from it. It is the time to set aside outdated practices that inhibit progress, and move confidently toward a new set of commercially proven practices and procedures that support innovation, collaboration and economy through internet-based services.



Workgroup Members and Contributors

Workgroup Members

Steve Nichols
Chief Technology Officer
Georgia Technology Authority

Jim Weaver
Secretary of Technology/
Chief Information Officer
State of North Carolina

Rob Main
Chief Risk Officer/
Chief Information Security Officer
State of North Carolina

Jonathan Shaw
General Counsel
North Carolina Department of Information Technology

Curtis Wood
Chief Information Officer
Commonwealth of Massachusetts

Gary Lambert
Assistant Secretary for Operational Services
Commonwealth of Massachusetts

Elizabeth Rooney
Director of Contract Management
Commonwealth of Massachusetts

Sean Hughes
Assistant Secretary for Technology, Security and Operations
Commonwealth of Massachusetts

William Cole
Chief Technology Officer
Commonwealth of Massachusetts

Anthony Oneill
Chief Risk Officer
Commonwealth of Massachusetts

Jack Harris
Chief Technology Officer
State of Michigan

Jayson Cavendish
Deputy Chief Security Officer
State of Michigan

Simon Baldwin
Category Director - IT Procurement
State of Michigan

Jared Ambrosier
(Interested Party)
Chief Procurement Officer
State of Michigan

Laura Clark
(Interested Party)
Chief Information Officer/Chief Information Security Officer
State of Michigan

J.R. Sloan
Chief Information Officer
State of Arizona

Steve Nettles
Statewide Procurement Group Manager
State of Arizona

John Red Horse
IT Procurement Group Manager
State of Arizona

Matt Kelly
Deputy Chief Information Security Officer
State of Texas

Amanda Crawford
(Interested Party)
Chief Information Officer
State of Texas

Nancy Rainosek
(Interested Party)
Chief Information Security Officer
State of Texas

Mike Homant
Chief Technology Officer/Deputy CIO
City of Detroit

Linda M. Bruton
Senior Assistant Corporation Counsel
Transactions and Economic Development
City of Detroit

John Katsorhis
Chief Contracting Officer
Comptroller's Office
New York City

Sarah Hurley
Senior Counsel
Department of IT & Telecommunications
New York City

Whitney Soenksen
Deputy CIO
City of New Orleans

Glenn Herdrich
Information Security Manager
Sacramento County, California

Contributors

Leah McGrath
Executive Director
StateRAMP

Rebecca Kee
Implementation Consultant
StateRAMP

Fay Tan
Legal Counsel
NASPO ValuePoint

Holly Scott
Procurement Content Manager
NASPO

Teri Takai
Senior Vice President
Center for Digital Government

Brian Cohen
Vice President
Center for Digital Government

Tricia Dugan
Chief of Staff
Office of the Senior Vice President
Center for Digital Government

Sean McSpaden
(Lead Facilitator)
Senior Fellow
Center for Digital Government

Dugan Petty
(Facilitator)
Senior Fellow
Center for Digital Government

Bob Woolley
(Facilitator)
Senior Fellow
Center for Digital Government

Otto Doll
(Facilitator)
Senior Fellow
Center for Digital Government

Jeana Bigham
Executive Director
e.Republic Content Studio

Steve Towns
Director of Content Strategy
e.Republic Content Studio

Jessica Walton
Program Manager
e.Republic Content Studio

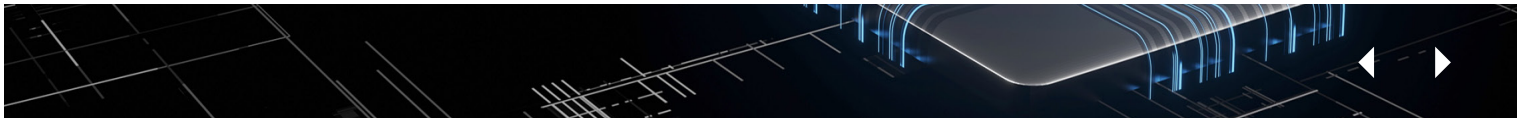
Underwritten By

Amazon Web Services (AWS) Worldwide Public Sector helps government, education, and nonprofit customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation across the globe. With AWS, you only pay for what you use, with no up-front physical infrastructure expenses or long-term commitments. Public Sector organizations of all sizes use AWS to build applications, host websites, harness big data, store information, conduct research, improve online access for citizens, and more. AWS has dedicated teams focused on helping our customers pave the way for innovation and, ultimately, make the world a better place through technology. Contact us to learn how AWS can help you with your biggest IT challenges. **aws.amazon.com/stateandlocal/digital-government/**

Knowledge Services is an Indianapolis, IN based software and professional services organization dedicated to "serving those who serve others." We are focused on helping public and private organizations improve their cyber posture, including 3rd party software supply chain cybersecurity verification. Our SaaS marketplace helps facilitate organizations of all sizes to identify and engage cyber related services and to share industry best practices. For more details go to: **www.knowledgeservices.com**

Citrix (part of Cloud Software Group) builds the secure, unified digital workspace technology that helps organizations unlock human potential and deliver a consistent workspace experience wherever work needs to get done. With Citrix, users get a seamless work experience, and IT has a unified platform to secure, manage, and monitor diverse technologies in complex cloud environments. **https://www.citrix.com/solutions/government/state-and-local-government.html**

VMware gives government agencies the smartest path to the cloud, edge, and app modernization, in order to deliver citizen services and meet mission demands. With VMware's Cross-Cloud services, you can control all apps and clouds through one management platform, where you can set unified security policies and quickly develop and deploy apps without refactoring. For more information visit: **vmware.com/go/slg**.



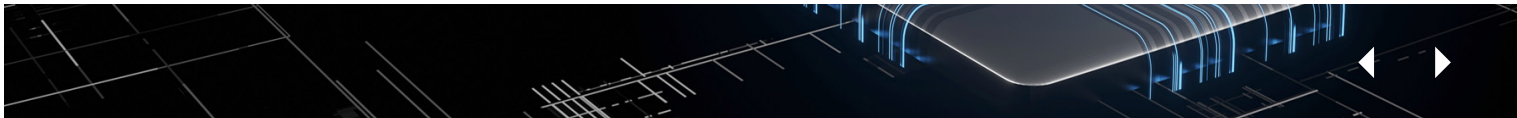
Appendix 1

Model Terms and Conditions Templates

The workgroup recommends that contracts for XaaS include four well-defined, mutually exclusive sections, along with any other sections required under the jurisdiction's established procurement processes. These sections are:

- **A Statement of Work (SOW),** which contains an array of functional requirements. While many SOWs repeat similar needs, those functional needs do not cross the boundary into terms and conditions. Such common functions may include daily activity reporting, alerts when certain conditions are met, etc.
- **Terms and Conditions,** which are the major focus of this document. For ease of maintainability, certain metrics and dynamic information should be placed into a separate document. We call this the service level agreement (SLA) metrics outline and refer to it in various places in the terms and conditions.
- **The SLA Metrics Outline,** which contains expected service metrics and describes the consequences for unmet agreed expectations.
- **Contact Details Outline,** which contains names and contact information of the individuals who represent the parties for operations purposes.

The workgroup offers three templates as model terms and conditions for each specific service model: SaaS, PaaS and IaaS. Each template is intended to accelerate XaaS adoption by providing a foundation or starting point for a public jurisdiction and a service provider to create a responsive and effective XaaS contract. As with any model document, the templates have no force or effect until used or adopted.



Software-as-a-Service

Clause 1. Definitions:

a. **Authorized Persons:** The service provider's employees, contractors, subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.

b. **Data Breach:** Unauthorized access by a non-authorized person/s that results in the use, disclosure or theft of a public jurisdiction's unencrypted personal data.

c. **Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[20]

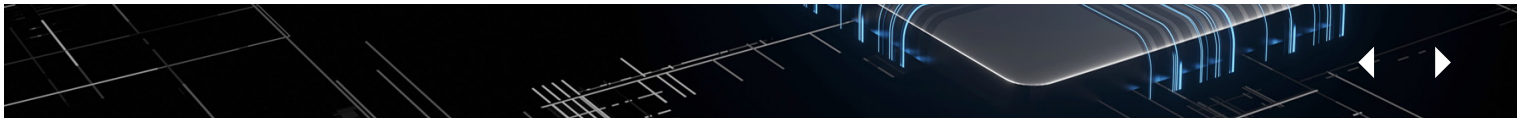
d. **Non-Public Data:** Data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

e. **Personal Data:** Data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or protected health information relating to a person.

f. **Protected Health Information (PHI):** Individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g; records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and employment records held by a covered entity in its role as employer.[21]

g. **Public Jurisdiction:** Any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

h. **Public Jurisdiction Data:** All data created or in any way originating with the public jurisdiction and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction,



whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

i. **Public Jurisdiction Identified Contact:** The person or persons designated in writing by the public jurisdiction to receive security incident or breach notifications.

j. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

k. **Service Level Agreement (SLA):** That part of the written agreement between the public jurisdiction and the service provider that is subject to the terms and conditions in this document and that unless otherwise agreed to includes (1) the technical service level performance promises, (i.e., metrics for performance and intervals for measure), (2) the amount of time required for notice by the provider to the public jurisdiction of upcoming changes, (3) security notice requirements, (4) timeframes for response to operational problems and failures, and (5) any remedies for performance failures.

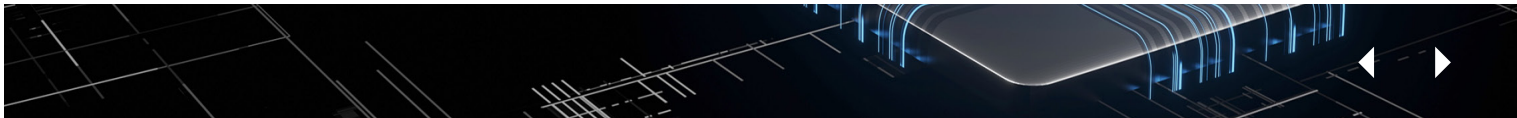
l. **Service provider:** The contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

m. **Software-as-a-Service (SaaS):** The capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure — including network, servers, operating systems, storage or even individual application capabilities — with the possible exception of limited user-specific application configuration settings.[22]

n. **Statement of Work:** A written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.

Clause 2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data except (1) during data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

Clause 3. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

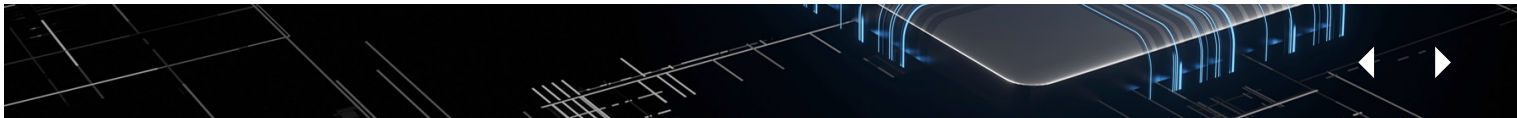


a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. Such security measures shall be in accordance with NIST SP 800-53 (current version) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.
b. All data obtained by the service provider in the performance of this contract shall become and remain property of the public jurisdiction.
c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (current version). Unless otherwise stipulated, the service provider is responsible for encryption of the personal data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the SLA or otherwise made a part of this contract.
d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.
e. At no time shall any data or processes that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
f. The service provider shall not use any information collected in connection with the service issued from this contract for any purpose other than fulfilling the service.

Clause 4. Data Privacy: The service provider's privacy controls must also abide by the following:

a. No type of data mining may be performed on any public jurisdiction data without permission from the public jurisdiction. This includes mining location data from users of applications running on behalf of the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls.
b. No public jurisdiction data may be sold or transferred to any third party, including service provider affiliates, without permission from the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls.

Clause 5. Data Location: The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S in accordance with NIST SP 800-53 (current version). The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.



Clause 6. Data Access: The service provider shall be responsible for:

a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800-53 (current version) Access Controls.
b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the public jurisdiction for Follow the Sun technical support under the contract.
c. Maintaining government data and allowing the downloading of that data for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After this period, the service provider will destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/deletion to the public jurisdiction.

Clause 7. Import and Export of Data: The public jurisdiction shall have the ability to import or export data:

a. In piecemeal or in entirety at its discretion without interference and with support from the service provider as described in the contract or SLA. This includes the ability for the public jurisdiction to import or export data to/from other service providers.
b. At intervals as frequent as the public jurisdiction requires.

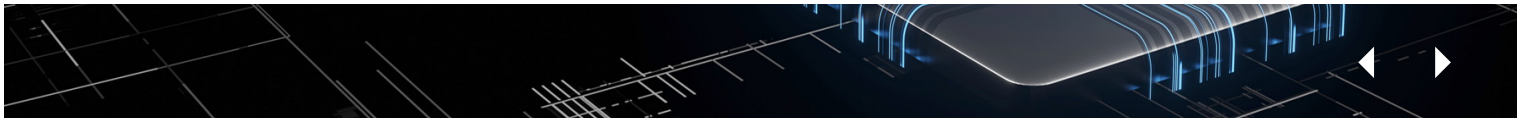
Clause 8. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any security incident or data breach.

a. Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

b. Security Incident Reporting Requirements: The service provider shall report a security incident to the appropriate public jurisdiction identified contact within the manner and timeframe defined in the SLA.

c. Breach Reporting Requirements: If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall notify the appropriate public jurisdiction identified contact within [select - 24/48/72] hours or sooner — unless shorter time is required by applicable law — and take commercially reasonable measures to address the data breach in a timely manner.

Clause 9. Breach Responsibilities: This section only applies when a data breach occurs with



respect to personal data within the possession or control of the service provider.

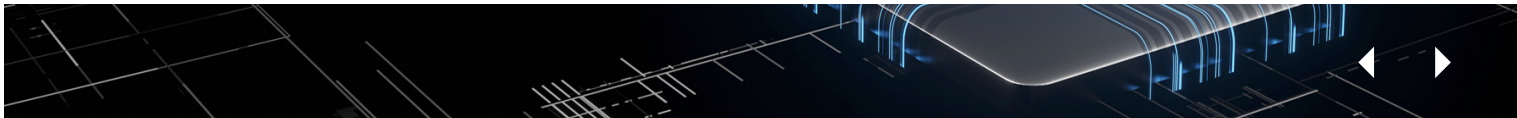
a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.
b. The service provider, unless stipulated otherwise, shall notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document actions taken in response to the data breach, including any post-incident review of events and changes in business practices.

Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifying individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law; (4) providing a website or a toll-free number and call center for affected individuals required by state law; and (5) completing all corrective actions as reasonably determined by the service provider based on root cause. These costs shall not exceed the average per-record, per-person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach. All actions [1 through 5] are subject to this contract's limitation of liability.

Clause 10. Background Checks: The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty. This includes but is not limited to criminal fraud or conviction of any felony or misdemeanor offense with an authorized penalty of up to one year of incarceration. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information.

Clause 11. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable NDAs and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

Clause 12. Right to Remove Individuals: The public jurisdiction may at any time require that the service provider remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall notify the



service provider of its determination and its reasons for requesting the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.

Clause 13. Security: The service provider shall disclose its non-proprietary security protocols, processes, tools and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. The service provider's disclosures shall include information related to:

- Governance and compliance
- Standards and policies
- Security and risk assessments
- Continuous monitoring and alerting
- Privilege and identity access management
- Data protections
- Infrastructure and application protections
- Native cloud service provider security information and event management (SIEM)/log management tools
- System health and resource monitoring
- Incident response and recovery

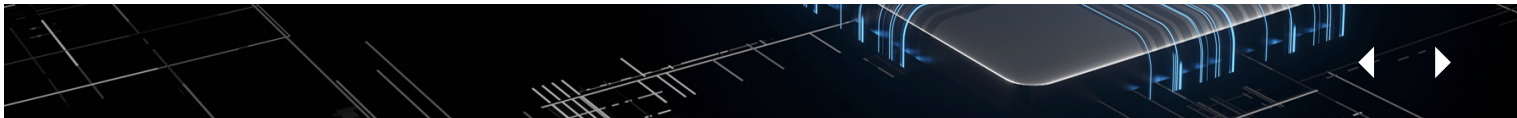
The public jurisdiction and the service provider shall understand each other's roles and responsibilities for security and document them within the SLA.

Clause 14. Access to Security Logs and Reports:

a. The service provider shall provide reports to the public jurisdiction in a format specified in the SLA. Reports shall include latency statistics, date and time stamps, user access IP addresses, source and destination IP addresses, system events (e.g., failed and successful events — system shutdown or starting a service, errors, anomalous/abnormal activity or system events, etc.), log-on/authentication attempts (failed and successful), user access history, account changes (e.g., account creation and deletion, account privilege assignment, etc.), security policy changes, system configuration changes, usage information (e.g., number of transactions occurring in a certain period of time) and transaction size (e.g., email message size, file transfer size, etc.), and security logs for all public jurisdiction data related to this contract.
b. The service provider and the public jurisdiction share security responsibilities. The service provider is responsible for providing a secure infrastructure (e.g., storage and servers), virtualization/ hypervisor, operating system, middleware and runtime, applications and networking. The service provider and the public jurisdiction typically share responsibility for identity, credential and access management; networking; and data.

The methods and conditions for authorized access to logs/reports and the format for the logs/reports shall be specified and agreed upon by both parties in the SLA. Specific shared responsibilities are identified in the SLA.

Clause 15. Retention, Preservation and Archival of



Security Logs and Reports: The service provider shall retain security logs and reports in a usable format for a minimum of _____ (days, months, years) and a maximum retention/archival of _____ (days, months, years or for a specific period beyond the termination of the contract). The methods and timeframes for the retention, reservation (i.e., legal hold) and archival for the logs and reports will be specified and agreed upon by both parties in the SLA.

Clause 16. Encryption of Data at Rest: The service provider shall prevent its employees and subcontractors from storing personal data on portable devices, except within data centers located in the United States. If personal data must be stored on portable devices to accomplish the work, the service provider must use hard drive encryption in accordance with cryptography standards referenced in FIPS 140-2, Security Requirements for Cryptographic Modules.

Clause 17. Contract Audit: The service provider shall cooperate with public jurisdiction audit of conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction. If information deemed confidential or proprietary must be reviewed during a contract compliance audit, either party may request the execution of a non-disclosure agreement (NDA), to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.

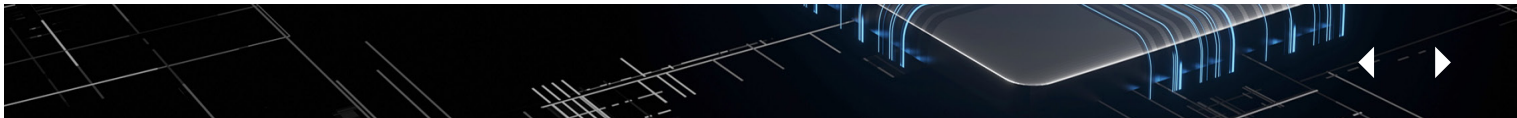
Clause 18. Data Center Audit: An annual audit as required by StateRAMP and/or FedRAMP shall be performed for all relevant data centers associated with the provision of a cloud service at the data center provider's expense. Providers must grant the government's information security office access to view the audit and artifacts through StateRAMP, if applicable.

Some governments may accept a SOC 2 Type 2 audit annually for all relevant data centers associated with the provision of the cloud service at the service provider's expense. The audit must be made available to the jurisdiction if requested under unilateral NDA or after being redacted.

Clause 19. Continuous Monitoring: The service provider shall, at service provider's expense, conduct continuous monitoring of its compliance with security controls required within the contract. Continuous monitoring shall be conducted via one or a combination of the following methods approved by the public jurisdiction:

a. Reliance on StateRAMP authorization and independent assessments by third-party assessment organizations (3PAOs)
b. Reliance on FedRAMP authorization and independent assessments by 3PAOs
c. Review of control documentation by internal staff or 3PAO
d. Acceptance of the service provider's third-party attestation (e.g. AICPA SOC2-Type 2 audit)
e. Self-assessment by service provider

Continuous monitoring reports shall be provided



to the public jurisdiction under mutual NDA.

Alternative: StateRAMP or FedRAMP shall provide continuous monitoring reports to the public jurisdiction and the 3PAO for the appropriate impact category under which the cloud service offering is authorized.

Clause 20. Responsibilities and Uptime Guarantee: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibility of the service provider. The system shall be available 24/7/365, with agreed-upon maintenance downtime, and provide service to customers as defined in the SLA.

Clause 21. Change Control and Advance Notice: The service provider shall give advance notice (to be determined at the contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades or system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version to bring the system up to date or improve its characteristics. It usually includes a new version number.

Clause 22. Subcontractor Disclosure: The service provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.

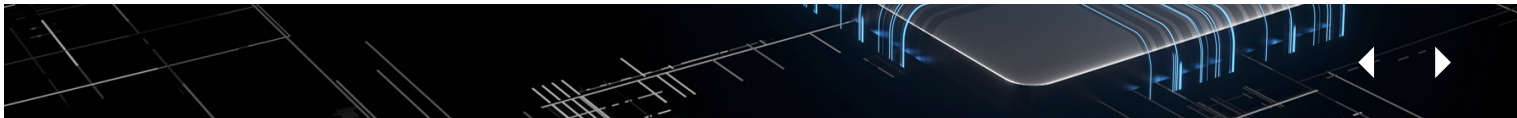
Clause 23. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan upon request and ensure that the public jurisdiction's recovery time objective (RTO) of XXX hours/days is met. (XXX shall be negotiated by both parties.)

Clause 24. Compliance with Accessibility Standards: The service provider shall comply with and adhere to accessibility standards of Section 508 Amendment to the Rehabilitation Act of 1973.

Clause 25. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

Clause 26. Subscription Terms: Contractor grants to a purchasing entity a license to: (1) access and use the service for its business purposes; (2) for SaaS, use underlying software as embodied or used in the service; and (3) view, copy, upload and download (where applicable), and use contractor's documentation.

Clause 27. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon



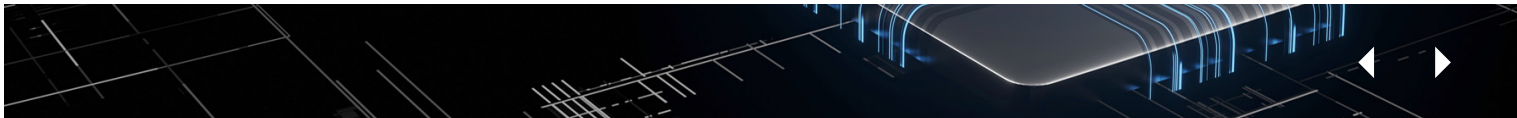
receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

Clause 28. Termination and Suspension of Service:

a. In the event of a contract termination, the service provider shall return public jurisdiction's data in a CSV or other mutually agreeable format at a time agreed to by the parties. The service provider also will provide for the subsequent secure disposal of public jurisdiction data.
b. During any period of service suspension, the service provider shall not intentionally erase any public jurisdiction data.
c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of:
   - 10 days after the effective date of termination, if the termination is in accordance with the contract period
   - 30 days after the effective date of termination, if the termination is for convenience
   - 60 days after the effective date of termination, if the termination is for cause

   After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

d. The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established in the SOW.
e. The service provider shall securely dispose of all requested data in all forms, such as disk, CD/DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.



Platform-as-a-Service

Clause 1. Definitions:

a. **Authorized Persons:** The service provider's employees, contractors, subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.

b. **Data Breach:** The unauthorized access by a non-authorized person/s that results in the use, disclosure or theft of a public jurisdiction's unencrypted personal data.

c. **Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[23]

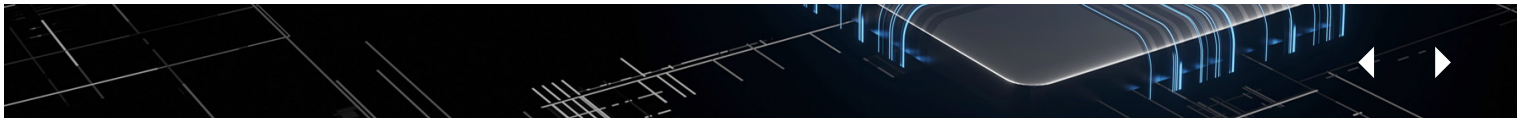
d. **Non-Public Data:** Data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

e. **Personal Data:** Data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or protected health information relating to a person.

f. **Platform-as-a-Service (PaaS):** The capability provided to the consumer to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.[24]

g. **Protected Health Information (PHI):** Individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.[25]

h. **Public Jurisdiction:** Any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

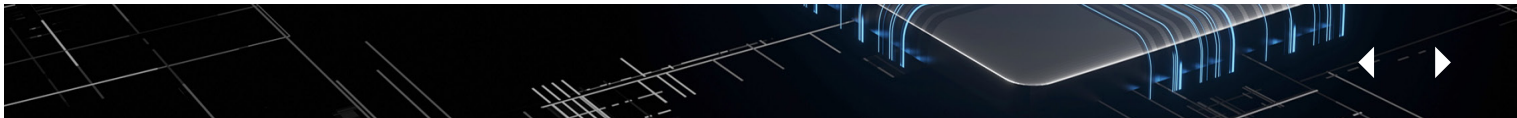


i. **Public Jurisdiction Data:** All data created or in any way originating with the public jurisdiction and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.
j. **Public Jurisdiction Identified Contact:** The person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.
k. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.
l. **Service Level Agreement (SLA):** That part of the written agreement between both the public jurisdiction and the service provider that is subject to the terms and conditions in this document and that unless otherwise agreed to includes (1) the technical service level performance promises (i.e., metrics for performance and intervals for measure); (2) the amount of time required for notice by the provider to the public jurisdiction for notification of upcoming changes; (3) security notice requirements; (4) timeframes for response to operational problems and failures; and (5) any remedies for performance failures.
m. **Service Provider:** The contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.
n. **Statement of Work:** A written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.

Clause 2. Data Ownership: The public jurisdiction will own all right, title and interest in its public jurisdiction data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data except (1) during data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract, or (4) at the public jurisdiction's written request.

Clause 3. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information within its control and comply with the following conditions:

a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data within its control. Such security measures shall be in accordance with NIST SP 800-53 (current version) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

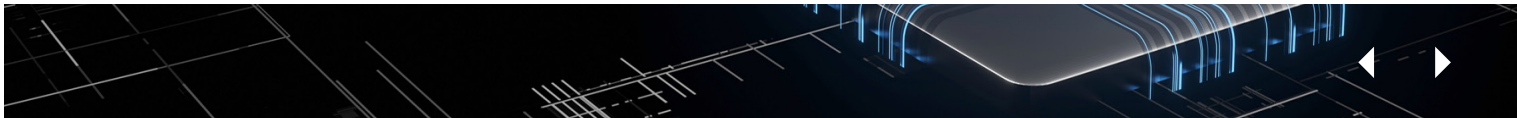


b. All data obtained by the service provider within its control in the performance of this contract shall become and remain property of the public jurisdiction.
c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (current version). The SLA and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the statement of work and the contract are silent, then the public jurisdiction is responsible for encryption and access control.
d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.
e. At no time shall any data or processes which either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

Clause 4. Data Privacy: The service provider's privacy controls must abide by the following:
a. No type of data mining may be performed on any public jurisdiction data without permission from the public jurisdiction. This includes mining location data from users of applications running on behalf of the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls.
b. No public jurisdiction data may be sold or transferred to any third party, including service provider affiliates, without permission from the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls.

Clause 5. Data Location: The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S in accordance with NIST SP 800-53 (current version). The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.

Clause 6. Data Access: The service provider shall be responsible for:
a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800-53 (current version) Access Controls.
b. Preventing any offshore access by service provider



employees and contractors, unless explicitly authorized by the public jurisdiction for Follow the Sun technical support under the contract.

c. Maintaining government data and allowing downloading for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After this period, the service provider will destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/deletion to the public jurisdiction.

Clause 7. Import and Export of Data: The public jurisdiction shall have the ability to import or export data:

a. In piecemeal or in entirety at its discretion without interference and with support from the service provider as described in the contract or SLA. This includes the ability for the public jurisdiction to import or export data to/from other service providers.
b. At intervals as frequent as the public jurisdiction requires.

Clause 8. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any security incident or data breach.

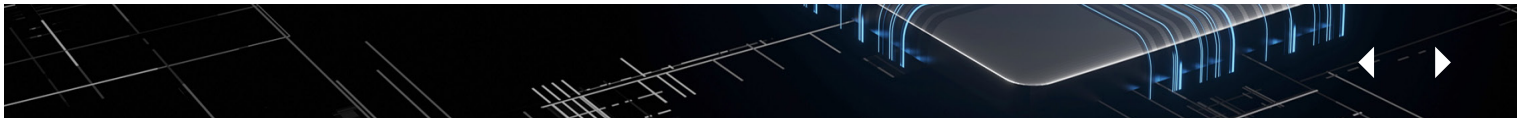
a. Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

b. Security Incident Reporting Requirements: The service provider shall report a security incident to the appropriate public jurisdiction identified contact within the manner and timeframe defined in the SLA.

c. Breach Reporting Requirements: If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall notify the appropriate public jurisdiction identified contact within [select 24/48/72] hours or sooner — unless shorter time is required by applicable law — and take commercially reasonable measures to address the data breach in a timely manner.

Clause 9. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider and related to the service provided under this contract.

a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.
b. The service provider, unless stipulated otherwise, shall notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes there has been a



data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document actions taken in response to the data breach, including any post-incident review of events and changes in business practices.

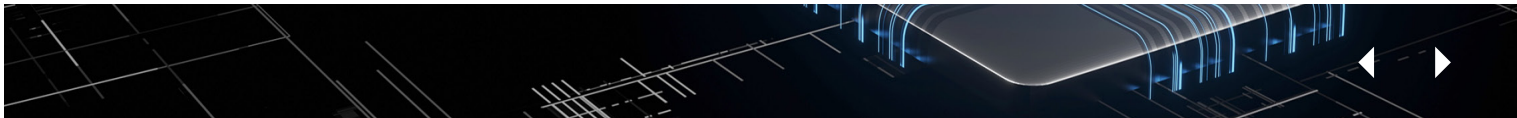
c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifying individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law; (4) providing a website or a toll-free number and call center for affected individuals required by state law; and (5) completing all corrective actions as reasonably determined by the service provider based on root cause. These costs shall not exceed the average per-record, per-person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach. All actions [1 through 5] are subject to this contract's limitation of liability.

Clause 10. Background Checks: The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to one year is an authorized penalty. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information.

Clause 11. Non-Disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of customer data to that which is absolutely necessary to perform job duties.

Clause 12. Right to Remove Individuals: The public jurisdiction may at any time require the service provider to remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.

Clause 13. Security: The service provider shall disclose its non-proprietary security protocols, processes, tools and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider.



The service provider's disclosures shall include information related to:

- Governance and compliance
- Standards and policies
- Security and risk assessments
- Continuous monitoring and alerting
- Privilege and identity access management
- Data protections
- Infrastructure and application protections
- Native cloud service provider SIEM/log management tools
- System health and resource monitoring
- Incident response and recovery

The public jurisdiction and the service provider shall understand each other's roles and responsibilities and document them within the SLA.

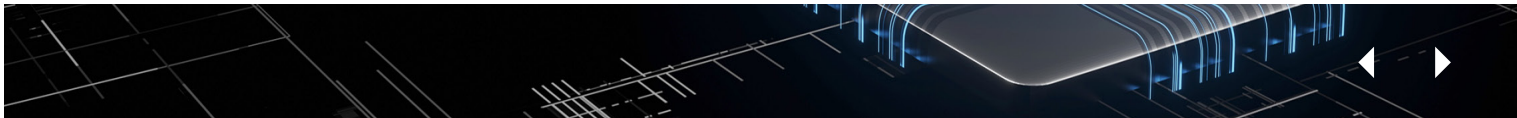
Clause 14. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in a format as specified in the SLA and agreed to by the service provider and the public jurisdiction. Reports will include latency statistics, date and time stamps, user access IP addresses, source and destination IP addresses, system events (e.g., failed and successful events — system shutdown or starting a service, errors, anomalous/abnormal activity or system events, etc.), log-on/authentication attempts (failed and successful), user access history, account changes (e.g., account creation and deletion, account privilege assignment, etc.), security policy changes, system configuration changes, usage information (e.g., number of transactions occurring in a certain period of time) and transaction size (e.g., email message size, file transfer size, etc.), and security logs for all public jurisdiction data related to this contract.

a. The service provider and the public jurisdiction recognize that security responsibilities are shared. The service provider is responsible for providing a secure infrastructure (e.g., storage and servers), virtualization/hypervisor, operating system, middleware and runtime. The service provider and the public jurisdiction typically share responsibility for identity, credential and access management; networking; and data. In certain instances, the public jurisdiction has sole responsibility for securing its applications and data that run within the PaaS computing environment.

The methods and conditions for access to logs/reports and the format for logs/reports shall be specified and agreed upon by both parties in the SLA. Specific shared responsibilities are identified in the SLA.

Clause 15. Retention, Preservation and Archival of Security Logs and Reports: The service provider shall retain security logs and reports in a usable format for a minimum of _____ (days, months, years) and a maximum retention/archival of _____ (days, months, years or for a specific period beyond the termination of the contract). The methods and timeframes for the retention, preservation (i.e., legal hold), and archival for the logs and reports will be specified and agreed upon by both parties in the SLA.

Clause 16. Encryption of Data at Rest: The service provider shall prevent its employees and subcontractors from storing



personal data on portable devices, except within data centers located in the United States. If personal data must be stored on portable devices to accomplish the work, the service provider must use hard drive encryption in accordance with cryptography standards referenced in FIPS 140-2, Security Requirements for Cryptographic Modules.

Clause 17. Contract Audit: The service provider shall cooperate with public jurisdiction audit of conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction. If information deemed confidential or proprietary must be reviewed during a contract compliance audit, either party may request the execution of an NDA, to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.

Clause 18. Data Center Audit: An annual audit as required by StateRAMP and/or FedRAMP shall be performed for all relevant data centers associated with the provision of a cloud service at the data center provider's expense. Providers must grant the government's information security office access to view the audit and artifacts through StateRAMP, if applicable.

Some governments may accept a SOC 2 Type 2 audit annually for all relevant data centers associated with the provision of the cloud service at the service provider's expense. The audit must be made available to the jurisdiction if requested under unilateral NDA or after being redacted.

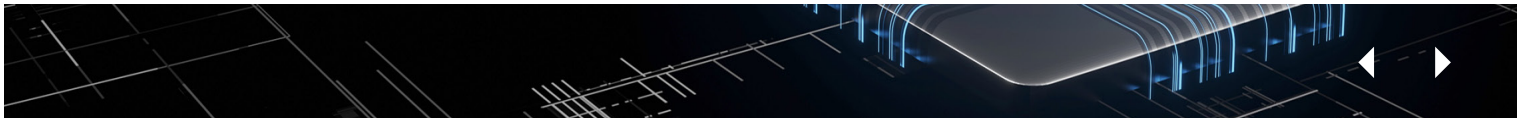
Clause 19. Continuous Monitoring: The service provider shall, at service provider's expense, conduct continuous monitoring of its compliance with security controls required within the contract. Continuous monitoring shall be conducted via one or a combination of the following methods approved by the public jurisdiction:

a. Reliance on StateRAMP authorization and independent assessments by third-party assessment organizations (3PAOs)
b. Reliance on FedRAMP authorization and independent assessments by 3PAOs
c. Review of control documentation by internal staff or 3PAOs
d. Acceptance of the service provider's third-party attestation (e.g. AICPA SOC2-Type 2 audit)
e. Self-assessment by the service provider

Continuous monitoring reports shall be provided to the public jurisdiction under mutual NDA.

Alternative: StateRAMP or FedRAMP shall provide continuous monitoring reports to the public jurisdiction and the 3PAO for the appropriate impact category under which the cloud service offering is authorized.

Clause 20. Responsibilities and Uptime Guarantee: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing



and maintaining the environment are the responsibility of the service provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime) and provide service to customers as defined in the SLA.

Clause 21. Change Control and Advance Notice: The service provider shall give advance notice (to be determined at contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades or system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version to bring the system up to date or improve its characteristics. It usually includes a new version number.

Clause 22. Sub-Contractor Disclosure: The service provider shall identify all strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who will be involved in any application development and/or operations.

Clause 23. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan upon request and ensure the public jurisdiction's recovery time objective (RTO) of XXX hours/days is met. (XXX shall be negotiated by both parties.)

Clause 24. Compliance with Accessibility Standards: The service provider shall comply with and adhere to accessibility standards of Section 508 Amendment to the Rehabilitation Act of 1973.

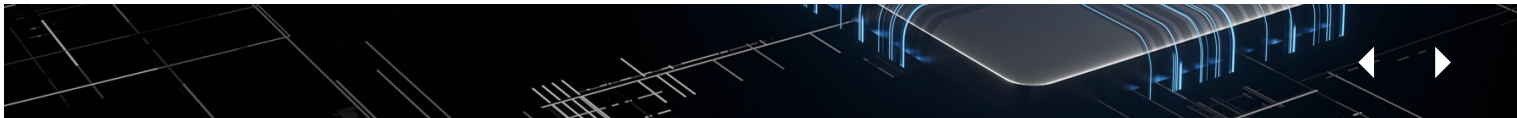
Clause 25. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

Clause 26. Subscription Terms: Contractor grants to a purchasing entity a license to: (1) access and use the service for its business purposes; (2) for PaaS, use underlying software as embodied or used in the service; and (3) view, copy, upload and download (where applicable), and use the contractor's documentation.

Clause 27. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

Clause 28. Termination and Suspension of Service:

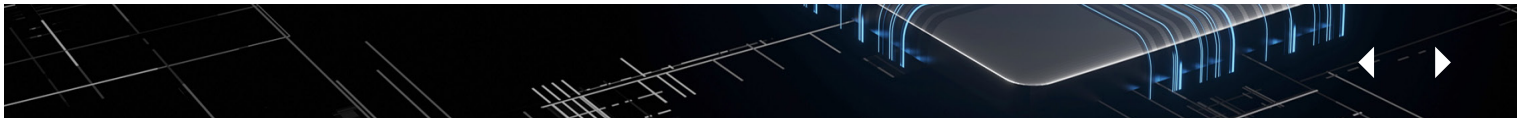
a. In the event of an early contract termination, the service provider shall allow the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content.
b. During any period of service suspension, the service



provider shall not intentionally erase any public jurisdiction digital content.

c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of 45 days after the effective date of a termination for convenience, or 60 days after the effective date of a termination for cause. After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of a termination for cause, the service provider will impose no fees the customer for access and retrieval of digital content.

d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all forms, such as disk, CD/ DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.



Infrastructure-as-a-Service

Clause 1. Definitions:

a. **Authorized Persons:** The service provider's employees, contractors, subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.

b. **Data Breach:** The unauthorized access by a non-authorized person/s that results in the use, disclosure or theft of a public jurisdiction's unencrypted personal data.

c. **Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[26]

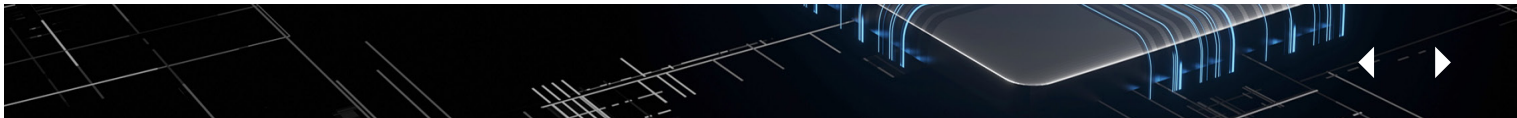
d. **Infrastructure-as-a-Service (IaaS):** The capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components (e.g., host firewalls).[30]

e. **Non-Public Data:** Data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

f. **Personal Data:** Data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or protected health information relating to a person.

g. **Protected Health Information (PHI):** Individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.[27]

h. **Public Jurisdiction:** Any government or government agency that uses these terms and conditions. The term



is a placeholder for the government or government agency.

i. **Public Jurisdiction Data:** All data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

j. **Public Jurisdiction Identified Contact:** The person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

k. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

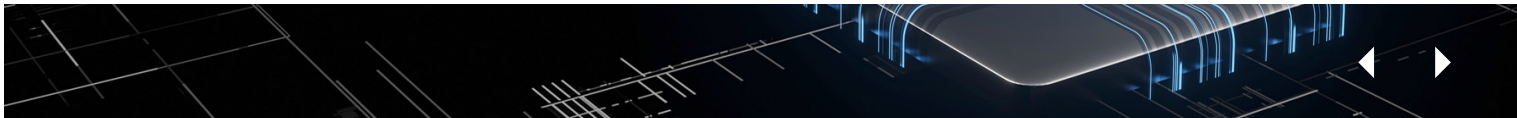
l. **Service Level Agreement (SLA):** That part of the written agreement between the public jurisdiction and the service provider that is subject to the terms and conditions in this document and that unless otherwise agreed to includes (1) the technical service level performance promises, (i.e., metrics for performance and intervals for measure), (2) the amount of time required for notice by the provider to the public jurisdiction of upcoming changes, (3) identification of contact persons, (4) security notice requirements, (5) timeframes for response to operational problems and failures, (6) any remedies for performance failures.

m. **Service Provider:** The contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

n. **Statement of Work:** A written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.

Clause 2. Data Ownership: The public jurisdiction will own all right, title and interest in its public jurisdiction data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data except (1) during data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

Clause 3. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information within its control and comply with the following conditions:

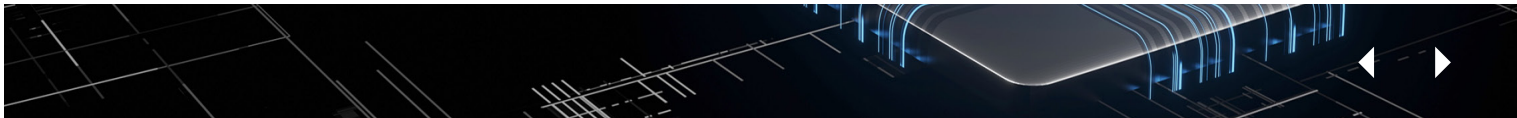


a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data within its control. Such security measures shall be in accordance with NIST SP 800-53 (current version) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.
b. All data obtained by the service provider within its control in the performance of this contract shall become and remain property of the public jurisdiction.
c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (current version). The SLA and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the statement of work and the contract are silent, then the public jurisdiction is responsible for encryption and access control.
d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.

At no time shall any data or processes which either belong to or are intended for the use of public jurisdiction or its officers, agents or employees be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

Clause 4. Data Privacy: The service provider's privacy controls must abide by the following:
a. No type of data mining may be performed on any public jurisdiction data without permission from the public jurisdiction. This includes mining location data from users of applications running on behalf of the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls.
b. No public jurisdiction data may be sold or transferred to any third party, including service provider affiliates, without permission from the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls.

Clause 5. Data Location: The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S in accordance with NIST SP 800-53 (current version). The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely



only as required to provide technical support. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.

Clause 6. Data Access: The service provider is responsible for:

a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800-53 (current version) Access Controls.
b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the public jurisdiction for Follow the Sun technical support under the contract.
c. Maintaining government data and allowing the downloading of that data for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After this period, the service provider will destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/deletion to the public jurisdiction.

Clause 7. Import and Export of Data: The public jurisdiction shall have the ability to import or export data:

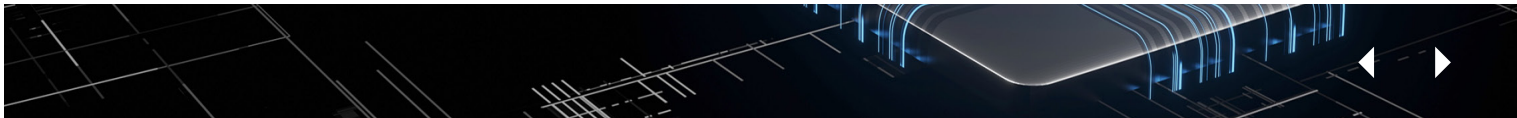
a. In piecemeal or in entirety at its discretion without interference and with support from the service provider as described in the contract or SLA. This includes the ability for the public jurisdiction to import or export data to/from other service providers.
b. At intervals as frequent as the public jurisdiction requires.

Clause 8. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any security incident or data breach.

a. Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

b. Security Incident Reporting Requirements: The service provider shall report a security incident to the appropriate public jurisdiction identified contact within the manner and timeframe defined in the SLA.

c. Breach Reporting Requirements: If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall notify the appropriate public jurisdiction identified contact within [select 24/48/72] hours or sooner — unless shorter time is required by applicable law —



and take commercially reasonable measures to address the data breach in a timely manner.

Clause 9. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of a service provider and related to service provided under this contract.

a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.
b. The service provider, unless stipulated otherwise, shall notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document actions taken in response to the data breach, including any post-incident review of events and changes in business practices.
c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifying individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law; (4) providing a website or a toll-free number and call center for affected individuals required by state law; and (5) completing all corrective actions as reasonably determined by the service provider based on root cause. These costs shall not exceed the average per-record, per-person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach. All actions [1 through 5] are subject to this contract's limitation of liability.

Clause 10. Background Checks: The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud or any felony or misdemeanor offense with an authorized penalty of incarceration for up to one year. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information.

Clause 11. Non-Disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure

agreements and limit staff knowledge of customer data to that which is absolutely necessary to perform job duties.

Clause 12. Right to Remove Individuals: The public jurisdiction may at any time require the service provider remove from interaction with the public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall notify the service provider of its determination and its reasons for requesting the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.

Clause 13. Security: The service provider shall disclose its non-proprietary security protocols, processes, tools and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. The service provider's disclosures shall include information related to:

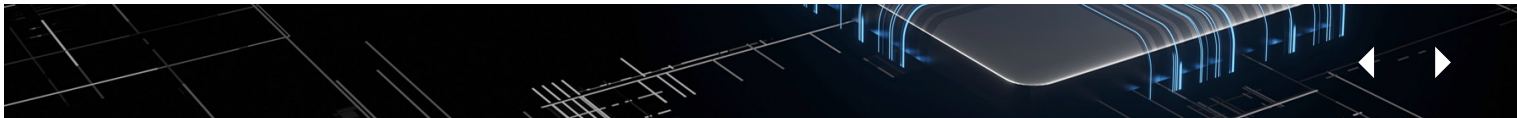
- Governance and compliance
- Standards and policies
- Security and risk assessments
- Continuous monitoring and alerting
- Privilege and identity access management
- Data protections
- Infrastructure and application protections
- Native cloud service provider SIEM/log management tools
- System health and resource monitoring
- Incident response and recovery

The public jurisdiction and the service provider shall understand each other's roles and responsibilities and document them within the SLA.

Clause 14. Access to Security Logs and Reports:

a. The service provider shall provide reports to the public jurisdiction directly related to the infrastructure that the service provider controls upon which the public jurisdiction account resides. Unless otherwise agreed to in the SLA, the service provider shall provide the public jurisdiction a history of all API calls for the public jurisdiction's account. This report shall include the identity of the API caller, the date and time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the service provider. The report will be sufficient to enable the public jurisdiction to perform security analysis, resource change tracking and compliance auditing.

b. The service provider and the public jurisdiction share security responsibilities. The service provider is responsible for providing a secure infrastructure (e.g., storage and servers) and virtualization/hypervisor. The service provider and the public jurisdiction typically share responsibility for identity, credential and access management; networking; and data. The



public jurisdiction is responsible for its secure guest operating system, middleware, runtime, applications, firewalls and other logs captured within the guest operating system.

The methods and conditions for access to logs/reports and the format for logs/reports are to be specified and agreed upon by both parties in the SLA. Specific shared responsibilities are identified within the SLA.

Clause 15. Retention, Preservation and Archival of Security Logs and Reports: The service provider shall retain security logs and reports in a usable format for a minimum of _____ (days, months, years) and a maximum retention/archival of _____ (days, months, years or for a specific period beyond the termination of the contract). The methods and timeframes for the retention, preservation (i.e., legal hold), and archival for the logs and reports will be specified and agreed upon by both parties in the SLA.

Clause 16. Encryption of Data at Rest: Not relevant to service model. Standards would be selected by the public jurisdiction.

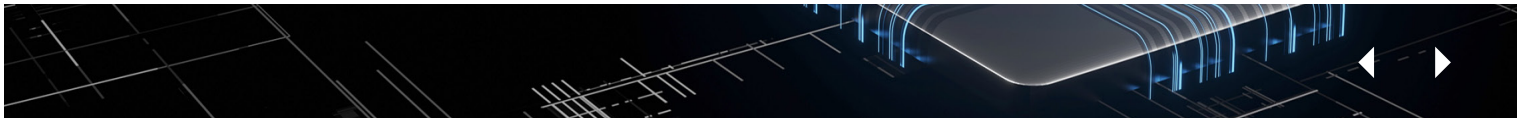
Clause 17. Contract Audit: The service provider shall cooperate with public jurisdiction audit of conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction. If information deemed confidential or proprietary must be reviewed during a contract compliance audit, either party may request the execution of a non-disclosure agreement (NDA), to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.

Clause 18: Data Center Audit: An annual audit as required by StateRAMP and/or FedRAMP shall be performed for all relevant data centers associated with provision of the cloud service at the data center provider's expense. Providers must grant the government's information security office access to view the audit and artifacts through StateRAMP, if applicable.

a. Some governments may accept a SOC 2 Type 2 audit annually for all relevant data centers associated with provision of the cloud service at the service provider's expense. The audit must be made available to the jurisdiction if requested under unilateral NDA or after being redacted.

Clause 19. Continuous Monitoring: The service provider shall, at the service provider's expense, conduct continuous monitoring of its compliance with security controls required within the contract. Continuous monitoring shall be conducted via one or a combination of the following methods approved by the public jurisdiction:

a. Reliance on StateRAMP authorization and independent assessments by third-party assessment organizations (3PAOs)
b. Reliance on FedRAMP authorization and independent assessments by 3PAOs
c. Review of control documentation by internal staff or 3PAOs



d. Acceptance of the service provider's third-party attestation (e.g. AICPA SOC2-Type 2 audit)
e. Self-assessment by the service provider

Continuous monitoring reports shall be provided to the public jurisdiction under mutual NDA.

Alternative: StateRAMP or FedRAMP shall provide continuous monitoring reports to the public jurisdiction and the 3PAO for the appropriate impact category under which the cloud service offering is authorized.

Clause 20. Responsibilities and Uptime Guarantee: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment are the responsibility of the service provider. The system shall be available 24/7/365, with agreed-upon maintenance downtime, and provide service to customers as defined in the SLA.

Clause 21. Change Control and Advance Notice: The service provider shall give advance written notice (to be determined at contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades or system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version to bring the system up to date or improve its characteristics. It usually includes a new version number.

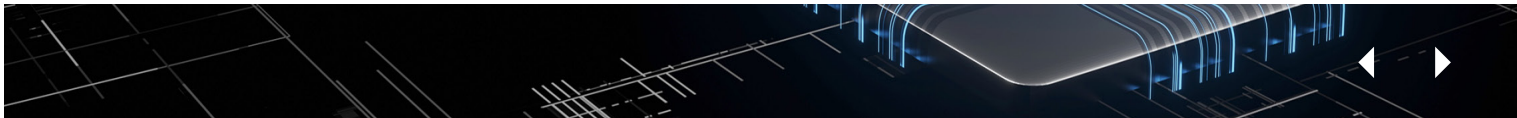
Clause 22. Subcontractor Disclosure: The service provider shall identify all strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider and who shall be involved in any application development and/or operations.

Clause 23. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan upon request and ensure the public jurisdiction's recovery time objective (RTO) of XXX hours/days is met. (XXX shall be negotiated by both parties.)

Clause 24. Compliance with Accessibility Standards: Not relevant to service model. Standards would be selected by the public jurisdiction.

Clause 25. Web Services: Not relevant to service model. Standards would be selected by the public jurisdiction.

Clause 26. Subscription Terms: Contractor grants to a purchasing entity a license to: (1) access and use the service for its business purposes; (2) for IaaS, use

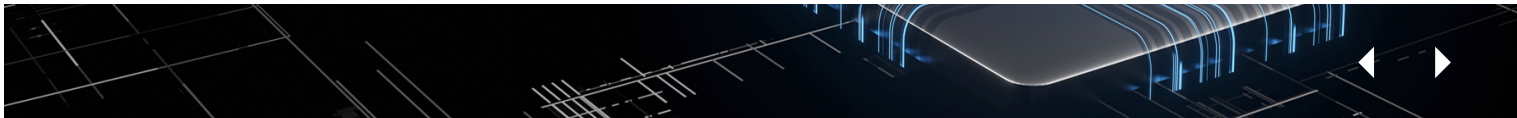


underlying software as embodied or used in the service; (3) view, copy, upload and download (where applicable), and use contractor's documentation.

Clause 27. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

Clause 28. Termination and Suspension of Service:

a. In the event of an early contract termination, the service provider shall allow the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content.
b. During any period of suspension, the service provider shall not intentionally erase any public jurisdiction digital content.
c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of 45 days after the effective date of a termination for convenience, or 60 days after the effective date of a termination for cause. After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of a termination for cause, the service provider will impose no fees the customer for access and retrieval of digital content.
d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all forms, such as disk, CD/ DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.



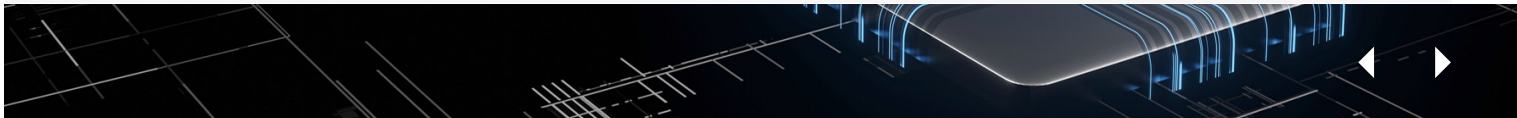
Appendix 2

Service Level Agreement (SLA)

The SLA is a subsection of the terms and conditions. It is separated as a subsection so that its content is treated more specifically to the particular business issues that the service handles. While most parts of the terms and conditions should be highly standardized, this short document is the place where contract-specific service level agreement content is addressed. We recommend that it occupy a section or page separate from the other sections.

Model SLA

1. Percentage uptime guarantee	99.90%
2. Intervals measured	Every 15 minutes during guaranteed periods
3. Time periods used for measuring uptime	Monthly, starting each first of month at 12:01 am Central Time
4. Committed periods during which uptime is guaranteed	Seven days/week, 2 am-12 midnight; Saturday
5. Exception periods, during which uptime is not guaranteed, in addition to agreed maintenance window.	Examples include: 1. Planned maintenance 2. Acts of God 3. Suspension of service due to legal reasons 4. Internet access outside control of provider
6. Maximun response time (for query & update functions), goal percentage	98% within four seconds
7. Maximum support response time	*Tier 1 support issues: 2 hours *Tier 2 issues: 4-6 hours *Tier 3 issues: 12+ hours *Tiers should be defined in SLA and may reflect a scale of standard issues to 'Code Red' service failures
8. Penalty or service credit calculation for recovery point objective failure interruption	5% off a future month service for each consecutive block of 12 hours of failure to meet recovery point objective
9. **Penalty or service credit calculation for service interruption	5% off a future month service for each block of three consecutive (at 15-minute intervals) failures to respond within 10 seconds



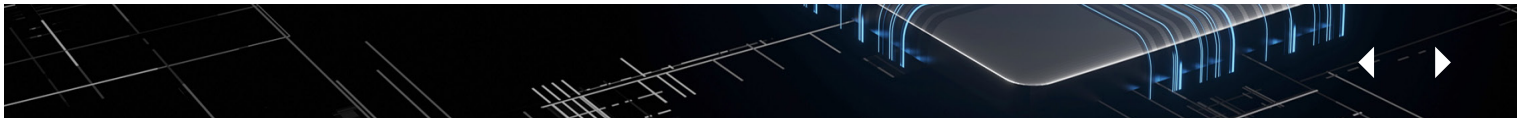
Appendix 3

Key Contact Information

This is a recommended document to include as a subsection to the terms and conditions. This document should be updateable and parties should make a point of reviewing active points of contact on an annual basis.

Model Key Contact Information

1. Customer contacts (primary & secondary) for operational and security emergencies
2. Customer contacts (primary & secondary) for contractual matters
3. Service provider contacts (primary & secondary) for operational and security emergencies
4. Service provider contacts (primary & secondary) for contractual matters



Appendix 4

Guiding Principles

Contracting for anything-as-a-service (XaaS) offerings can be confusing. There are different service models using different provider models that create a variety of options to consider. It can be difficult to determine the most appropriate service model. Whether it's a public cloud XaaS solution or private cloud model, a public jurisdiction must also consider a number of internal factors in order to make the best choice. These guiding principles can help as you consider procurement and contracts for XaaS.

1. We can have our cake and eat it too … if we can live with one flavor. XaaS providers offer value and benefits to the public due to scale and a standard business model. Consequently, unique requirements are counter to the model and should be discouraged where possible.

2. The law is the law. Public jurisdictions cannot enter into agreements that violate their laws. Providers and public jurisdictions must understand and respect statutory constraints. If the law truly prohibits a jurisdiction from accepting a particular service provider term or condition, then that term for condition must change, or the parties should not engage in a contractual relationship.

3. Want the business? Do what it takes. Public jurisdictions have unique requirements. If a service provider wants this business, it should understand the public environment and offer standard terms and conditions to which public jurisdictions can agree.

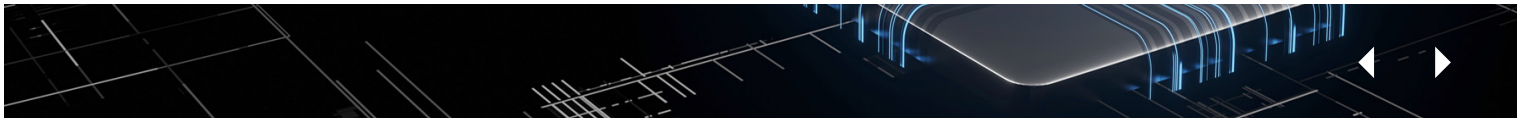
4. Not all service providers are created equal. The type of service to be acquired will determine which business model will be most advantageous. Public entities and service providers must work together to ensure they both clearly understand the requirements and share a common understanding of the service model in order to create appropriate contractual terms.

5. Data, data, understand the data. Public jurisdictions must understand and apply an appropriate security classification to their data. Consider the service provider's commitment to secure and protect the data based on the service model. If the service model is not right, don't use it.

6. It takes a partnership. Successful results between government and XaaS providers depend on a clear understanding of the roles and responsibilities of each based on the nature of the service model.

7. All good things must come to an end. Disengagement from the service relationship must be considered prior to the execution of the contract based on the specific service offering.

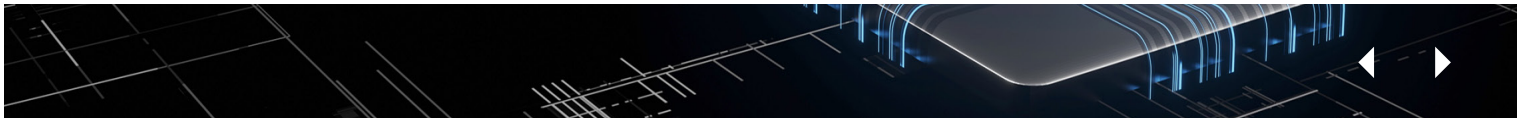
8. Pick the right dance partner. How well you dance depends on your partner. Picking a partner that is appropriate for your business needs is critical to successful results. Financial viability, maturity, agility, innovation, dependability and proven track record for similar clients are all factors to consider.



9. It's risky business. T&Cs are really about understanding how the public entity and the service provider share and manage risk in their relationship. Success requires a realistic assessment of the risks, a common understanding and a willingness to consider a variety of alternatives to effectively manage those risks.

10. Get by with a little help from your friends. Educate and engage other government policymakers to understand the benefits XaaS providers bring to government and include them early in the process when assessing if traditional contracting, control or auditing practices are the most effective way to protect the public's interest.

11. Trust, but verify. Controls should be commensurate with service provider model, type of data and risk.



Appendix 5

Procurement Approaches

Like IT service terms and conditions, sourcing methods have struggled to keep pace with rapidly evolving business technology alternatives driven by cloud service models. Traditional public procurement processes, designed to protect the public's interest, are challenged to find the proper balance between certainty and the flexibility necessary in today's market.

Traditional procurement methods with strict invitation to bid response rules require the proposer to comply with all the requirements of the solicitation or be rejected. These rules create a "take it or leave it" proposition for service providers. When this kind of sourcing method is used with subscription-based anything-as-a-service (XaaS) offerings, which by definition cannot be customized, procurements fail.

Often, traditional models attempt to prescribe solutions. It is important for a state or local government to understand business needs, but XaaS providers frequently limit customization. Prescriptive solutions might be right for some purchases, but not for XaaS. These new service models — driven by ever-changing technology innovation — do not include the purchase of either technology or software. XaaS models include the purchase of services that can be configured, but not customized, to meet the customer's needs.

Traditional procurement practices that prevent these new service models from fairly competing deprive governments and their taxpayers of modern, effective tools for managing their increasing digital demands.

Procurement methods are at their core a decision process with objective analytics upon which to base the decision. Decisions should be transparent and competitive and meet the public jurisdiction's business needs. If procurement processes do not support the acquisition of today's modern services, changes are needed in the practices, rules or statutes.

Here are some approaches or best practices that have improved public procurement results while protecting the public's interest. For some jurisdictions, specific statutes or ordinances may prevent adoption, but there are still useful takeaways from the examples that can help any jurisdiction improve their outcomes for XaaS procurements.

Take Advantage of Negotiations

Evolving business models require the RFP process to be flexible to allow for negotiations or discussions to receive clarification. Some state laws support the process of negotiating terms and conditions in this fashion. By including the ability to clarify terms and conditions throughout discussions or negotiations, the jurisdiction avoids the problem of rejecting providers that might be able to meet the jurisdiction's needs. One typical process is for the jurisdiction to identify certain terms in advance that it is willing to discuss and negotiate before award. By negotiating acceptable terms with the proposer in advance, the jurisdiction ensures it will get the best fit for the award and resolve differences

that otherwise might result in the rejection of an effective proposal.

There are several ways discussions or negotiations may occur. In some cases, the jurisdiction — through the development of its business case and market research — has a good idea of the terms and conditions likely to require negotiation. The jurisdiction can identify those in its RFPs. The jurisdiction can then avoid being forced to reject proposals as nonresponsive that it may otherwise find attractive.

Another way some jurisdictions determine when negotiations may be required is through the issuance of a draft RFP. Feedback from potential proposers can help identify terms that will not work within the market. This approach allows the jurisdiction to see which terms are problematic and provides the jurisdiction with the option to negotiate. Some RFPs require potential proposers to officially protest specifications they believe are unduly restrictive. This method, while appearing somewhat contentious, can allow the jurisdiction to identify terms and conditions that will be a problem for suppliers and amend the RFP before proposals are submitted. If the jurisdiction does not have the authority to negotiate specific items, that can be made known and help the jurisdiction avoid rejecting otherwise attractive offers.

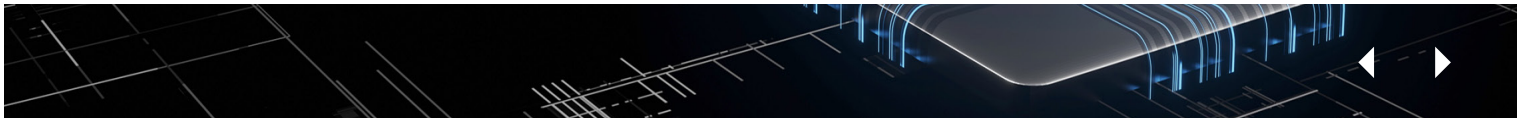
It is possible to negotiate terms before the final contract award with service providers when the law does not require a specific term or condition. Jurisdictions should change their policies, standards and rules to allow for greater use of negotiations in the competitive selection process.

Move Away from Requirements-Based Procurement

Traditional IT system solicitations often rely upon business requirements developed through a series of work sessions that document how the agency currently conducts its business. Getting these requirements perfectly right is a difficult process in the best of circumstances. If successful, these business requirement sessions document the historic business process that may, in itself, be antiquated and inefficient. If those requirements are then made a part of the RFP to be replicated by the service provider, the only solution may be a custom-made solution. This model does not work well for XaaS procurements.

Public agencies must understand their business objectives and performance needs, but they should not be so prescriptive in their solicitation that they dictate the system design and functionality. Instead, the jurisdiction should shop for the best business fit.

Rather than evaluate proposals on hundreds or even thousands of prescriptive requirements that may not lead to successful service, public jurisdictions should include evaluation criteria based on how well the service meets or enhances their business objectives, whether it achieves their performance needs and its ability to fine-tune business rules through configuration. Public jurisdictions can make big gains in quality and effectiveness of service in this way through XaaS applications.



Keep Negotiations Moving Forward

A great concern for the parties in any negotiation is how long it will take to reach final agreement. Delays are the enemy of everyone who has a stake in the award of an XaaS contract. Stalled procurements are often caused by long and drawn-out negotiations. Identifying and using generally agreeable standard terms and conditions at the beginning of the procurement helps limit negotiations to just those terms that are unique and must be tailored to the specific service. It is helpful if all parties do their homework to understand their needs, as well as their partner's needs, before negotiations begin. Successful contracts depend on successful partnerships. Negotiation strategies that find workable solutions and make both parties successful produce the best results over the life of the contract.

Create a Timeline for Negotiations

Setting a realistic, defined timeline for completion of negotiations can help keep everything on track and the procurement moving forward. If negotiations are not completed on time, jurisdictions can reserve the right to move to the next proposer. This approach requires both sides to act responsibly by fulfilling their obligations in a negotiation. It also requires tracking and documenting progress, and assigning responsibilities for task completions during negotiations.

Start with a Business Problem-Based Solicitation

The requirements section of a procurement document should always include a background statement that, among other things, defines the business problem to be solved. By clearly understanding and articulating the business problem they need to solve, jurisdictions can focus on the things they are best at and leave the range of potential solutions up to the service provider. This approach helps avoid overly prescriptive specifications and encourages innovation and a broader range of solutions on the part of proposers.

Minimize Mandatory Requirements

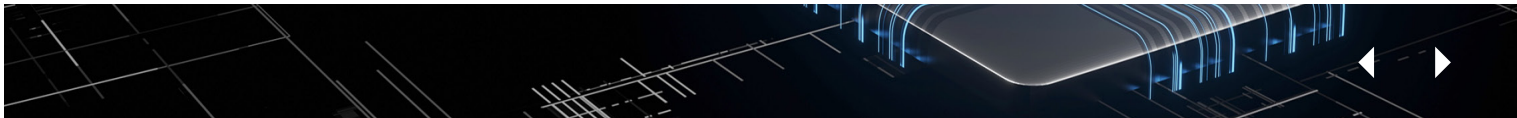
RFPs that include mandatory terms that are not negotiable are essentially a "take it or leave it" proposition for providers. If these terms are not acceptable, they can cause an otherwise acceptable proposal to be rejected. Jurisdictions should carefully consider the consequences of using mandatory terms unless it is a requirement of law. Jurisdictions should be certain about the need for a mandatory requirement or term because future negotiations are preempted by their classification as mandatory. The use of mandatory requirements or terms should be kept to an absolute minimum.

Establish Model Terms as Standards

The model terms and conditions could be used as a standard with which service providers certify compliance as a part of the RFP process. If there is agreement on standards, then a selection process can evaluate all potential service providers based on reasonable criteria calculated to acceptably manage identified risks and achieve the business needs of client agencies.

Develop National Minimum Standards

The creation of a nationally recognized standard, derived from best practices in XaaS operations — including data



handling, data security, confidentiality, availability, etc. — could streamline the procurement of XaaS in state and local governments that use a stricter and customized assessment of responsiveness. It would allow public jurisdictions to evaluate unique proposal offerings against the adopted national standard. By relying on the proposal's certification of compliance against the standard, the procuring organization could use minimum compliance against the standard as the baseline for evaluation of the proposal. Additional functionality beyond the standard could also be used for a more meaningful analysis of "value-added options" or "best value" in an RFP. Requiring the service provider to continue compliance with the standard over the life of the contract can also help keep the service current.

Improve Communication

Any effective procurement process for new and evolving business models such as XaaS requires a good deal of communication before the issuance of a solicitation, during the solicitation and evaluation, and in contract execution. Jurisdictions should examine and revise procurement processes, policies and rules wherever possible to eliminate barriers to effective communication.

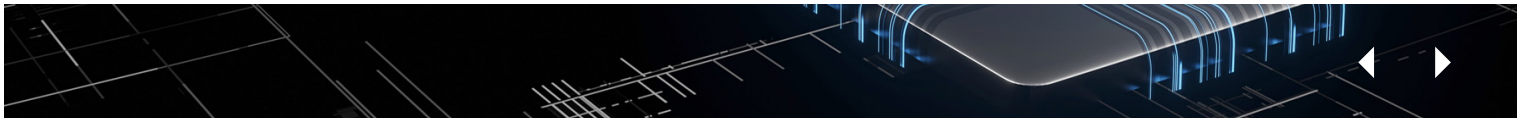
Conduct Market Research

Jurisdictions that conduct effective market research and share their background information and business needs in open forums with service providers before issuing a solution increase their chance for a successful procurement. Dialogue with service providers can help the jurisdiction understand various approaches in the market and how service models work. It can also help test assumptions. Other effective methods of market exploration before issuing a formal solicitation may include issuing a draft RFP to encourage provider comments and responses and holding one-on-one meetings with interested providers. The more a jurisdiction understands what is available in the market and how those solutions might work for its business needs, the better positioned it is to develop an effective business case and create an effective sourcing strategy. The more service providers understand the needs of the jurisdiction, the better prepared they are to offer the optimal solutions.

This exploratory process can also help the service provider and jurisdiction understand when a provider's offering is not a good match for the jurisdiction's business needs. In these cases, effective communication can help both parties be smart about what will and will not work in advance prior to their undertaking the burden of a formal procurement process. Procurement policies and rules should promote the increased use of market research to include public discussion forums, online research, service provider meetings and the sharing of background information.

Use Demonstrations

Often, RFPs include product demonstration scoring. This component allows the jurisdiction to evaluate the fit and, to some degree, the user acceptance of service provider solutions. Demonstrations should be encouraged whenever possible. Some jurisdictions have successfully used request



for demonstration (RFD) sourcing methods to award technology contracts. The scoring of the demonstration determined the award. An RFP typically includes some consideration of costs. With RFD awards, the jurisdiction could also consider cost as a part of the evaluation process. This approach can be an effective way for end users to test XaaS offerings and for the award decision to reflect the best fit for the jurisdiction's business needs.

This could be coupled with a certification process that invites service providers to pre-certify their agreement to abide by key standards like the model terms and conditions described in this document. Policies, rules and statutes should permit demonstration-based awards.

Implement a Multiple Round Selection Process

The use of multi-step processes, which narrow the field of total responses to a short list of final proposals most likely to result in award, can help a jurisdiction be more specific in the second round selection process. During a second round, the use of pilots, demonstrations or supplemental negotiations may result in gaining better clarity as to the fit of the proposed services to the jurisdiction's business needs. It also helps the jurisdiction maintain a competitive environment.

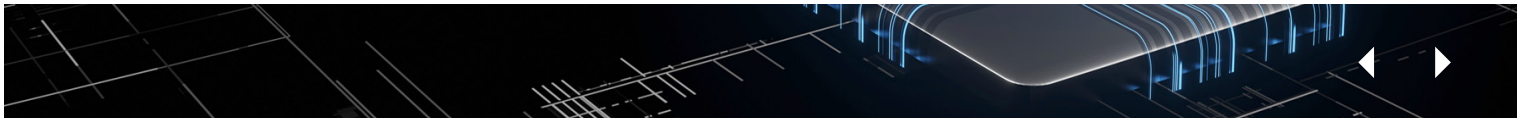
Permit Multiple Awards

RFP or other sourcing methods may be designed to award to either a single service provider or multiple service providers. The sourcing document must describe if a single award, multiple awards or some combination will be made. The ability to negotiate final awards with each service provider is critical. The solicitation must be clear regarding how awards are determined.

Depending on the need, it may be best for the jurisdiction to identify classes of services it needs and award indefinite delivery/indefinite quantity (IDIQ) contracts to a pool of potential suppliers. Agencies within the jurisdiction may then select suppliers from the pool. Effective use of multiple awards for XaaS applications can be very popular with customer agencies. It gives them options and allows them to select from service provider applications that best meet their needs. With rapidly emerging service models, it is a good idea to include the ability to reopen the award process annually to add new service providers. Multiple awards that result in contracts for most proposers in the class, rather than just the most competitive, are less controversial, but also may not result in the best pricing. A jurisdiction must consider such tradeoffs in relationship to its acquisition strategy and business case.

Create Alternative Sourcing Processes

Some states have the statutory authority to create new sourcing models that do not follow statutory requirements for competitive sealed proposals or invitations to bid. Known as "special procurement," the American Bar Association (ABA) Model Procurement Code sets out a competitive sourcing method that in limited circumstances may be used "where the application of all requirements of competitive bidding or competitive proposals is deemed to be contrary to the public interest." Several states have



passed similar laws. The flexibility afforded under these statutes allows for the design of accountable and innovative sourcing approaches that are not constrained by traditional sourcing methods. Public jurisdictions should have the ability in rule and statute to permit the development of effective sourcing methods when traditional methods will not work.

New procurement sourcing models allow governments to take advantage of new service models. Public jurisdictions that support and encourage innovation in procurement processes can benefit from more effective procurement outcomes. Successful solutions should be replicated and shared. Unsuccessful approaches should be evaluated from a lessons learned perspective and then discarded. By incubating and sharing successful procurement models, governments can improve their collective ability to successfully acquire the services they need.

The Importance of Cooperative Contracting Opportunities

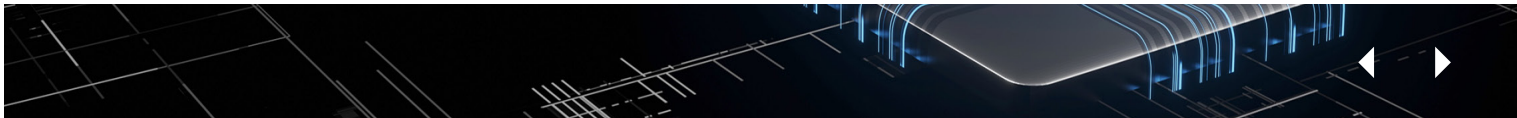
The U.S. Communities Purchasing Alliance — jointly sponsored by the National Association of Counties, Association of School Business Officials, National Institute of Government Purchasing, the National League of Cities and the U.S. Conference of Mayors — offers state and local governments the opportunity to participate and purchase from cloud service contracts. U.S. General Services Administration Schedule 70 Technology Contracts are also available to state and local governments through the cooperative purchasing program.

One of the best opportunities for effective public acquisition of XaaS contracts is with a multi-jurisdictional cooperative procurement. There is no doubt that IT service contracting by public jurisdictions will continue to grow, but one-off contracting processes that complicate service provider responses can limit it.

Smaller jurisdictions potentially stand to benefit from XaaS solutions, but they may lack the resources to put effective sourcing solutions together and come to agreement on terms and conditions. By leveraging multi-jurisdiction teams in the development and award of a menu of XaaS contracts, smaller jurisdictions can efficiently acquire service provider solutions that meet their needs and protect their interests.

Cooperative purchases can provide a supplier benefit by aligning disparate jurisdiction purchasers around a common set of terms and conditions and a single master contract award rather than different ones in each jurisdiction. Multi-jurisdiction procurements succeed because service providers have a standard acquisition process, terms and conditions, and ordering mechanism to navigate rather than different ones in each jurisdiction. That frees up providers to assist the jurisdiction in selecting the best fit.

Another option is to participate with another jurisdiction in a joint cooperative purchase. State laws or local ordinances

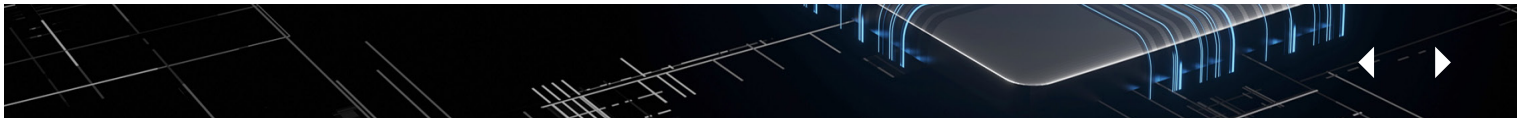


may prevent a state from "piggy backing" on another jurisdiction's contract, unless they were included in the solicitation at the beginning. Before buying from another jurisdiction's contract, it's a good idea to check local laws to see what is permissible.

As a vehicle for XaaS contracts, multi-jurisdictional cooperative purchasing is an efficient and effective procurement method. It resolves a number of issues in ways that benefit both the participating jurisdiction and service providers. Multi-jurisdictional cooperative purchasing:

- Addresses an unmet need for a more organized and effective way to aggregate multiple states' demands for common IT services and commodities. Individual state IT service purchases do not leverage the opportunity of volume buying or contracting efficiencies that come from multi-jurisdiction procurements.
- Aligns with XaaS models. Both cooperative purchasing and XaaS models benefit from consolidated volumes and common approaches to terms and conditions. In this way, one line of code can serve many.
- Creates a contractual mechanism for standard requirements and terms and conditions that help define realistic and practical expectations between public entities and service providers.
- Enables purchases from the cooperative's contract. Public jurisdictions want the ability to purchase from each other's contracts, but few have the statutory authority to do so without an upfront, coordinated effort. Most states now have authority to participate in cooperative procurements. Cooperative state procurements are typically made available for political subdivisions within the state.
- Provides negotiation leverage for cloud-based solutions through practical and aligned public requirements and aggregated customer volume.

Cooperative purchasing avoids duplication of effort. It leads to greater volume aggregation and typically drives more favorable pricing. With the continued evolution of cloud computing, the aggregation of market demand should provide leverage beyond what an individual jurisdiction could hope to achieve on its own and lead to benefits during this time of market realignment for both state and local governments and service providers.



Appendix 6

Glossary

"Anything as a Service" (XaaS) refers to cloud-based services delivered to customers over the internet. Typically, the services are purchased on a subscription model. The most common service models used in government today are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), but others are available such as Communications-as-a-Service (CaaS). The service offering will be extensive.

"Authorized Persons" as used in this document means the service provider's employees, contractors, subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services.

"Data Breach" as used in this document means the unauthorized access by non-authorized person(s) that results in the use, disclosure or theft of a public jurisdiction's unencrypted personal data.

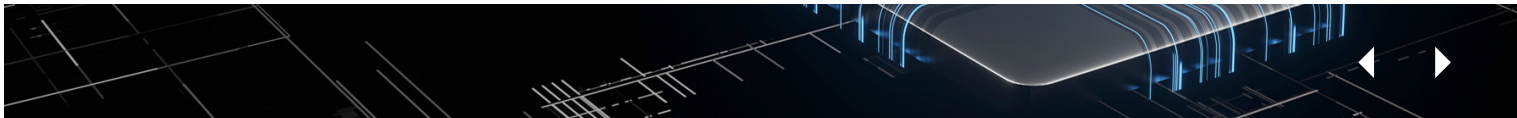
"Hybrid cloud" is a cloud computing environment which uses a mixture of on-premises, private cloud and third-party cloud services with orchestration between the two platforms. Hybrid cloud environments require a governance model that encompasses all of the environments used in any particular deployment.

"Individually Identifiable Health Information" as used in this document means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[28]

"Infrastructure-as-a-Service" (IaaS) as used in this document is defined as the capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and possibly limited control of select networking components (e.g., host firewalls).

"Personal Data" means data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number and credit or debit card numbers; or protected health information (PHI) relating to a person.

"Platform-as-a-Service" (PaaS) as used in this document is defined as the capability provided to the consumer to



deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the service provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.[29]

"Protected Health Information" (PHI) as used in this document is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.[30]

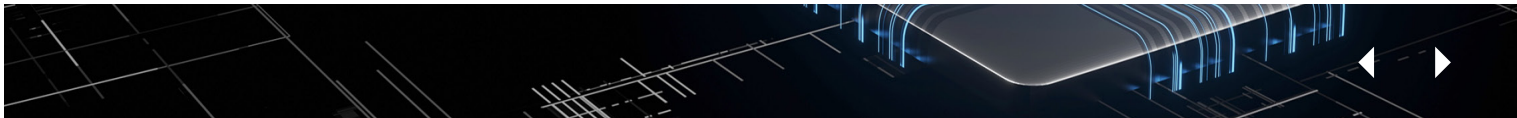
"Personally Identifiable Information" (PII) has no one definition that applies to all states. Generally, PII refers to a combination of data elements (e.g., Social Security number, driver's license or other government-issued identification number, passport number, financial account number, or credit or debit card number in combination with security codes) that, when linked to the individual's first name or first initial and their last name, and not encrypted, could lead to the loss, theft or unauthorized use of the individual's personal information.

"Public Jurisdiction" as used in this document means any government or government agency that uses these terms and conditions.

"Public Jurisdiction Data" as used in this document means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware or the service provider's hardware; or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

"Security Incident" means the potentially unauthorized access by non-authorized persons to personal data or non-public data that could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of a service provider. A security incident may or may not turn into a data breach.

"Service Level Agreement" (SLA) means that part of the written agreement between both the public jurisdiction and the service provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises (i.e., metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and

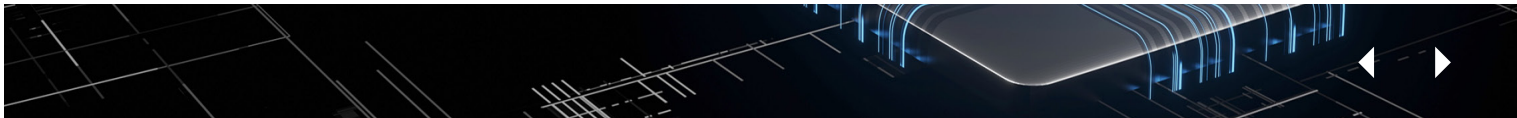


notice requirements, (5) how disputes are discovered and addressed, and (6) any remedies for performance failures.

"Service Provider" means the contractor, their employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

"Software-as-a-Service" (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[31]

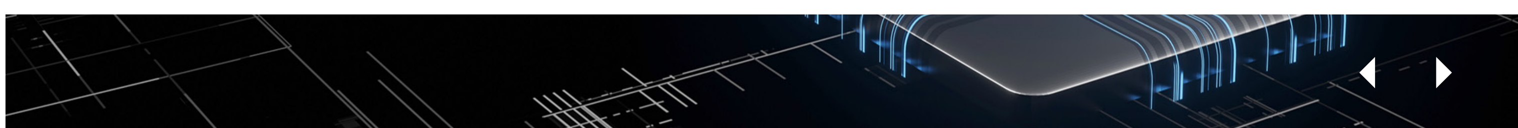
"Statement of Work" (SOW) is a written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.



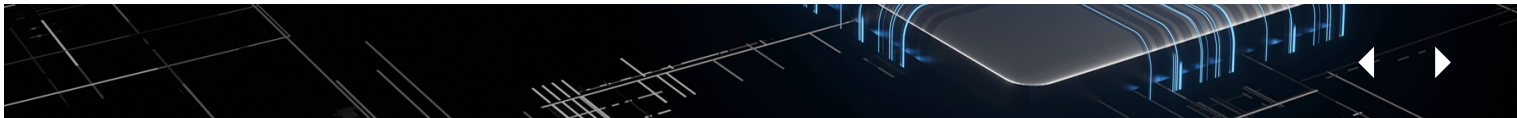
Appendix 7

Clause Comparison Matrix

Plain Language	SaaS	PaaS	IaaS
1. Definition of terms. Defines the service model and terms used. (See Appendix 1 for additional detail.)	**1. Software-as-a-Service (SaaS)** as used in this document is the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or individual application capabilities, with the possible exception of limited user-specific application configuration settings.	**1. Platform-as-a-Service (PaaS)** as used in this document is the capability provided to the consumer to deploy onto a cloud infrastructure consumer-created or acquired applications that are created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.	**1. Infrastructure-as-a-Service (IaaS)** as used in this document is the capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications and possibly limited control of select networking components (e.g., host firewalls).
2. The public jurisdiction owns all its data. The service provider will not access the data except as needed to do the work of the contract as authorized by the public jurisdiction.	**2. Data Ownership:** The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data except (1) during data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.	**2. Data Ownership:** The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data except (1) during data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.	**2. Data Ownership:** The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data except (1) during data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

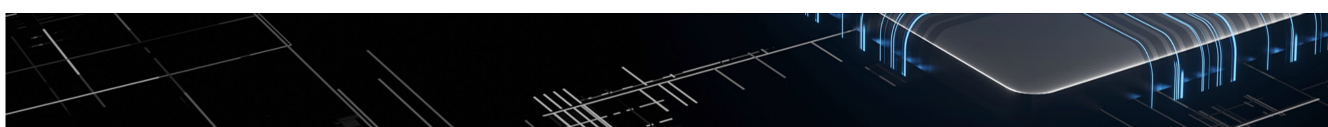


Plain Language	SaaS	PaaS	IaaS
3. The public jurisdiction owns all personal information. The service provider will protect it and will not use the data for anything not related to the customer. The service provider will encrypt personal data and non-public data both at rest and in transit.	**3. Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. The service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions: a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. Such security measures shall be in accordance with NIST SP 800-53 (current version) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. b. All data obtained by the service provider in the performance of this contract shall become and remain property of the public jurisdiction. c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (current version). Unless otherwise stipulated, the service provider is responsible for encryption of the personal data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the SLA or otherwise made a part of this contract. d. Unless otherwise stipulated, the public jurisdiction is responsible for identifying data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract. e. Data or processes which belong to or are intended for the use of a public jurisdiction or its officers, agents or employees shall never be copied, disclosed or retained by the service provider or any party related to the service provider for use in any transaction that does not include the public jurisdiction. f. The service provider shall not use any information collected in connection with the service issued from this contract for any purpose other than fulfilling the service.	**3. Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. The service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information within its control and comply with the following conditions: a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data within its control. Such security measures shall be in accordance with NIST SP 800-53 (current version) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. b. All data obtained by the service provider within its control in the performance of this contract shall become and remain property of the public jurisdiction. c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (current version). The SLA and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the statement of work and the contract are silent, then the public jurisdiction is responsible for encryption and access control. d. Unless otherwise stipulated, the public jurisdiction is responsible for identifying data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract. e. Data or processes which belong to or are intended for the use of a public jurisdiction or its officers, agents or employees shall never be copied, disclosed or retained by the service provider or any party related to the service provider for use in any transaction that does not include the public jurisdiction.	**3. Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. The service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information within its control and comply with the following conditions: a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data within its control. Such security measures shall be in accordance with NIST SP 800-53 (current version) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. b. All data obtained by the service provider within its control in the performance of this contract shall become and remain property of the public jurisdiction. c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (current version). The SLA and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the statement of work and the contract are silent, then the public jurisdiction is responsible for encryption and access control. d. Unless otherwise stipulated, the public jurisdiction is responsible for identifying data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract. e. Data or processes which belong to or are intended for the use of a public jurisdiction or its officers, agents or employees shall never be copied, disclosed or retained by the service provider or any party related to the service provider for use in any transaction that does not include the public jurisdiction.

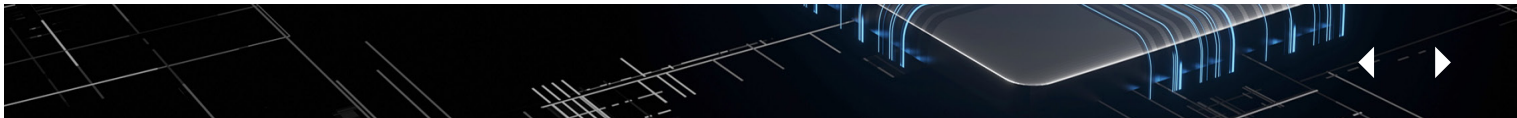


Plain Language	SaaS	PaaS	IaaS
4. Public jurisdiction data must be managed with respect to privacy.	**4. Data Privacy:** The service provider's privacy controls must abide by the following: a. No type of data mining may be performed on any public jurisdiction data without permission from the public jurisdiction. This includes mining location data from users of applications running on behalf of the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls. b. No public jurisdiction data may be sold or transferred to any third party, including service provider affiliates, without permission from the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls.	**4. Data Privacy:** The service provider's privacy controls must abide by the following: a. No type of data mining may be performed on any public jurisdiction data without permission from the public jurisdiction. This includes mining location data from users of applications running on behalf of the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls. b. No public jurisdiction data may be sold or transferred to any third party, including service provider affiliates, without permission from the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls.	**4. Data Privacy:** The service provider's privacy controls must abide by the following: a. No type of data mining may be performed on any public jurisdiction data without permission from the public jurisdiction. This includes mining location data from users of applications running on behalf of the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls. b. No public jurisdiction data may be sold or transferred to any third party, including service provider affiliates, without permission from the public jurisdiction in accordance with NIST SP 800-53 (current version) Privacy Controls.
5. The service provider shall not store any of the public jurisdiction's non-public data outside the U.S. Public jurisdictions retain ownership and control of their data, and they should assert responsibility for replication of their data in primary and secondary locations.	**5. Data Location**: The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S in accordance with NIST SP 800-53 (current version). The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide 24/7 technical user support using a Follow the Sun model, unless otherwise prohibited in this contract.	**5. Data Location:** The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S in accordance with NIST SP 800-53 (current version). The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide 24/7 technical user support using a Follow the Sun model, unless otherwise prohibited in this contract.	**5. Data Location:** The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S in accordance with NIST SP 800-53 (current version). The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support. The service provider may provide 24/7 technical user support using a Follow the Sun model, unless otherwise prohibited in this contract.
6. Access to public jurisdiction data must be closely guarded.	**6. Data Access:** The service provider is responsible for: a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800-53 (current version) Access Controls. b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the public jurisdiction for Follow the Sun technical support under the contract. c. Maintaining government data and allowing the downloading of that data for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After this period, the service provider will destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/deletion to the public jurisdiction.	**6. Data Access:** The service provider shall be responsible for: a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800-53 (current version) Access Controls. b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the public jurisdiction for Follow the Sun technical support under the contract. c. Maintaining government data and allowing the downloading of that data for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After this period, the service provider will destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/deletion to the public jurisdiction.	**6. Data Access:** The service provider shall be responsible for: a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800-53 (current version) Access Controls. b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the public jurisdiction for Follow the Sun technical support under the contract. c. Maintaining government data and allowing the downloading of that data for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After that period, the service provider will destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/deletion to the public jurisdiction.

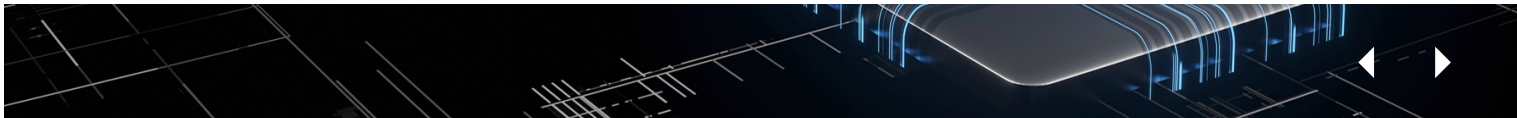
Plain Language	SaaS	PaaS	IaaS
7. The public jurisdiction can import or export its data when needed and as frequently as required.	**7. Import and Export of Data:** The public jurisdiction shall have the ability to import or export data: a. In piecemeal or in entirety at its discretion without interference and with support from the service provider as described in the contract or service level agreement. This includes the ability for the public jurisdiction to import or export data to/from other service providers. b. At intervals as frequent as the public jurisdiction requires.	**7. Import and Export of Data:** The public jurisdiction shall have the ability to import or export data: a. In piecemeal or in entirety at its discretion without interference and with support from the service provider as described in the contract or service level agreement. This includes the ability for the public jurisdiction to import or export data to/from other service providers. b. At intervals as frequent as the public jurisdiction requires.	**7. Import and Export of Data:** The public jurisdiction shall have the ability to import or export data: a. In piecemeal or in entirety at its discretion without interference and with support from the service provider as described in the contract or service level agreement. This includes the ability for the public jurisdiction to import or export data to/from other service providers. b. At intervals as frequent as the public jurisdiction requires.
8. The service provider will notify the public jurisdiction of a security incident or breach.	**8. Security Incident or Data Breach Notification**: The service provider shall inform the public jurisdiction of any security incident or data breach. a. Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract. b. Security Incident Reporting Requirements: The service provider shall report a security incident to the appropriate public jurisdiction identified contact within the manner and timeframe defined in the SLA. c. Breach Reporting Requirements: If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall notify the appropriate public jurisdiction identified contact within [select 24/48/72] hours or sooner, unless shorter time is required by applicable law, and take commercially reasonable measures to address the data breach in a timely manner.	**8. Security Incident or Data Breach Notification**: The service provider shall inform the public jurisdiction of any security incident or data breach. a. Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract. b. Security Incident Reporting Requirements: The service provider shall report a security incident to the appropriate public jurisdiction identified contact within the manner and timeframe defined in the SLA. c. Breach Reporting Requirements: If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall notify the appropriate public jurisdiction identified contact within [select 24/48/72] hours or sooner, unless shorter time is required by applicable law, and take commercially reasonable measures to address the data breach in a timely manner.	**8. Security Incident or Data Breach Notification**: The service provider shall inform the public jurisdiction of any security incident or data breach. a. Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract. b. Security Incident Reporting Requirements: The service provider shall report a security incident to the appropriate public jurisdiction identified contact within the manner and timeframe defined in the SLA. c. Breach Reporting Requirements: If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall notify the appropriate public jurisdiction identified contact within [select 24/48/72] hours or sooner, unless shorter time is required by applicable law, and take commercially reasonable measures to address the data breach in a timely manner.



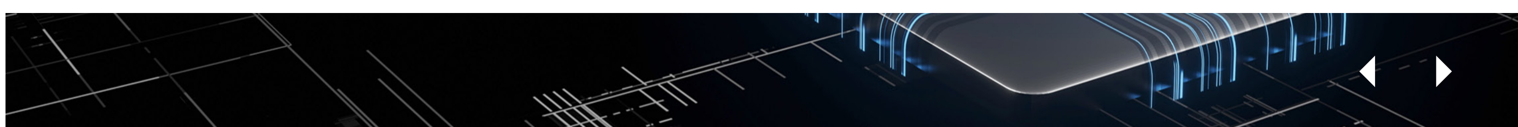
Plain Language	SaaS	PaaS	IaaS
9. If a service provider is responsible for a breach, it will pay the cost of the breach investigation, resolution, notification, credit monitoring and call centers up to a set amount per record/ per person. The service provider will take corrective action subject to any limitation of liability in the contract.	**9. Breach Responsibilities:** This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider. a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if the service provider reasonably believes there has been a security incident. b. The service provider, unless stipulated otherwise, shall notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document actions taken in response to the data breach, including any post-incident review of events and changes in business practices. c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifying individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law; (4) providing a website or a toll-free number and call center for affected individuals required by state law; and (5) completing all corrective actions as reasonably determined by the service provider based on root cause. These costs shall not exceed the average per-record, per-person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach. All actions [1 through 5] are subject to this contract's limitation of liability.	**9. Breach Responsibilities:** This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider and related to the service provided under this contract. a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident. b. The service provider, unless stipulated otherwise, shall notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document actions taken in response to the data breach, including any post-incident review of events and changes in business practices. c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifying individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law; (4) providing a website or a toll-free number and call center for affected individuals required by state law; and (5) completing all corrective actions as reasonably determined by the service provider based on root cause. These costs shall not exceed the average per-record, per-person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach. All actions [1 through 5] are subject to this contract's limitation of liability.	**9. Breach Responsibilities:** This section only applies when a data breach occurs with respect to personal data within the possession or control of a service provider and related to the service provided under this contract. a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident. b. The service provider, unless stipulated otherwise, shall notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document actions taken in response to the data breach, including any post-incident review of events and changes in business practices. c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifying individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law; (4) providing a website or a toll-free number and call center for affected individuals required by state law; and (5) completing all corrective actions as reasonably determined by the service provider based on root cause. These costs shall not exceed the average per-record, per-person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach. All actions [1 through 5] are subject to this contract's limitation of liability.



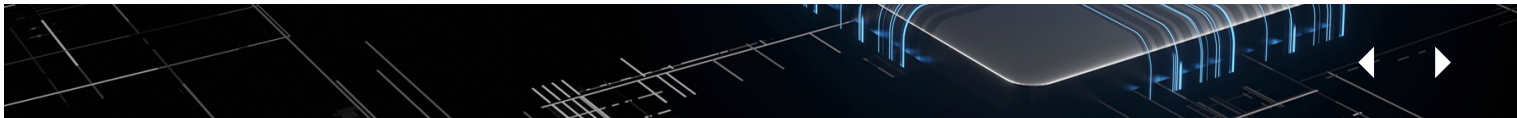
Plain Language	SaaS	PaaS	IaaS
10. The service provider will perform background checks on staff, including subcontractors. The service provider will not use staff who have criminal convictions.	**10. Background Checks:** The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information.	**10. Background Checks:** The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information.	**10. Background Checks:** The service provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information.
11. The service provider will limit staff knowledge of data and separate duties to protect the data. Non-disclosure agreements are required of service provider staff.	**11. Non-Disclosure and Separation of Duties:** The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.	**11. Non-Disclosure and Separation of Duties:** The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.	**11. Non-Disclosure and Separation of Duties:** The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.
12. The public jurisdiction may have the service provider remove staff.	**12. Right to Remove Individuals:** The public jurisdiction may at any time require that the service provider remove from interaction with the public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall notify the service provider of its determination and its reasons for requesting the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.	**12. Right to Remove Individuals:** The public jurisdiction may at any time require that the service provider remove from interaction with the public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall notify the service provider of its determination and its reasons for requesting the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.	**12. Right to Remove Individuals:** The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with the public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.



Plain Language	SaaS	PaaS	IaaS
13. The service provider will disclose its non-proprietary security protocols, processes, tools and technical limitations. The SLA will document individual security roles for the service provider and the public jurisdiction, as well as roles that are shared among the two organizations.	**13. Security:** The service provider shall disclose its non-proprietary security protocols, processes, tools and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. The service provider's disclosures shall include information related to: • Governance and compliance • Standards and policies • Security and risk assessments • Continuous monitoring and alerting • Privilege and identity access management • Data protections • Infrastructure and application protections • Native cloud service provider security information and event management (SIEM)/Log management tools • System health and resource monitoring • Incident response and recovery The public jurisdiction and the service provider shall understand each other's roles and responsibilities for security and document them within the SLA.	**13. Security:** The service provider shall disclose its non-proprietary security protocols, processes, tools and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. The service provider's disclosures shall include information related to: • Governance and compliance • Standards and policies • Security and risk assessments • Continuous monitoring and alerting • Privilege and identity access management • Data protections • Infrastructure and application protections • Native cloud service provider security information and event management (SIEM)/Log management tools • System health and resource monitoring • Incident response and recovery The public jurisdiction and the service provider shall understand each other's roles and responsibilities for security and document them within the SLA.	**13. Security:** The service provider shall disclose its non-proprietary security protocols, processes, tools and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. The service provider's disclosures shall include information related to: • Governance and compliance • Standards and policies • Security and risk assessments • Continuous monitoring and alerting • Privilege and identity access management • Data protections • Infrastructure and application protections • Native cloud service provider security information and event management (SIEM)/Log management tools • System health and resource monitoring • Incident response and recovery The public jurisdiction and the service provider shall understand each other's roles and responsibilities for security and document them within the SLA.

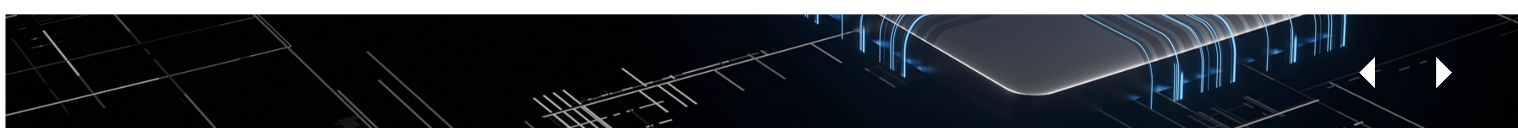


Plain Language	SaaS	PaaS	IaaS
14. The service provider will provide security logs and reports to the public jurisdiction for its accounts in a format agreed to in the SLA. The reports include latency statistics, date and time stamps, user access IP addresses, source and destination IP addresses, system events, log-on/ authentication attempts, user access history, account changes, security policy changes, system configuration changes, usage information and transaction size, and security logs for the data covered under the contract. The methods and conditions for authorized access to logs/reports and the format for the logs/reports shall be specified and agreed upon by both parties in the SLA.	**14. Access to Security Logs and Reports:** a. The service provider shall provide reports to the public jurisdiction in a format specified in the SLA agreed to by the service provider and the public jurisdiction. Reports shall include latency statistics, date and time stamps, user access IP addresses, source and destination IP addresses, system events (e.g., failed and successful events — system shutdown or starting a service, errors, anomalous/abnormal activity, etc.), log-on/authentication attempts (failed and successful), user access history, account changes (e.g., account creation and deletion, account privilege assignment, etc.), security policy changes, system configuration changes, usage information (e.g., number of transactions occurring in a certain period of time) and transaction size (e.g., email message size, file transfer size, etc.), and security logs for all public jurisdiction data related to this contract. b. The service provider and the public jurisdiction share security responsibilities. The service provider is responsible for providing a secure infrastructure (e.g., storage and servers), virtualization/ hypervisor, operating system, middleware and runtime, applications, and networking. The service provider and public jurisdiction typically share responsibilities for identity, credential and access management, and data security. The methods and conditions for authorized access to logs/reports and the format for the logs/reports shall be specified and agreed upon by both parties in the SLA. Specific shared responsibilities are identified in the SLA.	**14. Access to Security Logs and Reports:** a. The service provider shall provide reports to the public jurisdiction in a format as specified in the SLA agreed to by the service provider and the public jurisdiction. Reports will include latency statistics, date and time stamps, user access IP addresses, source and destination IP addresses, system events (e.g., failed and successful events — system shutdown or starting a service, errors, anomalous/abnormal activity, etc.), log-on/authentication attempts (failed and successful), user access history, account changes (e.g., account creation and deletion, account privilege assignment, etc.), security policy changes, system configuration changes, usage information (e.g., number of transactions occurring in a certain period of time) and transaction size (e.g., email message size, file transfer size, etc.), and security logs for all public jurisdiction data related to this contract. b. The service provider and the public jurisdiction share security responsibilities. The service provider is responsible for providing a secure infrastructure (e.g., storage and servers), virtualization/ hypervisor, operating system, middleware and runtime. The service provider and the public jurisdiction typically share responsibility for identity, credential and access management, networking, applications, and data security. In certain instances, the public jurisdiction has sole responsibility for securing its applications and data that run within the PaaS computing environment. The methods and conditions for access to logs/reports and the format for the logs/ reports shall be specified and agreed upon by both parties in the SLA. Specific shared responsibilities are identified in the SLA.	**14. Access to Security Logs and Reports:** a. The service provider shall provide reports to the public jurisdiction directly related to the infrastructure that the service provider controls upon which the public jurisdiction account resides. Unless otherwise agreed to in the SLA, the service provider shall provide the public jurisdiction a history of all API calls for the public jurisdiction's account. This report shall include the identity of the API caller, the date and time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the service provider. The report will be sufficient to enable the public jurisdiction to perform security analysis, resource change tracking and compliance auditing. b. The service provider and the public jurisdiction share security responsibilities. The service provider is responsible for providing a secure infrastructure (e.g., storage and servers) and virtualization/ hypervisor. The service provider and the public jurisdiction typically share responsibility for identity, credential and access management, networking, and data security. The public jurisdiction is responsible for its secure guest operating system, middleware, runtime, applications, firewalls and other logs captured within the guest operating system. The methods and conditions for access to logs/reports and the format for the logs/ reports are to be specified and agreed upon by both parties in the SLA. Specific shared responsibilities are identified within the SLA.

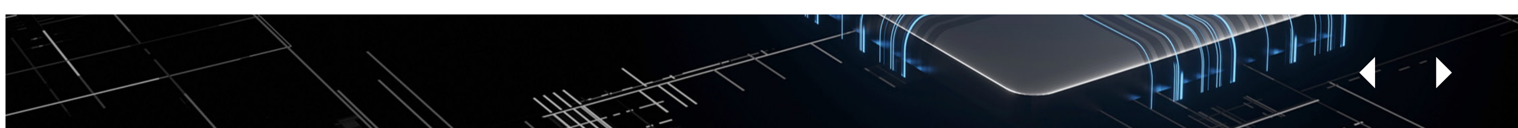


Plain Language	SaaS	PaaS	IaaS
15. The service provider and the public jurisdiction shall specify/agree on the methods and timeframes for the retention, preservation (i.e., legal hold), and archival of security logs and reports within the SLA.	**15. Retention, Preservation and Archival of Security Logs and Reports:** The service provider shall retain security logs and reports in a usable format for a minimum of _____ (days, months, years) and a maximum retention/archival of _____ (days, months, years or for a specific period beyond the termination of the contract). The methods and timeframes for the retention, preservation (i.e., legal hold), and archival for the logs and reports will be specified and agreed upon by both parties in the SLA.	**15. Retention, Preservation and Archival of Security Logs and Reports:** The service provider shall retain security logs and reports in a usable format for a minimum of _____ (days, months, years) and a maximum retention/archival of _____ (days, months, years or for a specific period beyond the termination of the contract). The methods and timeframes for the retention, preservation (i.e., legal hold), and archival for the logs and reports will be specified and agreed upon by both parties in the SLA.	**15. Retention, Preservation and Archival of Security Logs and Reports:** The service provider shall retain security logs and reports in a usable format for a minimum of _____ (days, months, years) and a maximum retention/archival of _____ (days, months, years or for a specific period beyond the termination of the contract). The methods and timeframes for the retention, preservation (i.e., legal hold), and archival for the logs and reports will be specified and agreed upon by both parties in the SLA.
16. The service provider will encrypt data at rest and data that resides on mobile devices.	**16. Encryption of Data at Rest:** The service provider shall prevent its employees and subcontractors from storing personal data on portable devices, except within data centers located in the United States. If personal data must be stored on portable devices to accomplish the work, the service provider must use hard drive encryption in accordance with cryptography standards referenced in FIPS 140-2, Security Requirements for Cryptographic Modules.	**16. Encryption of Data at Rest:** The service provider shall prevent its employees and subcontractors from storing personal data on portable devices, except within data centers located in the United States. If personal data must be stored on portable devices to accomplish the work, the service provider must use hard drive encryption in accordance with cryptography standards referenced in FIPS 140-2, Security Requirements for Cryptographic Modules.	Not relevant to service model. Standards would be selected by the public jurisdiction.
17. The public jurisdiction can audit conformance to contract terms.	**17. Contract Audit:** The service provider shall cooperate with public jurisdiction audit of conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction. If information deemed confidential or proprietary must be reviewed during a contract compliance audit, either party may request the execution of a non-disclosure agreement (NDA), to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.	**17. Contract Audit:** The service provider shall cooperate with public jurisdiction audit of conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction. If information deemed confidential or proprietary must be reviewed during a contract compliance audit, either party may request the execution of a non-disclosure agreement (NDA), to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.	**17. Contract Audit:** The service provider shall cooperate with public jurisdiction audit of conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction. If information deemed confidential or proprietary must be reviewed during a contract compliance audit, either party may request the execution of a non-disclosure agreement (NDA), to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.

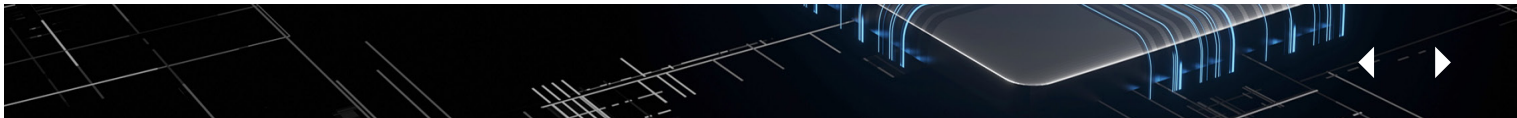
Plain Language	SaaS	PaaS	IaaS
18. The service provider will have an independent audit performed of its data centers annually.	**18. Data Center Audit:** An annual audit as required by StateRAMP and/or FedRAMP shall be performed for all relevant data centers associated with the provision of a cloud service at the data center provider's expense. Providers must grant the government's information security office access to view the audit and artifacts through StateRAMP, if applicable. Some governments may accept a SOC 2 Type 2 audit annually for all relevant data centers associated with the provision of the cloud service at the service provider's expense. The audit must be made available to the jurisdiction if requested under unilateral NDA or after being redacted.	**18. Data Center Audit:** An annual audit as required by StateRAMP and/or FedRAMP shall be performed for all relevant data centers associated with the provision of a cloud service at the data center provider's expense. Providers must grant the government's information security office access to view the audit and artifacts through StateRAMP, if applicable. Some governments may accept a SOC 2 Type 2 audit annually for all relevant data centers associated with the provision of the cloud service at the service provider's expense. The audit must be made available to the jurisdiction if requested under unilateral NDA or after being redacted.	**18. Data Center Audit:** An annual audit as required by StateRAMP and/or FedRAMP shall be performed for all relevant data centers associated with the provision of a cloud service at the data center provider's expense. Providers must grant the government's information security office access to view the audit and artifacts through StateRAMP, if applicable. Some governments may accept a SOC 2 Type 2 audit annually for all relevant data centers associated with the provision of the cloud service at the service provider's expense. The audit must be made available to the jurisdiction if requested under unilateral NDA or after being redacted.
19. The service provider must demonstrate that the security posture of its cloud service offering is acceptable to the public jurisdiction throughout the life of the contract. Continuous monitoring shall be conducted at the service provider's expense using third-party assessment organizations (3PAOs) and methods approved by the public jurisdiction. Continuous monitoring reports shall be provided to the public jurisdiction under mutual NDA. Alternative: StateRAMP or FedRAMP shall provide continuous monitoring reports to the public jurisdiction and the 3PAO for the appropriate impact category under which the cloud service offering is authorized.	**19. Continuous Monitoring:** The service provider shall, at the service provider's expense, conduct continuous monitoring of the service provider's compliance with security controls required within the contract. Continuous monitoring shall be conducted via one or a combination of the following methods approved by the public jurisdiction: a. Reliance on StateRAMP authorization and independent assessments by 3PAOs b. Reliance on FedRAMP authorization and independent assessments by 3PAOs c. Review of control documentation by internal staff or 3PAO d. Acceptance of the service provider's third-party attestation (e.g., AICPA SOC2-Type 2 audit) e. Self-assessment by service provider Continuous monitoring reports shall be provided to the public jurisdiction under mutual NDA. *Alternative:* StateRAMP or FedRAMP shall provide continuous monitoring reports to the public jurisdiction and the 3PAO for the appropriate impact category under which the cloud service offering is authorized.	**19. Continuous Monitoring:** The service provider shall, at the service provider's expense, conduct continuous monitoring of the service provider's compliance with security controls required within the contract. Continuous monitoring shall be conducted via one or a combination of the following methods approved by the public jurisdiction: a. Reliance on StateRAMP authorization and independent assessments by 3PAOs b. Reliance on FedRAMP authorization and independent assessments by 3PAOs c. Review of control documentation by internal staff or 3PAO d. Acceptance of the service provider's third-party attestation (e.g., AICPA SOC2-Type 2 audit) e. Self-assessment by service provider Continuous monitoring reports shall be provided to the public jurisdiction under mutual NDA. *Alternative:* StateRAMP or FedRAMP shall provide continuous monitoring reports to the public jurisdiction and the 3PAO for the appropriate impact category under which the cloud service offering is authorized.	**19. Continuous Monitoring:** The service provider shall, at the service provider's expense, conduct continuous monitoring of the service provider's compliance with security controls required within the contract. Continuous monitoring shall be conducted by via one or a combination of the following methods approved by the public jurisdiction: a. Reliance on StateRAMP authorization and independent assessments by 3PAOs b. Reliance on FedRAMP authorization and independent assessments by 3PAOs c. Review of control documentation by internal staff or 3PAO d. Acceptance of the service provider's third-party attestation (e.g., AICPA SOC2-Type 2 audit) e. Self-assessment by service provider Continuous monitoring reports shall be provided to the public jurisdiction under mutual NDA. *Alternative:* StateRAMP or FedRAMP shall provide continuous monitoring reports to the public jurisdiction and the 3PAO for the appropriate impact category under which the cloud service offering is authorized.



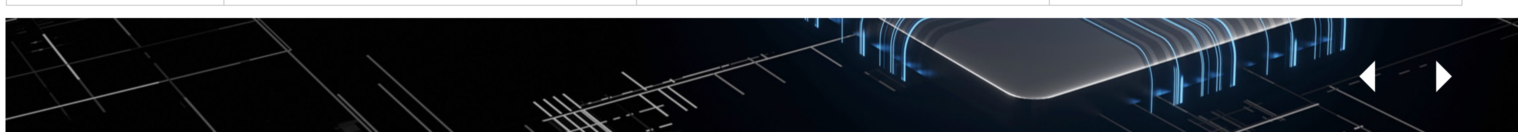
Plain Language	SaaS	PaaS	IaaS
20. The service provider is responsible for all hardware, software, personnel and facilities needed to deliver services. Service will be available 24/7.	**20. Responsibilities and Uptime Guarantee:** The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibility of the service provider. The system shall be available 24/7/365, with agreed-upon maintenance downtime, and provide service to customers as defined in the SLA.	**20. Responsibilities and Uptime Guarantee:** The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibility of the service provider. The system shall be available 24/7/365, with agreed-upon maintenance downtime, and provide service to customers as defined in the SLA.	**20. Responsibilities and Uptime Guarantee:** The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibility of the service provider. The system shall be available 24/7/365, with agreed-upon maintenance downtime, and provide service to customers as defined in the SLA.
21. The service provider will notify the public jurisdiction of upgrades and maintenance.	**21. Change Control and Advance Notice:** The service provider shall give advance notice (to be determined at the contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades or system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version to bring the system up to date or improve its characteristics. It usually includes a new version number.	**21. Change Control and Advance Notice:** The service provider shall give advance notice (to be determined at the contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades or system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version to bring the system up to date or improve its characteristics. It usually includes a new version number.	**21. Change Control and Advance Notice:** The service provider shall give advance notice (to be determined at the contract time and included in the SLA) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades or system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version to bring the system up to date or improve its characteristics. It usually includes a new version number.
22. The service provider will disclose all subcontractors.	**22. Subcontractor Disclosure:** The service provider shall identify all strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.	**22. Subcontractor Disclosure:** The service provider shall identify all strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.	**22. Subcontractor Disclosure:** The service provider shall identify all strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.
23. When asked by the public jurisdiction, the service provider will provide business continuity and disaster recovery plans. Both parties must agree on recovery time objectives (RTOs) in the contract. The service provider will meet the RTOs.	**23. Business Continuity and Disaster Recovery:** The service provider shall provide a business continuity and disaster recovery plan upon request and ensure that the public jurisdiction's recovery time objective (RTO) of XXX hours/days is met. (XXX shall be negotiated by both parties.)	**23. Business Continuity and Disaster Recovery:** The service provider shall provide a business continuity and disaster recovery plan upon request and ensure that the public jurisdiction's recovery time objective (RTO) of XXX hours/days is met. (XXX shall be negotiated by both parties.)	**23. Business Continuity and Disaster Recovery:** The service provider shall provide a business continuity and disaster recovery plan upon request and ensure that the public jurisdiction's recovery time objective (RTO) of XXX hours/days is met. (XXX shall be negotiated by both parties.)



Plain Language	SaaS	PaaS	IaaS
24. The service provider will comply with accessibility requirements.	**24. Compliance with Accessibility Standards:** The service provider shall comply with and adhere to accessibility standards of Section 508 Amendment to the Rehabilitation Act of 1973.	**24. Compliance with Accessibility Standards:** The service provider shall comply with and adhere to accessibility standards of Section 508 Amendment to the Rehabilitation Act of 1973.	Not relevant to service model. Standards would be selected by the public jurisdiction.
25. The service provider will use web services where possible to interface with public jurisdiction data.	**25. Web Services:** The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.	**25. Web Services:** The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.	Not relevant to service model. Standards would be selected by the public jurisdiction.
26. Service provider grants the public jurisdiction a license to: (1) access and use the cloud service for its business purposes; (2) for SaaS, PaaS or IaaS use underlying software as embodied or used in the cloud service; and (3) view, copy, upload and download (where applicable), and use the service provider's documentation.	**26. Subscription Terms:** Contractor grants to a purchasing entity a license to: (1) access and use the service for its business purposes; (2) for SaaS, use underlying software as embodied or used in the service; and (3) view, copy, upload and download (where applicable), and use contractor's documentation.	**26. Subscription Terms:** Contractor grants to a purchasing entity a license to: (1) access and use the service for its business purposes; (2) for PaaS, use underlying software as embodied or used in the service; and (3) view, copy, upload and download (where applicable), and use contractor's documentation.	**26. Subscription Terms:** Contractor grants to a purchasing entity a license to: (1) access and use the service for its business purposes; (2) for IaaS, use underlying software as embodied or used in the service; and (3) view, copy, upload and download (where applicable), and use contractor's documentation.



Plain Language	SaaS	PaaS	IaaS
27. The service provider will notify the public jurisdiction of any legal requests that might require access to the public jurisdiction's data.	**27. Notification of Legal Requests:** The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.	**27. Notification of Legal Requests:** The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.	**27. Notification of Legal Requests:** The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.
28. The service provider will not erase the public jurisdiction's data if a contract is suspended or when the contract is terminated. Specific time periods for data preservation by the service provider are based on the circumstances of termination and the type of service provided. The service provider will destroy data using a NIST- approved method when requested by the public jurisdiction.	**28. Termination and Suspension of Service:** a. In the event of a contract termination, the service provider shall return public jurisdiction's data in a CSV or other mutually agreeable format at a time agreed to by the parties. The service provider also will provide for the subsequent secure disposal of public jurisdiction data. b. During any period of service suspension, the service provider shall not intentionally erase any public jurisdiction data. c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of: • 10 days after the effective date of termination, if the termination is in accordance with the contract period • 30 days after the effective date of termination, if the termination is for convenience • 60 days after the effective date of termination, if the termination is for cause After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. d. The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services unless a unique data retrieval arrangement has been established in the SLA. e. The service provider shall securely dispose of all requested data in all forms, such as disk, CD/DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.	**28. Termination and Suspension of Service:** a. In the event of an early contract termination, the service provider shall allow the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content. b. During any period of service suspension, the service provider shall not intentionally erase any public jurisdiction digital content. c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of 45 days after the effective date of a termination for convenience, or 60 days after the effective date of a termination for cause. After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of a termination for cause, the service provider will impose no fees the customer for access and retrieval of digital content. d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all forms, such as disk, CD/DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.	**28. Termination and Suspension of Service:** a. In the event of an early contract termination, the service provider shall allow the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content. b. During any period of service suspension, the service provider shall not intentionally erase any public jurisdiction digital content. c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of 45 days after the effective date of a termination for convenience, or 60 days after the effective date of a termination for cause. After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of a termination for cause, the service provider will impose no fees the customer for access and retrieval of digital content. d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all forms, such as disk, CD/DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.



Appendix 8

Aligning Procurement with Risk Authorization and Management

This portion of the guide looks at changes and challenges in state and local government cloud contracting and new ways agencies can respond by integrating Risk Authorization and Management Programs (RAMPs) to assess, audit and manage risk in their cloud service model contracting using NIST SP 800-53 based controls.

Section 1: The Evolving Cloud Adoption Environment

Accelerating cloud adoption. Since 2014 when this guide was first published, cloud-based service offerings and government consumption have changed. Government use of cloud-based computing continues to accelerate, driven by increasing demands for digital business applications, declining government resources, increasing cybersecurity threats and ever-increasing cloud service offerings.

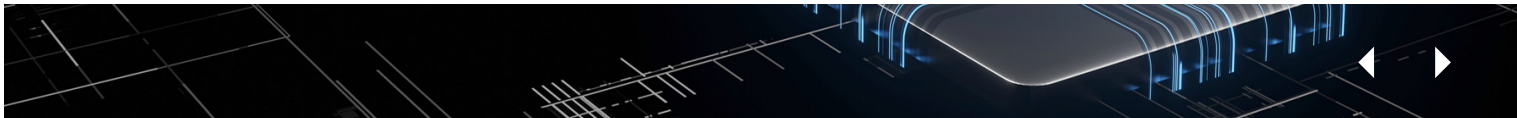
Many organizations now use cloud-first strategies to overcome long lead times associated with on-premises implementations. The ease of access in highly federated organizations has also spiked unauthorized shadow IT instances, which, left unchecked, can result in significant privacy and security risks. Accelerating adoption of authorized and unauthorized cloud services underscores the need for more collaboration between information security and contracting teams.

Changing cloud environment. In 2014, states were still following various standards for security and data control and just beginning to kick the tires on the NIST Cybersecurity Framework. A 2014 Deloitte/NASCIO annual cybersecurity study showed early interest in the NIST Cybersecurity Framework, reporting that "...nearly two out of five CISOs say they are currently reviewing the framework with an additional 47% saying they plan to leverage it within the next six months to a year."

By 2022, a study published by Accenture and NASPO showed more thorough adoption of NIST guidance by states. It found 60% of states depend on FedRAMP certification, and some states (9%) are pivoting to StateRAMP certification. The trend shows a move to more rigorous cybersecurity validation from suppliers using FedRAMP or StateRAMP authorizations to verify the presence of NIST SP 800-53 controls.

Today, if you are in a state or local government, chances are good that your security controls are based completely or in part on NIST SP 800-53 Rev. 4 or Rev. 5. If not, this might be the time to make the change to ease in the alignment of national cybersecurity initiatives like Executive Order 14028. At a time when cybersecurity is the recurring No. 1 priority for state and local CIOs, it is not a coincidence that NIST SP 800-53 has become the consensus standard for security and privacy controls for cloud service models.

Procurement practices impacted. Accelerating growth in cloud deployments and increasing expectations for cybersecurity are impacting state and local contracting practices. Governments are buying more cloud service-based solutions to support everything from replacing data centers and ERP systems to deploying specific software-as-



a-service (SaaS)-based business solutions. According to a 2022 CompTIA Public Technology Institute (PTI) state and local government survey, 37% of these agencies have moved their on-premises infrastructure to the cloud this past year, and 32% say migrating systems and applications to the cloud will be a top priority over the next two years. The survey showed SaaS-based products leading the way, with 80% of state and local IT respondents using new SaaS solutions this past year. However, without timely procurement processes aligned to appropriate cloud cybersecurity policies, effective government cloud service contracts are not possible. This is driving the need for RAMPs to strengthen security in cloud-based contracts and among service providers.

Section 2: Aligning the contracting process to RAMP

Starting and maintaining a RAMP in government requires cooperation and alignment between executive management in IT, cybersecurity, risk management and contracting. Each of these functional areas has an important role to play in developing and operating a RAMP. An effective program to assess and manage risk in cloud platforms requires harmonious policy development, coordinated governance and focused operational execution in each policy owner's respective role.

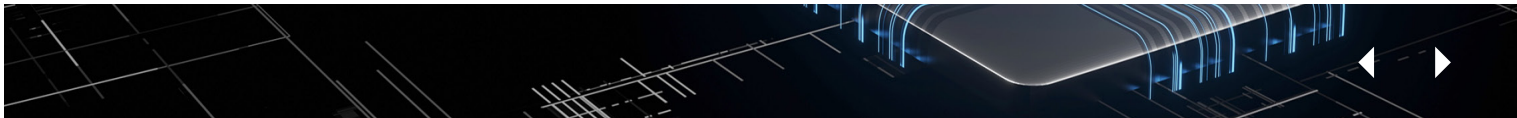
But even best efforts by government policy owners will not result in successful risk assessment and management of cloud-based services if service providers cannot or will not contract for services. Developing a RAMP requires governments to engage with the service provider community by communicating plans, proposed changes and timelines. It also requires governments to listen to suppliers. It's important for agencies to create a two-way channel of communication to get feedback from service providers on what will and will not work.

Here are recommended steps to consider when integrating a RAMP into procurement and contracting organizations.

1. Align procurement policies with cloud governance and RAMP.

While procurement policies guide the sourcing process, the requirements for contract compliance with cybersecurity, privacy and data protection must come from policies developed outside the typical scope of procurement. A knowledgeable team of key stakeholders familiar with all policies involved (i.e., cloud adoption, governance, security, privacy, etc.) should review and revise procurement and contracting policies and procedures that guide both centralized cloud procurement and government-wide acquisition and contract administration. These policies and procedures must align with CISO and IT enterprise policies for system governance and RAMP. Empowering this cross-functional RAMP adoption team to support the implementation and operation of RAMP is an excellent way to streamline RAMP coordination, decision-making and adoption.

An iterative process coupled with a recognized and highly adopted framework like NIST SP 800-53 Rev. 5



allows for the most critical risks to be addressed initially and a clear understanding of what is to come. Compatibility between policies, adopted RAMP controls and process is critical — at initial policy development and over time. Policies should accommodate changes as controls and standards will evolve. Referencing standard frameworks keeps policies current because when controls change in the framework, the policy does not become out of date.

Procurement policies should be modified or developed along with procedures, model clauses, approved templates and other artifacts to guide the development of practices to harmonize and support adopted cybersecurity control and RAMP policies. Typically, once policies are adopted, more detailed and specific guidance follows to implement policies, but in a dynamic environment where changes are fluid and outcomes are needed quickly, leap-frogging procedures with more agile interim solutions like version-dated templates may be necessary. Table 1 provides a process flow and key elements to consider when building RAMP into your procurement policy.

Templates can be an effective way to guide organizational behavior even when policy and more detailed guidance are still in development. The state of Michigan provides a good example of using templates as a primary tool to implement cloud policies. As RAMP requirements develop, templates for cloud contracting should be updated to identify RAMP-related actions and placed into a cloud contracting library. Guidance on getting started with RAMP — including updating policies, incorporating requirements in procurement and a variety of templates — can be found in Getting Started with StateRAMP.

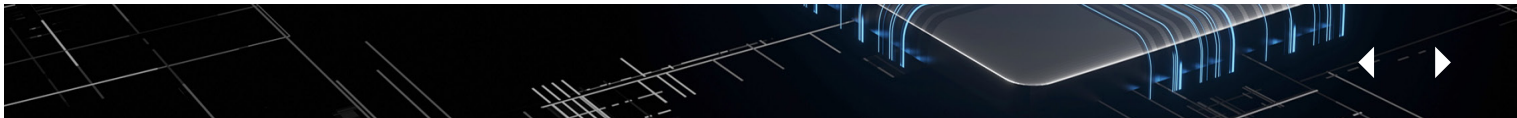
IT procurement teams should watch for cloud procurement practices they could simplify or improve with a template or new clause and work with key stakeholders to create template amendments and clause libraries for cloud procurements.

2. Work from a common understanding of cloud and service models.

To align policies developed by different owners and effectively procure cloud products, a common understanding of what cloud means is essential. The enterprise IT organization led by the state CIO should take the lead here with a common definition and education on what is meant by cloud. These definitions must include the various service models (SaaS, PaaS and IaaS) and deployment strategies. When it is time to procure a cloud service, all policy owners, stakeholders and potential contractors must have a common understanding of what cloud computing is, including a particular service model. Including clauses in solicitations and contracts that define cloud and RAMP requirements is essential in a government that has adopted a RAMP approach.

NIST's technical definitions can be helpful. NIST SP 800-145 provides the following:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of



configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models and four deployment models…"

3. Identify must-have security controls in the solicitation and contract.

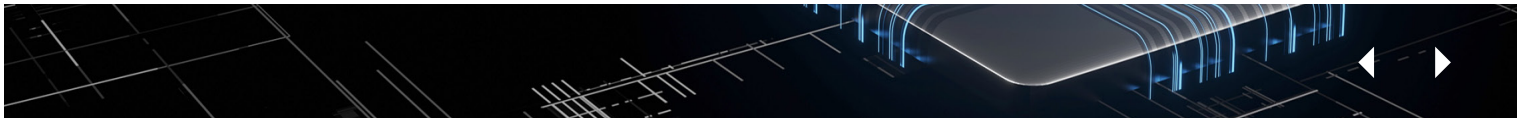
According to NIST, the NIST SP 800-53 security controls "facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent/repeatable manner — thus contributing to the organization's confidence that security requirements continue to be satisfied on an ongoing basis." Government sourcing and contract documents must contain clear and specific controls a service provider must adhere to in the performance of its contract.

Most state and local governments have a project review and assessment process spelled out in their governance policy. This is where key stakeholders, policy owners and the client business owner select the appropriate security controls based on threats, vulnerabilities and the likelihood of exploits resulting in adverse impacts. Typically, in a RAMP, the CISO and the business owner's representative help set the appropriate controls. The procurement officer's role is to make sure the controls are clearly identified in the solicitation.

Once the control set is identified for a specific cloud service acquisition, other requirements, terms and conditions normally included in the solicitation should be examined for conflicts and redundancy with the adopted controls. This offers a great opportunity to simplify the RFP by eliminating duplicative and potentially conflicting requirements and terms and conditions. By harmonizing terms and conditions with controls, more service providers are likely to respond, and contract outcomes will improve.

Controls required for a particular cloud service application may differ from project to project, depending on the sensitivity of the data provided to the vendor. A one-size-fits-all approach to security controls will either overkill security requirements or be insufficient. The commonwealth of Massachusetts uses a security control matrix to establish the appropriate level of controls.

StateRAMP offers a "pre-ready" assessment, known as the StateRAMP Security Snapshot, to service providers and state and local governments. It is similar to the FedRAMP Readiness Assessment Report process, although FedRAMP reports may contain federal data and would require redaction prior to authorization to share with any non-federal entity. The StateRAMP assessment includes a score that evaluates the cyber maturity for a cloud product that does not yet have a verified security status. A government can use the assessment to determine the risk associated with products being considered for procurement. When



incorporated into a solicitation requirement, it will help a government assess NIST compliance upfront while a provider works to achieve RAMP authorization. The assessment can be a good way to bridge the transition to StateRAMP for providers and governments. Six key Security Snapshot steps include:

1. Identify the security impact level required (use the StateRAMP Data Classification Tool to identify recommended impact level).
2. Require a Security Snapshot score that is no older than six months at submission as a deliverable for solicitation response (StateRAMP Ready, Authorized or Provisional Certifications exceed this requirement).
3. Require an updated Security Snapshot within six months after contract execution.
4. Require StateRAMP Ready certification within 12 months of contract execution (continuous monitoring begins).
5. Require the service provider to grant the contracting jurisdiction access to continuous monitoring reporting within the StateRAMP secure portal.
6. Require StateRAMP Provisional/Authorized within 18 months of contract execution (continuous monitoring begins).

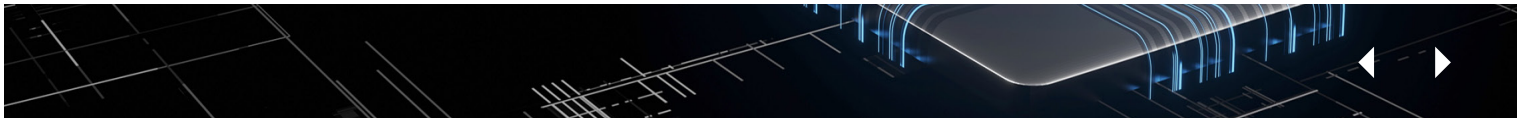
The state of Arizona includes its baseline security infrastructure security controls in its solicitation document attached to IT system RFPs. A recent RFP requires proposers to follow State of AZ Data Security Std S8120 and agree that NIST SP 800-53 Security and Privacy Controls will be exclusively followed. It outlines not only specific requirements a proposer must meet but also the award path for a proposer with StateRAMP or FedRAMP product authorization and an award path contingent on the proposed cloud product achieving key milestones and StateRAMP authorization within the first year of the contract award.

StateRAMP provides a Data Classification Tool to help state or local governments determine the appropriate StateRAMP security requirements and StateRAMP impact level for a solicitation of SaaS, IaaS and/or PaaS solutions that process, store and/or transmit government data, including personal identifiable information (PII), protected health information (PHI) and/or payment card industry (PCI) information, similar to FedRAMP's use of FIPS 199 Security Categorization. The self-assessment tool is based on the NIST SP 800-53 Rev. 4 requirements and helps organizations develop the appropriate package of NIST SP 800-53 baseline controls for the cloud service to be acquired. Solicitation documents and contracts are incomplete if the security requirements and controls are not clearly identified.

Broader adoption of a common and rigorous control framework such as NIST SP 800-53 will encourage more qualified service providers that have NIST SP 800-53 controls in place to compete for government contracts. State and local programs that integrate a RAMP using baseline NIST SP 800-53 controls will benefit from more competitive offers, which can readily be audited and monitored through the life of the contract.

Sample Solicitation Language

Security and control requirements – The successful proposer's cloud product offering must comply with the (insert jurisdiction and include any specific security and RAMP policies) information security policies and adhere to the National Institute of Standards and Technology (NIST) Special Publication 800-53 (select rev. 4 or 5) controls for StateRAMP or FedRAMP Impact Level (insert selected Impact Level for appropriate NIST SP 800-53 control package; for example, Low, Low Plus, Moderate or High).



4. Clearly identify what is in scope for RAMP.

A common understanding of cloud definitions within the government organization is also the first step to understanding what IT services are subject to RAMP authorization policies. States like Texas and Arizona, which have implemented RAMPs, have been careful to define what cloud applications are subject to RAMP.

Texas administrative code requires TX-RAMP Level 1 controls to be applied as a baseline for cloud computing services that store, process or transmit non-confidential data or host low-impact information resources. More robust Level 2 controls must be applied as a baseline for cloud computing services that store, process and transmit confidential data and host moderate- or high-impact information resources.

While it is getting harder to find any service purchased by a government that doesn't have a cloud computing component, it is not practical from an administration and resource standpoint to cover all cloud computing applications from the outset.

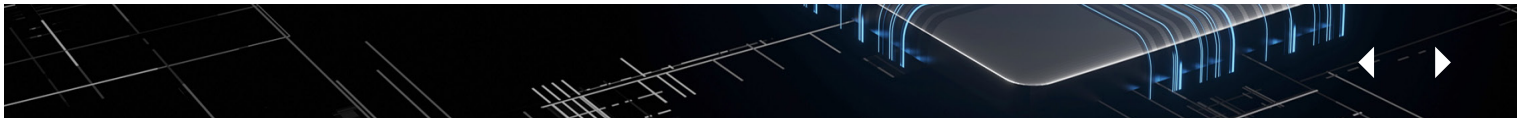
Strategies might include starting with a smaller group of cloud applications that have a higher risk assessment or beginning with a pilot for a specific procurement. As the organization matures in expertise and capability, it can add more cloud service products. Both Texas and Arizona have stressed the importance of clearly defining what is subject to RAMP authorization and what is not.

This becomes an organizational risk-reward question that an organization should address within the context of its cybersecurity risk management practices. Organizations should also consider the resource impacts both internally and within the marketplace. This approach will help mitigate organizational impacts and give service providers more time to transition to RAMP authorization.

The jurisdiction's project review process is the best place to identify if the cloud service to be procured is subject to RAMP authorization. When a solicitation for a cloud service product is developed, it should include notice to potential offerors if the scope includes RAMP authorization. If the jurisdiction has a RAMP coverage policy, it should consider including the specific coverage in all potential cloud service solicitations to inform potential offerors.

Sample Solicitation Language

Cloud service products subject to RAMP authorization - All cloud service products that process, store and/or transmit government data must demonstrate compliance with NIST SP 800-53 at the specified Impact Level.



5. Limit shadow cloud services.

The growth of SaaS cloud models specifically tailored to effective government business solutions is exploding. It is no surprise many state agencies are interested in these business solutions to help improve their services to constituents. Most governments have project review processes required by their governance policy to ensure that appropriate security and system requirements compatibility are met by potential service providers. One concern with cloud-based products is that the proliferation of multi-cloud environments increases the complexity of monitoring and managing security.

The article "21 Shadow IT Management Statistics You Need to Know" highlights some of the costs and adverse security impacts of shadow IT.

Procurement offices can help limit the proliferation of maverick cloud services by issuing solicitations or approving agency solicitations for only reviewed and approved projects. Access to price agreements or other pre-awarded or pre-qualified CSP contracting processes should have a similar review built in to ensure all cloud products are compatible with adopted cloud policies and approved cloud platforms.

Sample Solicitation Language

Authorized use cloud service products – Use of this contract is limited to agencies authorized to purchase from the agreement by the (identify the jurisdiction and approving official or body) and only for IT projects that have been authorized by the (identify the authorizing person or body that approved the procurement of the project or relevant project approval information).

6. Address the challenge of transition to RAMP authorization.

Transitioning to a RAMP model must give service providers reasonable time to obtain third-party assessments and certifications for the appropriate authorization levels established by the government organization. It will not happen overnight and will take planning and scheduling.

Service providers and state and local governments will have new adoption paths and timelines to follow as they move to RAMP. As governments and service providers mature, the timelines will shorten, and the adoption stages will become more defined. At the beginning of a RAMP implementation for a government, each sourcing event should examine reasonable targets for RAMP compliance based on the government's needs and the perceived service provider market readiness. As state and local governments become more familiar with their RAMP process, each procurement will be less of a custom event designed from the ground up and become more consistent and replicable by using templates with accepted targets for readiness and authorization levels. As service providers mature with a stable of RAMP-authorized cloud products, their ability to prepare proposals and execute contracts will be much simpler and faster. Table 1 breaks down the stages necessary to build RAMP into the contracting process.

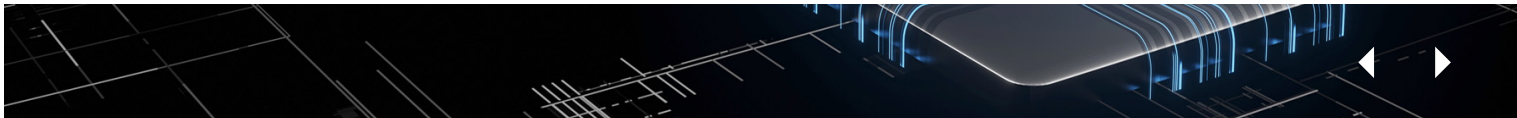
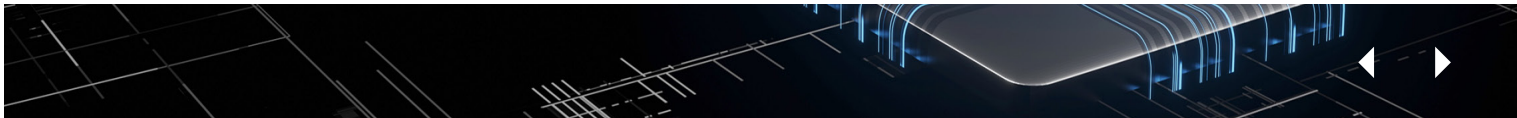


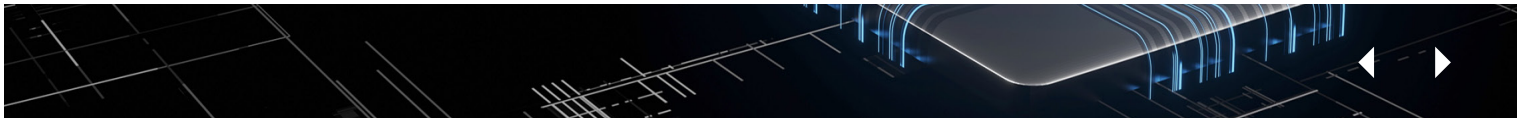
Table 1: Building RAMP into Contracts

Set Control Requirements	Identify Impact Level Category	Identify Security Status Level	Set Status Level Deadline	Set Continuous Monitoring	Confirm Category Impact Level Compliance with Auditor	Monitor Compliance Review Controls
Solicitation Development					Eval/Award	Contract Admin
1. Governance process stakeholders, CISO and client business unit must decide what controls are appropriate for the application	1. In accordance with governance polices during project review	1. CISO and client business unit must decide what is appropriate for the application	1. Client business unit, CISO and procurement officer must agree on what is reasonable	1. Will continuous monitoring be required for all awards?	1. Before completing evaluation, confirm that controls identified in the solicitation have been assessed and found acceptable by an independent certified third-party assessment organization (3PAO)	1. Who in the government is responsible for continuous monitoring and serves as the representative on authorizing body in using StateRAMP or FedRAMP?
2. What controls are needed to adequately mitigate risks incurred by the expected cloud services using this specific government information?	2. Should at a minimum include CISO and client business unit	2. If full impact level authorization is not required at award, determine what progress toward certification is acceptable	2. Consider the number of service providers with authorization	2. Solicitation document must include a requirement for approved third-party continuous monitoring	2. Any exceptions to controls proposed must be approved by the CISO and the client business unit representative before accepted by the contracting officer	2. What is reviewed to ensure controls at the time of award are still valid?
3. Control families are defined and listed in NIST SP 800-53	3. StateRAMP: • Low • Low + • Moderate • High Fed RAMP: • Low • Moderate • High	3. StateRAMP progressing offering: • Active • In process • Pending	3. Consider reasonableness of the timeline to achieve full certification	3. Remedies identified for failure to comply with control?	3. Keep a confirmation copy of 3PAO's report in the award file with appropriate documentation of any approved exceptions	3. What are the continuous monitoring reporting frequencies for the service provider?



Set Control Requirements	Identify Impact Level Category	Identify Security Status Level	Set Status Level Deadline	Set Continuous Monitoring	Confirm Category Impact Level Compliance with Auditor	Monitor Compliance Review Controls
Solicitation Development					Eval/Award	Contract Admin
4. StateRAMP controls are identical to NIST SP 800-53 Rev. 4 but do not include federal agency specific controls	4. Before beginning the sourcing, check that controls are identified per governance process	4. StateRAMP progressing offering: • Active • In process • Pending	4. Assess risk involved in delayed certification			4. What are the continuous monitoring reporting frequencies for the service provider?
5. Avoid customizing controls with deletions, amendments or supplemental controls			5. Cloud procurement policy should set general parameters			5. Who has the designated authority to represent the contracting officer when overseeing contractor performance?

StateRAMP architects recognized the unavoidable lags that will occur as participating governments and service providers move through the stages of RAMP to full authorization. To aid governments with this transition, the Security Status Levels used in StateRAMP are grouped in two basic stages: 1) progressing, which includes substages, and 2) verified, which allows for a different status. These stepped progression levels allow a government to identify when a service provider must accomplish various stages in its solicitation and contract. This aspect is important because it gives a service provider without full authorization the ability to participate in a solicitation and potentially receive a contract award conditioned on attaining a certain stage within the prescribed time. The ability to move through the status levels helps the service provider compete for the award and the government entity receive



the benefits of performance from a service provider that has received third-party authorization measured against NIST SP 800-53 controls. It also gives a government entity the necessary flexibility to soft launch a RAMP program.

Here are a few recommendations to consider:

- Set reasonable schedules by determining a date or time by which service providers are required to meet specific RAMP requirements. A date will assist both the government and the service provider with the transition to the desired RAMP level.
- Develop an effective ongoing communication plan between the government and supplier community concerning updated policies and procedures.
- Align procurement and contracting document requirements to identify the authorization and readiness levels with timelines and dates a service provider must meet to be considered for an award, receive a contract or get authorization to proceed with work.

Sample Solicitation Language

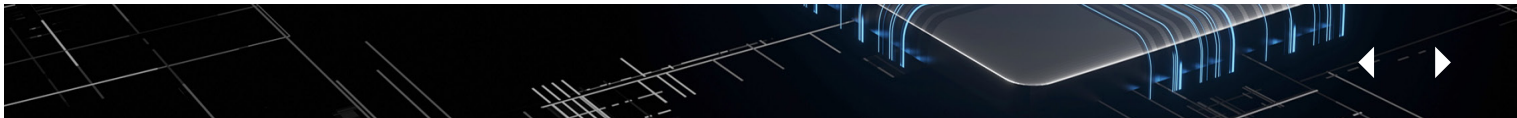
RAMP ready status - Award will be made to selected proposers offering a cloud product that processes, stores and/or transmits government data, only if the proposal includes written documentation that the cloud product **has achieved** (*select the minimum status acceptable to the jurisdiction for this specific cloud product:* ***Ready, Provisional or Authorized***) at (***the time of proposal submission;*** *select the time by which the cloud product must achieve the minimum status level)* which serves as an attestation to the provider's capabilities to achieve full authorization.

Compliance with requirements - By signature of the proposal, the offeror represents and warrants that the cloud product offered in the proposal complies with the requirements of this section (*if there is written policy that supports this section for the jurisdiction's RAMP, add the reference here*), and the proposer agrees that, if awarded a contract, it shall maintain the most recent authorization adopted by FedRAMP or StateRAMP (*select StateRAMP or FedRAMP*) and comply with the program requirements throughout the performance of the contract. In the event of a revision to NIST SP 800-53 or a change in (*select StateRAMP or FedRAMP*) authorization status, the contracting jurisdiction may grant (*select the amount of the amount of time the service provider has to a new authorization.*) ____ to obtain full authorization.

7. Consolidate and simplify the service provider compliance process.

Effective compliance at the simplest level requires adoption of appropriate requirements and controls to protect a cloud system from vulnerabilities, breach of information and data, and loss of privacy. The procurement process must be designed to include appropriate cloud service requirements and controls not just during the solicitation and evaluation phase, but throughout the lifecycle of the contract.

This starts with the adoption of an appropriate framework and controls. Developing and adopting the protections and controls is a daunting task. When it comes to developing appropriate controls for cloud applications, states or local governments lack the full range of technical expertise that the National Insitute of Standards and Technology (NIST), International Organization for Standardization (ISO) and Center for Internet Security (CIS)



possess. A best practice is to consolidate and simplify compliance using a robust and effective standard — without modification — that is accepted in the marketplace and designed for specific government use cases. Use of NIST SP 800-53 Rev. 5 opens the door to competitive value for all users because, at the appropriate level of control families, it is designed for government cloud service models. State and local governments save time and resources and get more robust cloud security by adopting NIST SP 800-53 Rev. 5 controls at the appropriate impact level category for the cloud service needed for their business requirements.

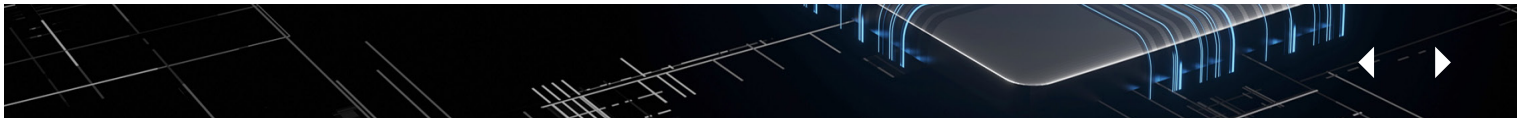
Each time a jurisdiction creates a one-off scenario in their security requirements and compliance, it changes the cost model for the provider, which can result in fewer competitors and higher costs. One way to minimize cost is by using a common catalog of cybersecurity, data protection and privacy controls applied through a common set of RAMP control bundles that cover a full range of SaaS, PaaS and IaaS products based on the classification of the data and the criticality of the workload.

Once baseline controls are adopted, a RAMP can scale the control impact level up or down to meet its cloud service need and greatly simplify cloud service acquisition and deployment with a standard process. Using the FedRAMP or StateRAMP control baseline levels designed specifically for cloud services is far more practical than trying to develop your own.

Cloud service models — particularly SaaS — offer effective and competitively priced services at scale. To keep users satisfied, SaaS offerings must have cybersecurity, data protection and privacy levels that are commonly accepted by their customers. If each engagement involves a different set of compliance requirements, it simply would not be possible to provide the product at a competitive value.

Both FedRAMP and StateRAMP were founded to address the need for a standardized approach to cybersecurity in government cloud service contracts using NIST SP 800-53 controls.

FedRAMP, administered through the General Services Administration (GSA), was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government, with an emphasis on security and protection of federal information.[32] FedRAMP is governed by federal executive branch entities that work to develop, manage and operate the program. The Joint Authorization Board (JAB), the primary governance and decision-making body for FedRAMP, consists of the chief information officers from the Department of Defense (DoD), the Department of Homeland Security (DHS) and the GSA.[33] FedRAMP standardizes security requirements for the authorization and ongoing cybersecurity of cloud services in accordance with the Federal Information Security Modernization Act (FISMA), Office of Management and Budget Circular A-130 and FedRAMP policy. FedRAMP



leverages NIST standards and guidelines to provide standardized security requirements for cloud services, a conformity assessment program, standardized authorization packages and contract language, and a repository for authorization packages.[34]

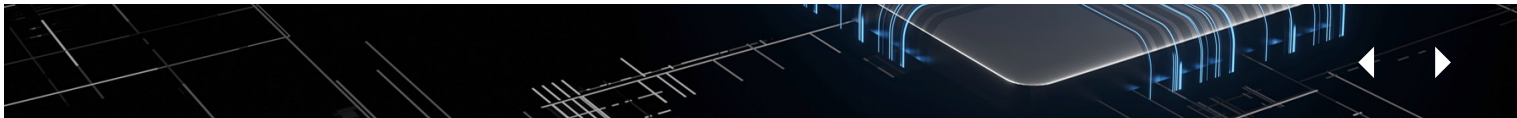
Although FedRAMP is focused on federal government agencies and the protection of federal information, state and local governments have generally accepted a service provider's achievement of FedRAMP Marketplace designations for their cloud service offerings (Ready, In Process or Authorized) for specific impact levels (Low, Moderate or High) as a verification of the cybersecurity posture of a cloud service provider and its offering(s). Prior to achieving a FedRAMP Authorized designation, a service provider's offering(s) must, among other requirements, be audited (initially and via continuous monitoring) by an authorized third-party assessment organization (3PAO) and be in use by a federal agency. However, not all service providers operate in the federal government marketplace and instead focus their cloud service offerings on the state and local government and education (SLED) marketplace. In addition, the readiness and security assessment reports, 3PAO audit and continuous monitoring reports, authorization packages, and other foundational documentation generated within the FedRAMP program may contain federal data and would require redaction prior to authorization to share with any non-federal entity.

More information on specific FedRAMP requirements, documents and resources can be found at https://www.fedramp.gov/documents-templates/.

StateRAMP, established in 2020 as an independent nonprofit organization, is modeled in part after FedRAMP and, like FedRAMP, relies on FedRAMP Authorized 3PAOs and, more recently, StateRAMP-registered 3PAOs to conduct assessments. StateRAMP offers RAMP services designed specifically for state and local governments, public education institutions and special districts. StateRAMP's Standards and Technical Committee, composed of both government and service provider members, makes recommendations to the StateRAMP Board of Directors regarding verification policies, security standards, best practices, and audit and assessment processes to create common standards that are acceptable to state and local governments and service providers. To be verified, service providers must meet minimum security requirements and provide an independent audit conducted by an authorized 3PAO. StateRAMP recognizes three verified statuses (Ready, Provisional and Authorized). To ensure ongoing security compliance and risk mitigation, service providers must comply with continuous monitoring requirements to maintain a verified security status. Verified cloud service offerings on the StateRAMP Authorized Product List (APL) can be found at https://stateramp.org/product-list/.

StateRAMP fast track for cloud service offerings with FedRAMP designations.

StateRAMP and FedRAMP have similar requirements based on NIST SP 800-53, and both rely on independent audits and continuous monitoring by approved 3PAOs. Recognizing these shared best practices, StateRAMP



has developed a fast-track process for service provider offerings that have achieved FedRAMP marketplace designations (Ready, In Process or Authorized) for specific impact levels (Low, Moderate or High).

The fast-track process allows service provider offerings with designations of FedRAMP Ready, Authorization to Operate (ATO) from a federal agency, or a Provisional ATO from the FedRAMP Joint Authorization Board (JAB) to leverage their FedRAMP audit reports and associated documentation to become StateRAMP Ready or Authorized. The service provider does not have to complete a new audit for StateRAMP and may use FedRAMP templates for ease of compliance. The StateRAMP Security Team, operating within the StateRAMP Program Management Office (PMO), works with cloud service providers to validate and authenticate relevant security packages and reviews recent continuous monitoring audits and reports. Service providers participating in the fast-track process can also utilize the same reporting they provide FedRAMP for StateRAMP.

Sample Solicitation Language

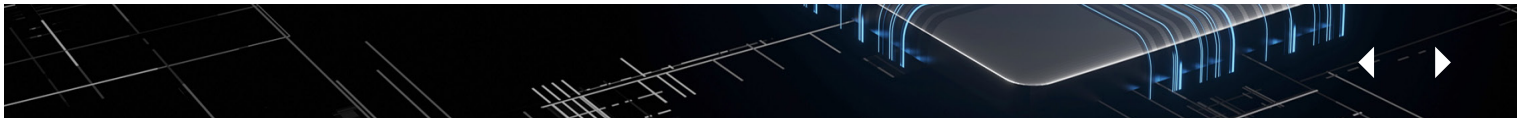
RAMP impact level requirement - All cloud product offerings submitted in response to the RFP that process, store and/or transmit government data must demonstrate compliance with NIST SP 800-53 Rev __ (*identify revision version*) at the RAMP impact level __ (*select the appropriate impact level: StateRAMP Low/Low Plus/Moderate/High or FedRAMP Low/Moderate/High*) by achieving full RAMP authorization within ____ (*insert time by which full authorization must be obtained; example: 12 months*) of contract execution for the appropriate data classification.

8. Use RAMP for assurance and security due diligence during evaluation and award.

A fundamental tenant of the procurement award process is the determination that the contractor can do what the solicitation document requires. With technology procurements that can be challenging. An assessment and adequate due diligence should demonstrate that the service provider can meet the performance requirements and also has controls in place to meet the government's security, data, privacy and other requirements that support its contract performance. This is difficult for any contracting office to determine without expert resources that can test and validate the service provider's purported controls.

For a government to gain assurance that required controls are in place, it can a) rely on StateRAMP authorization, b) rely on FedRAMP authorization, c) conduct an internal review of control documentation, d) contract for a third-party audit, e) rely on a proposer's third-party attestation or f) rely on self-assessment by the proposer. Regardless of which option the government chooses, the responsibility for this basic due diligence decision ultimately rests with the government making the award. Let's look at the options in more detail.

Awards for cloud solutions require considerable expertise to validate that the offeror's proposal fulfills the requirements. With a RAMP-integrated award process, service provider applications authorized under FedRAMP or StateRAMP have independent certified third-party validation that NIST SP 800-53 controls required by the state or local government are in place.



Each option has factors to consider, but FedRAMP and StateRAMP provide reliable audits through certified assessors that procurement offices can rely on to validate that appropriate NIST SP 800-53 controls are in place for a full range of cloud computing contracts. Table 2 provides a high-level comparison of NIST 800-53 SP Rev. 5 control audit options as a part of evaluation award due diligence.

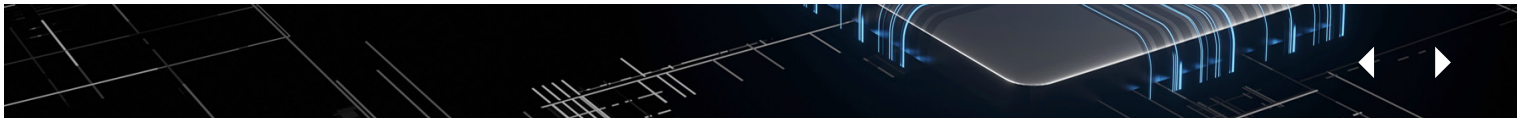
Table 2: Comparison of Audit Options

Factors to Consider	StateRAMP	FedRAMP	Internal	Contract for Third Party	Third Party from Service Provider	Service Provider Self-Assessment
Scales to meet full range* of cloud contract demand	Y	Y	?	?	?	?
Certified independent assessors	Y	Y	?	?	?	N
Integrated into continuous monitoring	Y	Y **	N	N	N	N
Resilient staffing capacity	Y	Y	N	N	?	?
NIST 800-53 certified expertise	Y	Y	N	Y***	?	N
Limits adverse staffing resource impact on jurisdiction	Y	Y	N	?	Y	Y
Paid for by contractor	Y	Y	N	N	Y	Y
Requires additional contracts	N	N	N	Y	N	N

* Full range means all cloud computing service models (SaaS, IaaS, PaaS and XaaS) at all impact levels

** No direct relationship with state or local government contracting jurisdiction

*** If specifically required in the contract



9. Use RAMP to strengthen contract administration.

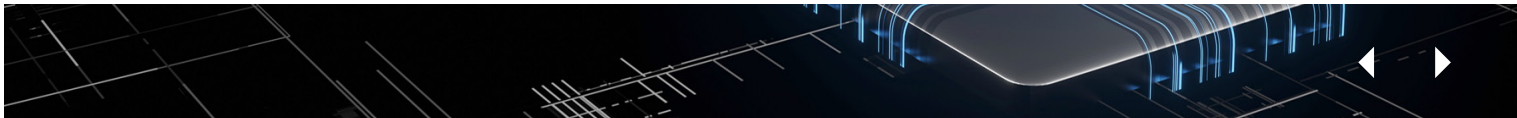
Once a contract is awarded with appropriate controls, the contracting organization has the responsibility to administer the contract and must have a way of monitoring contract obligations, including security and privacy, throughout the performance of the contract. RAMPs allow for assessment and risk management of security that can be used by the CISO and client agency. They also help procurement officials track and monitor contract compliance with contract-driven requirements for security and privacy controls.

Some states have automated this component of their contract administration process. Michigan developed a security accreditation process that automates the security status of a contract and triggers a review of a contractor's security. A post-award review schedule sets a designated person to review the service provider's application to ensure appropriate controls and security requirements are maintained. If it has a FedRAMP or StateRAMP authorization listing, this can be as simple as validating this listing is still in place; with StateRAMP, monthly continuous monitoring reports, along with many other reports or artifacts, are available.

As RAMPs develop, procurement offices gain the opportunity to include continuous monitoring of service provider contracts to ensure that controls that were agreed to before the award continue or are upgraded throughout the life of the contract. Without continuous monitoring, a government's resiliency can be at stake if a security breach occurs because a service provider failed to maintain appropriate security controls. The StateRAMP continuous monitoring program, based on NIST SP 800-13, requires a service provider to maintain a continuous monitoring program once they gain a "Ready "or "Authorized" status. At that point the service provider must deliver specific documentation to the StateRAMP independent third-party auditors who will review and analyze the deliverables. State or local governments participating in StateRAMP designate

Continuous Monitoring Actions (state and local government)

- ☐ **Review service provider's continuous monitoring artifacts.**
- ☐ **Meet with the service provider to define corrective actions that will be incorporated into the plan of action and milestones (POA&M) if a party is not satisfied with the findings.**
- ☐ **Decide if additional continuous monitoring is necessary.**
- ☐ **Approve continuous monitoring documentation.**
- ☐ **Identify any concerns that could address the service provider's authorization status.**
- ☐ **Use documentation as needed to administer contract.**



individuals to view and approve the service provider's submitted reports, the third-party auditor's analysis and the executive summary. StateRAMP is designed to engage the state and local government in the monitoring process and to provide monthly and annual checkpoints on service provider risks, vulnerability assessments and compliance with the continuous monitoring plan. StateRAMP provides robust insight into the service provider's control execution and operation to identify vulnerabilities and implement actions to mitigate as needed. It is a powerful tool that provides protection in the overall administration of the contract. FedRAMP also provides continuous monitoring, but the reporting relationship is with the service provider and not directly with the state or local contracting agency.

FedRAMP audit and continuous monitoring reports may be available to the state or local contracting agency if the service provider participates in the StateRAMP fast-track authorization process. (See 7. Consolidate and simplify the service provider compliance process.) Additional FedRAMP continuous monitoring resources can be found at:

FedRAMP Continuous Monitoring Strategy Guide
FedRAMP Documents and Templates

Sample Solicitation Language

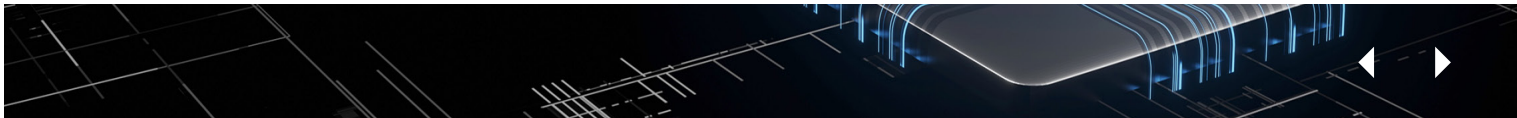
Continuous Monitoring – a) The awarded contractor will create a continuous monitoring plan in coordination with a FedRAMP- or StateRAMP-certified independent third-party assessment organization (3PAO) that meets StateRAMP continuous monitoring standards, and all specific requirements identified by the (*identify jurisdiction*) authorizing body for the impact level category of the cloud product. The continuous monitoring plan must be implemented not later than 90 days after award by the contractor after approval by the (*identify jurisdiction*) authorizing body.

b) The awarded contractor will furnish continuous monitoring and all related reports based on the continuous monitoring plan and assessments and reviews by a 3PAO certified by FedRAMP or StateRAMP to the StateRAMP PMO in machine readable and human readable format or as otherwise directed throughout the life of the contract once a FedRAMP or StateRAMP Ready or Authorized status is achieved. Continuous monitoring and reports will adhere to the continuous monitoring process described in NIST 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organization, and the FedRAMP Continuous Monitoring Strategy Guide in the FedRAMP documentation assets. Copies of the machine readable and human readable files shall be retained for a period of not less than one year.

c) The awarded contractor agrees to provide reports identified in the continuous monitoring plan to the (*identify jurisdiction*) authorizing body at (*identify specific intervals or times for regular reports – recommend monthly*) and upon request. The (*identify jurisdiction*) reserves the right to request and review any or all 3PAO audits, risk assessments, vulnerability assessments and penetration tests of the contractor's environment.

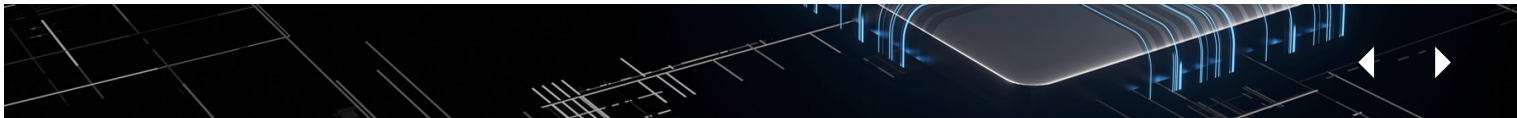
d) The awarded contractor will remediate to the (*identify jurisdiction*)'s satisfaction all discovered high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days and low-risk vulnerabilities within 180 days – or in a timeframe acceptable to (*identify jurisdiction*) to resolve the issue and/or implement a mitigating/compensating control that resolves the issue to the satisfaction of the (*identify jurisdiction*).

e) All continuous monitoring reports including any 3PAO audits, risk assessments, vulnerability assessments or penetration tests as described in this paragraph provided by the awarded contractor to the (*identify jurisdiction*; *if participating StateRAMP government, add via the StateRAMP secure portal*) will be under a mutual non-disclosure agreement acceptable to the contractor and (*identify jurisdiction*).



Solicitation Checklist

- ☐ What are the cloud security, data and privacy standards, and controls that the service provider must meet?
- ☐ What level of RAMP authorization (impact levels) must the service provider meet?
- ☐ What status level must the service provider product meet (StateRAMP pending, authorized, etc.)?
- ☐ When must the service provider achieve this status level?
- ☐ What is mandatory for compliance and what is subject to negotiations?
- ☐ What is the basis upon which the jurisdiction will consider exceptions?
- ☐ Has the solicitation been reviewed for redundancy and conflicts in terms and conditions and any security controls and requirements?
- ☐ Will resellers be eligible for awards?
- ☐ If resellers are eligible for awards, are there flow down requirements that will place sufficient compliance and performance obligations on the ultimate service provider providing the resold product or service?
- ☐ If resellers are eligible for award, are they required to resell FedRAMP and/or StateRAMP authorized offerings and, if so, does the authorization apply specifically to the cloud service products involved in the solicitation?
- ☐ Is there a process to negotiate terms and conditions with the service provider providing the product sold by the reseller?



10. Select the best RAMP alternative for assessing NIST SP 800-53 controls.

RAMP solutions strengthen and streamline the solicitation, award and contract management processes by providing credible and timely assessments.

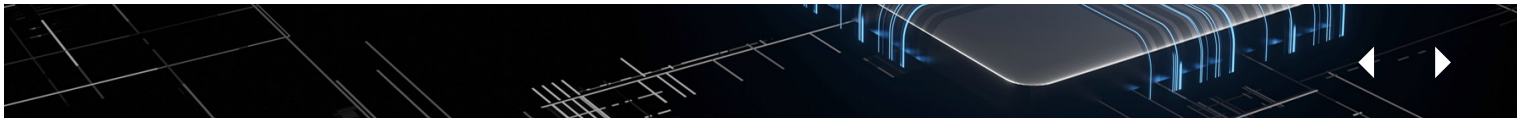
- Solicitations include clear requirements service providers must meet to be considered for award.
- Awards include verification that appropriate NIST SP 800-53 security controls are in place.
- Reliable continuous monitoring helps ensure the appropriate security controls remain in place during the life of the contract.

However, there are different paths a government may choose to implement its RAMP. The path selected should provide the best fit to the state or local government's policies, governance models and resources. Table 3 provides a high-level view of what can be expected from five basic options for the assessment of a cloud service product's security and privacy controls.

Table 3: Comparison of Assessment Options

	StateRAMP	FedRAMP	Govt.-Performed Audit	Third-Party Attestation	Self-Assessment
Based on NIST SP 800-53 Rev. 5	✔	✔	✔		
Requires annual audit by independent third-party assessment organization	✔	✔			
Requires monthly continuous monitoring	✔	✔			
Impact levels of low, moderate and high	✔	✔	✔	✔	
Verified statuses of Ready and Authorized	✔	✔			
Available to any provider, regardless of federal contract status	✔		✔	✔	✔
Documentation available to federal, state and local governments; public education institutions; and special districts.	✔	*		✔	
Centralized PMO reviews all security packages to ensure consistent application of standards and verification	✔				
Fast-track option for products with FedRAMP or StateRAMP	✔		✔		
Plans for mapping to other compliance frameworks: CJIS, MARSE, MMIS, IRS	✔		✔	✔	
Nonprofit mission to improve cyber posture for state and local government; education; special districts; and the providers who serve them	✔				

** NOTE: a limited set of FedRAMP documentation or redacted versions of specific documentation can be shared by a cloud service provider with non-federal entities.*



Section 3. Leveraging Cooperative Purchasing for RAMP

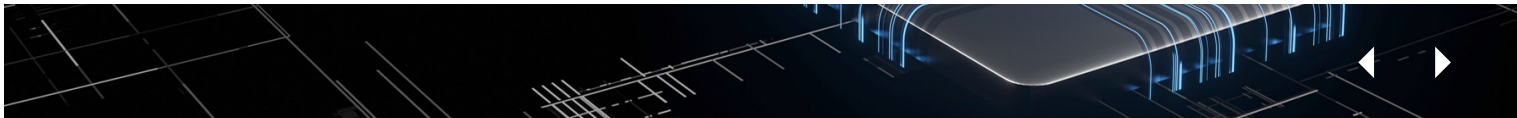
One of the fasted growing methods for cloud service acquisition in state and local government is cooperative purchasing. The demand for cloud-based services is expanding in all areas of government. Procurement offices challenged to keep pace with the demand are turning to competitively awarded cooperative contracts. Since this guide was first published in 2014, most major cooperative purchasing groups have added some type of cloud service contract.

Cooperative purchases can provide a supplier benefit by aligning disparate state purchases around a common, approved set of terms and conditions in a single master contract award. These procurements succeed because providers can more efficiently respond to a standard acquisition process, terms and conditions, and ordering mechanism instead of navigating different processes for each jurisdiction. The more standardization and consistency there is in buyer requirements — including security — the better value a supplier can provide.

The cooperative cloud service contracts available now allow a government to select the best fit from a menu of qualified providers for a wide variety of cloud products. When coupled with a RAMP authorization like StateRAMP or FedRAMP, the cloud product selected can include assurances of appropriate security and privacy controls and continuous monitoring for the life of the contract.

There are some things to consider before ordering a product from a cooperative contract.

- If you execute a contract with a reseller, will the terms and conditions bind the service provider, or will the service provider have different expectations in their terms and conditions to override? Having a reseller agree to RAMP requirements will be of little value if your ultimate service provider will not meet the requirements. To address this, look for cooperative contracts with awards directly to the service provider that will provide the cloud product, or make sure you negotiate your requirements into the agreement with the service provider. You may already have a licensing agreement with the service provider for other products that can be appended to your agreement.
- FedRAMP and StateRAMP authorizations are just for the cloud service product and not for the service provider's entire catalog. If the reseller is selling a service provider's FedRAMP- or StateRAMP-authorized product, resellers and service providers should be willing to provide appropriate assurance that the service provider will maintain the RAMP authorization throughout the life of your contract. From a risk perspective, the need for a direct contract with the service provider is lessened if the cloud product authorization validates a full range of rigorous controls at the time of award and through the life of the contract.
- Understand what security and data requirements the ultimate service provider is obligated to meet. Most cooperative purchase agreements do not specifically call for either StateRAMP or FedRAMP authorization, but if you are seeking a cloud service product that is authorized, and the cooperative contract permits it, you should be able to order it. If the product is



not clearly identified in the cooperative contract documentation, check with the person responsible for administering the cooperative contract to confirm that a RAMP-authorized product is within the scope of the cooperative contract.

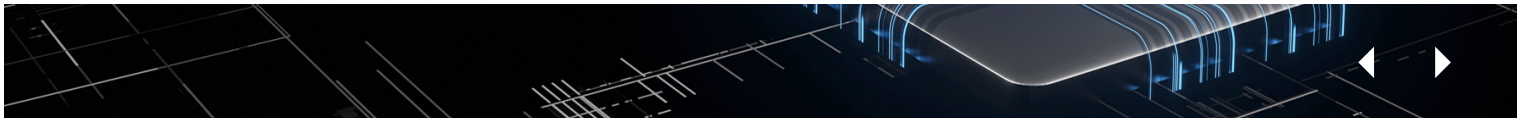
- Who will be required to conduct the due diligence on security, data and privacy controls? In most cooperative contracts, it is left up to the purchasing entity to validate the presence of controls. If the cloud service product is StateRAMP-authorized or if a service provider with FedRAMP-authorized offerings participates in the StateRAMP fast-track process, you'll be able to use the audits and reports from 3PAOs to validate and test security, data and privacy controls. If contracting with a service provider with FedRAMP-authorized offering(s) at the appropriate impact level, include a contract requirement that the service provider provide audit and continuous monitoring reports (with redaction as required to protect federal information) within an acceptable timeframe.

- Consider using a secondary selection process to require compliance with your security and privacy policy. Select from the service providers that will agree to provide a cloud product that meets your jurisdiction's RAMP. This could also include conformance to the cloud adoption policy, alignment with the enterprise cloud architecture, or compliance with project governance policy and review requirements.

With the rapid pace of change in cybersecurity, many first-generation cooperative contracts may have out-of-date security compliance standards for state and local governments. Most cooperative contracts leave any security due diligence to the purchasing jurisdiction. Some contracts help the government perform due diligence by requiring cloud products sold to be listed on the Cloud Security Alliance R-STAR listing. Using the CSA's Cloud Maturity Matrix — which cross-maps standards — a jurisdiction can determine how the product compares to its requirements. In other cooperative contracts, the jurisdiction may have to make an assessment based only on information from the provider.

There is an opportunity for cooperative purchasing groups to help state and local governments improve their security and increase the use of their next-generation cloud contacts by leveraging RAMP authorization. Standardizing on security requirements such as NIST SP 800-53 Rev. 5 in cooperative purchases would facilitate the use of more cooperative contracts across jurisdictions. Use of requirements such as StateRAMP Ready or StateRAMP Authorized would illustrate to all potential contract users that NIST SP 800-53 security standards are in place for the product and service at the time of award and throughout the duration of the contract. Use of a RAMP authorization program allows appropriate security, data and privacy controls to improve as NIST makes changes to address new issues and will keep longer-term contracts' controls fresh.

Smart execution of cooperative purchases can avoid duplication of efforts and speed up cloud contracting and deployment in government. Cooperative contracts that aggregate demand typically drive more favorable pricing. Cybersecurity and privacy risks are reduced when contracts include the appropriate NIST SP 800-53 controls and continuous monitoring. With the continued evolution of cloud computing, the aggregation of market demand and inclusion of an effective RAMP should provide leverage beyond what an individual state could hope to achieve on its own and provide lower-risk cloud service products.



Section 4. What's Coming Next: Over the Horizon

Don't forget constituent privacy. Privacy expectations are growing. Some states have organizationally separated privacy from security. For example, California and New Jersey have increased the visibility and priority of privacy by adopting new regulations.

While there is an upsurge in privacy legislation in states, most of the bills are aimed at consumer privacy and not constituent privacy, according to a July 7, 2022, article by Steve Nichols, former chief technology officer for the state of Georgia. He makes the point that "consumer privacy bills are creating a patchwork quilt of regulation" and goes on to say that "citizen privacy programs are going to have the same problem." In the article, he promotes NIST SP 800-53 Rev. 5 privacy controls that are blended with security controls as a good step for a state to take to bring consistency to the management of citizen privacy in state-provided applications.[35]

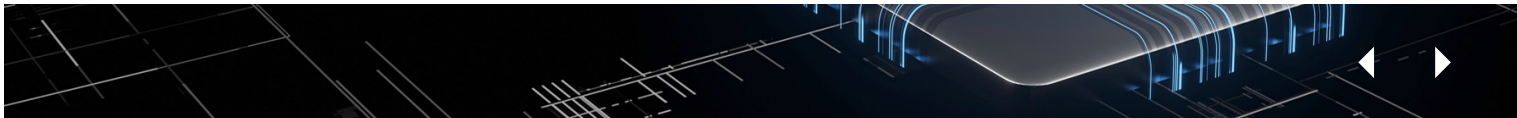
State and local governments can expect to see more demand for the protection of constituent data. Growing constituent privacy expectations need to be addressed in solicitations and contracts when constituent information is contained in data handled by a service provider. Most states have a PII statute, but that may not be sufficient. Greater constituent privacy expectations will require harmonizing various PII statute requirements with specific privacy controls built into contracts and solicitations.

Solicitations and contract documents should clearly identify the privacy controls required for the cloud product. Specific privacy controls should be determined in the project governance review process with input from the client agency, privacy officer or other position deemed responsible for constituent privacy. NIST SP 800-53 Rev. 5 has strengthened its family of privacy controls and is an excellent baseline to include in cloud solicitations and contracts along with cybersecurity.

Supply chain vulnerability in cloud services. With several significant breaches over the past few years in trusted partner's software, supply chain risk management (SCRM) is gaining traction. NIST defines SCRM as "The process of identifying, assessing and mitigating the risks associated with the distributed and interconnected nature of product and service supply chains…" In a nutshell, NIST says the SCRM process includes "(1) the conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; and (3) employment of techniques and procedures for the continuous monitoring of the security state of the information systems."

When suppliers apply risk management to their supply chains, vulnerability can be identified and mitigated. Large private companies are beginning to address threats in their supply chains, including cloud services, by including requirements for third-party SCRM through their contracts. With the challenges and resource constraints facing state and local government, SCRM is not a high priority for government procurement today but is on the horizon as a threat vector that can best be addressed through contracts that include appropriate SCRM measures and controls.

Fortunately, NIST has updated two special publications that provide up-to-date guidance that can improve supply



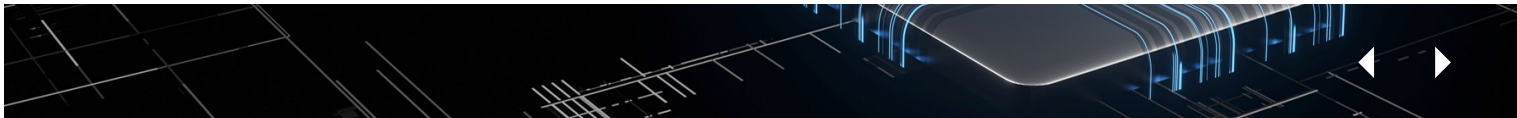
chain resiliency. NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, updated in May 2022, adds broad guidance to improve supply chain resiliency. When coupled with the new supply chain controls family added in NIST SP 800-53 Rev. 5, state and local governments can greatly reduce risk and improve their supply chain resiliency.

Other excellent resources are the assessments, reports and materials gathered by the Information and Communications Supply Chain Management Task Technology Task Force reports. Since its inception in December of 2018, the task force has worked with industry and U.S. government agency partners to develop resources to address IT supply chain risk that are available on the Cybersecurity and Infrastructure Security Agency website at https://www.cisa.gov/ict-scrm-task-force. In 2022, NASPO and NASCIO joined the task force as partners to help develop actionable solutions that can work for a broader range of government organizations. IT supply chain risk related to promoting software assurance and the utility of software bill of materials is now under scope development.

With the development of StateRAMP, state and local governments now have a resource upon which to rely for standardized assessment and access to continuous monitoring. With StateRAMP's verify-once, serve-many approaches, service providers find value in the model as well. The ability for a government to partner with StateRAMP to provide the resources of a RAMP specifically designed with state and local government input means existing resources can be reallocated. With more services transitioning to the cloud and as the Internet of Things grows ever larger, it becomes more evident that StateRAMP provides an invaluable resource to state and local governments.

Rising cost of cyber insurance. Over the past decade, the use of cybersecurity insurance in state and local government insurance portfolios, as well as a requirement for contractors in many IT contracts, became a fairly common practice to address cyber risk. However, the high cost of cyber insurance coverage and growing exclusions — driven largely by the proliferation of ransomware attacks — make risk transfer through cyber insurance a less attractive practice.

In a recent report, the Government Finance Officers Association emphasized a three-pronged approach to risk management as they concluded, "Savvy risk management requires making smart use of strategies to manage that risk, including reducing risk by implementing cybersecurity controls, absorbing risk with self-insurance, and transferring risk to the insurance market by purchasing a commercial insurance policy." When developing future RFPs and contracts, officials should carefully consider the benefits and costs before requiring the provider to acquire cyber insurance. This idea also applies when adding or continuing cyber coverage as a part of the jurisdiction's insurance portfolio. Investment in prevention through control implementation can result in greater risk reduction than the purchase of cyber insurance.



Appendix 9

Risk and Authorization Management Program (RAMP) Checklist

This RAMP checklist provides guidance to state and local governments that intend to pursue the procurement, deployment and use of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS) or anything-as-a-service (XaaS) solutions.

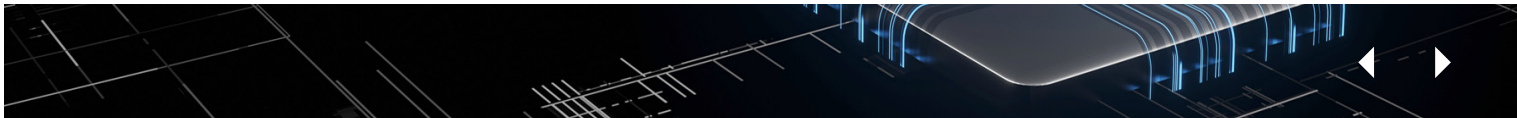
The foundations of RAMP for cloud security have been established and standardized by the Federal Government through FedRAMP and the nonprofit governing committees of StateRAMP. These foundations include:

- NIST SP 800-53 security and privacy controls and standards
- Impact levels based on data sensitivity and the nature of privacy
- Independent audit by accredited organizations
- Validation and verification of security package and audit
- Monthly continuous monitoring and reporting
- Annual audit for continuous improvement and monitoring

FedRAMP, administered through the General Services Administration (GSA), was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government, with an emphasis on security and protection of federal information.[36] FedRAMP is governed by federal executive branch entities that work to develop, manage and operate the program. The Joint Authorization Board, the primary governance and decision-making body for FedRAMP, consists of the CIOs from the Department of Defense, Department of Homeland Security and GSA.[37] FedRAMP standardizes requirements for the authorization and ongoing cybersecurity of cloud services in accordance with the Federal Information Security Modernization Act, Office of Management and Budget Circular A-130 and FedRAMP policy. FedRAMP leverages NIST standards and guidelines to provide standardized security requirements for cloud services, a conformity assessment program, standardized authorization packages and contract language, and a repository for authorization packages.[38]

Although FedRAMP is focused on federal government agencies and the protection of federal information, state and local governments have generally accepted a service provider's achievement of FedRAMP marketplace designations for their cloud service offerings (Ready, In-Process, Authorized) for specific impact levels (Low, Moderate or High) as a verification of the cybersecurity posture of the service provider and its offering(s). Prior to achieving a FedRAMP Authorized designation, a service provider's offering(s) must be audited — initially and via continuous monitoring — by an authorized third-party assessment organization (3PAO) and be in use by a federal agency.

However, not all cloud service providers operate in the federal government marketplace. Some providers focus their cloud service offerings on the state and local government



and education (SLED) marketplace. In addition, foundational documentation generated within the FedRAMP program — readiness and security assessment reports, 3PAO audit and continuous monitoring reports, authorization packages, etc. — may contain federal data and would require redaction before sharing with any non-federal entity.

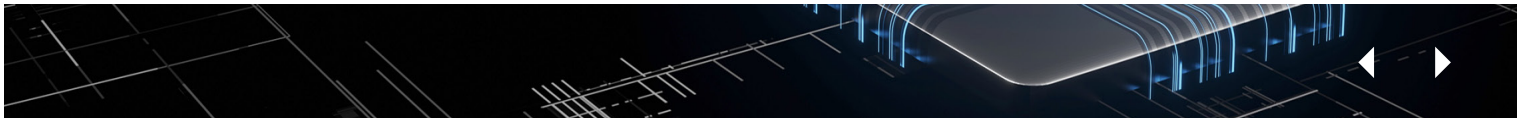
More information on specific FedRAMP requirements, documents and resources can be found at https://www.fedramp.gov/documents-templates/.

StateRAMP, established in 2020 as an independent nonprofit organization, is modeled in part after FedRAMP. It relies on FedRAMP Authorized 3PAOs and, more recently, StateRAMP-registered 3PAOs to conduct assessments. StateRAMP offers RAMP services designed for state and local governments, public education institutions, and special districts. StateRAMP's Standards and Technical Committee, comprising both government and service provider members, makes recommendations to the StateRAMP Board of Directors regarding verification policies, security standards, best practices, and audit and assessment processes to create common standards that are acceptable to state and local governments and service providers. To be verified, cloud service providers must meet minimum security requirements and provide an independent audit conducted by an authorized 3PAO. StateRAMP recognizes three verified statuses: Ready, Provisional and Authorized. To ensure ongoing security compliance and risk mitigation, service providers must comply with continuous monitoring requirements to maintain a verified security status. StateRAMP verified cloud service offerings can be found at https://stateramp.org/product-list/.

StateRAMP Fast Track for Cloud Service Offerings with FedRAMP Designations

StateRAMP and FedRAMP have similar requirements based on NIST SP 800-53, and both rely on independent audits and continuous monitoring by approved 3PAOs. Recognizing these shared best practices, StateRAMP offers a fast-track process for verifying service provider offerings that have achieved FedRAMP Marketplace designations.

The fast-track process allows service provider offerings with designations of FedRAMP Ready, Authorization to Operate (ATO) from a federal agency, or a Provisional ATO from the FedRAMP Joint Authorization Board to leverage their FedRAMP audit reports and associated documentation to become StateRAMP Ready or Authorized. The service provider does not have to complete a new audit for StateRAMP and may use FedRAMP templates for ease of compliance. The StateRAMP Security Team, operating within the StateRAMP Program Management Office, works with service providers to validate and authenticate relevant security packages and review recent continuous monitoring audits and reports. Service providers participating in the StateRAMP fast-track process can utilize the same reporting they provide to FedRAMP.



RAMP Checklist

☐ **Identify key government stakeholders**
Starting and maintaining a RAMP within a state or local government organization takes cooperation and alignment among enterprise-level executive management and program leaders in IT, cybersecurity and privacy, risk management, procurement, and legal counsel. Each of these functional areas plays an important role in developing and operating a RAMP. An effective risk assessment and management program for cloud procurements and deployed cloud solutions requires harmonious policy development, coordinated governance and oversight, and focused operational execution in each policy owner's respective role.

Procurement, implementation and secure use of a cloud service requires that all appropriate stakeholders are notified and engaged. Depending on the scope and scale of the effort, some or all of the following stakeholders should be involved:

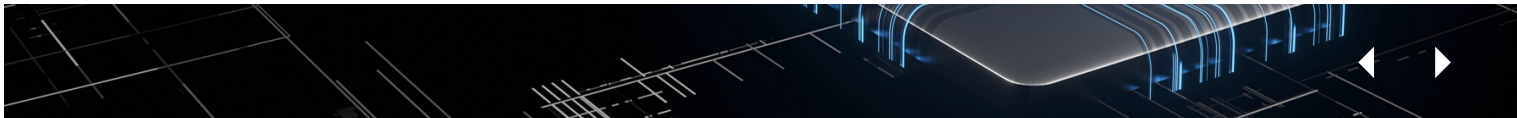
- Executive and program leaders
- Chief information officer
- Chief procurement officer
- Legal counsel (if possible)
- Chief information security officer
- Chief privacy officer
- Chief risk officer
- Chief technology officer
- Others on an as-needed basis

☐ **Establish a governance body and oversight process**
Once key stakeholders are identified and committed to participate in the effort, jurisdictions need to create and adopt a governance and oversight charter. The charter should clearly describe the governance body's purpose and scope of authority; the process for making, communicating and adopting decisions; the method for selecting and replacing governance body leaders and members; the roles, responsibilities and decision rights of individual members; the process to form and abolish subcommittees and for considering and acting upon subcommittee findings and recommendations; how often the governing body will meet; and the frequency for reviewing and revising the charter.

☐ **Adopt a cybersecurity framework and security controls for the acquisition, deployment and continuous monitoring of cloud solutions**
The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the NIST Special Publication (SP) 800-53 provide standards, guidelines, best practices and controls to help organizations manage cybersecurity and privacy risk. Both publications are living documents that are refined and improved over time.

The primary RAMPs that have been initiated for use by federal, state and local government organizations are:

- FedRAMP — For federal agencies and their service providers
- StateRAMP — For state and local government member organizations and their service providers



- AZ-RAMP (State of Arizona) — For Arizona state agencies and their service providers. (Arizona is transitioning to StateRAMP.)
- TX-RAMP — For Texas state agencies and their service providers. (TX-RAMP recognizes StateRAMP or FedRAMP authorizations and provides automatic reciprocity for any StateRAMP authorized products, including a weekly sync with StateRAMP's authorized product list.)

The NIST CSF and NIST SP 800-53 security controls are foundational to each of these RAMPs and are familiar to the service providers who seek authorization to operate under these programs. With that in mind, the Center for Digital Government recommends that state and local governments consider adopting the NIST CSF and associated NIST SP 800-53 security controls as soon as possible.

There are notable differences between the NIST CSF and NIST SP 800-53 security controls. Jurisdictions need a clear understanding of these differences and how key NIST CSF functional areas and specific NIST SP 800-53 security controls align with and support one another.

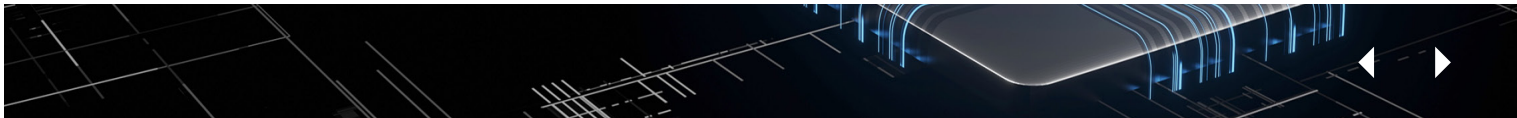
Mapping of NIST CSF Version 1.1 to NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations.

State and local jurisdictions are also using other common cybersecurity frameworks and associated security controls, including:

- International Standards Organization (ISO) 27000 Series (27001 and 27002)
- Center for Internet Security (CIS) Critical Security Controls
- Service Organization Control (SOC) Type 2
- ISACA Control Objectives for Information Technology (COBIT)
- HITRUST Common Security Framework
- Payment Card Industry (PCI) Data Security Standard (DSS)

State and local governments are free to adopt and use alternative cybersecurity frameworks and security controls for their cloud service acquisitions and deployments, either on a wholesale basis or to augment the NIST SP 800-53 security controls. However, governments should carefully consider the benefits and impacts when adding controls that duplicate or conflict with security controls recommended within NIST SP 800-53. They should also be cautious about customizing controls or using self-generated security controls when a nationally recognized set of standard security controls already exists.

Broader adoption of the common and rigorous cybersecurity framework and associated security controls published and regularly updated by NIST for use by federal, state and local governments will encourage and allow more qualified service providers to compete for government contracts at all levels. State and local government RAMPs that integrate baseline NIST SP 800-53 controls will benefit from more competitive service provider offers that can readily be audited against their adopted security controls. Broader acceptance of a standard set of controls used by government organizations in cloud service



contracting will reduce the number of exceptions and speed up contracting, deployment and continuous monitoring processes for all concerned, including the service providers who must comply with those controls.

☐ **Inventory, review and update existing policies, contract templates, and terms and conditions**

Business alignment and risk management depend on effective governance and oversight. Governance body members should participate in and (where appropriate) lead RAMP discussions, planning and implementation. They should engage in the development and adoption of internal policies, procedures, and standards related to cybersecurity and the procurement, deployment and continuous monitoring of cloud solutions acquired to support government operations.

Informed decisions and proper care and due diligence rely on timely, accurate and complete information. Jurisdictions should inventory and review their policies, procedures, standards, contract templates, contract terms and conditions, and recent requests for proposal in the following areas:

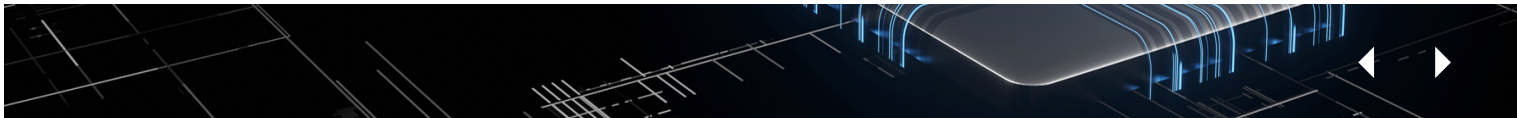
- Cloud acquisition, contract management, risk assessment/management and implementation policies.
- Data classification; data privacy; information security; and risk assessment statutes, policies, standards and requirements. Include any policies or guidance that describe how your jurisdiction decides on the level of data classification and controls for cloud services it procures.
- Cloud RFPs, contract templates, and terms and conditions for each cloud service model (SaaS, PaaS, IaaS, XaaS) your jurisdiction acquires. Focus on provisions or sections related to data ownership, privacy and confidentiality; breach or security incident notification; audit; and compliance with security standards.

Once the inventory and review are complete, make appropriate revisions to relevant policies, procedures, standards, contract templates, and associated contract terms and conditions to align them with the adopted cybersecurity framework and associated security controls. Consider establishing an exception or waiver process to accommodate unique situations.

☐ **Decide whether to develop and manage your own RAMP or join and utilize StateRAMP**

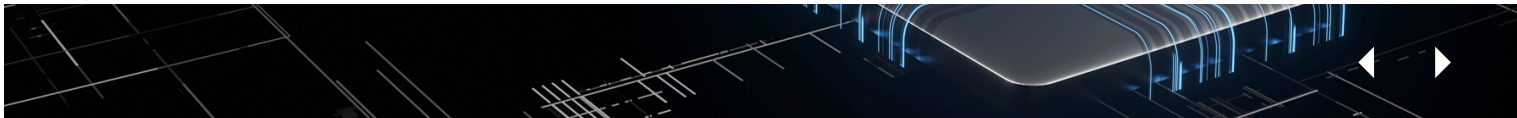
State and local governments must make some foundational choices once they decide to use a RAMP for the acquisition, deployment and continuous monitoring of cloud services. Generally, the jurisdiction can choose to join and utilize StateRAMP or develop and manage a do-it-yourself (DIY) RAMP.

Note: State and local government organizations can't "join" FedRAMP. But they may choose, as part of StateRAMP or a DIY RAMP, to accept a service provider's FedRAMP Marketplace designations as verification of the cybersecurity posture of the cloud service provider and its offering(s). Documentation generated within the FedRAMP program may contain federal data and would require redaction prior to authorization to share with any non-federal entity.



The following table provides a high-level comparison of StateRAMP and DIY RAMP options. With either StateRAMP or a DIY RAMP, the public jurisdiction will need to define and adopt an exceptions process for occasions when an alternative method of verification and monitoring is acceptable based on risk.

StateRAMP: A Shared Service for Government	Do-It-Yourself (DIY) RAMP
Standardized requirements that are developed and maintained with annual review by governance committees comprising multiple state, local government and private sector members.	Unique requirements developed and maintained by the state or local government organization. May or may not include adoption/acceptance of FedRAMP or StateRAMP requirements, authorizations, audit and continuous monitoring reports, and other documents.
StateRAMP provides resources, including staff, to maintain policies, procedures, security reviews and continuous monitoring.	Estimated staff resources needed to operate a statewide DIY RAMP: 25 or more full-time employees.
StateRAMP provides a secure, FedRAMP Authorized repository for storing provider documentation and continuous monitoring reports.	The state or local government organization must procure and implement a secure repository for storing provider documentation and continuous monitoring reports.
StateRAMP offers assistance for updating policies, procedures and procurement language.	The state or local government organization must develop, update and maintain policies, procedures and procurement language on its own.
StateRAMP provides ongoing training for state or local government stakeholders.	The state or local government organization must develop, update and maintain stakeholder education training programs and materials.
StateRAMP provides ongoing education, training and resources for service providers.	The state or local government organization must develop, update and maintain service provider education programs, resources and materials.
No cost to the state or local government.	Significant investment of government staff time and money.



The states of Arizona and Texas have initiated the development and management of a DIY RAMP. Arizona's initial RAMP deployment was discretional, while the Texas Department of Information Resources (DIR) was directed to develop and deploy TX-RAMP by Senate Bill 475 (2021). More information on TX-RAMP can be found at:

- TX-RAMP Program Overview
- TX-RAMP Overview for State Agencies
- TX-RAMP Overview for Vendors

TX-RAMP recognizes StateRAMP or FedRAMP authorizations. Further, if a cloud computing service is TX-RAMP certified through the FedRAMP or StateRAMP equivalent authorization process, the service provider is not required to provide continuous monitoring artifacts to the Texas DIR. Arizona and Texas provide automatic reciprocity for StateRAMP-authorized products, and Arizona is making a full transition to StateRAMP.

Both states recommend that other state and local governments take a measured and thoughtful approach to RAMP development and adoption. They recommend a phased approach — balancing level of effort with perceived risk — and clearly defined requirements and expectations for the public jurisdiction and its service providers. Developing and managing a stand-alone DIY RAMP program is resource-, expertise- and time-intensive and difficult to sustain. State and local governments should use a formal feasibility/business case analysis to carefully consider initial and ongoing costs, resource requirements and constraints, and benefits and risks of a pursuing a DIY approach versus viable alternatives such as StateRAMP.

Additional StateRAMP Resources:

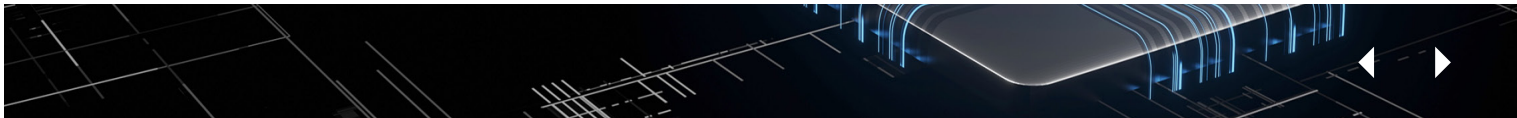
- StateRAMP Overview
- Introduction to StateRAMP
- Getting Started with StateRAMP
- StateRAMP Minimum Mandates for Cloud Service Provider "Ready Status" at Moderate and High Impact
- StateRAMP Minimum Mandates for Cloud Service Provider "Ready Status" at Low Impact
- StateRAMP FAQs
- StateRAMP BLOG

Additional FedRAMP Resources:

- FedRAMP Overview
  - Program Basics
  - Governance
- FedRAMP Partners
  - Federal Agencies
  - Cloud Service Providers
  - Assessors
- FedRAMP Authorization Process
  - Federal Agency Authorization
  - Joint Authorization Board (JAB) Authorization
- FedRAMP Documents and Templates
- FedRAMP FAQs
- FedRAMP Blog

☐ **Conduct a data discovery and classification process**
(Source: Michigan - 1340.00.150.02 DATA CLASSIFICATION STANDARD)

Data classification identifies and categorizes information and information systems based on their sensitivity, criticality and risk. Without data classification, a state or

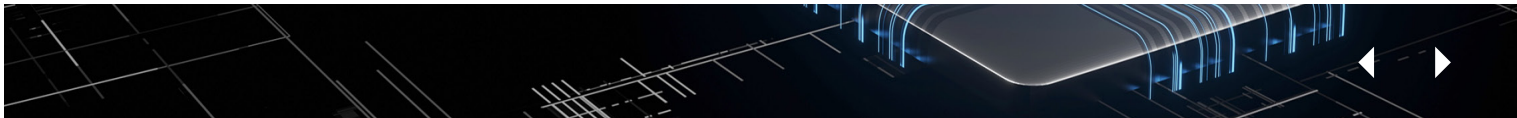


local government agency may have inadequate security controls for its data, which may lead to a security incident or data breach. Data discovery and classification are critical to making decisions about technical architecture, information security and privacy, procurement, and contracting.

The first step in the data classification process involves identifying data that is collected, processed, stored and/or transmitted via information systems regardless of their hosting location. Next, agencies must identify and understand applicable state and federal laws and regulations, policies, procedures, standards, and privacy compliance requirements that direct how they protect information systems and data from unauthorized disclosure, modification, destruction, access, use or dissemination. Additional security requirements may be found in external contractual agreements that require special handling or protection of the data.

Once that information is known, agencies must determine the proper regulatory levels of protection for in-scope data and information systems. Not all information systems or data require the same level of security controls or pose the same risk, so data classification levels are used to identify the sensitivity and criticality of the information. The following table gives a brief description of a sample set of data classification levels.

Data Classification Level	Description	Examples
Public	Public data is information that has been explicitly approved for distribution to the public and can be disclosed to anyone without violating an individual's right to privacy or causing any potential harm. Public data is not sensitive in context or content, and it does not require special protection. If disclosed or compromised, public data will not expose the organization to financial loss or embarrassment, compromise a competitive advantage or jeopardize security information.	• Agency public websites • Brochures • News releases • Publicly available financial reports • Executive budgets • Non-exempt FOIA documents
Internal	Internal data is information that is not sensitive to disclosure within the organization. Data created, updated or stored by the organization is considered by default to be internal information intended for use by employees and authorized agents, although it may be accessed by trusted partners covered by non-disclosure agreements. This information shall be shared internally to support internal operations, lower costs, prevent duplication and otherwise enhance the condition or operation of an organization's systems.	• Agency policies and procedures • Customer information • Driver history records • Internal announcements and communications • Internal phone directories and organizational charts • Network diagrams • Non-sensitive operational reports



Data Classification Level	Description	Examples
Confidential	Confidential data is sensitive information wherein unauthorized disclosure could cause serious financial, legal or reputational damage to an organization. Confidential data may include personally identifiable information (PII) or confidential non-public information that relates to an organization's business. Confidential data should only be made available to authorized personnel on a need-to-know basis and should require a signed non-disclosure agreement.	• Social Security numbers • Credit card numbers • Civil investigative data • Criminal history data • Confidential business information • Financial statements • Health and medical records
Restricted	Restricted data is information that is extremely sensitive. Disclosure or corruption of restricted data could be hazardous to life or health, cause extreme damage to integrity or image, and/or impair the effective delivery of services. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship and major economic impact. Restricted data can be made available to named individuals or specific positions on a need-to-know basis.	• Sensitive law enforcement data • Investigative records and communications systems • Disaster recovery and business continuity plans • Protected critical infrastructure information

The next step involves assigning a high, moderate or low potential impact level to each security objective for each data type or information system being classified. Table 2 is an excerpt from Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems. The same set of standards can be used for state and local government data and information systems. The table summarizes potential impacts on confidentiality, integrity and availability. This table is used when determining the data impact level for each data type or information system.

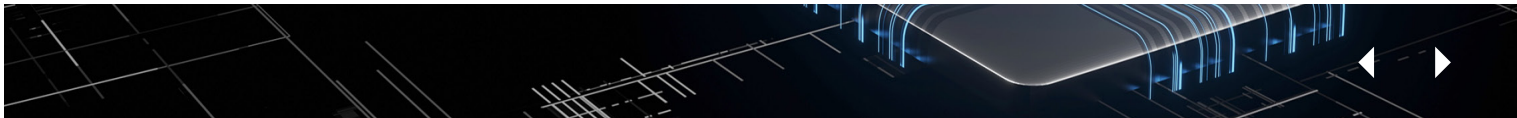


Table 2 – Impact Level and Definition

Security Objective	Potential Impact Low	Potential Impact Moderate	Potential Impact High
Confidentiality Defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	Unauthorized disclosure of this information could have a limited adverse effect on organizational operations and assets or individuals.	Unauthorized disclosure of this information could have a serious adverse effect on organizational operations and assets or individuals.	Unauthorized disclosure of this information could have a severe or catastrophic adverse effect on organizational operations and assets or individuals.
Integrity Defined as guarding against improper information modification or destruction. It includes ensuring information non-repudiation and authenticity.	Unauthorized modification or destruction of this information could have a limited adverse effect on organizational operations and assets or individuals.	Unauthorized modification or destruction of this information could have a serious adverse effect on organizational operations and assets or individuals.	Unauthorized modification or destruction of this information could have a severe or catastrophic adverse effect on organizational operations and assets or individuals.
Availability Defined as ensuring timely and reliable access to and use of information.	Disruption of access to or use of this information or information system could have a limited adverse effect on organizational operations and assets or individuals.	Disruption of access to or use of this information or information system could have a serious adverse effect on organizational operations and assets or individuals.	Disruption of access to or use of this information or information system could have a severe or catastrophic adverse effect on organizational operations and assets or individuals.

StateRAMP, NIST and FedRAMP offer additional data classification resources.

StateRAMP has worked with multiple government and industry leaders to develop a data classification tool for state and local government. This tool is evaluated and updated annually by the StateRAMP Standards & Technical Committee.

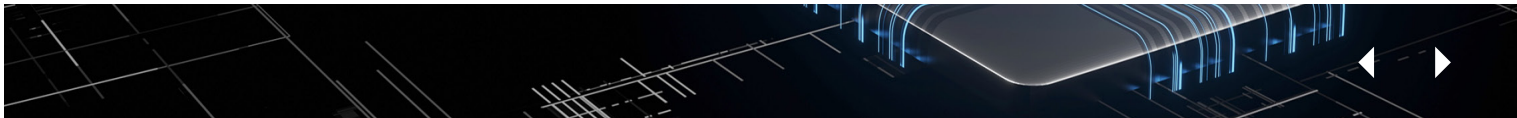
- 2022 Data Classification Tool
- Other StateRAMP templates and resources

NIST Resources:

- NIST SP 800-60 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-60 Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST FIPS-199 Guidance on Standards for Security Categorization of Federal Information and Systems

FedRAMP Resources:

- FedRAMP templates and resources



☐ **Determine the security impact and required security category**

(Source: Michigan - 1340.00.150.02 DATA CLASSIFICATION STANDARD)

This step establishes the appropriate security category of the data being classified. Security categorization is the basis for selecting the proper security control to protect the information. It is determined at the data type and information system level. Once the data impact levels have been selected for each security objective, the security categorization is assigned to each information system or data type as defined in Table 3.

Table 3 – Security Categorizations

Security Categorization	Impact Designation
Low	An information system and/or data type in which all three security objectives — confidentiality, integrity and availability — are assigned a FIPS 199 potential impact value of low.
Medium	An information system and/or data type in which at least one security objective — confidentiality, integrity or availability — are assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact of high.
High	An information system and/or data type in which at least one security objective — confidentiality, integrity or availability — is assigned a FIPS 199 potential impact value of high.

Security categorization of an information data type

Establishing the appropriate security categorization for a data type merely requires determining the potential impact for each security objective associated with the specific data type and using the highest values from the impact designations (see Table 3).

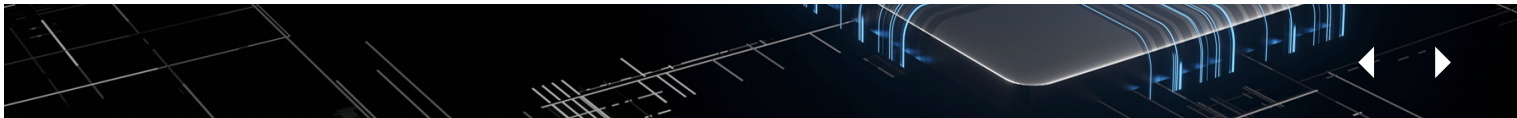
Example 1: A law enforcement agency manages extremely sensitive information. The information owner determines that the potential impact from the loss of confidentiality is high, the potential impact from the loss of integrity is moderate and the potential impact from a loss of availability is moderate. The resulting categorization for this data is defined as:

Data Type	Confidentiality	Integrity	Availability
Extremely Sensitive Information	High	Moderate	Moderate

Based on the security objectives and the overall data impact level, the security categorization for this data type would be high.

Security categorization applied to an information system

Determining the security category of an information system requires the organization to analyze all the security categories of all data types that reside on the information system. The potential impact values assigned to the security objectives — confidentiality, integrity and availability — shall be the highest values among the security



categories that have been determined for each type of data residing on the information system (see Table 3).

Example 2: An information system used by multiple departments for large contracts contains both sensitive contract information and non-sensitive administrative information.

The information system owner has determined for contract information that the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate and the potential impact from a loss of availability is low. For administrative information, the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low and the potential impact from a loss of availability is low. The overall security categorization of this information system would be:

Data Type	Confidentiality	Integrity	Availability
Contract Information	Moderate	Moderate	Low
Administrative Information	Low	Low	Low

Based on the security objectives and the overall impact level, the security categorization for this information system would be moderate.

Example 3: An information system used by a single department for tracking small projects contains only non-sensitive project information. For this project information, the potential impact from a loss of confidentiality is low, the loss of integrity is low and the potential impact from a loss of availability is low. The overall security categorization of this information system would be:

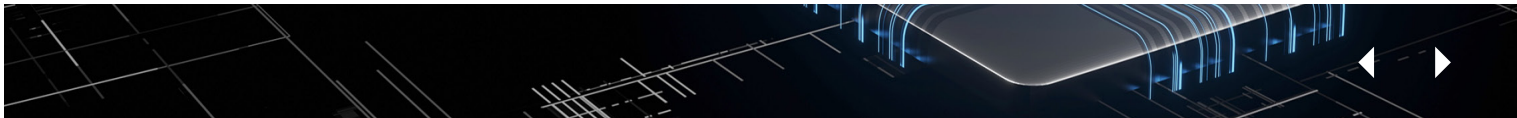
Data Type	Confidentiality	Integrity	Availability
Project Information	Low	Low	Low

Based on the security objectives and the overall impact level, the security categorization for this information system would be low.

StateRAMP, NIST and FedRAMP offer additional security impact/categorization resources.

StateRAMP Resources:
- StateRAMP 2022 Data Classification Tool (StateRAMP's Standards & Technical Committee evaluates this tool annually)
- StateRAMP templates and resources

NIST Resources:
- NIST SP 800-60 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-60 Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories



- NIST FIPS-199 Guidance on Standards for Security Categorization of Federal Information and Systems

FedRAMP Resources:
- Understanding Baselines and Impact Levels in FedRAMP
- FedRAMP templates and resources

☐ **Determine baseline security controls for the cloud service procurement**

(Source – StateRAMP Security Controls – Baseline Summary v1.2 April 29, 2022)

Next, the state or local government organization must select a baseline set of security controls. StateRAMP and FedRAMP provide baseline controls by impact level. For standardization, the Center for Digital Government recommends that organizations incorporate these baseline controls into their requirements.

NIST SP 800-53 provides a comprehensive set of security controls that may be applied to IaaS, PaaS or SaaS cloud service offerings. Not all security controls generally recommended within NIST SP 800-53 will be applicable or appropriate to all cloud services. The specific data classification, security impact and required security category for each data type or information system should drive the selection of specific security controls applied to the cloud service being procured.

StateRAMP and FedRAMP offer additional resources:
- StateRAMP Security Controls — Baseline Summary v1.2 (April 29, 2022)
- StateRAMP Templates and Resources
- FedRAMP Security Controls Baseline (based on NIST SP 800-53) is available on FedRAMP.gov. Search for "security controls baseline" for the current version.

☐ **Identify continuous monitoring and reporting requirements**

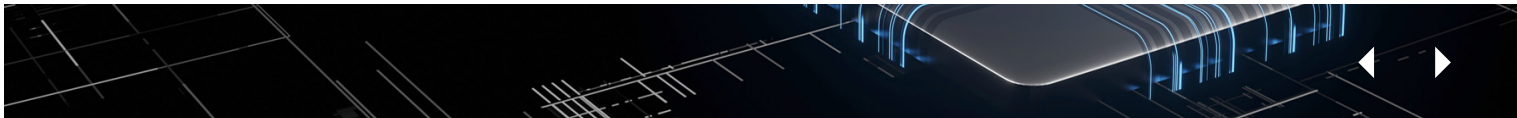
(Source – FedRAMP Continuous Monitoring Strategy Guide, Version 3.2 April 4, 2018)

Monitoring security controls is part of the overall risk management framework for information security. Performing ongoing security assessments determines whether the security controls for a cloud information system remain effective considering new exploits and attacks and planned and unplanned changes that occur in the system and its environment over time.

State and local governments should require service providers to monitor their security controls (using client-approved self-assessments or assessments performed by a 3PAO), assess them on a regular basis and demonstrate that the security posture of their cloud service offering is continuously acceptable to the state or local government client throughout the life of the contract.

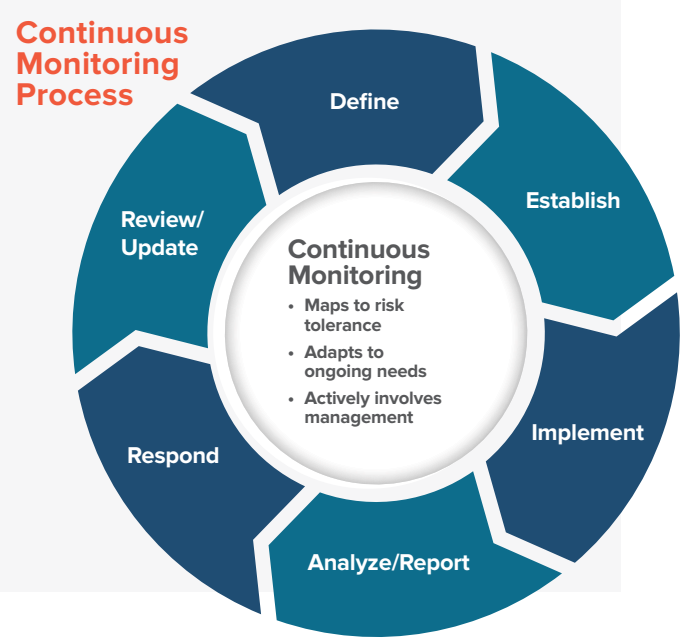
NIST SP 800-137 says the continuous monitoring process should include the following initiatives:

- Define a continuous monitoring strategy based on risk tolerance that maintains clear visibility into assets and awareness of vulnerabilities and utilizes up-to-date threat information.



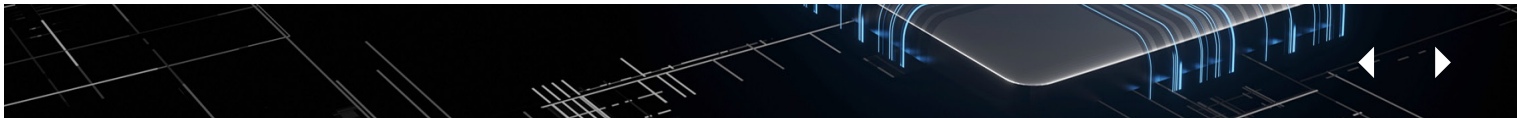
- Establish measures, metrics, and status monitoring and control assessment frequencies. These activities should make known the organization's security status and detect changes to information system infrastructure and environments of operation and changes in the status of security control effectiveness in a manner that supports continued operation within acceptable risk tolerances.
- Implement a continuous monitoring program to collect the data required for the defined measures and report on findings. Automate collection, analysis and reporting of data where possible.
- Analyze the data gathered and report findings accompanied by recommendations. Agencies may need to collect additional information to clarify or supplement monitoring data.
- Respond to assessment findings by deciding whether to mitigate technical, management, and operational vulnerabilities; accept the risk; or transfer it to another authority.
- Review and update the monitoring program, revising your continuous monitoring strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enhance data-driven control of the security of your information infrastructure, and increase organizational flexibility.

Security control assessments performed periodically validate whether stated security controls are implemented correctly, operating as intended and meet baseline security controls set by the state or local government as part of the cloud service contract. Security status reporting gives state and local government officials information they need to make risk-based decisions. It also provides assurance regarding the security posture of the cloud information system.



StateRAMP's governance committees have developed continuous monitoring requirements that are reviewed annually. These requirements include monthly reporting from the service provider on the product's security posture to the StateRAMP Program Management Office. They also include an annual audit conducted by a 3PAO.

Any product with a StateRAMP certification of Ready, Authorized or Provisional must comply with StateRAMP's continuous monitoring requirements to maintain its certification. StateRAMP recommends that government organizations require service providers to grant them access to StateRAMP's continuous monitoring reporting.



StateRAMP governance committees also have developed a Continuous Monitoring Escalation Guide to notify participating government organizations of issues before a problem occurs or the product is out of compliance.

View StateRAMP's continuous monitoring requirements and policies on the StateRAMP templates and resources and below:

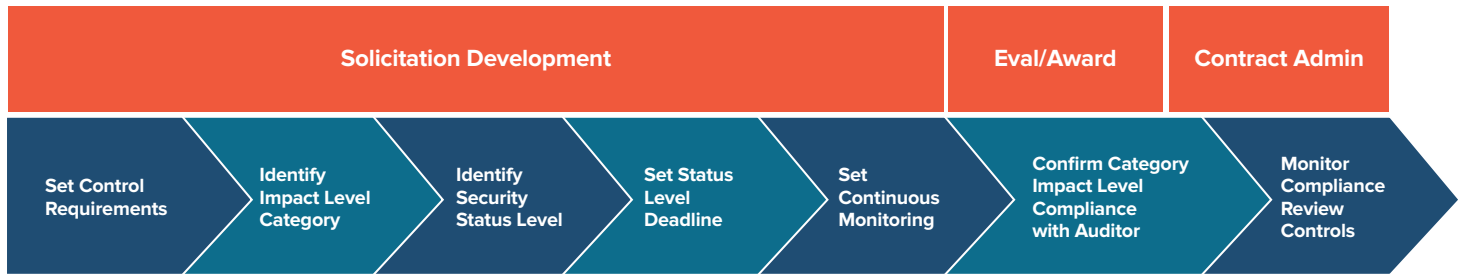
- StateRAMP Continuous Monitoring Guide
- StateRAMP Continuous Monitoring Escalation Process
- StateRAMP Security Assessment Framework
- StateRAMP Incident Communication Procedures
- StateRAMP Vulnerability Scan Requirements Guide

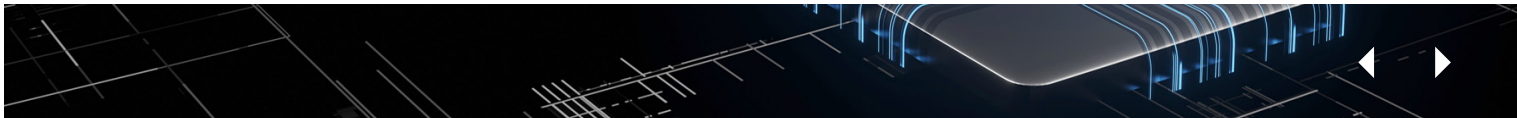
☐ **Align the procurement process with RAMP requirements**

Government organizations must align procurement processes and practices with their RAMP strategy. Appendix 8, section 2, offers 11 steps state or local governments can take to make changes in procurement practices to facilitate RAMP implementation. While these steps are common to most cloud procurement and contracting elements, the specific details of each step must be adopted to meet the government jurisdiction's specific RAMP strategies and procurement regulations.

Organizations can develop some of the procurement alignment steps in parallel with this RAMP checklist. But some procurement process changes that involve continuous monitoring requirements, baseline security controls, the application of security impact categories, readiness status and others will depend on work completed earlier in this checklist.

Procurement Activities to Align with RAMP



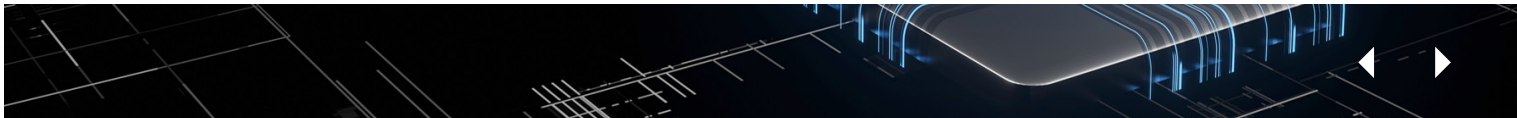


☐ **Communicate RAMP requirements to internal stakeholders and service providers**

(Source – Getting Started with StateRAMP, A Guide for Government (V1.5, December 2022)

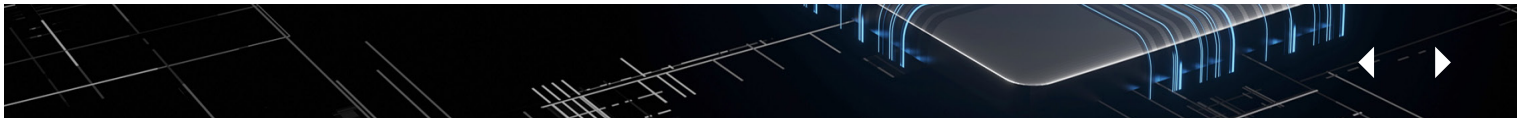
Those responsible for leading the state or local government RAMP should proactively communicate about the RAMP to internal government stakeholders and the vendor community, including service providers that may have responded to solicitations within the last three years. Communications to internal stakeholders and notices to the service provider community should include the following information about the RAMP:

- Mission, goals and objectives
- Governance and oversight
- Adoption of a cybersecurity framework
- Review and update of cybersecurity policies and standards
- Review and update of request for proposal, contract templates, and associated terms and conditions
- Adoption of security controls and continuous monitoring requirements for the acquisition, deployment and continuous monitoring of all cloud service solutions moving forward
- Training regarding the updated procurement process and impacts on each stakeholder's regular business processes



Appendix 9: Risk and Authorization Management Program (RAMP) Checklist

- ☐ Identify key government stakeholders
- ☐ Establish governance body and oversight process
- ☐ Adopt a cybersecurity framework and security controls
- ☐ Inventory, review and update existing policies, contract templates, and terms and conditions
- ☐ Decide whether to develop and manage a DIY RAMP or join and utilize StateRAMP
- ☐ Conduct a data discovery and classification process
- ☐ Determine the security impact and required security category
- ☐ Determine baseline security controls for the cloud service procurement
- ☐ Identify continuous monitoring and reporting requirements
- ☐ Align the procurement process with RAMP requirements
- ☐ Communicate RAMP requirements to internal stakeholders and the service provider community



Expert Spotlight: *Danielle Hinz, AWS*

Danielle Hinz *is an executive government advisor at Amazon Web Services (AWS) and former chief procurement officer for King County, Washington. In this Q&A, she discusses shared responsibility models for securing data and systems, the importance of reimagining procurement to provide value to contituents, and the cultural changes required to make cloud work for government.*

Q: How are government cloud procurement policies evolving?

One of the big themes is moving to outcomes-based procurement models. Public sector organizations are defining the problems they're trying to solve and asking industry to respond with solutions. A lot of organizations are realizing it's better to ask industry how to solve a problem rather than providing a predefined solution.

We're also seeing a shift — a good shift — where procurement is partnering with IT and others in the organization to think through how to serve the public interest in terms of securing systems and making sure they are adequately supported over a multi-year period. Procurement is really leaning into working with partners to execute on the strategic vision and modernize applications.

Q: How have AWS offerings evolved to meet changing government needs?

We're expanding our participation in cooperative contracts. We know public sector organizations, especially smaller ones, like cooperative contracts because of the scale they offer. These contracts also let agencies move faster because they provide an established procurement process.

We've modified our AWS Marketplace to provide specific features that better meet government needs, including standard contract terms that are being adopted by more and more of our partners selling through the marketplace. With 80% of terms standard, organizations only have to work on the few that are specific to them.

In addition, we're working with executive-level government officials to help them think about budgeting, procurement, cultural transformation, and the role of a centralized organization when it comes to cloud technology. And we're providing upskilling and reskilling programs to help organizations build a staff with the right skills to operate in a cloud-first environment.

Q: How do you help governments focus on the cultural changes needed to make cloud work?

In our educational offerings, we do sessions and coursework around how you transform the culture of an organization to support cloud technology. The goal is to draw a direct line between culture and technology — how you shift culture to support a new way of doing things that is better for the organization. We have former government executives who serve as advisors to help organizations plan for what they need to do. We can be a sounding board and provide examples of how other agencies

have addressed similar issues. And on the technical side, we collaborate with customers to develop proofs of concept to test solutions before deploying them across the organization and help agencies get quickly to where they want to go.

Q: How does the AWS shared responsibility model translate to work with government organizations?

In our shared responsibility model, AWS is responsible for the security of the cloud — our infrastructure, for example. Our customers are responsible for the security of what they put in the cloud, whether it's data or software. We provide tools and support so they know what their options are, but it's up to them to decide who has access to those resources and how they are used across their enterprise or organization.

That's important because we want customers to be fully empowered to secure all of what they have in the cloud.

Q: What do you recommend for government customers attempting to integrate RAMP processes?

We've seen good adoption of FedRAMP at the federal level and now StateRAMP. When public sector organizations can use an industry security standard rather than creating their own standards, that helps us meet their needs.

Procurement's role is to figure out a way, within regulations and policies, to deliver the right outcome and truly partner with internal customers. It's about the mindset of getting to 'yes.'

Consider the resources required to deal with thousands of different security requirements. Where standards exist, it helps us be a better provider because we're able to move faster, and it assures agencies they're working with quality companies that know how to manage risk.

Q: Where do you see the biggest remaining barriers to effective cloud procurement?

Legacy thinking around the role of procurement still exists. When I was in public sector procurement, I would tell staff to think of themselves as a customer service organization. Procurement's role is to figure out a way, within regulations and policies, to deliver the right outcome and truly partner with internal customers. It's about the mindset of getting to "yes." We know there are rules to work through, but we need to be open to rethinking how we operate. Processes must be open and fair while producing the best outcome.

Other barriers involve policy issues. We still see procurement regulations that mandate line-item bidding and invoicing, and it's difficult for many modern solutions to comply with that. As complex as it is, changing statutes, codes, and policies is important for staying relevant as a procurement partner. Procurement offices can really bring value to themselves and their internal customers by taking that on. Otherwise, you take away the power of procurement by not being responsive to the organization's needs.

Q: Any other advice for procurement professionals?

Procurement offices need to constantly reimagine how they can provide value to the organization. When I was a government procurement professional, I would remind myself that we could be cut from the budget if we didn't provide value. It's important to remember that procurement performs its role best when it partners with internal customers to provide solutions. For IT solutions, that means being closely aligned with IT on what the organization wants to do and on what timeline.

Expert Spotlight: *David L. Smith, Citrix*

In this Q&A, **David L. Smith**, *Citrix managing director for state and local government and aerospace and defense integrators, discusses the challenges involved in procuring and managing hybrid multicloud environments — including the impact of adding agency-specific security controls and the value of adaptive access and authentication systems.*

Q: How have state and local government cloud procurement policies evolved in recent years?

We've seen more collective decision-making — things like multiple governments and organizations collaborating on cloud procurement. It still isn't to the point that other software and hardware procurements are, but it's moving more in that direction.

At the same time, individual states are creating their own processes. One example is TX-RAMP in Texas. Many times, the policies are the same, but they are stated slightly differently. For vendors, adapting to multiple procurement policies makes it more difficult for us to go to market with our solutions. That leads to business decisions — either we're not going to participate in the government market because of barriers to entry, or we're going to support StateRAMP, but not individual state procurement policies. That results in less competition and innovation.

Q: How have Citrix offerings evolved to meet government needs?

We've achieved FedRAMP certification, and we're working on StateRAMP certification, which should be finalized in the not-so-distant future. Like product enhancement requests, we need to justify the internal investments needed to meet these certification requirements, and as with anything else there are tradeoffs.

We try to standardize our offerings as much as possible to meet the greatest number of needs for customers, and we continue to address different requirements on a one-off basis almost daily. We also try to participate in cooperative buying agreements that improve customers' ability to procure our services and our ability to go to market.

Q: What are the biggest challenges to effective cloud procurement?

Some procurement policies are stuck in a non-cloud world. They don't fully recognize the details behind how a service is provided. For example, a SaaS solution you acquire from one vendor may be hosted on cloud infrastructure that is controlled by another vendor.

There are other things around contracts that I don't think government procurement has caught up with. Software vendors want to contract for multiyear agreements, and governments often aren't budgeted for multiyear schedules. But if you want the vendor to invest in building the solution and aren't willing to

commit to the consumption of the solution for an extended time, that raises questions.

Q: What are the challenges in managing multicloud environments?

Customers are going to be in some type of hybrid multicloud environment for the foreseeable future — they're not going to adopt one specific cloud or do everything out of data centers. Governments need to support multiple cloud providers and the data center, as well as the ability to potentially move applications and workloads between those environments. They need to connect those networks and appropriately govern and secure those different connections.

Every cloud has its own way of handling access control, security policy and configuration. When organizations have to manage multiple clouds in different ways, that's where gaps arise and security challenges pop up.

It's important to leverage tools that can talk to all those different clouds and adapt to different environments. They help you treat all clouds as one, so it doesn't matter if you're in cloud A or B, the way you configure something is the same. Tools that let agencies manage access to applications and data that live across multiple clouds make it easier for IT departments to provide services and simpler for end users, because they don't need to know where something lives.

Q: What is the value of adaptive access and authentication systems?

Adaptive access and authentication is important because as agencies consume more cloud services — especially in a hybrid work environment — they need to understand the types of services being accessed and the scenarios by which they are accessing them. That scenario could be the device, the network or the geographic location of the user. Changing the level of access based on those parameters is critical to managing the services governments are offering their end users. It's also about understanding how to secure the different types of resources, manage users connected to a cloud service and maintain a common language across all the different environments.

Q: What's the impact of requiring state- or agency-specific security controls?

Agencies should consider why they would add to existing security controls, such as FedRAMP or those developed by NIST. Is there a value to what's being added or changed? And if there is a specific need to add something, can you do it in a way that makes it easy for suppliers to meet multiple requirements?

In general, I think it's better to make sure you're implementing the existing controls properly. Just because a supplier provides a FedRAMP-compliant service, that doesn't mean you'll deploy it in a compliant way. It's important to look at your deployment resources and ensure you're deploying technology correctly and taking into consideration different access scenarios versus adding a ton of new controls to the equation.

Q: What else do governments need to know about multicloud deployment?

People don't always think about what it takes to get out of a cloud. What do you do if you decide to end your relationship with a cloud provider for cost or security reasons? What would it take to get out?

Think about smartphones: If you decide to switch from Apple to Android, that's a massive change because of the stickiness that's built in. The same thing can happen with a cloud service. Some of it is contractual — what is your flexibility to make a change? From a technology standpoint, it's about architecting solutions in a way that a specific cloud isn't required to leverage that solution. It's important to build in a model that's oriented for the potential to change.

Expert Spotlight: *Joe Bielawski, Knowledge Services*

Joe Bielawski *is president of Knowledge Services and a founding member of the nonprofit StateRAMP. In this Q&A, he discusses the potential of StateRAMP to streamline and improve cloud procurement, what effective risk management programs should look like, and strategies to assess progress and review contracts with vendors.*

Q: How have procurement policies for cloud evolved in recent years?

State and local governments have acknowledged that security risks are increasing every day. Procurement provisions related to cloud have evolved to require attestation that a provider meets security policies, disclosure of security incidents and increasing amounts of cyber insurance.

In particular, cyber insurance requirements have reached the point where we've seen vendors unable to obtain a policy large enough to comply. It's not just about cost — some insurance companies are no longer underwriting cyber policies.

As it becomes more difficult to obtain cyber insurance, preventative measures become even more important. The next evolution we are seeing in cloud procurement policies is a shift away from accepting self-attestation of a product's security posture toward a verification model, such as StateRAMP.

Q: How have Knowledge Services offerings evolved to meet changing government needs?

It's been a multiyear evolution for us as a SaaS provider to government. We looked at government cybersecurity procurement policies in place and, realizing most all required NIST 800-53 compliance, asked how we could differentiate ourselves. It was clear from the increasing velocity of data breaches that self-attestation would soon be unacceptable. So we looked for third-party verification to validate that our technology complies with government cybersecurity policies. The only recognized program was FedRAMP, so we pursued and achieved FedRAMP Ready authorization. We have not yet done much business with the federal government, but it was an investment we made hoping state governments would see a FedRAMP status as meeting their requirements. Many states now recognize FedRAMP as valid third-party verification. But a FedRAMP authorization is not always available to providers because a company must have a federal agency sponsor and a federal government contract for its product to maintain a FedRAMP authorization. This is what led us to be involved with StateRAMP.

And while achieving FedRAMP Ready was an important step, we have also made significant investments in cybersecurity workforce training, facilities security and NIST compliance for ancillary support systems. We have evolved from a focus on

meeting government cybersecurity contract requirements for a defined product to include the entire organization's cyber resilience.

Q: What are the biggest barriers to effective cloud procurement?

Governments have deep experience in procurement. However, most government procurement organizations don't have the depth of experience or budget to support cybersecurity expertise. There's work to be done in standardizing and simplifying procurements. And there's the need for abundant yet confidential cyber transparency — without it, governments can't say whether a vendor meets their security requirements. That adds costs, creates an uneven playing field, and puts constituents and governments at risk.

Q: What are the greatest benefits of StateRAMP for governments and vendors?

It comes down to cost and procurement efficiencies. Procurement teams are not staffed with cybersecurity experts to perform continuous security monitoring. Government IT and information security teams don't have the resources for this either — they're focused on battening down their own applications, data centers and physical spaces. For solution providers, there's also a cost; every government regulation carries a cost. What we are trying to do with StateRAMP is bring verification transparency and standardization to cloud procurement, which are the critical components to reducing the cost of continuous security monitoring and increasing speed to award.

What we are trying to do with StateRAMP is bring verification transparency and standardization to cloud procurement.

Q: What do solid risk management programs look like?

FedRAMP established a model for a solid risk management program. StateRAMP's governing committees leverage the work of FedRAMP to incorporate the best practices and chief characteristics that include independent audits, continuous security monitoring and NIST-based standards.

Q: How do you recommend governments assess progress and review contracts with their providers?

For more than 20 years, Knowledge Services has served governments, helping them manage vendors more efficiently to improve outcomes and compliance. We have seen how meaningful it can be for our customers to have greater transparency and reporting.

StateRAMP is doing the same. Its focus is to help governments make informed decisions. If agencies have a system that's wide open and at a high risk of failure or exposure, they should know that and take appropriate steps. Putting your head in the sand or making false assumptions is no longer a safe option.

It's also important to recognize that even if a vendor doesn't meet all the StateRAMP security requirements now, government isn't going to come to a screeching halt. The StateRAMP Security Snapshot is a tool designed to help providers and governments get started by providing a NIST maturity score for products that have not yet achieved StateRAMP authorization. This helps government and providers better understand where the gaps are and potential for risk. Throughout the contract period StateRAMP works with each vendor, continuously monitoring and sharing their cyber posture changes. Governments are then able to quickly and easily see the steps vendors are taking and determine the amount of risk they are willing to take.

Expert Spotlight: *Herb Thompson, VMware*

In this Q&A, VMware's **Herb Thompson** *discusses the need for flexibility in cloud contract terms and conditions, the importance of cybersecurity frameworks and end-to-end visibility, and an enduring paradox in cloud pricing models. Thompson is VMware's state and local government strategist and the former deputy CIO for the state of Wisconsin.*

Q: How have state and local government policies for cloud procurement evolved in recent years?

During the pandemic, the control gates for procurement were lifted so CIOs could do things quickly. They could buy equipment, software and cloud services at a fast pace. What I hear now is that some procurement offices are putting those administrative rules back in place, so things don't flow as quickly as they did. Most procurement law is very specific — whether in statute or administrative rules — and was created to buy physical assets. Cloud, where everything is a service, has always been a sticking point.

Most states have existing procurement contracts with the big cloud providers. Otherwise, they rely on cooperatives to help with developing agreements. A best practice is what I call a prequalification — a zero-cost RFP that gets companies on a list of vendors. Prequalification narrows the scope of who can compete for a statement of work, and it allows agencies to get services relatively quickly. When I was in Wisconsin government, we had prequalifications for everything from Salesforce consulting to cloud security services. I've seen this repeated across the country.

Q: How have VMware's offerings evolved to meet changing needs?

As a vendor, we try to figure out what procurement vehicle a city, county or state can use to buy our cloud services. Vendors are so cognizant now about how agencies buy. That's become a kind of secret sauce. We need a procurement vehicle, and a lot of organizations don't know how to do that.

Q: What are the biggest barriers to effective cloud procurement?

States often have terms and conditions that don't allow us to use a standard contract. Cooperatives like NASPO ValuePoint can help address this issue by creating a standard set of terms and conditions vendors can agree to.

Another challenge is itemized pricing. It's a tough area because we try to bundle professional services, products and best practices into an agreement to give customers flexibility. But procurement offices want to know exactly what they're purchasing. Agencies need to be able to switch out products, to buy more professional services or support, and adjust up and down based on where they are in their cloud journey. Vendors and government customers need the flexibility to say, based on all the things we put together, the contract

value is this amount — not that this widget costs $5 and you bought 100 of them.

Professional consulting organizations also like to weigh in on the best prices agencies are getting across the country, which adds a wrinkle to negotiations. In a bundled deal, it is hard to compare prices when there are multiple products that can be switched in or out based on the customer's needs.

Q: How should governments think about aligning with existing cybersecurity frameworks?

All the government organizations I talk to have settled on the NIST cybersecurity framework as the base standard — that's a given. And every vendor knows that and says they align to the framework, even if they only cover a small slice of the overall pie. It can be tough for governments to figure out how much of the alignment vendors actually do — are they picking a platform that addresses everything, or a program to fill one particular niche? That's why governments are moving to a platform approach.

FedRAMP is important to federal organizations, and many states adopted it as well. StateRAMP is picking up steam, and you're going to see StateRAMP compliance if vendors don't have FedRAMP going forward. These standards allow government organizations to separate good vendors from one-trick ponies that don't do continuous monitoring for security vulnerabilities and supply chain issues.

The typical government customer has 100 security products — for the desktop, network and so on. Bringing all that intelligence into a platform is an imperative for the future.

Q: What is the importance of end-to-end visibility?

End-to-end visibility is easy to say and tough to do. Some vendors have separate mechanisms for dealing with vulnerabilities and remediation. Compare that to having a single platform that provides insight on devices, networks, users, the data center and every cloud to identify suspicious activity.

The typical government customer has 100 security products — for the desktop, network and so on. Bringing all that intelligence into a platform is an imperative for the future. Having simple procedures for achieving that end-to-end visibility is also going to be critical. If you have a product that provides end-to-end visibility through a log aggregation tool, for example, it will take a lot of time because it is customizable and requires many people hours to create an alert that says you have an issue. Delivering visibility through a single platform is going to be a differentiator going forward.

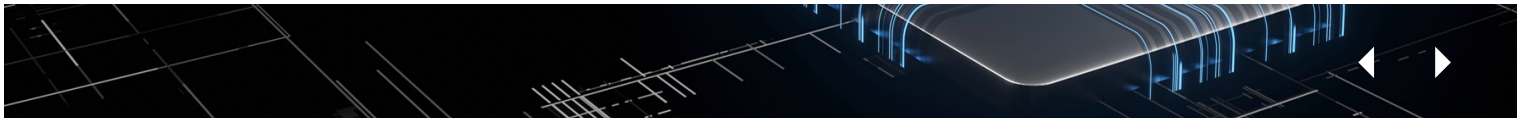
Q: What else needs to be addressed to improve cloud procurement?

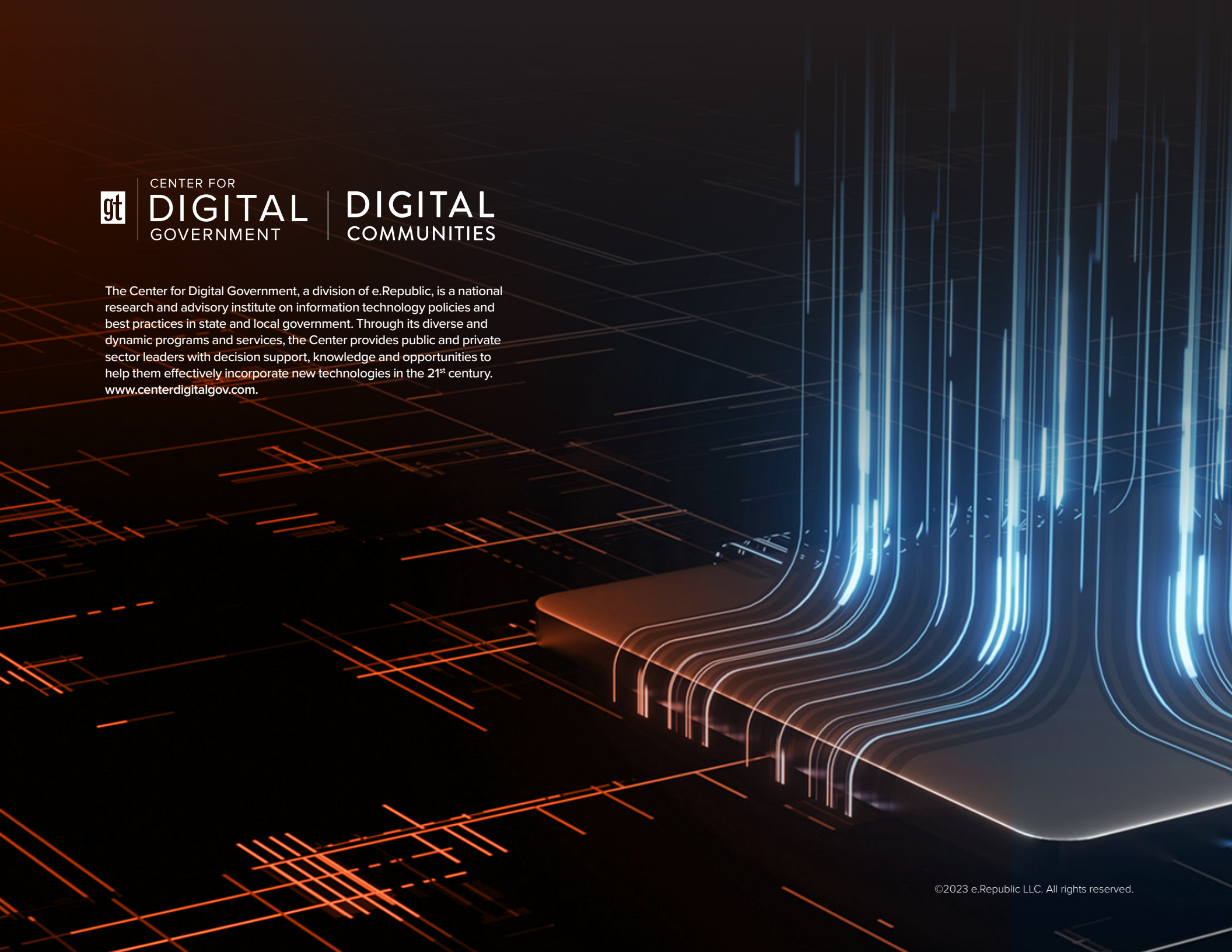
We always talk about the value of the cloud. We say we can scale up and scale down, and we have this agility. But what's the first thing organizations do to lower the price? They go from a consumption model — paying "by the drip" — to buying cloud services in bulk to reduce the unit cost. In other words, you commit x amount of consumption to lower your rate, even if you don't have that level of consumption.

It's a paradox: If you want to get the best price, you have to buy all these reserved instances for a multi-year deal. That's counterintuitive to the whole idea of the cloud. How can you sign a long-term agreement to lock in the best price and still pay only for what you use? That's something that remains to be determined.

Endnotes

1. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations," National Institute of Standards and Technology, 2012. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf
2. Ibid.
3. Ibid.
4. State Security Breach Notifications Laws, National Conference of State Legislatures, website, December 2022. https://www.ncsl.org/technology-and-communication/security-breach-notification-laws
5. P2-1, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," Special Publication 800-122, National Institute of Standards and Technology, April 2010. https://csrc.nist.gov/publications/detail/sp/800-122/final
6. P11, "There is a New Sheriff in Town; The Auditor, Internal Controls and You," Contract Management, September 2006, Richard Pennington J.D
7. P1, "2022 Cost of Data Breach Study: A million-dollar race to detect and respond," Ponemon Institute, and sponsored, analyzed and published by IBM Security.® Note: To calculate the average cost of a data breach, this research excluded very small and very large breaches. Data breaches examined in the 2022 study ranged in size between 2,200 and 102,000 compromised records. https://www.ibm.com/downloads/cas/3R8N1DZJ
8. P2-3, NIST SP 800-111, "Guide to Storage Encryption Technology for End-User Devices," November 2007. https://csrc.nist.gov/publications/detail/sp/800-111/final
9. FedRAMP program basics web page. https://www.fedramp.gov/program-basics/
10. FedRAMP governance web page. https://www.fedramp.gov/governance/
11. NIST SP 800-53 Revision 5.1, Pg 70. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
12. StateRAMP Security Assessment Framework, Version 1.4 (April 29, 2022) – pg 8. https://stateramp.org/wp-content/uploads/2022/05/2022-StateRAMP-Security-Assessment-Framework_Revised.pdf
13. Ibid.
14. FedRAMP Third Party Assessment Organizations (3PAOs) web page. https://www.fedramp.gov/assessors/
15. StateRAMP Security Assessment Framework, Version 1.4 (April 29, 2022) – pg. 8. https://stateramp.org/wp-content/uploads/2022/05/2022-StateRAMP-Security-Assessment-Framework_Revised.pdf
16. StateRAMP Security Assessment Framework, Version 1.4 (April 29, 2022) – pg 9. https://stateramp.org/wp-content/uploads/2022/05/2022-StateRAMP-Security-Assessment-Framework_Revised.pdf
17. NIST SP 800-53 Revision 5.1, Pg. 77. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
18. FedRAMP Continuous Monitoring Strategy Guide (Version 3.2, April 4, 2018. https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf
19. Ibid.
20. HIPAA Privacy Rule, Definitions, U.S. Department of Health and Human Services, National Institute of Health. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
21. Ibid.
22. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations" National Institute of Standards and Technology, May 2012. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf
23. HIPAA Privacy Rule, Definitions, U.S. Department of Health and Human Services, National Institute of Health. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
24. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations," National Institute of Standards and Technology, May 2012. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf
25. HIPAA Privacy Rule, Definitions, U.S. Department of Health and Human Services, National Institute of Health. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
26. Ibid.
27. Ibid.
28. Ibid.
29. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations," National Institute of Standards and Technology, May 2012. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf
30. HIPAA Privacy Rule, Definitions, U.S. Department of Health and Human Services, National Institute of Health. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
31. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations," National Institute of Standards and Technology, May 2012. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf
32. FedRAMP program basics web page. https://www.fedramp.gov/program-basics/
33. FedRAMP governance web page. https://www.fedramp.gov/governance/
34. FedRAMP program basics web page. https://www.fedramp.gov/program-basics/
35. Steve Nichols, Consumer Privacy vs Citizen Privacy, July 7, 2022. Linked In
36. FedRAMP program basics web page. https://www.fedramp.gov/program-basics/
37. FedRAMP governance web page. https://www.fedramp.gov/governance/
38. FedRAMP program basics web page. https://www.fedramp.gov/program-basics/





CENTER FOR DIGITAL GOVERNMENT | DIGITAL COMMUNITIES

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. www.centerdigitalgov.com.