Federal financial sector: Enterprise cloud security management and governance

December 2020

perspecta™

Table of contents

Background	**4**
Security management and governance in the cloud	**4**
Organizational change management and Cloud Center of Enablement and Excellence	**9**
Summary	**9**

Ensuring the highest level of information security in the cloud (whether a hybrid or multicloud architecture) is the topmost concern for federal financial sector agencies.

Background

Federal agencies and organizations in the financial sector are either considering cloud adoption or have started migrating to cloud for internal business operations and citizen service delivery. Federal financial agencies have different strategies for cloud adoption and are at different phases of the cloud journey, but many have adopted varying degrees of software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) cloud services. Some agencies also leverage containers, cloud native services and the DevSecOps business model for modernizing legacy applications and developing new mission applications. Due to the sensitive nature of financial data, transaction information and associated privacy data, ensuring the highest level of information security in the cloud (whether a hybrid or multicloud architecture) is the topmost concern for federal financial sector agencies.

Perspecta has extensive experience in delivering cloud solutions and cloud related security services to government organizations including a classified federal financial customer, the Department of Homeland Security (DHS), the Department of Health and Human Services (HHS), the Department of Defense (DOD), the United States Postal Service (USPS) and others with similar mission criticality and requirement complexities. We also deliver enterprise security services to the U.S. Army, DHS and other federal agencies. Perspecta Labs supports many cybersecurity research and development projects for DOD and Intelligence Community (IC) customers by developing innovative technologies and methodologies to address the increasing challenges of cybersecurity.

We offer the following suggestions for implementing a secure, compliant, hybrid and multicloud architecture that achieves financial sector goals for IT modernization, while providing reliable end-to-end security for data, application and cloud services.

Security management and governance in the cloud

By nature, cloud is a software-defined IT environment that enables rapid and dynamic elasticity and "everything as code" configuration. Because of these unique characteristics, the organization of security controls in the cloud environment is not the same as in on-premise environments. Cloud security is a “shared responsibility model” that requires different levels of security cooperation and ownership among IaaS, PaaS and SaaS cloud platforms.

Agencies need to understand their responsibility for managing security policies and controls, selecting the right cloud solutions, applying appropriate security models and managing risk.

Recommendations and factors to consider

We recommend agencies consider the following factors in managing information security related to cloud.

Build cloud security considerations into the earliest acquisition phase

Securing the confidentiality, integrity and availability (CIA) of financial workloads, applications and data in the cloud is fundamentally different than in the datacenter. In the datacenter, the owner is 100% responsible for the system—from the user input or data source to retirement of the data at the end of a long legal archive period.

In the cloud, there is a shared security model (figure 1) where the cloud service provider (CSP) and cloud service users share the responsibility for the overall security and compliance of the system. The Federal Risk and Authorization Management Program (FedRAMP) certifies CSPs for the security control compliance “of the cloud.” We recommend agencies consider FedRAMP accreditation as a prerequisite for all cloud service acquisitions.

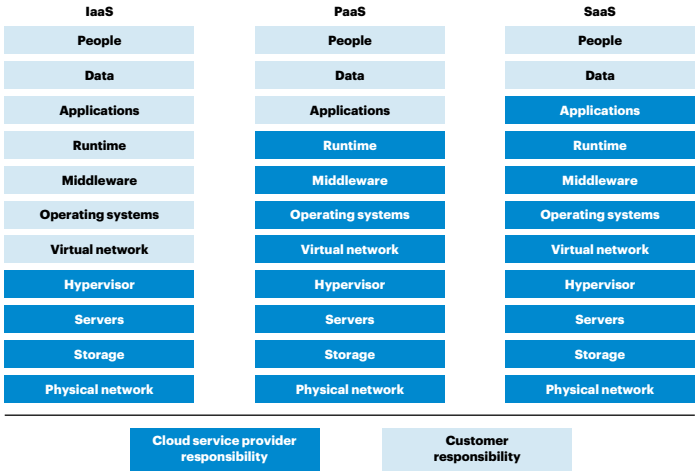

Figure 1: Shared responsibility model in coud security

Regardless of the cloud services procured, agencies are still responsible for security "in the cloud." Security in the cloud consists of data security, identity and access management, application security, network access security and their workloads and services that are not in the security boundary of the CSPs. We strongly recommend agencies include holding the vendors accountable for delivering cloud security assurance by including specific requirements for security solution implementations, compliance management and cloud security management services in their procurements for professional and managed services related to cloud.

Adopt “cloud native” security solutions

Cloud, containers and DevSecOps are key enablers for rapid innovation and agile application development. Cloud is highly elastic and scalable. Most cloud services may be consumed as ephemeral resources that can be spun up and spun down almost instantly. In rapid client / server model release cycles, developers may resist anti-malware scanning, dependency checking and the completion of vulnerability scanning. In the cloud, components are virtual resources and physical separation is no longer an option. Interactions among the cloud service components are through software-defined controls and software interfaces. Command line and console interfaces inherently increase the difficulty in maintaining consistent

security control visibility. Vulnerabilities in certain service components may give attackers relatively easy access to other cloud service components if robust security configuration control is not well implemented. In July 2019, a hacker accessed a Capital One Financial Corporation server hosted in AWS by leveraging a vulnerability in a flawed cloud firewall configuration and exposed the personal information of more than 100 million customers and applicants.

Managing cloud security requires cloud native security solutions. Native solutions are developed and deployed on a cloud platform so the soutions are aware of and consistent with the platform's security architecture. Native solutions integrate and interoperate with other native services provided by the CSP. Many traditional security tools are not ready for operation in an elastic environment. But cloud native solutions are designed to embody "modularity, programmability, elasticity and resiliency."[1] They scale up and down with user application workloads, provide high degrees of automation, employ data analytic-driven intelligence and natively support containers, microservices, Kubernetes and serverless applications in cloud. Cloud-based security solutions also offer the benefit of managing security in close proximity to the actual events and data. They eliminate the need to send raw event data between the cloud and on-premise security systems, reducing egress traffic that can be an unpredictable cost factor. At a tipping point when more than half the daily workload is processed in the cloud, it will become practical to send datacenter information to the cloud and eliminate on-premise physical capacity.

Apply comprehensive security controls to manage end-to-end cloud security

Based on federal cloud security requirements and published frameworks, cloud service providers' best practice standards and our own experiences, Perspecta recommends agencies consider a cloud security control model that implements the following key elements.

Secure the virtual data center environment in cloud

Agencies should implement a complete general support system (GSS) at each IaaS cloud service used by the agency. This includes separating network services, shared application support and system management, and security services for all workloads into virtual data center segments (e.g., AWS Virtual Private Clouds (VPCs), Azure VNet, etc.). This GSS implementation supplies a cloud landing zone that needs to be planned and deployed at the very beginning of cloud migration or cloud application development.

The GSS security controls, at the minimum, should include the following elements: cloud network traffic segmentation, inspection and filtering; application delivery controller (ADC); load balancers; proxies; cloud web application firewall (WAF) and virtual network firewalls; identity and access management (IAM); encryption, tokenization and key management within a "transit" virtual private cloud (VPC). Likewise, logging, log integration and security incident and event management (SIEM); threat intelligence and risk detection for network, workloads, accounts and application activities in a separate security VPC. Figure 2 illustrates the implementation of this security architecture. Artificial intelligence and machine learning (AI / ML)-enabled cyberthreat detection and security operation automation solutions are highly recommended for rapid risk identification and remediation.

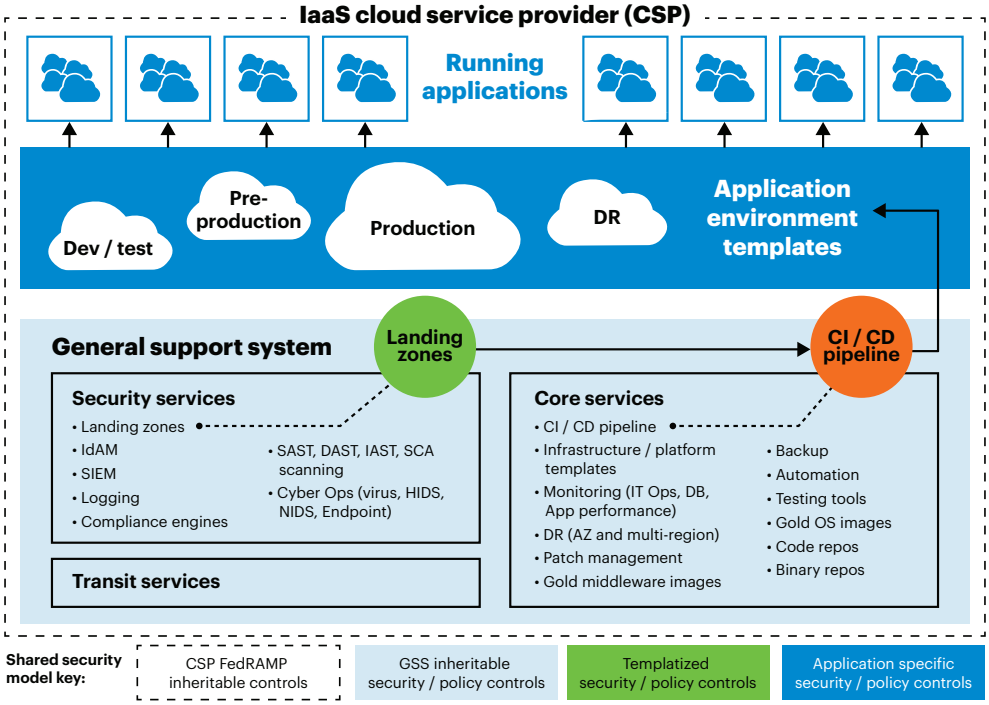

Figure 2: Architecture model for securing virtual data center environment in cloud

For example, in an AWS cloud implementation, account structure, GSS control structure and VPCs need to be designed and set up properly so that GSS services can be provided to all workloads added to the environment. Business applications should be in their own "per system" VPCs connected to the central service VPCs. Pushing all traffic through the transit VPC (a virtual router in the cloud) allows network teams to monitor and manage traffic more effectively. The security service VPC should include separate accounts so that logging and security services can be managed with separation of duties. The "core" services VPC is home to the balance of centrally provided agency IT services.

[1] https://blogs.gartner.com/tony-iams/containers-serverless-computing-pave-way-cloud-native-infrastructure/

Secure data to, from and in the cloud

Data security should be the top priority for any organization. In just the first eight days of December 2020, five major cyber events targeting sensitive and proprietary data were reported by Reuters News agency—including a presumed state actor theft of detection evading penetration test tooling from one of the government's preeminent security testing firms. The only real protection for any type of sensitive data is encryption. For financial service agencies, it is extremely important to apply robust encryption on both data in transit and data at rest. At rest, physically encrypting media is not a defense. Software-invoked full-time encryption should be a mandatory policy for any data. Key management is the critical factor to apply it. We recommend agencies implement the most secure and reliable key management solutions and tailor their operations to ensure the accessibility and integrity of encryption keys. All three large IaaS CSPs offer excellent data storage encryption options and we recommend that agencies implement them.

In transit, at a minimum, secure sockets layer / transport layer security (SSL / TLS) encryption for all traffic needs to be implemented. Decryption and inspection should be performed at the host where the session is terminated. Consider inspecting traffic that moves laterally east / west from service to service in microservices based architectures. For greater data access control, agencies should consider data classification and dynamic data masking. Dynamic data masking is a column-level data security feature that uses masking policies to selectively mask plain text data in tables and views at query time.

Two additional data security issues that require security solutions are:

1. **Data loss prevention (DLP):** a DLP should be deployed to monitor content placed in every publicly available storage location to examine outgoing traffic and halt exfiltration. Additionally, we recommend agencies implement a cloud access security broker (CASB) solution (figure 3), particularly for SaaS, so that all data traffic to cloud applications can be inspected to detect and prevent inappropriate movement of sensitive data. Many CASB solutions allow compliance and risk assessment to identify cloud configuration issues (such as open shares, unprotected storage, etc.) that may lead to data loss. Adaptive access control and user and entity behavior analytics are other important features to consider.

   The DLP can also serve as a detection or prevention measure for shadow IT sprawl—stopping users from uploading business files and content to cloud applications or SaaS sites that are unknown and invisible to the organization without a CASB solution deployed.

   Current cloud spending patterns indicate that SaaS has been a more significant area of government cloud computing than IaaS. Almost all software vendors are transitioning to subscription-based cloud offerings. SaaS consumption in the federal market has grown significantly in last several years. The lack of visibility and management over SaaS could lead to security and compliance failures. CASB, as well as identity governance and access management, are important security control solutions for SaaS.

2. **Resiliency from ransomware attacks:** cloud workloads are subject to ransomware attacks just like on-premise systems. At a December 8, 2020 FedInsider forum of federal financial officials and IT services vendors, ransomware was a significant area of concern at federal financial agencies.[2] Perspecta recommends that cloud and data center backups operate under a protected account in a segmented cloud environment. This methodology provides additional protection for data compromise by ransomware attack and allows for successful recovery of production systems.

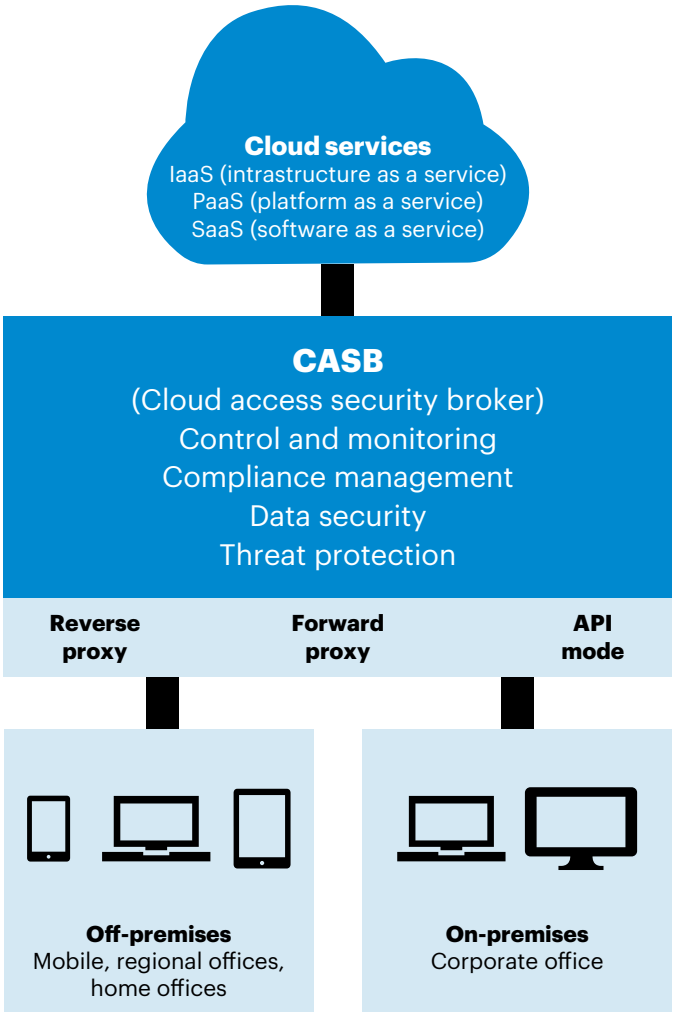

Figure 3: Cloud access security broker

Manage security on workloads, services and applications in the cloud

It is important to apply effective operational hygiene, endpoint security, application security, vulnerability management and workload-hardening solutions to manage security at workload, service and application level. Continuous monitoring, workload behavioral analytics, vulnerability assessment, malware and suspicious activity analysis need to be implemented. Additional workload protections may include application whitelisting, memory exploit protection, identity base workload segmentation, system integrity assurance (such as file integrity monitoring required by the Payment Card Industry Data Security Standard (PCI-DSS), workload configuration drift monitoring, etc.).

[2] **https://www.fedinsider.com/conversations-on-risk-cybersecurity-in-the-financial-sector/**

In cloud, there are different types of workloads, ranging from virtual machines to containers, to serverless PaaS (e.g., AWS Lambda, Azure Function, etc.). Each type of workload has its own unique life cycle pattern, life span and security profile. Security solutions for workload management need to support all cloud workload types. For example, with managed container services, containers are provisioned with locked-down minimal kernels and security software agents cannot be installed. Workload security management may need to be implemented in a privileged container or as a sidecar in Kubernetes pods and service mesh architectures. For serverless PaaS, agents and privileged containers / sidecars will not work. New security approaches need to be considered such as layering in security controls and creating a parent / child relationship from a security wrapper to the serverless function.

At Perspecta, we apply AI- / ML-enabled multicloud end point security solutions and compliance as code solutions to manage workloads and cloud services. Our solution can quickly identify security vulnerabilities and threats, automate drift correction and take security remediation actions. Policies can be implemented so that configuration deviation can be automatically detected and resolved. For application security, a DevSecOps approach with integrated tool chains that automate security testing and validation for cloud native security and application components is highly recommended.

Configuration management

Misconfiguration is the number one root cause of cloud data breaches. Gartner estimates that up to 95% of cloud breaches are due to errors such as configuration mistakes.[3] Unfortunately, configuring cloud services securely is a tedious, error-prone and complex process if done manually. Applying automation in compliance governance with a policy as code technology implementation ensures the cloud environment and cloud services are configured properly. Cloud provides a wealth of data to security and privacy risk managers that can be exploited to automate security and assurance processes. The simple structure of the JSON configuration files used to create cloud infrastructures means configuration compliance can be managed with a high degree of automation.

With the increasing adoption of containers, agencies are embracing the concept of immutable infrastructure, which is an operational model in which no configuration changes, patches or software updates are allowed on production systems. Patches and updates are applied to the base image and then the production workloads are refreshed from these images and replaced, rather than patched. The benefit of this operation model is that it avoids downtime associated with traditional patching processes and allows zero trust enablement (default: deny any changes) at runtime on the workload level. With this model, workloads are "born secure" from the moment they are instantiated. This places a stronger focus on vulnerability management, security scanning and testing on images and configuration templates during development in the continuous integration / continuous delivery (CI/CD) pipeline. Left-shift operational security activity into the development team by incorporating vulnerability, configuration and dependency scanning into the CI / CD pipeline and put in check-valves to prevent insecure code from reaching production. Figure 4 describes a sample architecture for implementing this shift-left security configuration management.

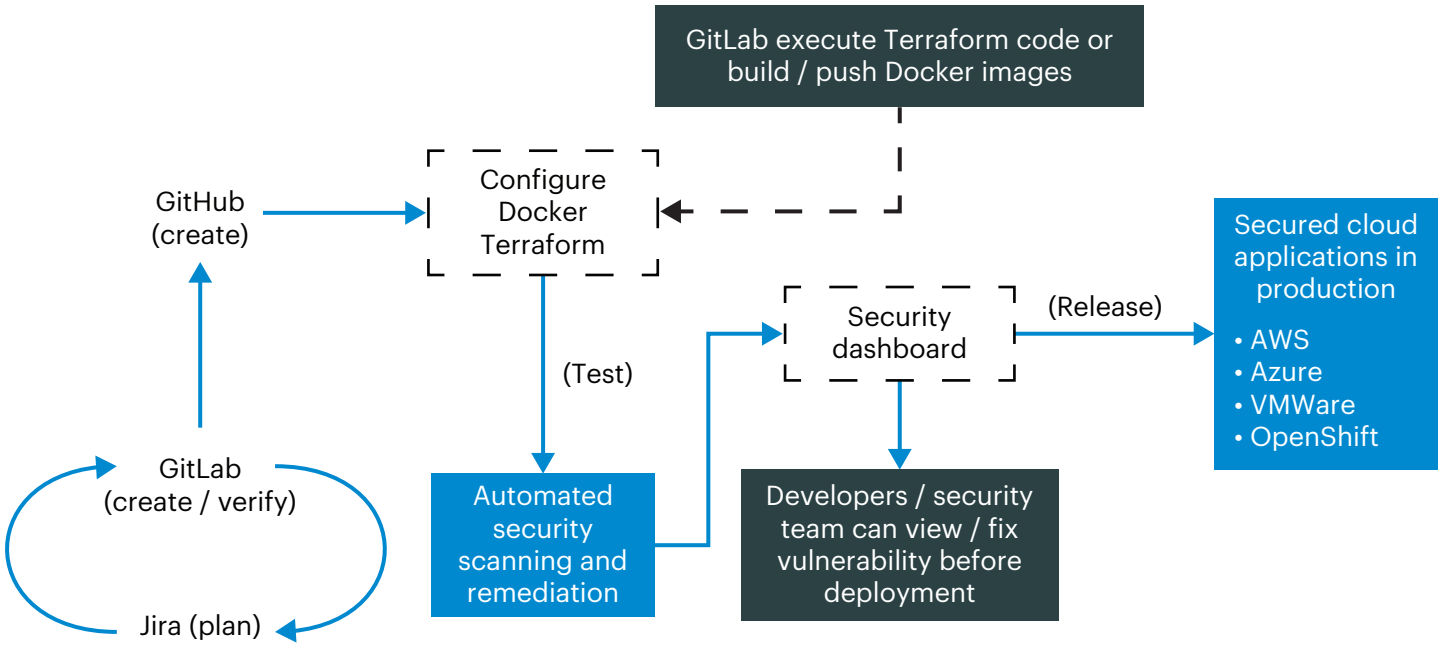

Figure 4: A sample DevSecOps implementation for shift-left security configuration management

Identity and access management

It is highly critical to design and deploy a well-architected cloud account structure with a protection plan for identity and access controls. This includes privileged access management for cloud accounts, cloud service authentication and authorization and multifactor authentication. Contextual access security with zero trust enablement, continuous access monitoring and assessment and enforcement of least privilege policies across the hybrid multicloud environment are necessary security measures. The necessity to implement and manage cloud IAM account structures and protections cannot be overstated. There should be a dedicated access management team.

[3] **https://www.gartner.com/smarterwithgartner/why-cloud-security-is-everyones-business**

Accelerate Authorization to Operate (ATO) and operate with continuous assurance

Agencies are required by law to determine if residual risk due to security control vulnerability can be accepted for an IT system before releasing it into production use through the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and Authorization to Operate (ATO) process. A FedRAMP ATO demonstrates control compliance and risk acceptance for the components within the CSP's security boundary.[4] As noted earlier in figure 1, the CSP ATO boundary is very different depending on whether the cloud service consumed is IaaS, PaaS or SaaS. Agencies remain responsible for the security and compliance of systems, workloads, applications and data "in" the cloud.

The basic architectural model for federal agency IT is unchanged in the cloud. The regulations continue to differentiate between major applications (MA) that automate processes for internal constituents / the public, and GSS, the IT department-owned and operated backbone infrastructure, security and support systems. Agencies are still obligated to perform centralized security management and oversight and to assess systems migrated to, or built on, cloud services for security risks prior to issuance of an ATO. As currently implemented, the RMF process adds 7-12 months to every system development timeline and the periodic reauthorization and continuous monitoring activities act as a continuous drain on security resources. Perspecta recommends agencies implement a continuous assurance practice to standardize control requirements and implementation strategies, expand control inheritance leveraging and automate the assessment, vulnerability remediation and security document generation tasks required for ATO and continuous monitoring.

The reliance on system-specific documentation of security control information stands out as the greatest obstacle to automation of NIST RMF processes. Agile development velocity and the prevalence of cyberthreats to misconfigured systems requires a new, standardized, leveraged, data-driven and automation accelerated approach to RMF implementation. This approach starts with standardizing the basis for security control implementation across the agency enterprise.

The NIST special publication 800-53 control catalog and the baselines built therefrom provide agencies with guidance on "what to do" to implement the RMF. Typically, control implementation documents like the system security plan (SSP) are the method used to supply information to security compliance stakeholders. The root of the problem is this method for information exchange, which is a specifically human interaction. Perspecta strongly recommends transforming the RMF implementation to focus on data that can be consumed and compared with automation. NIST has long recognized the necessity to move to data, rather than information, for assessing and authorizing systems. Revision 5 of the 800-53 control catalog, the creation of the Open Security Controls Assessment Language (OSCAL), and the concepts of shared responsibility and control inheritance pioneered by FedRAMP steer federal IT towards the common goal of generating data for automation rather than information for people. Agencies must reframe their RMF processes around repeatable, specific, measurable, time-bound, data generating requirements that establish security controls. Security is an outcome. Implementation information documentation should be standardized on the outcome of the implemented control, specifically describing what data is produced, how it is produced and the value of the control in the context of the security of the system. Security controls, whether performed by humans or machines, consist of a standard set of tasks. Every task must be focused on generating a recordable bit of data. Comparison of the recorded data over time demonstrates compliance and establishes whether the control is operating effectively.

It is also recommended that agencies should engage vendors who are experienced with cloud and cloud security testing to perform assessment and penetration testing to make sure effective controls—based on requirements, data production and outcomes—are in place. Likewise, Perspecta recommends applying modern DevSecOps approach for continuous and automated security testing in application development and code updates, as well as implementing effective vulnerability scanning, hardening and access control on image and code repositories, to achieve continuous ATO. Adopting the DevSecOps strategy and automated "in the cloud" cybersecurity reduces the time required to assess during initial ATO while also reducing the time required for reassessment of the compliance status and security posture of a system after ATO.

Adopt TIC 3.0 and cloud native virtual CAP (cloud access point) architecture

Federal agencies are experiencing a transition to an increasingly mobile workforce. The COVID-19 pandemic is also driving increased remote access among government employees. Moving applications and workloads to public clouds, continual increases in adoption of SaaS and the need for remote access and mobile access to enterprise applications requires new network and security architectures that enable a positive user experience. The DHS Cybersecurity and Infrastructure Security Agency (CISA) laid out their policy and architecture guidance on TIC3.0. TIC3.0 architecture allows users to access cloud services through internet access with distributed security controls without network backhauling.

Perspecta recommends agencies in federal financial sectors apply a cloud-based virtual cloud access point (vCAP) solution to implement the TIC3.0 architecture that allows ubiquitous secure access to cloud applications and services from any user location and device. The vCAP solution leverages FedRAMP certified commercial solutions deployed in cloud and global data centers to provide low latency, high performance, rapid elasticity, lower cost and high security. It includes packet capture, traffic analysis, real-time threat detection and data protection for accessing cloud services, websites and private apps from anywhere, on any device. It provides a scalable approach to integrate CASB, DLP, secure web gateway (SWG), next-gen firewall, advanced threat protection and cloud security posture management (CSPM) functionality into a secure access service edge (SASE)-ready platform supporting a multicloud strategy. Cloud based vCAP is a very effective solution to support agencies' cloud access security and performance requirement without high capital expenditure.

[4] **Federal organizations are still required to periodically evaluate the work done by the issuer of the FedRAMP Authority to Operate (ATO) and accept any residual risks to their own systems**

Organizational change management and cloud center of enablement and excellence

Perspecta views cloud adoption as a major transformation that has profound impacts on operation and security processes, IT service delivery and a host of nontechnical functions that support the services organization, such as finance, contracting and supply chain / procurement. The success of a cloud project is not just dependent on the technology, but more often dependent on the people and organizational change management. We regard people transformation and effective governance as foundational to achieving comprehensive and sustainable cloud adoption. Gartner's publication of "2018 CIO Agenda: Government Insights" reported that 84% of surveyed government CIOs identified challenges related to organizational readiness (skills, resources and culture) as the most important barrier to delivering digital government transformation at scale. Transitioning to and securing a cloud architecture will require adopting new processes, new methodologies and a new mindset in procuring, managing and delivering IT services to the enterprise. Federal financial organizations should consider a service provider's solutions, capabilities and experiences in supporting organizational change management in cloud and security services.

To drive enterprise level cloud adoption and transformation readiness, Perspecta recommends agencies establish a cloud center of excellence and enablement model to foster stakeholder engagement, practice and knowledge sharing, CSP partnership, architecture standardization and joint problem solving and strategy development. The center also drives unified cloud-enabled governance models from IT governing bodies focused on financial management, security, performance and operations management. It supports maintenance of technical standards for cloud referenced architectures, code repositories, build templates and hardened images. Additionally, the center helps bring expertise to support operational transformation through advisory cloud assessment and accelerated adoption workshops.

Summary

The sensitive nature of financial data, transaction information and associated privacy data makes implementing the highest level of information security in cloud architectures the topmost concern of federal financial agencies. Cloud computing provides a technical environment that can be leveraged for a leap forward in federal IT agility and operational efficiency.

The fully software-defined environment of cloud is naturally data rich and allows for a significant increase in both depth and breadth of automated examination. Over time, federal security requirements have bent towards faster, more predictable, data-centric methods for establishing effective security. While the data rich nature of cloud computing enhances the agency's ability bring greater security agility to its enterprise, it also requires increased standardization and centralized control.

Many of the same IT security issues presented by distributed computing in an agency managed data center exist in the cloud including organizational components working outside the services provided by their IT department (shadow IT) and developers and outsourced operations teams experimenting with novel tooling and methods (IT sprawl). A decade ago, cloud computing also presented some new security challenges such as maintaining standardization over configuration, centralized control over identity and access and losing physical command of IT resources. NIST, FedRAMP and federal IT security organizations, along with the CSPs and the vendor community, have worked to develop standards and solutions to address these challenges. When well-architected, built using FedRAMP authorized services and operated to generate meaningful security data that can be validated via automation, today's cloud computing environment is more secure than any agency data center environment.

In addition to the specific recommendations and factors to consider discussed above, Perspecta recommends agencies consider the following factors in their cloud approach:

- Use a standard architecture to manage cloud security in IaaS, PaaS and SaaS
- Implement a complete GSS with a transit cloud implementing TIC 3.0 connections, security cloud and services cloud at each IaaS vendor
- Shift operational security focus left, by implementing security testing prior to deployment to production. Assign security officers directly to application development teams or designate a specific developer as the security specialist
- Maintain operational hygiene by cycling the entire cloud environment through a monthly, vulnerability testing and remediation release. Remove all privileged user access to production systems prior to deployment. Apply robust encryption on data in transit and data at rest
- Manage identity as the boundary. Have a dedicated access management team and embed zero trust in the standard architecture
- Prioritize comprehensive configuration management

Author

Marilyn Hays
CISSP, CAP, CCP

Marilyn Hays has spent her entire career in IT, from digitization of paper records, as a developer, IT department head and since 2001 in various roles in security. Marilyn specialized in the Ab Initio development of regulated security programs, performed the first independent third-party assessment of a cloud service provider implementing the FedRAMP Moderate controls, then managed the HP / Perspecta clouds from their initial ATO through 8 annual renewals. She may be reached at marilyn.hays@perspecta.com.

Learn more at perspecta.com

perspecta™

perspecta.com | contactus@perspecta.com
14295 Park Meadow Drive
Chantilly, Virginia 20151