PRESENTATION

Cloud Security…on the Cheap!

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Presenters: Christie Hall and Randy Wheeler

Prepared For: 2023 NYS Cybersecurity Conference

June 7, 2023

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Presentation Points

- Federal and State Cybersecurity and Cyber Defense Focus
- Move to Cloud, Shared Security Roles and Responsibilities
- Cloud Security Challenges
- Overview and Benefits of free/low-cost cloud security and compliance frameworks and resources
- Use Cases and Considerations
- Review Handout

Disclaimer: It should be noted that NYSTEC is vendor neutral. Any reference to specific products or cloud service providers are used for illustrative purposes only. Implementation of any of these resources, tools, or services, is at the sole discretion of your organization based on its needs and should be reviewed with your legal counsel.

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Presidential National Cybersecurity Strategy*

Vision

"Our rapidly evolving world demands a more intentional, more coordinated, and more well-resourced approach to cyber defense. We face a complex threat environment, with state and non-state actors developing and executing novel campaigns to threaten our interests. At the same time, next-generation technologies are reaching maturity at an accelerating pace, creating new pathways for innovation while increasing digital interdependencies."

This Strategy sets out a path to address these threats and secure the promise of our digital future.

- **Defensible**, where cyber defense is overwhelmingly easier, ***cheaper***, and more effective;
- **Resilient**, where cyber incidents and errors have little widespread or lasting impact; and,
- **Values-aligned**, where our most cherished values shape—and are in turn reinforced by— our digital world.

*FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

New York State Cybersecurity Focus

- NYS $61.9 million cybersecurity investment in the FY 2023 Budget, an increase of $35.2 million from previous years
  - Protect critical infrastructure and manufacturing systems/industrial controls
- Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)
- NYS Department of Financial Services (NYSDFS) Cybersecurity Regulation (23 NYCRR 500)

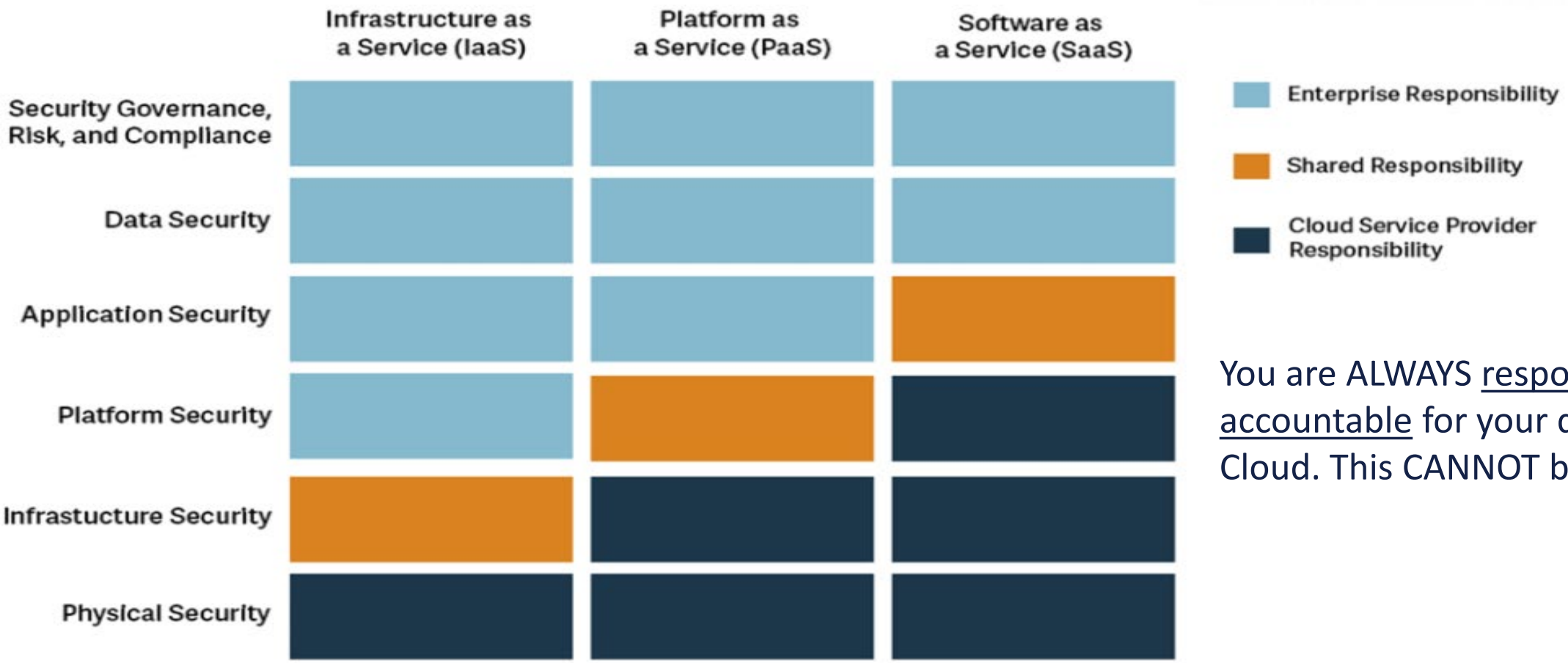
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Why Move to the Cloud?

- Cost reduction
  - Capital Expenditure (CapEx) to Operational (OpEx)
- Scalability
  - Elastic resourcing
- Security
  - Shared responsibility model
- Reliability
  - Most CSPs have 99.9999999% uptime SLAs
- Fast Implementation
  - Technical flexibilities, digital innovation
- Availability
  - Access applications anywhere, anytime

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Cloud Shared Security Roles and Responsibilities



You are ALWAYS responsible and accountable for your data in the Cloud. This CANNOT be delegated!

Fig. 1 Responsibility depending on type of cloud service from The Official (ISC)² Guide to the CCSP CBK, 2nd Edition.

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Top Cloud Security Challenges in 2023*

- **Misconfigurations**
  - Leading cause for cloud security breach
  - Poor cloud administration
  - Insider threat
- **Insufficient Cloud Security Expertise**
  - Applying on-premises security controls in the cloud is problematic
  - Not using native cloud security tools
  - Lack of train for security teams
- **Lack of Visibility**
  - Multi-cloud approach to prevent vendor lock-in
  - No centralized view of each environment
- **Account Takeovers**
  - Cloud control plane takeover
  - Attack on user identities, services and applications
- **Cloud Vulnerabilities**
  - Lack of cloud workload protections
    - E.g., missing patches, insecure coding, excessive permissions, etc.
- **API Security Mistakes**
  - Not maintaining an inventory
  - Not Requiring API authentication
  - Overly broad API access controls
  - Exposing unnecessary APIs

*Posted by Cloud Security Alliance; Originally published by InsiderSecurity 4/2023

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Overview of Cloud Security and Compliance

Cloud compliance (frameworks) **help align data security policies and mitigate the risks of deploying third-party cloud infrastructure**.*

- CIS Critical Security Controls
- Cloud Security Alliance (CSA)*
- FEDRAMP
- HITRUST
- ISO 27001 / 27017
- NIST 800-53
- NIST Cybersecurity
- OWASP

cloud CSA security alliance®

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

FR FedRAMP

ISO International Organization for Standardization

OWASP®

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Benefits of using Free Cloud Security Frameworks and Resources

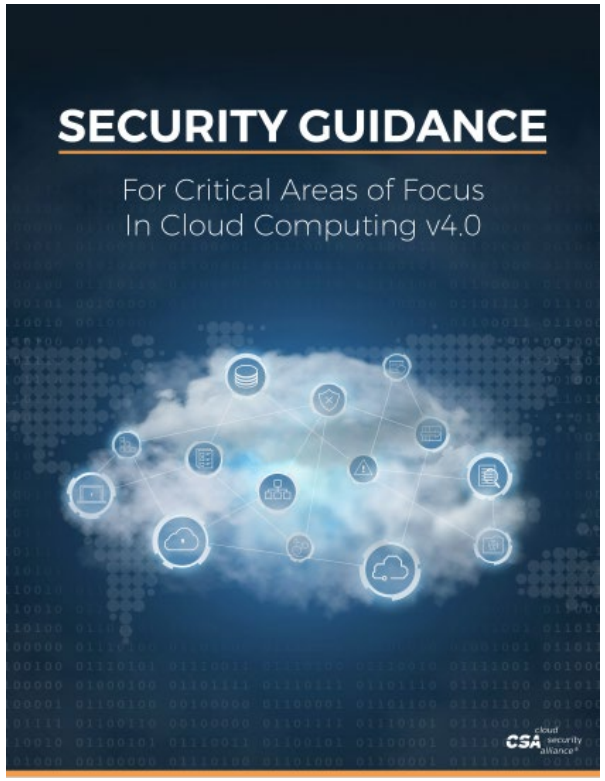
- Save time, money and effort using established / vetted security frameworks
- Provides baseline for which policies and supporting procedures are developed from
- Measure for compliance consistently
- Reduce exposure to known vulnerabilities
- Flexibility and Adaptability of the Framework
- Bridge the gap between technical and business-side stakeholders

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Free / On the Cheap Cloud Security Frameworks

- CSA Cloud Controls Matrix (CCM)
  - CSA Security, Trust, Assurance and Risk (STAR)
- FEDRAMP Authorization
- CISA
- NIST 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- ISO 27017 Security Standard Developed for Cloud Service Providers

CSA Cloud Controls Matrix (CCM)

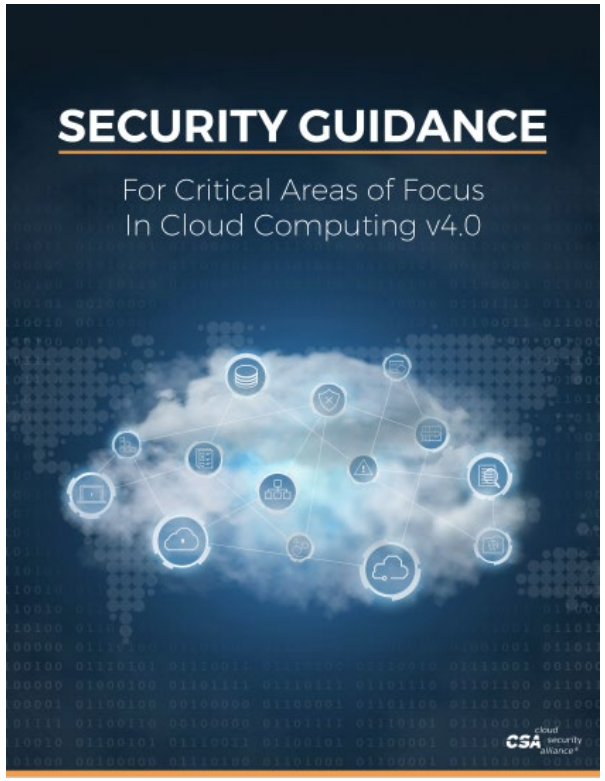


A&A	Audit and Assurance
AIS	Application & Interface Security
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control and Configuration Management
CEK	Cryptography, Encryption and Key Management
DCS	Datacenter Security
DSP	Data Security and Privacy
GRC	Governance, Risk Management and Compliance
HRS	Human Resources Security
IAM	Identity & Access Management
IPY	Interoperability & Portability
IVS	Infrastructure & Virtualization Security
LOG	Logging and Monitoring
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management
UEM	Universal EndPoint Management

Composed of:
- 17 security domains
- 197 Controls

Encompasses:
- Control Applicability and Ownership
- Architectural Relevance – Cloud Stack Components
- Organizational Relevance

CSA CCM Authoritative Source Control Mappings



CCM v4 maps to:

- ISO/IEC 27001/27002/27017/27018
- CCM V3.0.1
- CIS Controls V8
- AICPA Trust Services Criteria (TSC)

Mappings in development:

- PCI-DSS
- NIST 800-53 Rev.5

CSA Cloud Controls Matrix (CCM)

Control Specification	Implementation Guidelines	Auditing guidelines	SSRM
Specifies the control requirement(s) & objective(s)	Provides guidance for the implementation of control specifications	Provides guidance for the assessment of control specifications	Delineates control implementation responsibility for CSPs & CSCs

				Typical Control Applicability and Ownership (CSP-Owned, CSC-Owned, Shared)		
				IaaS	PaaS	SaaS
STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	Cloud service implementations involve a Shared Security Responsibility Model (SSRM) between the Cloud Service Provider (CSP) and the Cloud Service Customer (CSC) which…	1. Examine the policy for assessing, demarcating, and documenting the interfaces at the edges of the organization's responsibility. 2. Determine if the delineation has been done, and is current. 3. …	CSP-Owned	CSP-Owned	CSP-Owned

CSA CAIQ and STAR

- Consensus Assessment Initiative Questionnaire (CAIQ)
  - Security questionnaire (CAIQ v4) based on the CCM v4 submitted to the STAR Registry
- Security, Trust, Assurance and Risk (STAR)
  - Star Level 1
    - No cost self-assessment
    - Transparency around security controls in place
    - Listed in publicly available STAR Registry
    - Compliance Mark valid for 1 year

A Quick Note on CSA CCM & Privacy

- General Data Protection Regulation (GDPR) Code of Conduct (CoC) self assessment
  - Submitted to STAR Registry
  - Cost to use and register the GDPR CoC
  - Contact CSA for more details

FEDRAMP and its Benefits

What is FEDRAMP?

- Government-wide program for cloud technologies and federal agencies
- Promotes the adoption of secure cloud services across the federal government
- Provides a standardized approach to security and risk assessment
- Leverages NIST standards and guidelines
- Meets FISMA requirements to protect federal information
- Publicly available at no cost
- Easy to use Excel format
- Free resources (documents, templates, training, FAQs, baselines)

Benefits

- Framework and resources are available at no cost
- FEDRAMP certification by third party assessment organization (3PAO) is required to provide any cloud service to the federal government
  - Control inheritance

FEDRAMP NIST Control Catalog

	A	B	C	D	E
1	NIST SP 800-53, Revision 5 Security and Privacy Controls for Information Systems and Organizations				
2	Control Identifier	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
3	AC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.	IA-1, PM-9, PM-24, PS-8, SI-12 .

FEDRAMP Low Impact SaaS (LI-SaaS)

FedRAMP® Tailored LI-SaaS Baseline Worksheets

There are five (5) categories of FedRAMP *Tailored* Low Impact-Software as a Service (LI-SaaS) Baseline controls, based on the FedRAMP Low Impact Baseline, that are required to be addressed by the Cloud Service Provider (CSP). The following table provides a list of the tailoring symbols with a short description of the tailoring criteria.

Tailoring Symbol	Tailoring Criteria
FED	The control is typically the responsibility of the Federal Government, not the CSP.
NSO	FedRAMP has determined the control does not impact the security of the Cloud SaaS.
Document and Assess	The control must be documented in Appendix B, and independently assessed. This does not mean that a vendor will necessarily have each control fully implemented or implemented as stated. A vendor must address how they meet (or don't meet) the intent of the control so that it can be independently assessed and detail any risks associated with the implementation.
Document and Assess (Conditional)	If the condition exists, the control must be documented in Appendix B and independently assessed as above. If the condition does not exist, the CSP must attest to this in Appendix E.
Attest	The control must exist; however, the CSP may attest to its existence in Appendix E. (No documentation or independent assessment is required.)

The LI-SaaS Baseline worksheet provides provides details of the FedRAMP tailoring criteria for all FedRAMP Low Impact Baseline controls.

Click here to view the LI-SaaS Baseline worksheet

- FedRAMP Tailored is intended to speed up the adoption of cloud services in low-risk use cases
- LI-SaaS is a lightweight version of Low in terms of security baseline requirements
- Specific requirements to qualify as LI-SaaS such as:
  - Must meet NIST 800-145 definition of SaaS
  - Does not contain any PII
  - Must meet FIPS low-security-impact definition
  - Must use FEDRAMP Authorized PaaS or IaaS or use its own systems

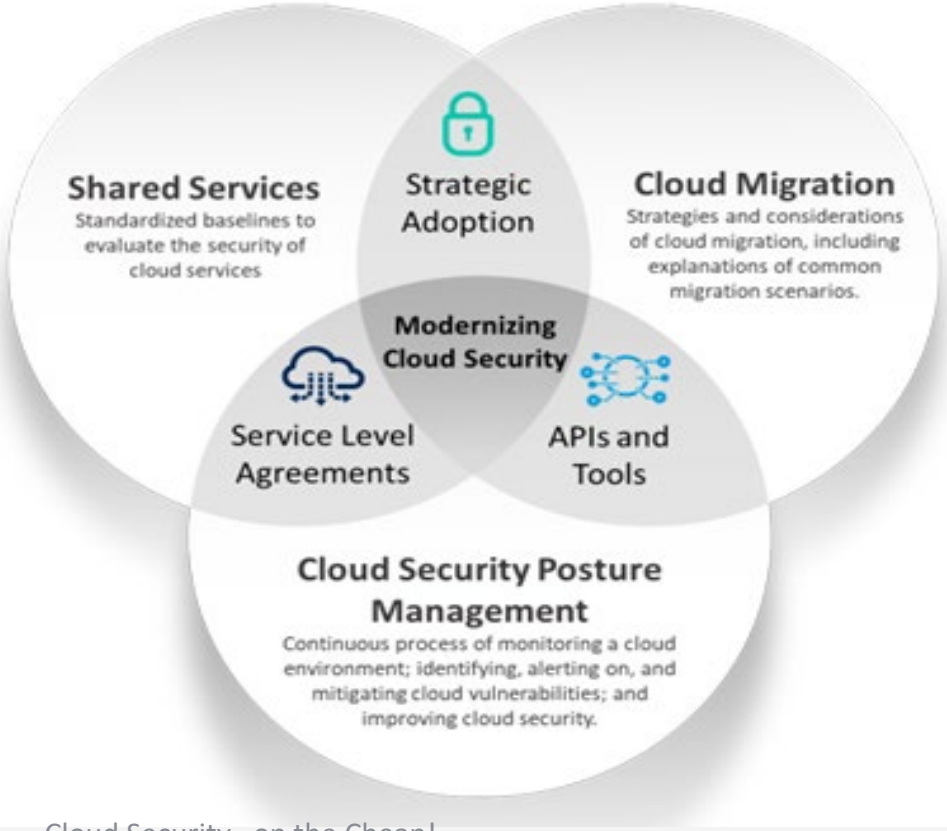
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

CISA Cloud Security Technical Reference Architecture

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Cloud Security Technical Reference Architecture (CSTRA) v2



- CSTRA focuses on how Federal agencies and their suppliers can avoid preventable cloud breaches that have downstream impacts on local communities and citizens.*
- Based on FEDRAMP
- Key focus areas include:
  1. Shared Services
  2. Strategic Adoption
  3. Cloud Migration
  4. Modernizing Cloud Security
  5. Service Level Agreements
  6. APIs and Tools
  7. Cloud Security Posture Management

*Orca Security, "Understanding CISA's Cloud Security Technical Reference Architecture," (2022)

CISA CSTRA Shared Security Roles and Responsibilities

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

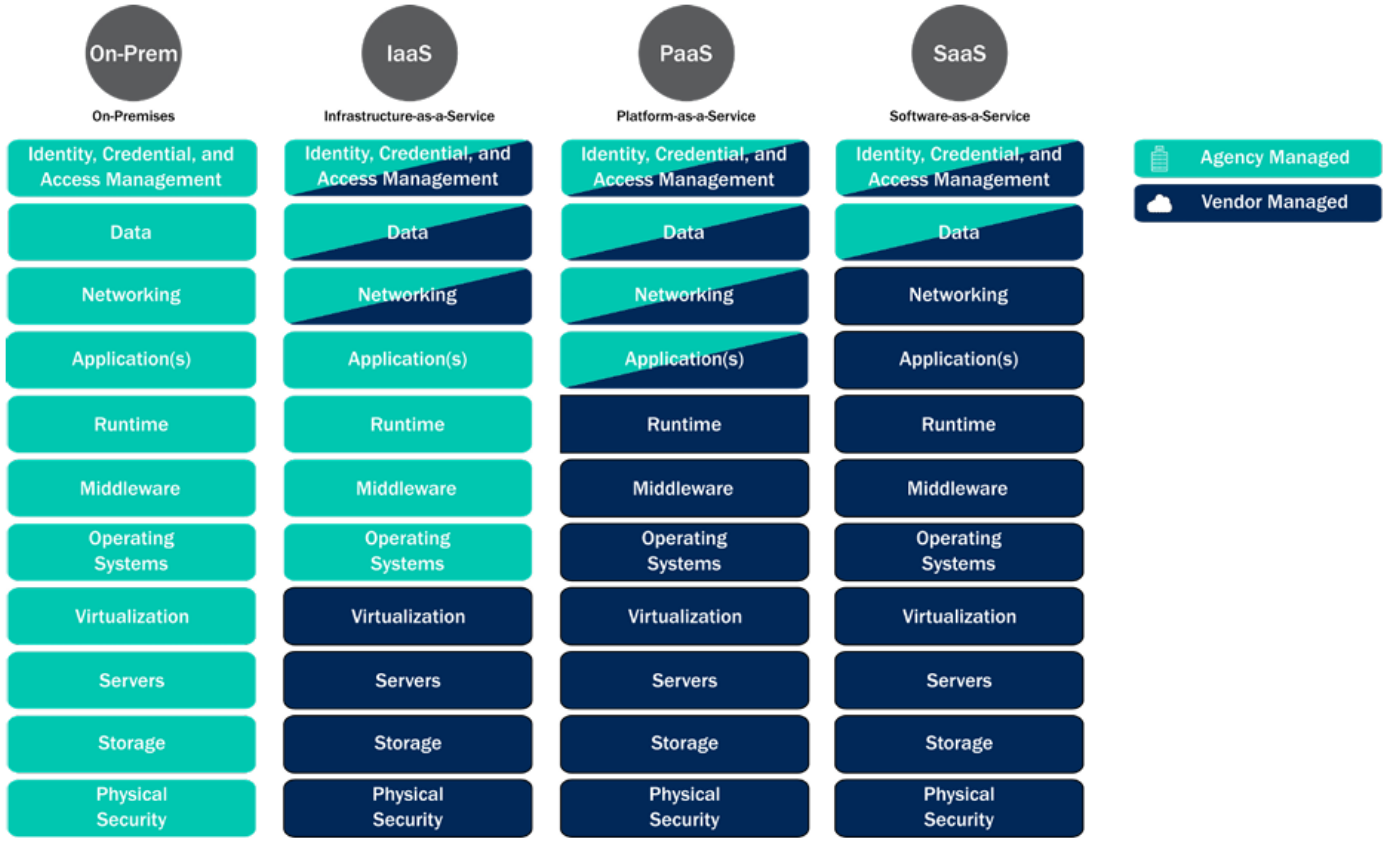


Figure 2: Responsibilities for Different Service Models

- CISA's Shared Security Roles and Responsibilities is based on where digital assets reside and who is responsible for those assets

Use Case 1 – Strategic Use of Free Cloud Security Frameworks to Align with Business Needs

- Strategically selecting the right framework to meet your business needs
  - Manufacturing – CSA CCM -> ISO framework
  - Healthcare – FEDRAMP -> NIST based framework

- Challenges with defining impact level for a system
  - **FISMA and System Impact level Assignment**
    - Industry influences impact level
    - NIST 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories
    - Data classification may drive the need for additional controls of specific datasets

Use Case 3 – Governance Requirements and Compliance

Based on data classification, sensitive data like PHI requires protection which meets both CMS and IRS requirements.

In review of NIST 800-53 Account Management (AC-2) Control (J)

- **NIST 800-53 Rev 5**

  Review accounts for compliance with account management requirements **[*Assignment: organization-defined frequency*].**

- **CMS Acceptable Risk Safeguards (ARS) v5** (more specific)

  Review accounts for compliance with account management requirements at **least every 365 days for all systems**.

✓ **IRS 1075** (even more specific, and rigorous)

  Review accounts for compliance with account management requirements **annually for user account and semi-annually for privileged accounts.**

When documenting how this control requirement has been implemented, the IRS 1075 requirement must be used to ensure compliance for all governances.

General Considerations

- Considerations
  - Resource constraints
  - Workforce knowledge
  - Control alignment between frameworks
  - Multiple governance requirements
  - Contractual or regulatory requirements specifying third party security assessment and certification
    - ISO, HITRUST, PCI, IEEE, etc.
  - Cyber Liability Insurance – no such thing as zero risk
  - Collaboration
  - Reasonable, not applicable (N/A) and documentation
  - Be auditable

Review of Handout

- Cloud Security Free/Low-Cost Resources
  - Educational
  - Planning
  - Training and Certifications
  - Security Baselines and Benchmarks
  - Tools and Service Offerings
  - Miscellaneous Links

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Wrap Up

- Importance and Challenges of Implementing Cloud Security
- Free and Low-cost Cloud Security and Compliance Frameworks and Resources
- Don’t forget to look at our e-handout!
- Thank you!

NYSTEC

YOUR INDEPENDENT TECHNOLOGY ADVISOR

(888) 969-7832
nystec@nystec.com
www.nystec.com