State of Washington – Cybersecurity Awareness Month

Cloud Security Challenges and Solutions

An Overview of the Approach Oregon Takes

October 13, 2025

Sean McSpaden, Principal Legislative IT Analyst
Committee Administrator – Joint Legislative Committee on Information Management and Technology

LFO
LEGISLATIVE FISCAL OFFICE

Table of Contents

- Oregon Legislative Fiscal Office (LFO)
- Joint Legislative Committee on Information Management and Technology (JLCIMT)
- Cloud Computing - Essential Characteristics, Delivery & Deployment Models
- Common Risks, Issues, and Challenges – Cloud and as a Service (XaaS) Solutions
- Oregon Information Technology (IT) Profile - Organizational Structure
- Oregon's approach to Cybersecurity
- Questions & Contact Information

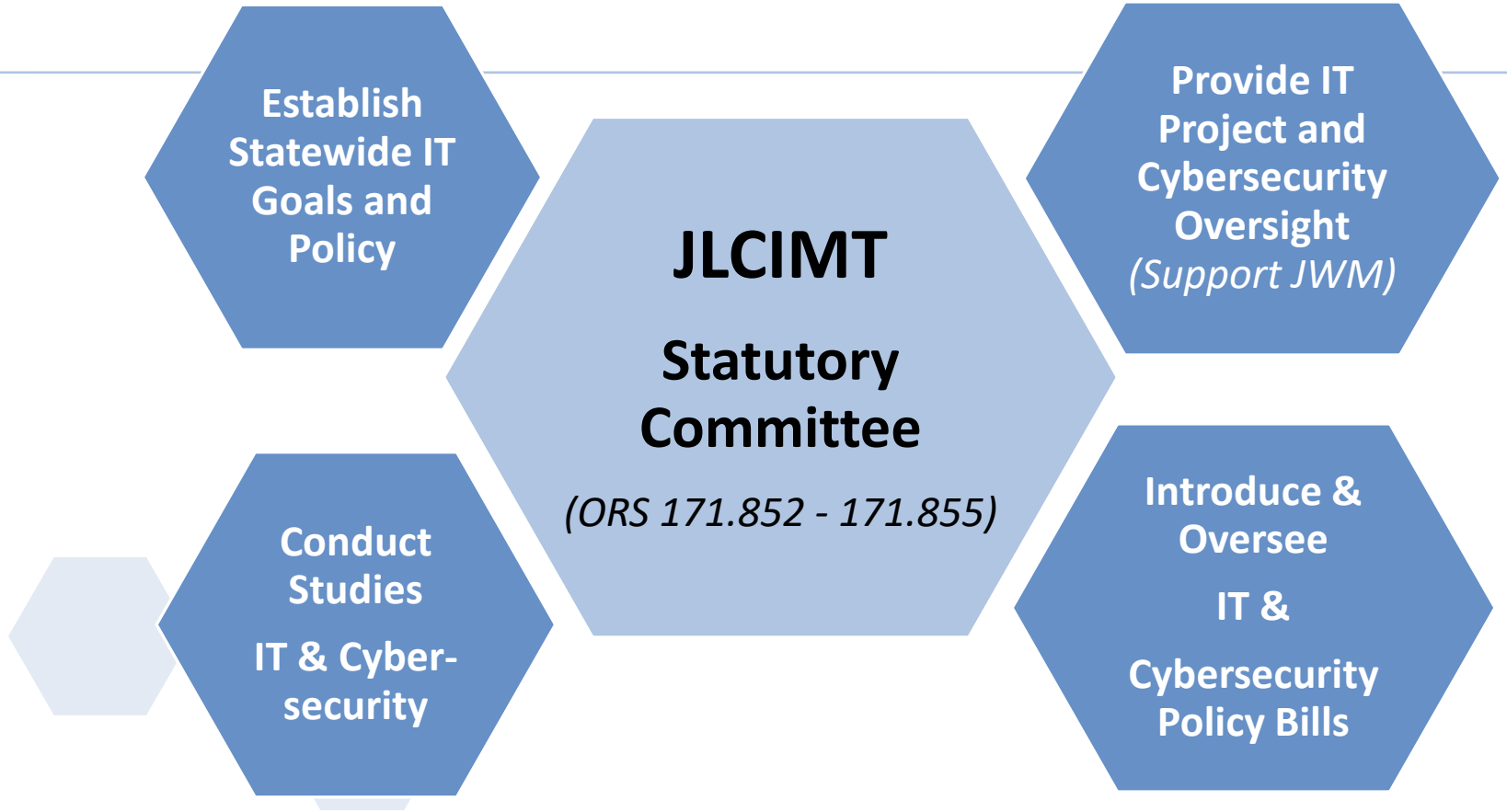
Oregon Legislative Fiscal Office

- Legislative Fiscal Officer is appointed by co-chairs of Joint Committee on Ways and Means
- The Legislative Fiscal Office (LFO) is a permanent nonpartisan legislative service agency that:
  - Provides comprehensive research, analysis, and recommendations on state's biennial budget
  - Evaluates state expenditures, program administration, and agency organization
  - Assists in developing Legislature's adopted balanced budget
  - Prepares fiscal impact statements on legislative measures
  - Publishes detailed analyses, summary documents, and briefs on budget-related topics
  - Performs other duties as directed by the Legislative Fiscal Officer
- https://www.oregonlegislature.gov/lfo

Oregon Legislative Fiscal Office (LFO)
Provides Professional Staff Support

- **Emergency Board** *(Legislative Interim)*
- **Joint Committee on Ways and Means**
- **Joint Legislative Audits Committee**
- **Transparency Oregon Advisory Commission**
- **Joint Legislative Committee on Information Management and Technology**
- **Other Special Committees or Task Forces**

Joint Legislative Committee on Information Management and Technology

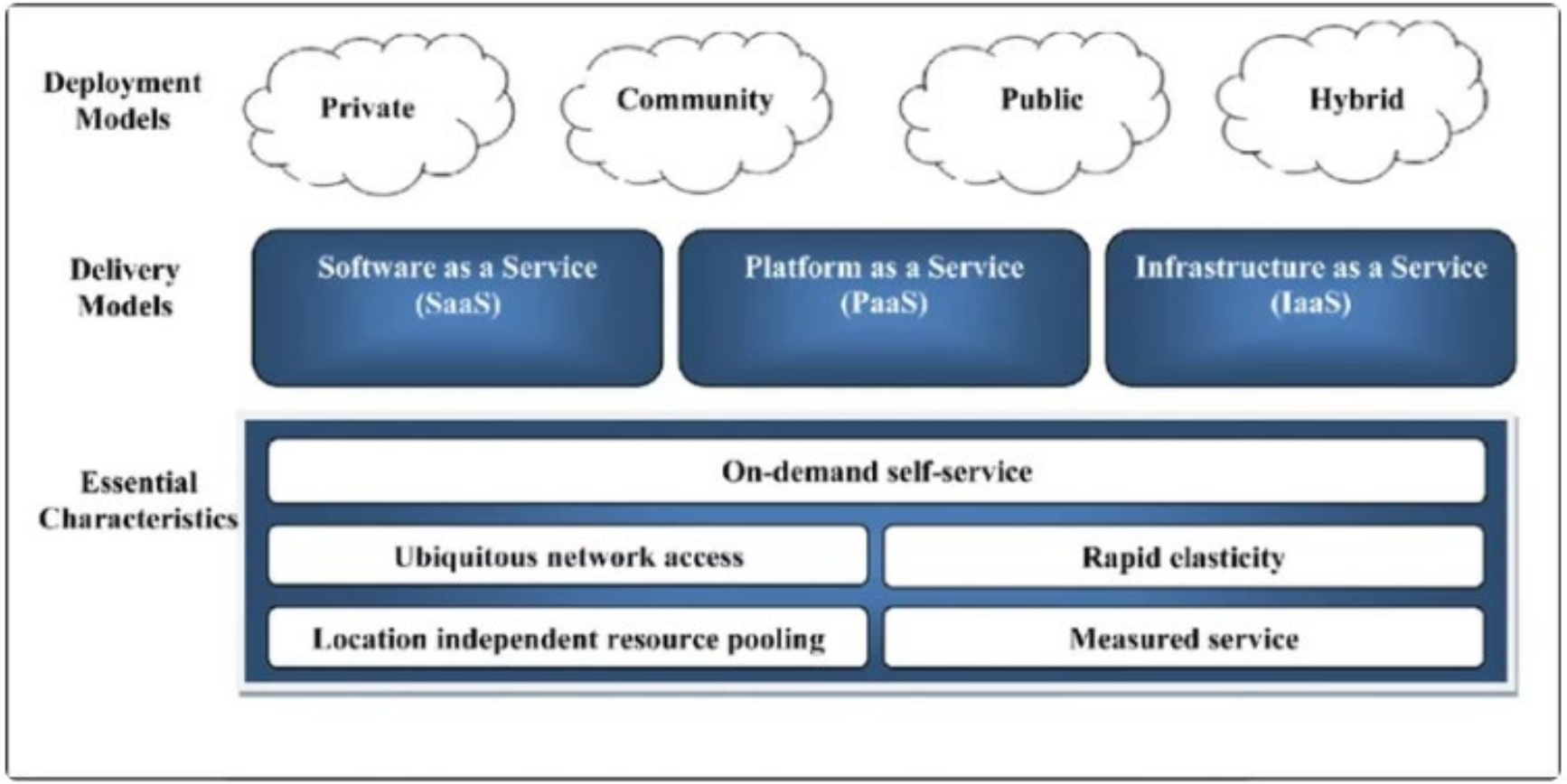


- https://www.oregonlegislature.gov/bills_laws/ors/ors171.html
  https://olis.oregonlegislature.gov/liz/2025I1/Committees/JLCIMT/Overview

CLOUD COMPUTING

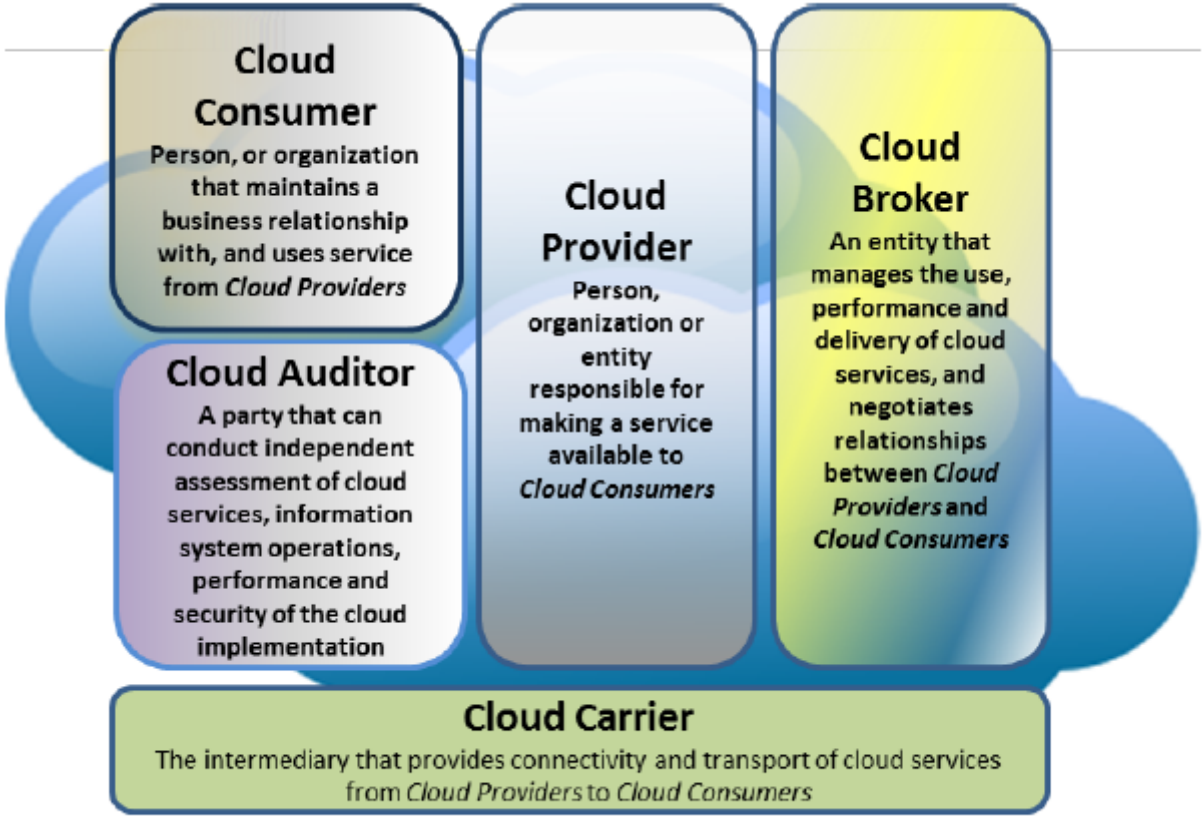
ESSENTIAL CHARACTERISTICS, DELIVERY & DEPLOYMENT MODELS

Cloud Computing
Essential Characteristics, Delivery & Deployment Models



Source – NIST Special Publication 800-145 (September 2011)

NIST Cloud Computing Standards Roadmap Cloud Actors



Source – [NIST Special Publication 500-291, Version 2 (July 2013)]

NIST Cloud Computing Standards Roadmap Service Models Cloud Consumer & Provider Activities

Service Models	Consumer Activities	Provider Activities
SaaS	Uses application/service for business process operations.	Installs, manages, maintains, and supports the software application on a cloud infrastructure.
PaaS	Develops, tests, deploys, and manages applications hosted in a cloud system.	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment, and administration tools to platform consumers.
IaaS	Creates/installs, manages, and monitors services for IT infrastructure operations.	Provisions and manages the physical processing, storage, networking, and the hosting environment and cloud infrastructure for IaaS consumers.

Table 1 – Cloud Consumer and Cloud Provider

Source – NIST Special Publication 500-291, Version 2 (July 2013)

NIST Cloud Computing Standards Roadmap

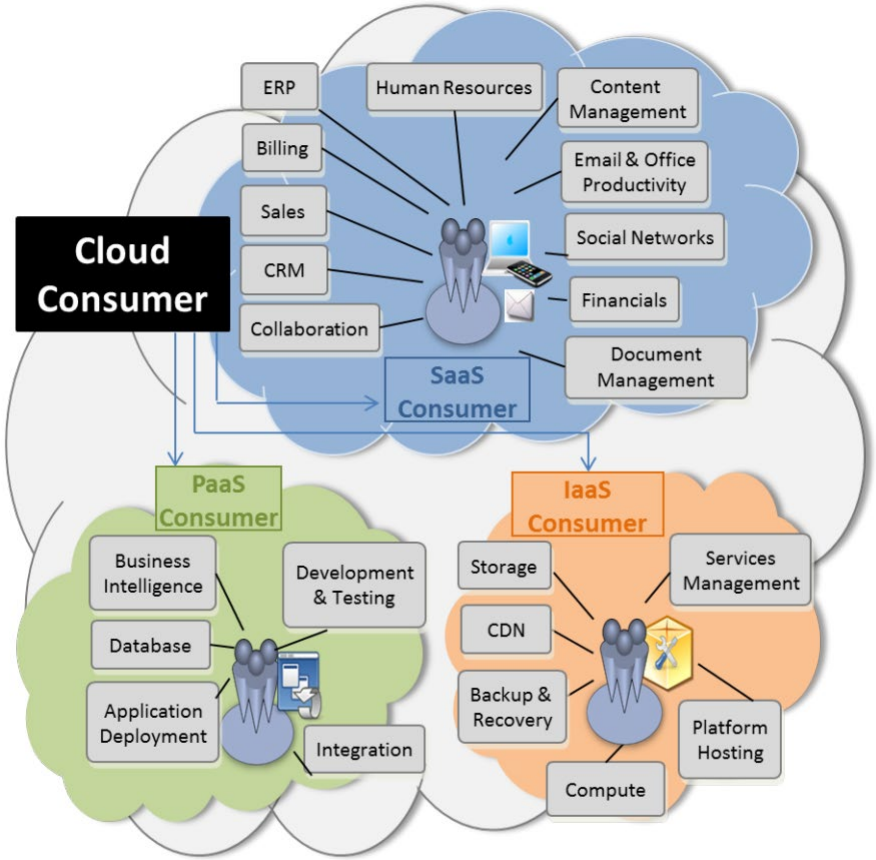


Figure 3 – Example of Services Available to a Cloud Consumer

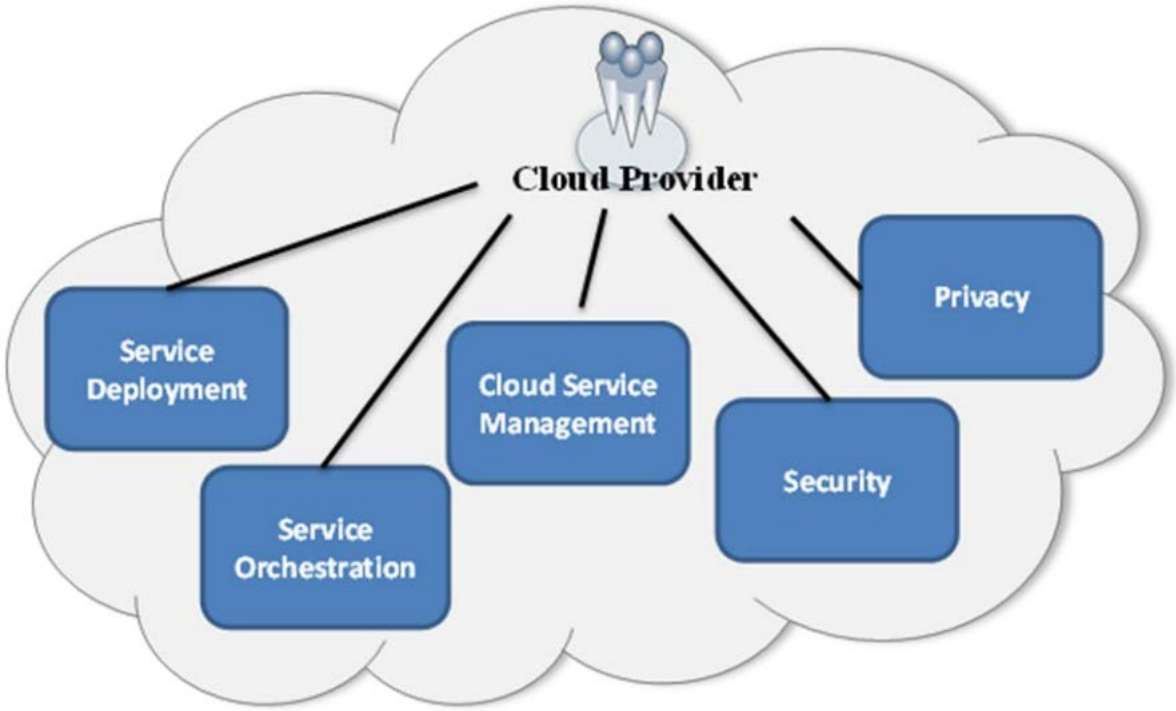
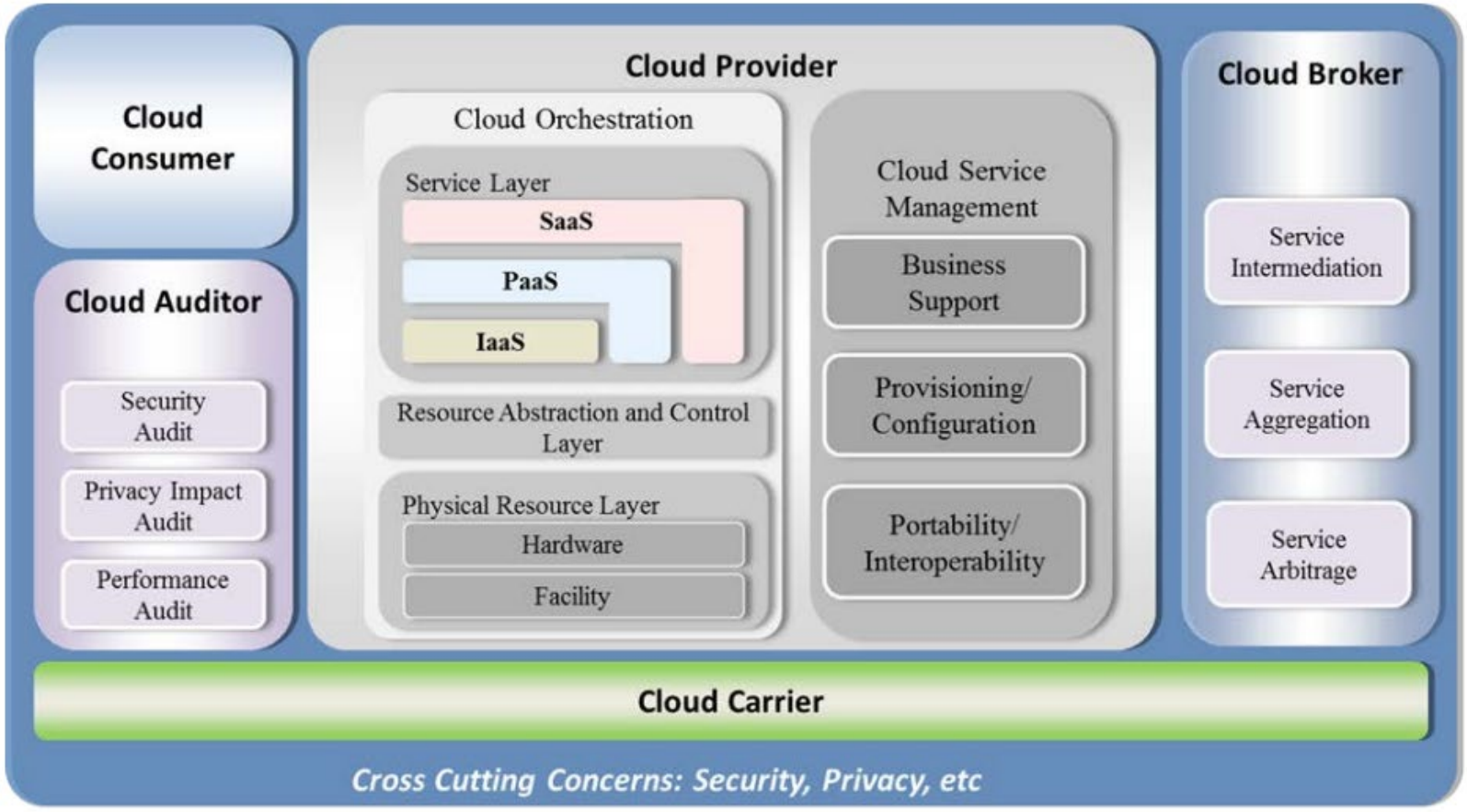


Figure 4 – Cloud Provider: Major Activities

Source – [NIST Special Publication 500-291, Version 2 (July 2013)]

NIST Cloud Computing Reference Architecture Combined Conceptual Reference Diagram



Source – [NIST Special Publication 500-291, Version 2 (July 2013)]

Cloud Delivery Models – Technology Stack Controls

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

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

Table 3: IaaS Technology Stack Controls[3]

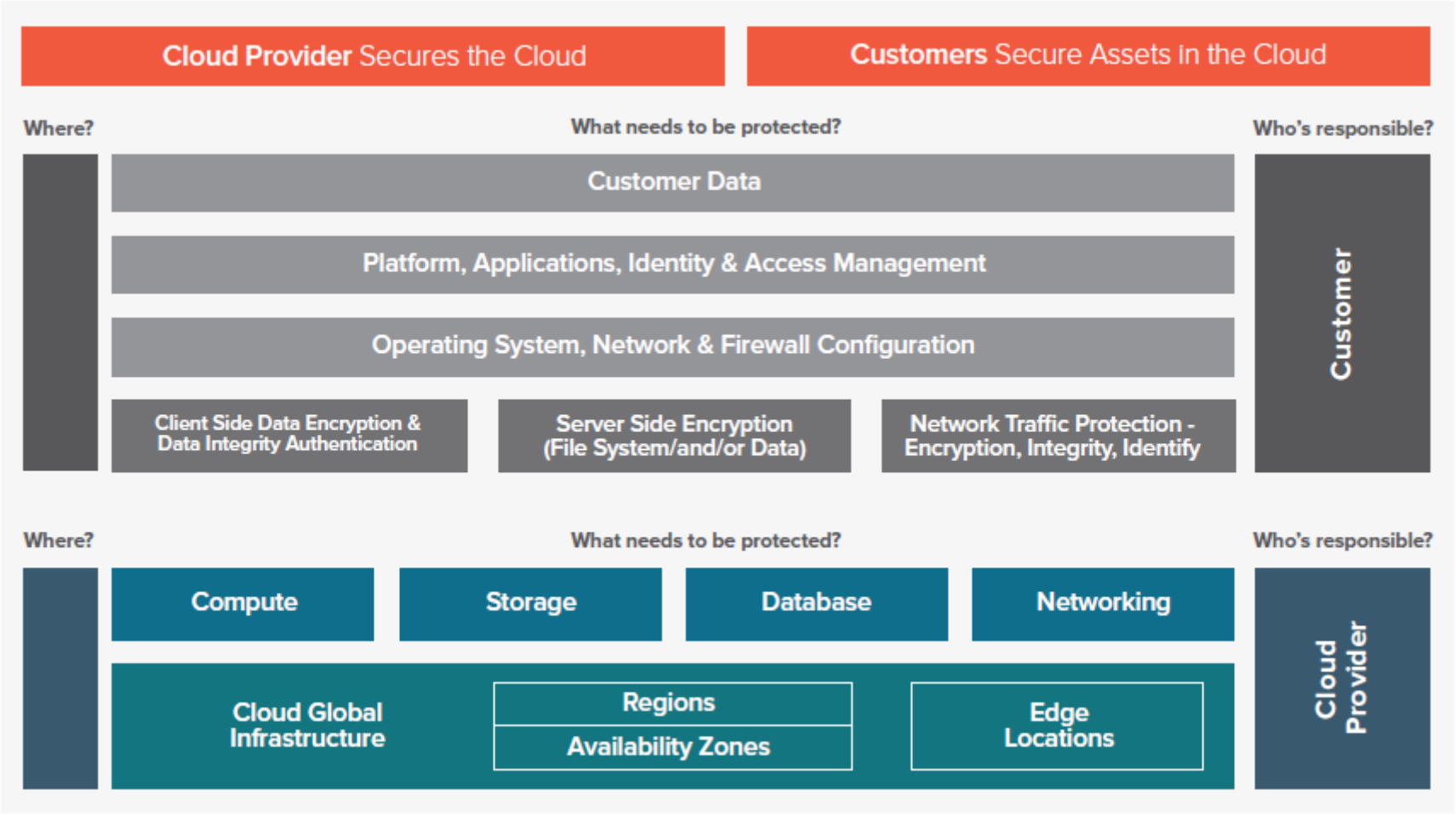
Service Provider	Technology Stack	Public Jurisdiction
No Control	Application (e.g., mail)	Total Control
No Control	Middleware (e.g., java)	Total Control
No Control	Guest Operating System	Total Control
Administrative Control	Hypervisor	Make Requests
Total Control	Hardware	No Control

https://papers.govtech.com/Best-Practice-Guide-for-Cloud-and-As-A-Service-Procurements-141869.html

Cloud Delivery Models – Anything-as-a-Service (XaaS)

Cloud Service Security – Who's Responsible?

It's a Shared Obligation/Responsibility



https://papers.govtech.com/Best-Practice-Guide-for-Cloud-and-As-A-Service-Procurements-141869.html

COMMON RISKS, ISSUES, AND CHALLENGES

CLOUD AND AS A SERVICE (XAAS) SOLUTIONS

Cloud Solutions - Risks, Issues, and Challenges (Governance, Policy, Operational)

1. Governance, Policy and Oversight
2. Procurement (Contracting) and Legal
3. Organizational and Cultural Barriers

Cloud Solutions - Risks, Issues, and Challenges (Governance, Policy, Operational)

4. Workforce and Training Deficits

5. Data Governance and Compliance

6. Incident Response and Business Continuity

Cloud Solutions - Risks, Issues, and Challenges (Governance, Policy, Operational)

7. Cost, Budget and Financial Oversight
8. Compliance and Audit Limitations
9. Vendor Lock-in and Exit Strategy (Disentanglement)
10. Multi-jurisdictional & Policy Alignment (laws, rules, policies)

Cloud Solutions - Risks, Issues, and Challenges

Risk / Issue	Description
1. Identity, Credential, & Access Management Weaknesses	Over-permissioned roles, missing MFA, unmanaged keys or service accounts.
2. Insecure APIs and Interfaces	Unprotected endpoints, poor input validation, and weak authentication.
3. Misconfiguration and Poor Change Management	Open ports, default passwords, open storage, unmonitored configuration drift.
4. Weak Cloud Security Architecture & Segmentation	Flat networks, poor segmentation, unclear shared-responsibility boundaries.
5. Insecure Software Development	Unverified dependencies & libraries, lack of code scanning/testing, unprotected registries
6. Unsecured Third-Party Integrations	Weak trust models, external connectors without validation or continuous monitoring.
7. System and Application Vulnerabilities	Unpatched operating systems, libraries, or middleware, vulnerable APIs.
8. Data Leakage and Exfiltration	Unencrypted data, public buckets, or weak access policies, unmonitored environment.
9. Insufficient Encryption & Key Management	Improper rotation, key exposure, or non-FIPS algorithms.
10. Inadequate Monitoring & Logging	Missing or siloed logs, poor anomaly detection, no automated alerting.
11. Resource Sprawl & Shadow IT	Unmanaged cloud accounts or SaaS subscriptions, rogue XaaS purchasing.
12. Backup & Recovery Gaps	Sole reliance on provider, no tested recovery plans or immutable backups.
13. Multi-Tenancy Risks	Cross-tenant vulnerabilities and side-channel attacks, hypervisor misconfigurations
14. Legacy or Hybrid Integration Issues	Insecure connections between on-prem and cloud systems, inconsistent patching, etc.
15. Insufficient Security Testing/Continuous Assurance	Limited scanning, testing, or continuous assurance controls.

Cloud Security Alliance
Top Threats to Cloud Computing Deep Dive

Top Cloud Threats Coverage

In the *Top Threats to Cloud Computing 2024 survey*, we surveyed over 500 industry experts on security issues in the cloud industry. Our respondents identified eleven important security issues to their cloud environment (ranked in order of concern indicated by the survey):

TT1. Misconfiguration and Inadequate Change Control	**TT7.** Accidental Cloud Disclosure
TT2. Identity and Access Management (IAM)	**TT8.** System Vulnerabilities
TT3. Insecure Interfaces and APIs	**TT9.** Limited Cloud Visibility/Observability
TT4. Inadequate Selection/Implementation of Cloud Security Strategy	**TT10.** Unauthenticated Resource Sharing
TT5. Insecure Third-Party Resources	**TT11.** Advanced Persistent Threats (APT)
TT6. Insecure Software Development	

Cloud Security Alliance
Top Threats to Cloud Computing Deep Dive

The top cloud concerns manifested in the breach cases covered this year are:

	Snowflake	Football Australia	CrowdStrike	Toyota	Darkbeam	Retool & Fortress	FTX	Microsoft
TT1								
TT2								
TT3								
TT4								
TT5								
TT6								
TT7								
TT8								
TT9								
TT10								
TT11								

Cloud Security Alliance
Top Threats to Cloud Computing Deep Dive

Tier 1 - Most Frequent (4 to 7 appearances) – The most commonly observed security threats across breach cases.

- IAM – Weak access controls, lack of multifactor authentication (MFA), and privilege escalation enabled unauthorized access.
- Misconfiguration and Inadequate Change Control – Improperly secured cloud environments led to prolonged data exposure.
- Insecure Software Development – Weak software development, delivery, and deployment practices introduced security flaws that attackers exploited.

Tier 2 - Notable (3 appearances) – These threats appeared in multiple cases and represent significant security concerns.

- Insecure Interfaces and APIs – Publicly exposed or weakly secured APIs served as attack vectors in multiple incidents.
- Inadequate Selection/Implementation of Cloud Security Strategy – Organizations without well-defined cloud security strategies faced governance and risk management challenges.
- System Vulnerabilities – Unpatched software and outdated configurations contributed to security breaches.

Tier 3 - Less Frequent (1 or 2 appearances) – Less frequently observed threats but still relevant.

- Limited Cloud Visibility/Observability – Unintentional exposure of sensitive data due to human error in cloud configurations.
- Unauthenticated Resource Sharing – Publicly accessible cloud resources (e.g., confidential or sensitive data) increase the risk of unauthorized access.
- Insecure Third-Party Resources – Supply chain risks reinforced the need for proactive vendor security assessments and continuous monitoring.
- APT – Threat actors leveraged credential theft, privilege escalation, and lateral movement.

Cloud Security Alliance Summary (Threats, Control Failures, and Loss)

Case	Year	Key Threats	Key Control Failures	Est. Loss
Snowflake	2024	TT2, TT11	IAM, DSP, LOG	$2M+
Football AU	2024	TT1, TT2, TT6, TT7, TT10	CCC, DSP, IAM, STA, LOG	$370K+ (est.)
CrowdStrike	2024	TT6, TT1, TT4, TT5	QA, TVM, A&A, SEF	$5.4B (est.)
Toyota	2023	TT1, TT2, TT9	IAM, CCC, IVS	Ongoing risk
DarkBeam	2023	TT1, TT3, TT7	DCS, IAM, LOG	Undisclosed
Retool/Fortress	2023	TT2, TT5, TT10	IAM, SEF, STA	$15M
FTX	2022	TT2, TT4, TT8	IAM, SEF, IVS	$400M+
Microsoft	2024	TT2, TT6, TT8	DSP, IAM, DSI	Global impact

Cloud Security Alliance - Top Threats to Cloud Computing Key Takeaways

Cloud Security Must Account for Human Error and Persistent Threats

- Cloud architectures and security strategies must assume misconfigurations and human mistakes will occur as threat actors seek to exploit them.
- Continuous improvement requires continuous auditing, security automation, security awareness initiatives, and integrating lessons learned from past incidents.

Identity and Access Security Controls Are Essential

- Strong IAM practices, including MFA, least privilege access control, and privileged access management (PAM) must be rigorously enforced.
- Excessive privileges, weak authentication, and poor access control policies frequently enable lateral movement and privilege escalation in breaches.

Shared Responsibility in Cloud Security Must Be Enforced

- Cloud providers and users must work together to secure their environments by implementing configuration management, access controls, and security monitoring.
- Vendors should promote secure defaults, enforce strong configurations, and proactively detect abuse within cloud services.

Continuous Monitoring and Real-Time Detection Are Critical

- Automated monitoring, anomaly detection, and centralized logging are necessary to identify misconfigurations, unauthorized access, and malicious activities quickly.
- Many cloud breaches remain undetected for extended periods due to insufficient visibility and alarms/notifications.

Cloud Security Alliance - Top Threats to Cloud Computing Key Takeaways

Supply Chain Security Must Be Strengthened

- Threat actors target weaknesses in supply chains, open-source components, and third-party integrations to infiltrate cloud environments.
- Organizations must assess vendor security, enforce strict security requirements, and continuously monitor dependencies for potential threats.

Proactive Cloud Governance Reduces Long-Term Risk

- Weak governance, a lack of consistent misconfiguration review, and compliance monitoring allow security gaps to persist for years.
- Organizations must enforce cloud security policies, maintain secure configuration baselines, and conduct regular governance reviews to ensure timely remediation of security risks in compliance with regulations such as GDPR and HIPAA.

Incident Response and Recovery Must Be Cloud Specific

- Traditional incident response plans fail to account for cloud complexity, leading to delayed detection and mitigation.
- Organizations must enforce cloud security policies, maintain secure configuration baselines, and conduct regular governance reviews to ensure timely remediation of security risks in compliance with data protection and industry-specific regulations such as GDPR and HIPAA.

Security Testing and Validation Must Extend Beyond Production

- Many breaches originate from vulnerabilities in development and testing environments, where security controls are often weaker than in production.
- Least privilege, access controls, and security monitoring must be enforced across all cloud environments to prevent attackers from exploiting non-production systems.

SECURE CLOUD SERVICE ACQUISITION, DEPLOYMENT & USE

RISK AND AUTHORIZATION MANAGEMENT PROGRAMS

Risk and Authorization Management Program - 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 notice the service provider community

https://papers.govtech.com/Best-Practice-Guide-for-Cloud-and-As-A-Service-Procurements-141869.html

Cloud and as-a-Service Procurement – Terms and Conditions

- Clause 1. Definitions
- Clause 2. Data Ownership
- Clause 3. Data Protection
- Clause 4. Data Privacy
- Clause 5. Data Location
- Clause 6. Data Access
- Clause 7. Import/Export of Data
- Clause 8. Security Incident or Data Breach Notification
- Clause 9. Breach Responsibilities
- Clause 10. Background Checks
- Clause 11. Non-Disclosure and Separation of Duties
- Clause 12. Right to Remove Individuals
- Clause 13. Security
- Clause 14. Access to Security Logs and Reports
- Clause 15. Retention, Preservation and Archival of Security Logs and Reports
- Clause 16. Encryption of Data at Rest
- Clause 17. Contract Audit
- Clause 18: Data Center Audit
- Clause 19. Continuous Monitoring
- Clause 20. Responsibilities and Uptime Guarantee
- Clause 21. Change Control and Advance Notice
- Clause 22. Subcontractor Disclosure
- Clause 23. Business Continuity and Disaster Recovery
- Clause 24. Compliance with Accessibility Standards
- Clause 25. Web Services
- Clause 26. Subscription Terms
- Separation of Duties
- Clause 27. Notification of Legal Requests
- Clause 28. Termination and Suspension of Service

Note: May/may not be applicable to each cloud service model (IaaS, PaaS, SaaS)

https://papers.govtech.com/Best-Practice-Guide-for-Cloud-and-As-A-Service-Procurements-141869.html

Cloud and as-a-Service Procurement – Building RAMP into Contracts

https://papers.govtech.com/Best-Practice-Guide-for-Cloud-and-As-A-Service-Procurements-141869.html

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?

Cloud and as-a-Service Procurement – Terms and Conditions

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?

https://papers.govtech.com/Best-Practice-Guide-for-Cloud-and-As-A-Service-Procurements-141869.html

Risk and Authorization Management Program - Alternatives

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.

DIY RAMP

- ARIZONA
- TEXAS (TX-RAMP)

https://papers.govtech.com/Best-Practice-Guide-for-Cloud-and-As-A-Service-Procurements-141869.html

GovRAMP Statuses

GovRAMP

https://govramp.org/

Snapshot

Cyber **NIST Score of 40 Controls**

Progressing Snapshot

Cyber **NIST Score of 40 Controls** + Monthly Advisory + Quarterly Snapshot Updates

Core Status

Demonstrates achievement with assessment of **60 NIST Controls by PMO**, Quarterly ConMon + Documentation

Ready Status

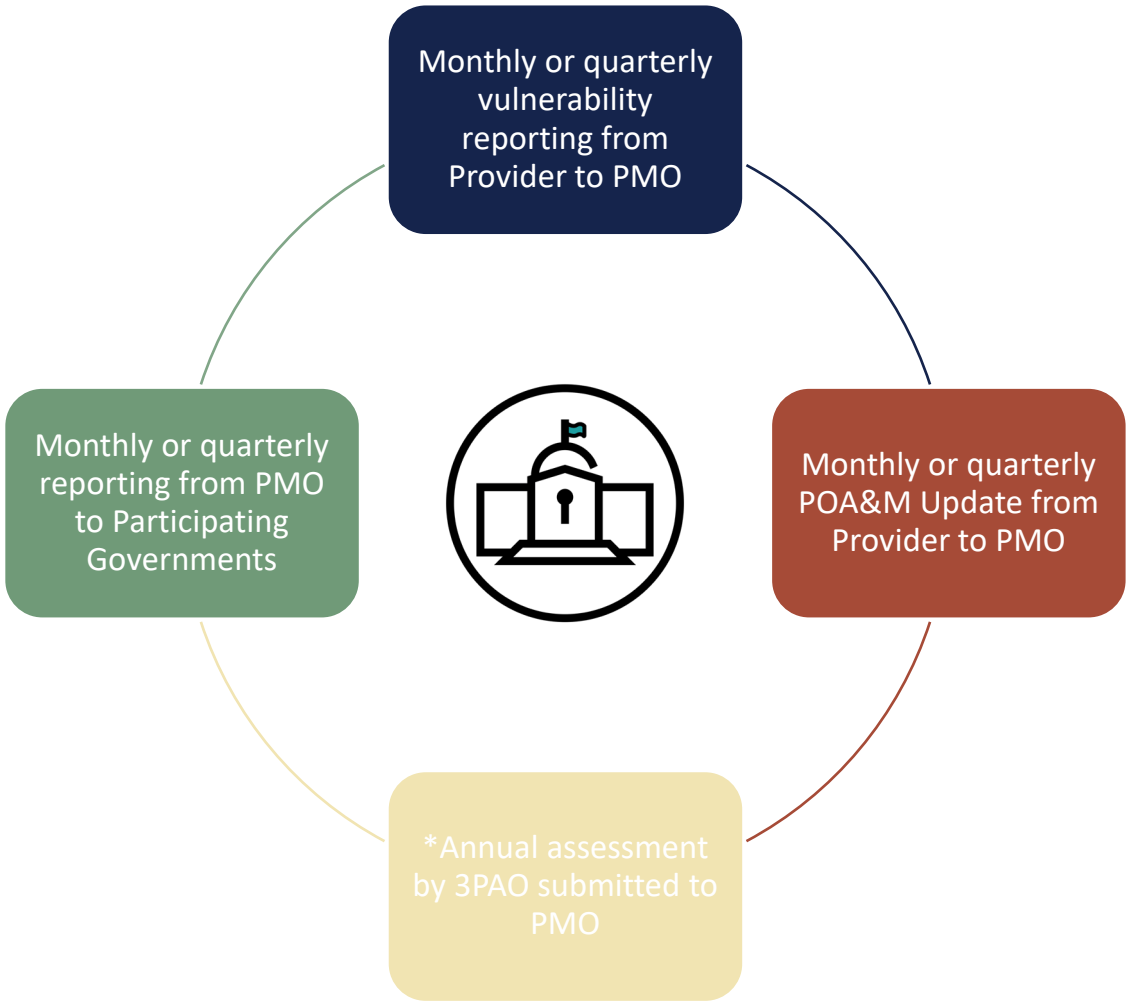
Demonstrates achievement with Ready Audit of **80 NIST Controls by 3PAO**, Monthly ConMon + Annual Assessment + Documentation

Authorized or Provisionally Authorized Status

Demonstrates achievement with Security Audit of **300+ NIST Controls by 3PAO**, Monthly ConMon + Annual Assessment + Documentation

Assessment & Validation Conducted by PMO

Assessment by 3PAO, with PMO Validation & ConMon



Continuous Monitoring

Providers must comply with Continuous Monitoring requirements to maintain the status of Core, Ready, Authorized, or Provisionally Authorized.

Providers may grant viewing access to Participating Governments at the Standard Access level or the Elevated Access level.

View Continuous Monitoring Policies & Escalation Process for more: www.GovRAMP.org/templates-resources.

GovRAMP Adoption Tiers for SLED Agencies

GovRAMP Best Practice

Accept	Prefer	Require
Indicates that an organization **allows a GovRAMP assessment to satisfy a business requirement** in addition to other assessments.	Indicates that an **organization offers preference or additional evaluation points** for GovRAMP assessed products.	Indicates that an organization **fully adopts & requires GovRAMP** from solicitation through award & contract management.
Examples: 1. Accepts GovRAMP Snapshot, Core, Ready or Authorized for all contracts in addition to other risk assessments. 2. Accepts GovRAMP Ready at solicitation, in addition to other risk assessments for IT contracts, satisfying the requirements for the organization's internal risk assessment management program.	**Examples**: 1. Gives the highest preference to GovRAMP products. 2. Offers additional evaluation points for GovRAMP engagement (e.g. full points for GovRAMP Ready/Authorized, half points for Security Snapshot, no additional points if not GovRAMP engaged).	**Examples**: 1. Requires GovRAMP Ready or Authorized for all cloud contracts. Providers must grant visibility as a requirement of the contract. 2. Requires GovRAMP Security Snapshot at the minimum at the point of solicitation and then require they achieve Core status within 12 months of contract award.

GovRAMP

Best Practice Case Study: State of Utah

- ✓ **Go-live Date:** July 1, 2025
- ✓ **Adoption Level:** GovRAMP Required
- ✓ **Adoption Model:** The Two-Year On-Ramp Model [Learn more]

New Contracts and Solicitations

- Product must be GovRAMP or FedRAMP engaged to bid and be selected; or
- If the product does not have a FedRAMP or verified GovRAMP status, the product must:
  - Be enrolled in the GovRAMP **Progressing Snapshot Program**
  - Achieve a verified status of **Core within 12 months** of contract
  - Achieve a verified status of **Ready within 12 – 18 months** of contract
  - Achieve a verified status of **Authorized/Provisionally Authorized within 18 – 24 months** of contract

Existing Contracts Not Up for Renewal – At point of new solicitation

Effective July 1, 2027 – All solicitations with a requirement of GovRAMP or FedRAMP must hold Core, Ready, or Authorized/Provisionally Authorized status

OREGON INFORMATION TECHNOLOGY (IT) PROFILE

OPERATIONAL MODEL, CLOUD STRATEGY, CYBERSECURITY

Oregon Information Technology Profile

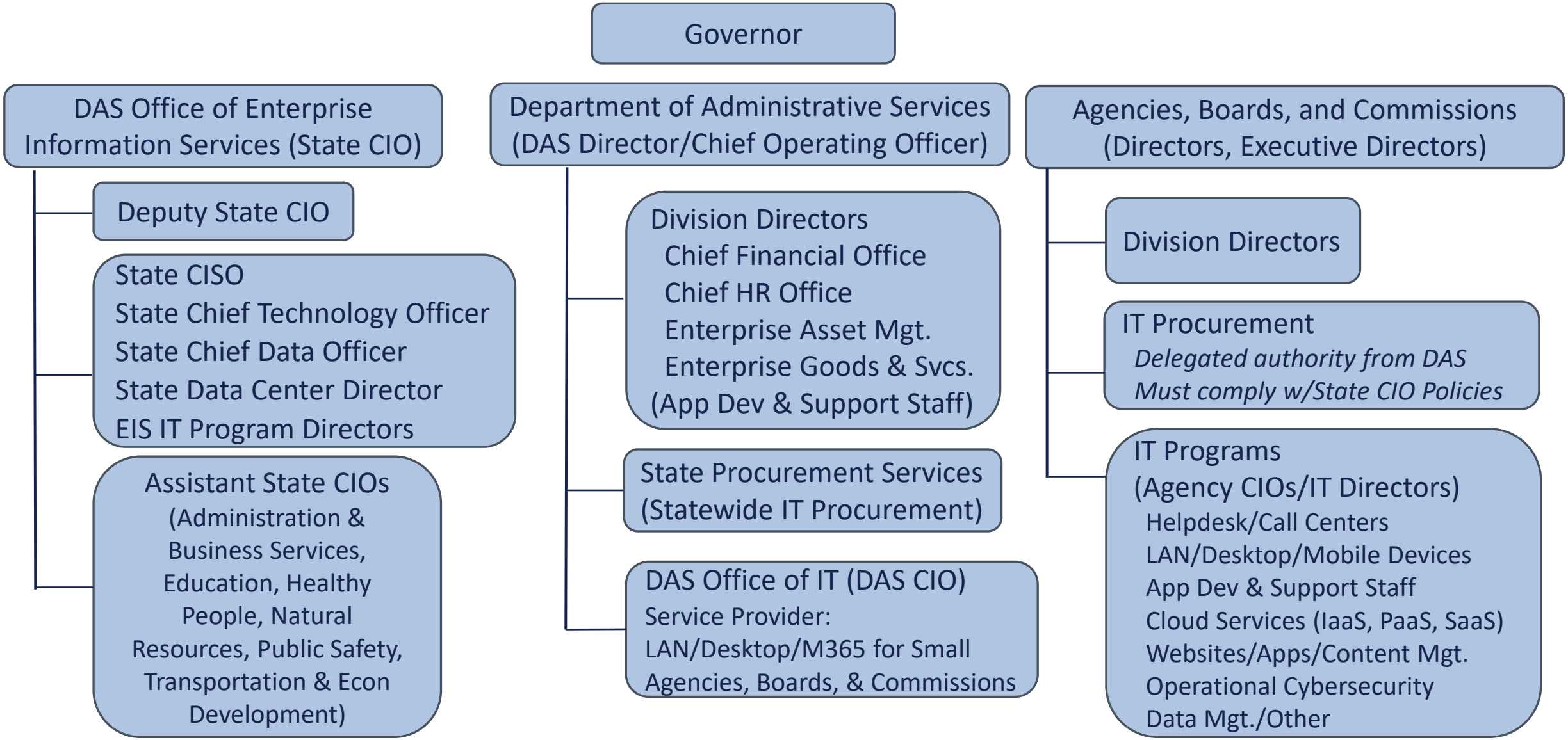
Executive Branch IT Governance/Organizational/Operating Model - Decentralized to slightly federated
State CIO Enterprise IT Services – Enterprise IT Planning, Policy/Standards, & Oversight; Enterprise IT Projects; State Network, Data Center, Cybersecurity (Unified in Exec Branch), e-Government Web Portal, Enterprise Open Data/GIS
Agency IT Services – Agency IT Planning, Policy/Standards; Agency IT projects; Application Development & Support, Local Area Network/Desktop Support, cybersecurity (in partnership with State CIO), Agency Websites, Data/GIS

IT Workforce – Executive Branch (2023-25)
* 2344 IT Classified Positions across 50 agencies
Only 254 positions under State CIO supervision (< 11%)
47680 Exec Branch Positions - IT support ratio – 1:20

Legislative Branch, Judicial Branch, & Constitutional Offices
Govern/Manage IT operations independently
Not subject to State CIO Authority
Overseen by Legislative Fiscal Office

IT Expenditures – Executive, Legislative, Judicial (2023-25)
$2.3 B USD (IT spend) vs $127.7 B USD (All Funds Biennial Budget) ~ 1.8 %
Estimate 75-80% of IT spend - Legacy Systems/Technical Debt
Limited $ available for IT innovation & modernization

Executive Branch IT Organizational Structure



Office of Enterprise Information Services
Cloud Forward Strategy

Cloud Forward

A Framework for Embracing the Cloud in Oregon – version I. 0

Vision.

Oregon will strive to conduct 75% of its business via cloud-based services and infrastructure by 2025–leveraging these platforms to modernize state IT systems and make Oregon a place where everyone has an opportunity to thrive.

Cloud Forward – Guiding Principles

- **Cloud-First.** Cloud will be the first and preferred option for all new IT investments. It should not be conflated with the idea of "cloud everything."
- **Agility Counts.** Cloud migration decisions will be driven by considerations of business agility and overall cloud value, in addition to considerations of cost, time, effort and risk.
- **Saas, please.** Software-as-a-Service (SaaS) will be the preferred cloud tier and be evaluated before other cloud tiers (i.e., PaaS or IaaS) or migration models.
- **Lift-and-Shift Last.** As a migration strategy, re-hosting or "lifting and shifting" provides little (if any) cloud value or cost savings. Re-hosting should only be considered as last resort.
- **Multicloud.** Embracing multicloud positions the state to leverage the unique value propositions and capabilities offered by leading cloud service providers.
- **Upskilling.** As a state we are committed to upskilling our existing IT workforce and preparing them for a cloud-defined future.
- **Business Enablement.** Embracing the cloud frees up IT organizations from having to manage traditional IT infrastructure and operations tasks and provides opportunities to enable their business and program units through strategic use of data, business intelligence, integrations, and agile development.

ENTERPRISE information services

CYBERSECURITY

OREGON EXECUTIVE BRANCH

Unifying Cybersecurity in Oregon's Executive Branch

Office of the Governor
State of Oregon

EXECUTIVE ORDER NO. 16-13

UNIFYING CYBER SECURITY IN OREGON

WHEREAS, information systems, networks, and critical infrastructure around the world are threatened by increasing and evermore sophisticated cyber-attacks; and

WHEREAS, the people of and businesses operating within Oregon have entrusted state government with a large repository of information that they expect will be protected and secured; and

WHEREAS, information is a strategic asset of the state of Oregon that should be managed and secured as a valuable state resource; and

WHEREAS, the continuous and efficient operation of state government information systems is both vital and necessary to the mission of providing government services in Oregon; and

WHEREAS, vulnerabilities of the state's information systems underscore the need to enhance the security of Oregon information systems, networks, and critical infrastructure; and

WHEREAS, aging information technology infrastructure and antiquated legacy information systems in use by state agencies remain vulnerable to cyberattack, placing private information about state employees and their dependents, consumers of state services, taxpayers, and the residents and businesses of Oregon at risk; and

WHEREAS, responsibility and accountability for the security of state information systems is currently dispersed and decentralized with the exception of the enterprise information resources, technology, and telecommunications infrastructure managed and overseen by the State Chief Information Officer.

WHEREAS, ORS 182.122 imposes on state agencies the responsibility to secure their information systems or implement information security plans, policies, standards, and procedures established by the State Chief Information Officer; and

WHEREAS, unification of the state's cyber security functions under the leadership of the State Chief Information Officer is necessary to protect the availability, integrity, and confidentiality of state information systems and the information stored in state information systems pursuant to ORS 182.122;

Enrolled

Senate Bill 90

Printed pursuant to Senate Interim Rule 213.28 by order of the President of the Senate in conformance with presession filing rules, indicating neither advocacy nor opposition on the part of the President (at the request of Governor Kate Brown for Oregon Department of Administrative Services)

CHAPTER .....

AN ACT

Relating to information technology security; creating new provisions; amending ORS 291.041; and declaring an emergency.

Be It Enacted by the People of the State of Oregon:

SECTION 1. Unification of agency information technology security functions. (1) As used in this section:

(a) "Executive department" has the meaning given that term in ORS 174.112, except that "executive department" does not include:

(A) The Secretary of State.

(B) The State Treasurer.

(C) The Attorney General.

(D) The Oregon State Lottery.

(E) Public universities listed in ORS 352.002.

(b) "State agency" means an agency, as defined in ORS 183.310, in the executive department.

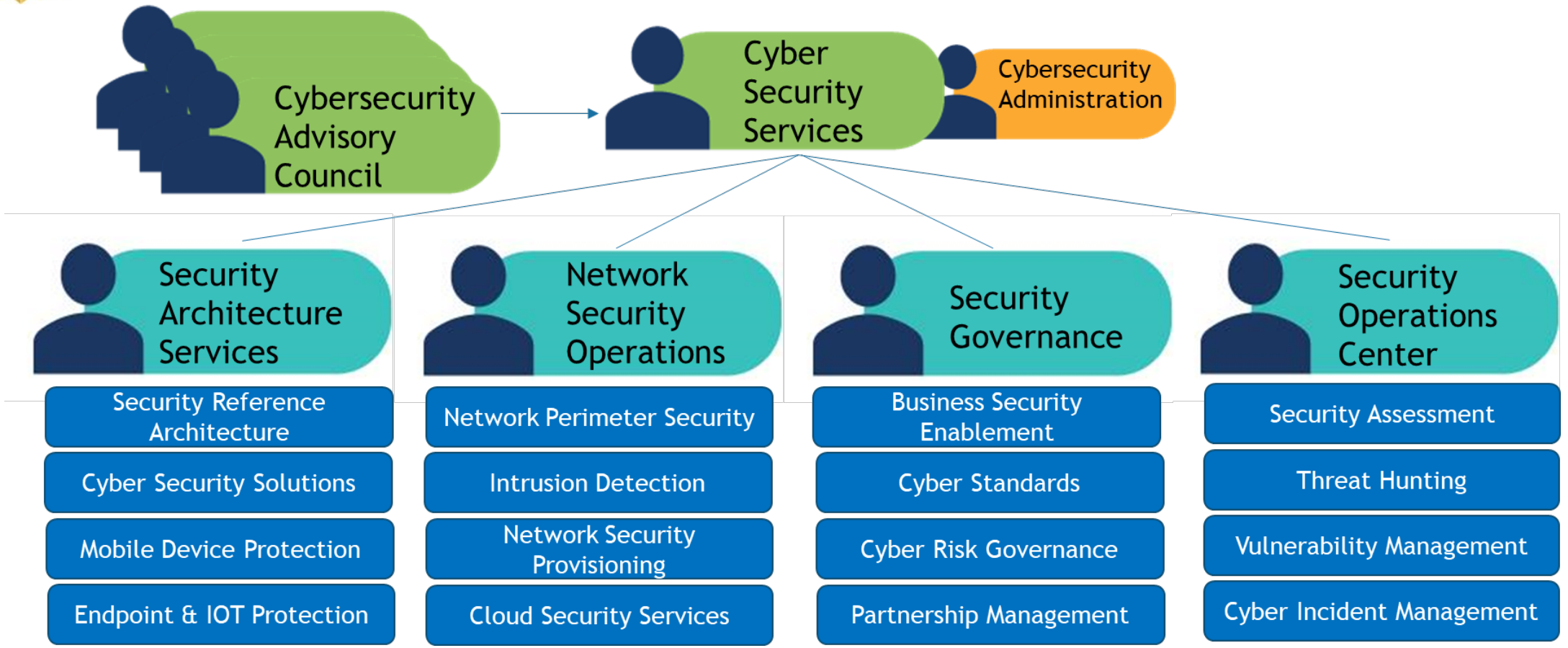
(2) All state agencies shall carry out the actions necessary to unify agency information technology security functions across the executive department.

(3) The State Chief Information Officer, or a designee of the State Chief Information Officer, and state agencies shall work cooperatively to develop a plan to transfer agency information technology security functions, employees, records and property to the office of the State Chief Information Officer no later than January 1, 2018.

(4) The unexpended balances of amounts that a state agency is authorized to expend during the biennium beginning July 1, 2017, from revenues dedicated, continuously appropriated, appropriated or otherwise made available for the purpose of administering and enforcing the duties, functions and powers transferred by this section shall remain with the state agency.

(5) In accordance with the plan developed under this section, the director of each state agency shall deliver to the State Chief Information Officer or a designee of the State Chief Information Officer all records and property related to the performance of the agency information technology security functions transferred to the State Chief Information Officer under this section. The property may include contracts pertaining to the functions trans-

Office of Enterprise Information Services
State Cyber Security Services (CSS)



Cyber Security Services Organization

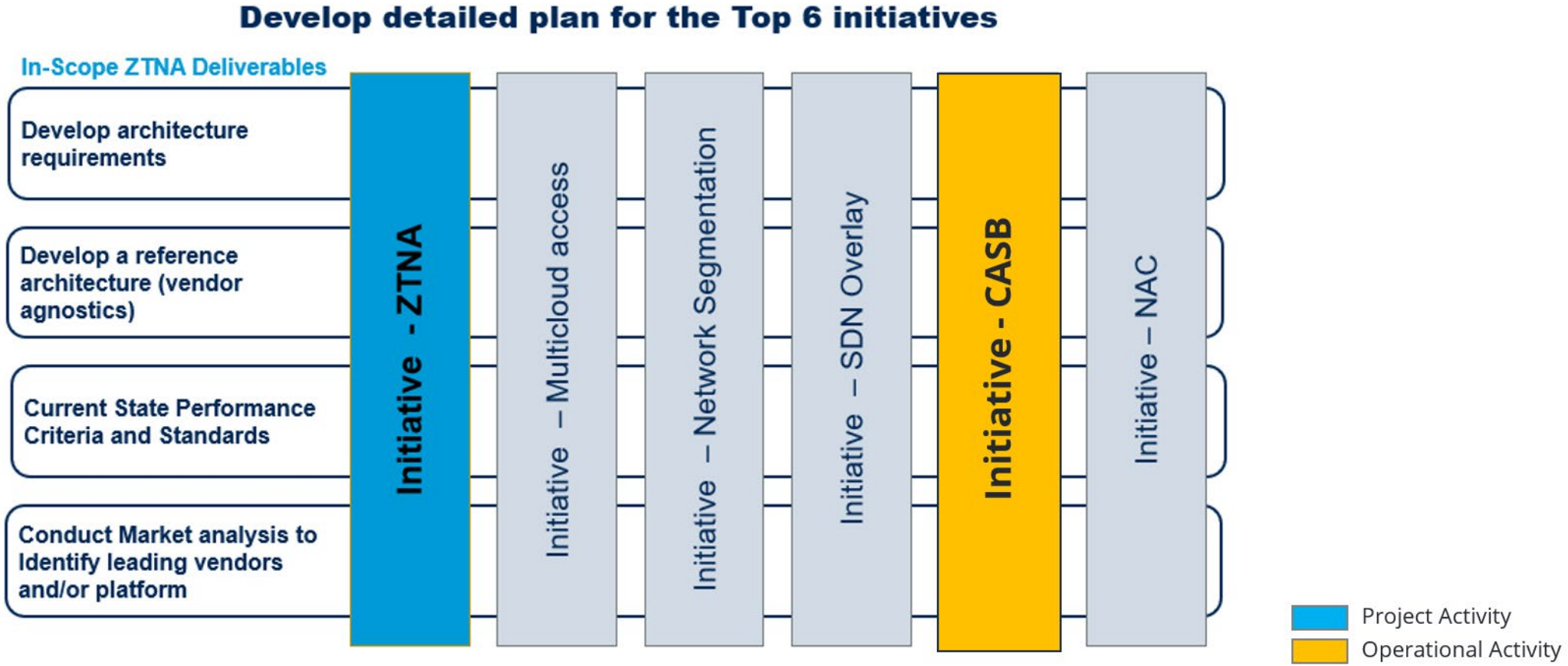
Full Cybersecurity suite of services

Office of Enterprise Information Services
State Cyber Security Services (CSS)

Cybersecurity Operational Initiatives

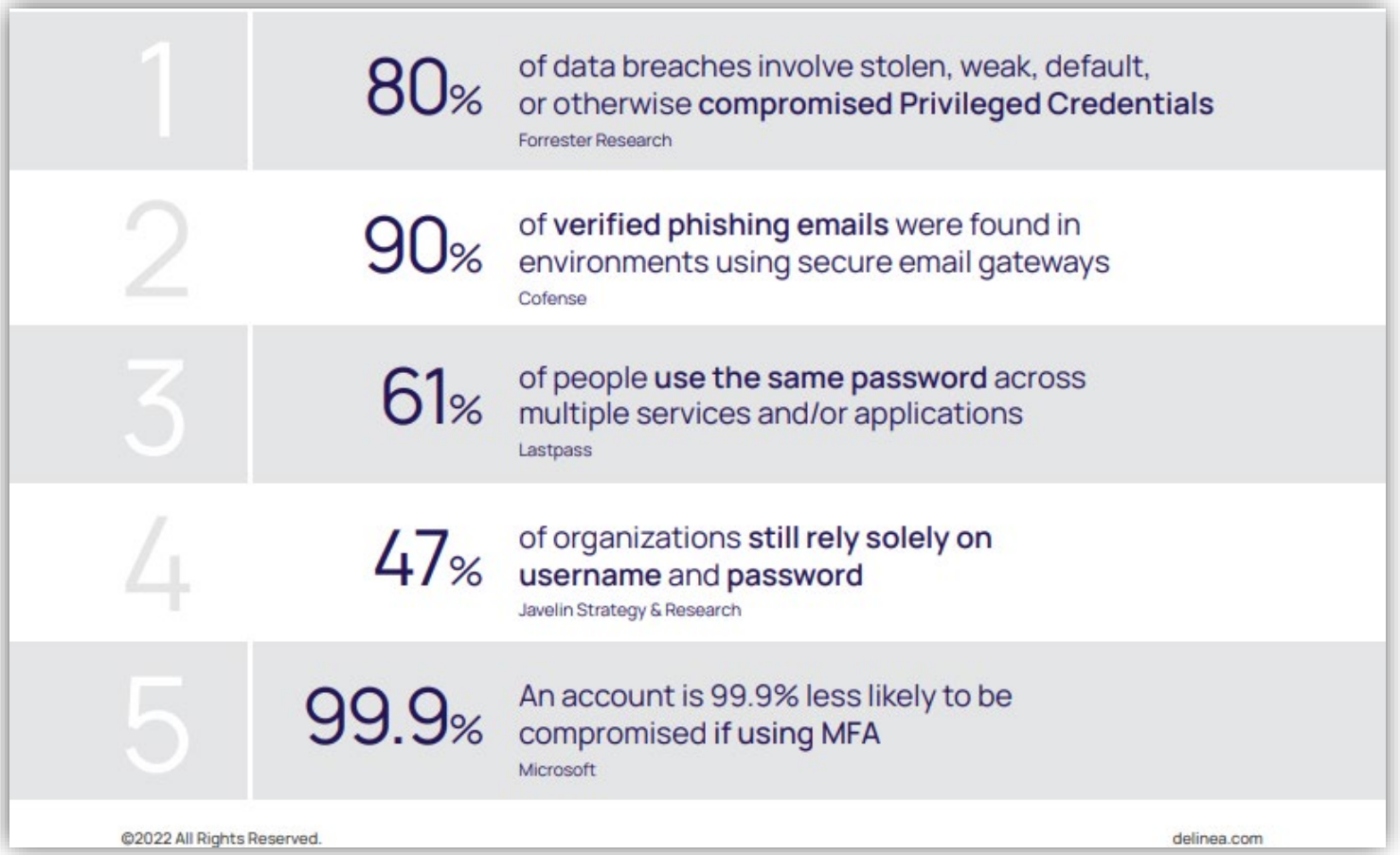
Office of Enterprise Information Services
State Cyber Security Services (CSS)

CSS Initiatives in Flight:



Office of Enterprise Information Services
State Cyber Security Services (CSS)

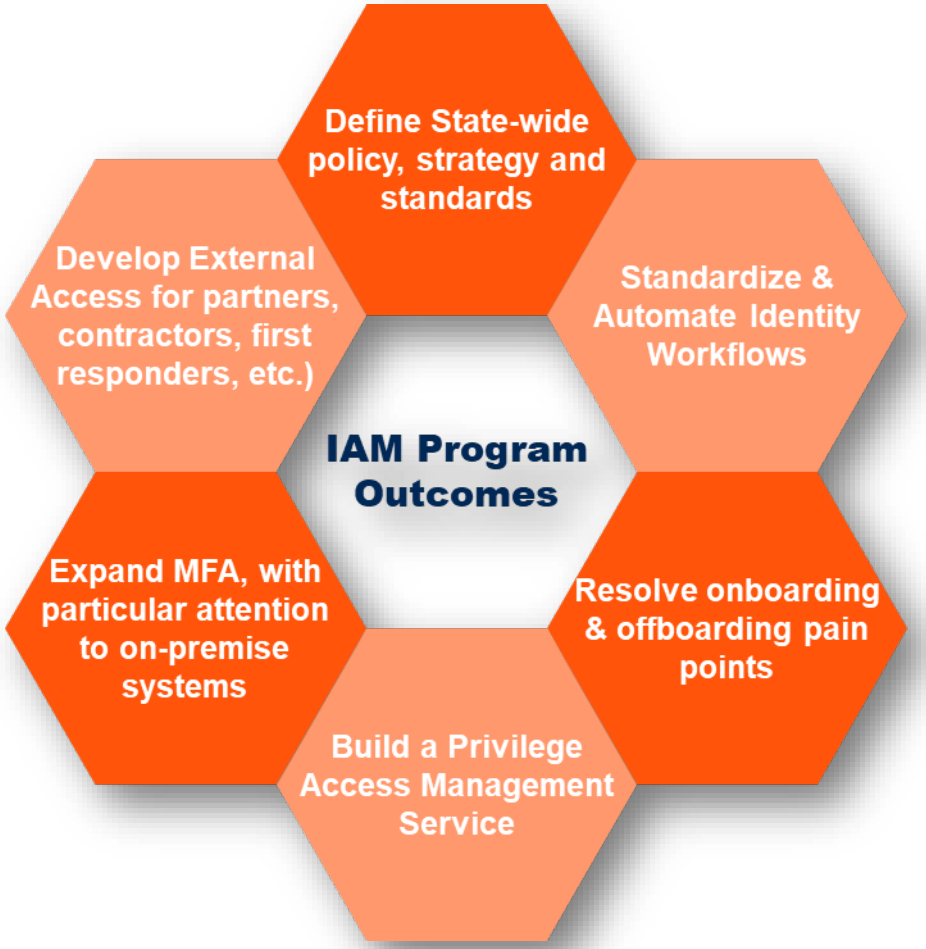
Why discuss
Zero Trust



Office of Enterprise Information Services (EIS) State Cyber Security Services (CSS)

EIS IAM/IGA – Strategy

EIS, and agency stakeholders have identified initial key program outcomes for a whole-of-state Identity Program that focuses on implementing an identity governance approach with complimentary identity management technologies to support agency identities, including State-employees, vendors/contractors, first-responders, retirees, commission members.

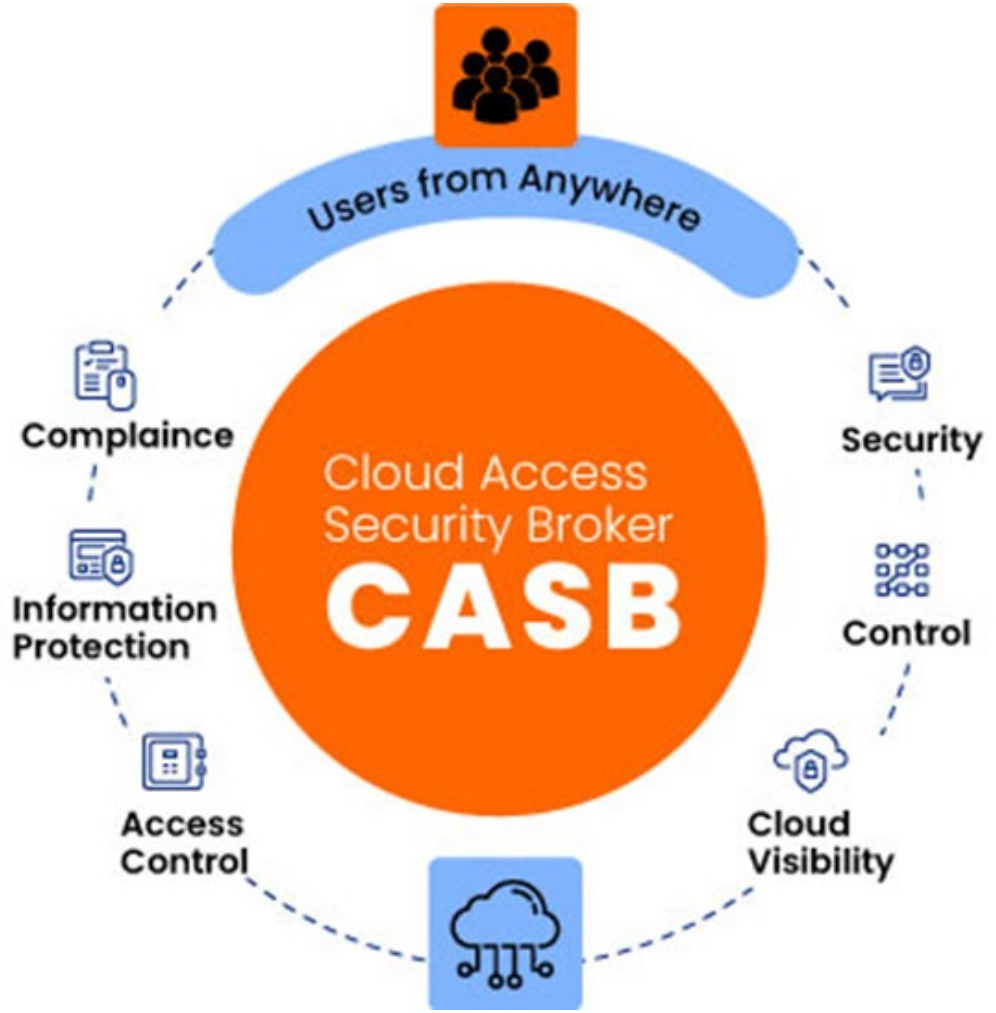


Enterprise Identity and Access Management/Identity Governance Approach Planning

Office of Enterprise Information Services
State Cyber Security Services (CSS)

CASB Overview:

MS CASB Planned Implementation Overview



Office of Enterprise Information Services
State Cyber Security Services (CSS)

Human Risk Management Improvements

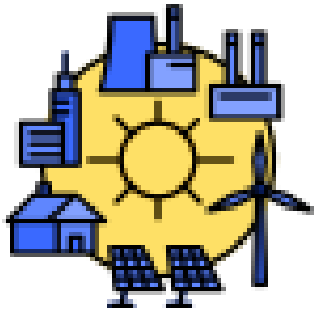
Security Awareness

AI Security Awareness

Cloud Security Awareness

Mobile Security Awareness

DevOps Security Awareness



IOT Security Awareness

Spear, Whale, Smishing, Vishing, Angler

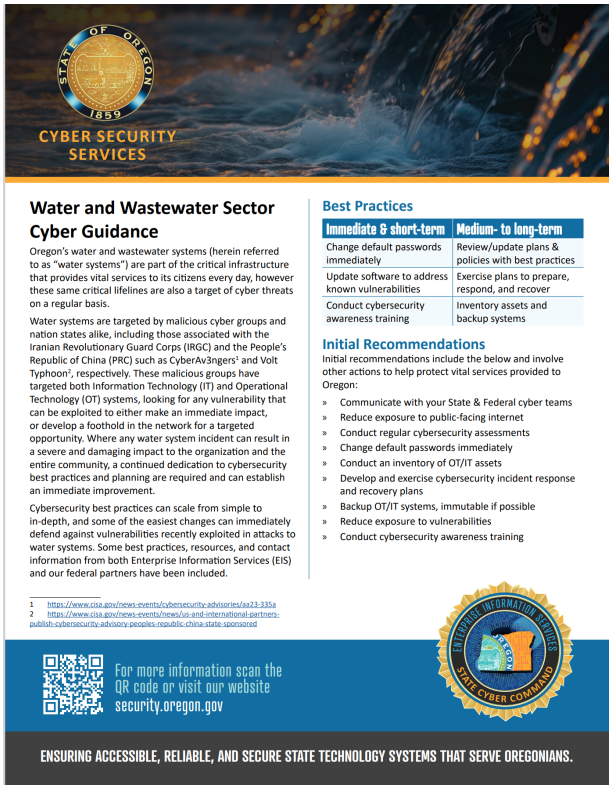
41%
41% of attacks used phishing

26%
26% of attacks exploited public-facing apps

16%
16% of attacks abused valid accounts

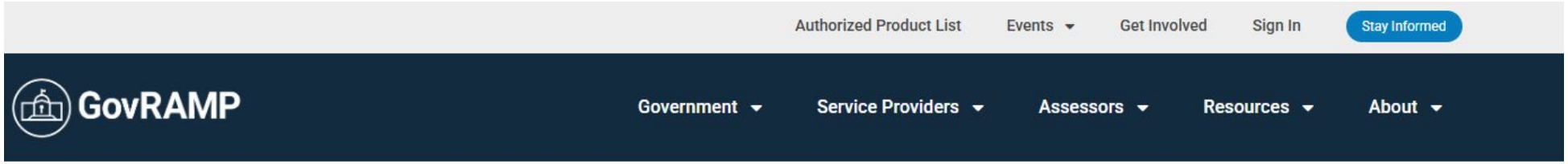
Multi Discipline Quarterly Training

Office of Enterprise Information Services
State Cyber Security Services (CSS)



Cybersecurity Awareness Campaign

State of Oregon and GovRAMP (formerly StateRAMP)



State of Oregon
GovRAMP Program Page

Learn more about the partnership between the State of Oregon and GovRAMP and how it benefits you.

https://programs.govramp.org/oregon-and-stateramp/

State of Oregon and GovRAMP (formerly StateRAMP)

State of Oregon Enterprise Information Services – Cyber Security Services

Cyber Security Services (CSS) brings together enterprise security capabilities into a single organization.

Visit Website

State of Oregon Procurement Services

State of Oregon website for state agencies, local government entities, and suppliers meet to buy and sell products and services for the benefit of Oregonians.

Visit Website

GovRAMP Overview

Click the link below to view a general overview about GovRAMP.

Watch Video

GovRAMP Authorized Product List

Verified and Progressing Products are listed on the Authorized Product List and updated daily.

View List

https://programs.govramp.org/oregon-and-stateramp/

OREGON CLOUD SECURITY POLICIES

OREGON OFFICE OF ENTERPRISE INFORMATION SERVICES (STATE CIO)

EIS – Cybersecurity Services – Cloud Security – Cloud Guardrails Implementation Guide December 2024

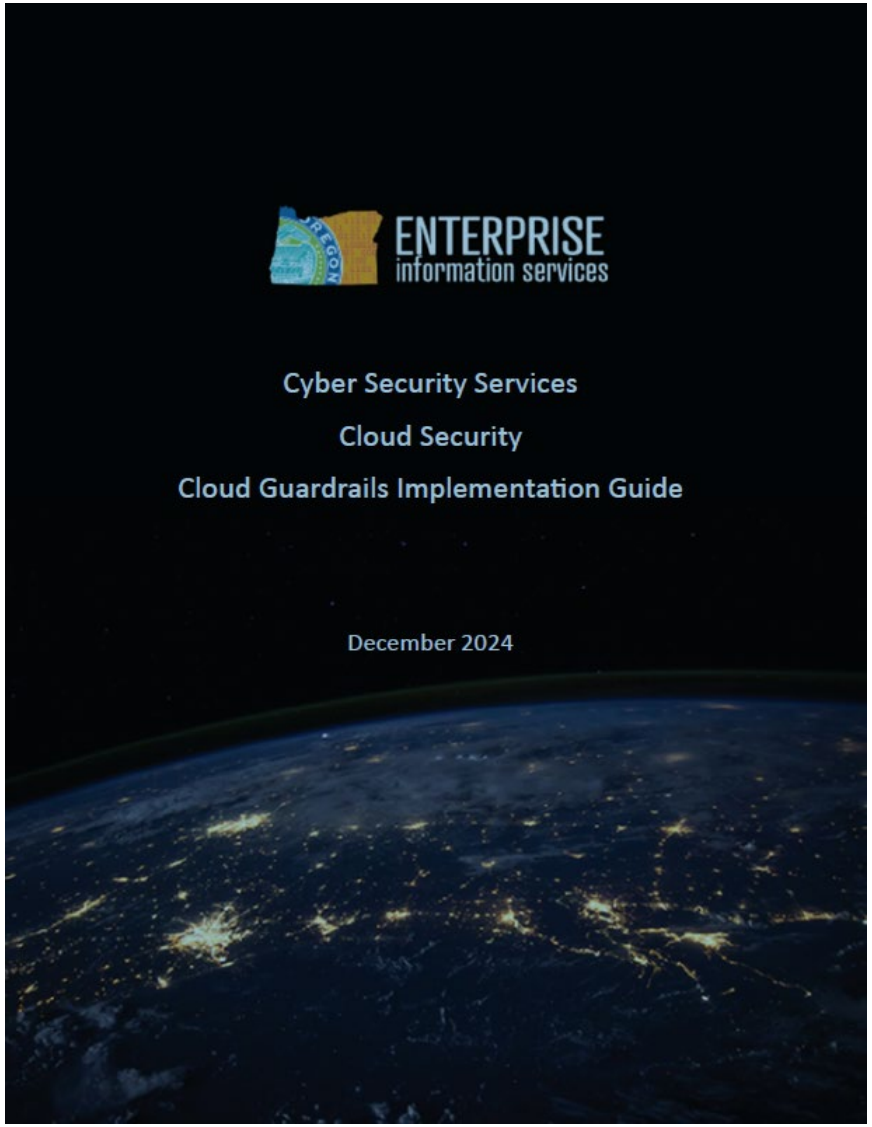


Table of Contents

Change History 2
Attribution 2
Mission Statement 4
Introduction 4
Background 4
Objectives 5
Assumptions 6
Project Risks to Success 6
Resource Requirements 6
Team Composition 6
Roles and Responsibilities 7
Sub-Efforts 8
Timeline 9
Success Criteria 9
Appendix 10
CIS Foundations Benchmarks Control Families for Security Guardrails 10
Identified Gaps 10
Team Members 12

State of Oregon Cloud and Hosted Systems Policy and Procedure

OSCIO statewide policy

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

NUMBER	SUPERSEDES
107-004-150	107-004-150 | 7/18/2016

STATEWIDE POLICY

EFFECTIVE DATE	DATE OF LAST REVIEW
5/1/2019	5/25/2019

DIVISION	REFERENCE/AUTHORITY
Office of the State Chief Information Officer	ORS 276A.206 Cloud and Hosted Systems Procedure: 107-004-150_PR.

POLICY OWNER
Enterprise IT Governance

SUBJECT	APPROVED SIGNATURE
Cloud and Hosted Systems	**Terrence Woods, State Chief Information Officer** ***(Signature on file with DAS Business Services)***

PURPOSE
This policy establishes standards to ensure that state agencies:

- Appropriately analyze and document the benefits, costs, and risks to the state before contracting for a Cloud or Hosted Service.
- Assess the readiness of a Cloud or Hosted Service Provider to deliver a solution that meets the state's requirements.
- Conduct planning to ensure that state information and financial assets are appropriately protected when adopting a Cloud or Hosted Service.

APPLICABILITY
This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division, or office within the Oregon Executive Branch. The following agencies and boards are excluded:

- Secretary of State.
- State Treasurer.
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice.
- Oregon State Lottery.
- State Board of Higher Education or any public university listed in ORS 352.002.

FORM(S), EXHIBIT(S) & INSTRUCTIONS
These governing statutes, policies and rules must be reviewed prior to contracting for a Cloud or Hosted Service:

- Information Technology Investment Oversight Policy: 107-004-130.
- Information Security Policy: 107-004-052.
- Information Security Incident Response Policy: 107-004-120.
- Information Asset Classification Policy: 107-004-050.
- Cloud and Hosted Systems Procedure: 107-004-150_PR.
- ORS 291.047; 192.005; 192.311 to 192.478; and 279A.157.

https://www.oregon.gov/das/policies/107-004-150.pdf

OSCIO statewide procedure

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

NUMBER	SUPERSEDES
107-004-150_PR	107-004-150_PR | 7/18/2016

STATEWIDE PROCEDURE

EFFECTIVE DATE	DATE OF LAST REVIEW
5/1/2019	5/1/2019

DIVISION	REFERENCE/AUTHORITY
Office of the State Chief Information Officer	ORS 276A.206 Cloud and Hosted Systems Policy: 107-004-150

POLICY OWNER
Enterprise IT Governance

SUBJECT	APPROVED SIGNATURE
Cloud and Hosted Systems	**Terrence Woods, State Chief Information Officer** ***(Signature on file with DAS Business Services)***

PURPOSE
This cloud computing procedure describes how agencies must show that they have exercised due diligence in the consideration and acquisition of cloud technology and services.

APPLICABILITY
This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division, or office within the Oregon Executive Branch. The following agencies and boards are excluded:

- Secretary of State.
- State Treasurer.
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice.
- Oregon State Lottery.
- State Board of Higher Education or any public university listed in ORS 352.002.

FORM(S), EXHIBIT(S) & INSTRUCTIONS

- Cloud and Hosted Systems Policy: 107-004-150.
- Information Technology Investment Oversight Policy: 107-004-130.
- Cloud and Hosted Systems Workbook Guide, Exhibit A to Policy: 107-004-150.
- Cloud and Hosted Systems Workbook (form)

DEFINITIONS
Refer to the Cloud Computing Policy: 107-004-150.

https://www.oregon.gov/das/policies/107-004-150_PR.pdf

State of Oregon Cloud and Hosted Systems Workbook Guide and Form

OREGON | Office of the State
Chief Information Officer

Cloud and Hosted Systems Workbook Guide
Exhibit A

Version 2.0
Date: 25 APRIL 2019
For the latest version, visit:
https://www.oregon.gov/das/OSCIO/Pages/OSCIO-templates-and-forms.aspx

For additional information, please contact:
Your Senior IT Portfolio Manager, or
ITinvestment.Review@oregon.gov

Enterprise IT Governance office

Table of Contents

Introduction 2
How to use this guide 2
General Information 3
Work Reduction and Reusability 4
OSCIO-approved boilerplate language 4
Re-use of completed workbooks 4
Fast-Lane Renewals 4
First-time review of existing contracts 4
Question-by-question guidance 5
***Guidance on* Section A: Risk FACTORS Determination** 6
***Guidance on* Section B Sub-Section 1: Requirements** 12
***Guidance on* Section B Sub-Section 2: Contract and related planning** 16
***Guidance on* Section C: (Renewal/Reuse)** 20
Document revision history 22

Exhibit A: https://www.oregon.gov/das/policies/107-004-150.pdf

State of Oregon Cloud and Hosted Systems Workbook Guide and Form

SECTION A: RISK FACTORS DETERMINATION

Always required except for renewals of Service Contracts & cloud workbooks previously approved by OSCIO.

Agency/division: [Enter agency name and division]

IT Service/Product name: [Enter service or product name]

Agency contact name, email address, and phone number:

[First name] [Last name]

[Email address] [Phone number]

ESO contact name, email address, and phone number:

[First name] [Last name]

[Email address] [Phone number]

A1: What is the main function of the proposed Cloud or Hosted Service and how will it be used to support one or more business functions? Briefly describe and include the number of records anticipated and how that number is anticipated to grow over time; the number of users; and the anticipated cost. A completed IT Investment form with the same information may be attached instead, if available.

[Click here to enter text.]

A2: What data classification level information will the Service store, process, or transmit? Check all that apply. Consult DAS Policy 107-004-050 "Information Asset Classification" for definitions.

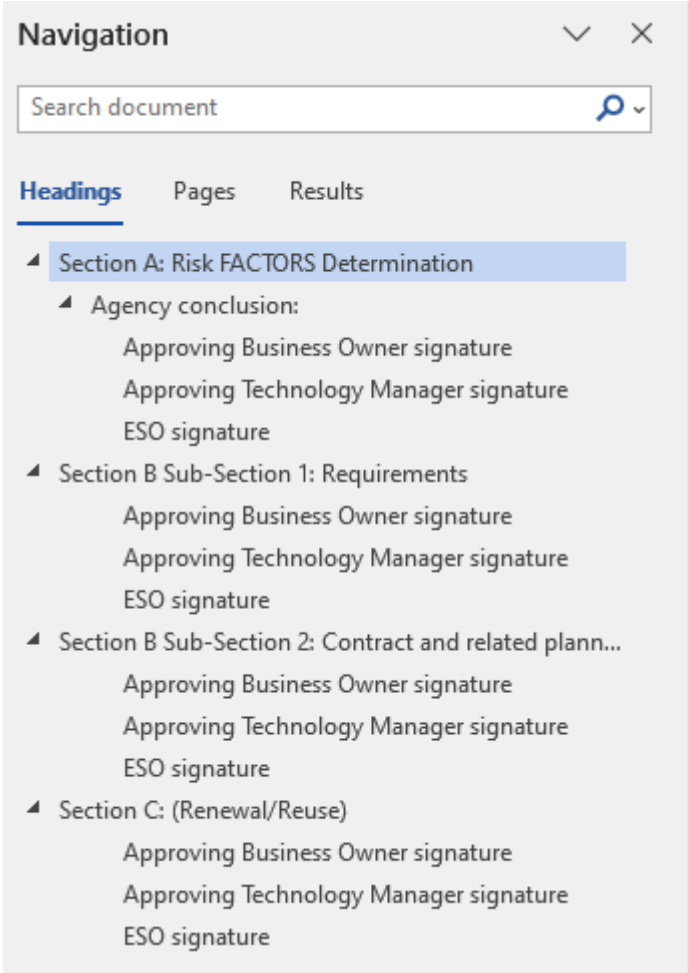
- ☐ Level 1
- ☐ Level 2
- ☐ Level 3 -> **significant risk; also complete Section B if checked**
- ☐ Level 4 -> **significant risk; also complete Section B if checked**

A3: Will the proposed Service store, process, or transmit data that must be protected according to the following specialized rules or standards? Check all that apply.

If any items below are checked, the investment has significant risk; also complete Section B.

- ☐ HIPAA (Protected Health Information)
- ☐ CJIS (Criminal Justice Information)
- ☐ IRS Publication 1075 (Federal Tax Information)
- ☐ FERPA (certain education records)
- ☐ PCI (payment card data)
- ☐ SSA (Social Security Administration)
- ☐ Other, please identify the rule or standard:
- ☐ FISMA (Federal Information Security Modernization Act)
- ☐ MARS-E (Minimum Acceptable Risk Standards for Exchanges)
- ☐ OCITPA (Oregon Consumer Identity Theft Protection Act)
- ☐ No checkboxes apply

[Click here to enter text.]



https://www.oregon.gov/das/Policies/107-004-150_PR_Attachment.docx

Executive Branch: Updated Interim Generative AI Access and Usage Guidance

AI Access and Usage Guidance

Oregon
Tina Kotek, Governor

Enterprise Information Services
State Chief Information Officer
550 Airport Road SE, Suite C
Salem, OR 97301
503-378-3175

MEMORANDUM

To: Agency IT Leadership

From: Terrence Woods, State CIO

Date: April 15, 2025

Subject: Updated Interim Generative AI Access and Usage Guidance

Purpose
Outline requirements for Oregon state agency users accessing Generative AI (GenAI) tools, including Microsoft Copilot and AI embedded in software applications. Users must follow the guidance to ensure that such tools are used while safeguarding data in accordance with existing policies on data classification and security.

Scope
This guidance applies to all Executive Branch agencies, boards and commissions under the purview of the State Chief Information Officer, as defined in ORS 276A.230. The use of Microsoft Copilot and similar GenAI tools shall be restricted to Level 1 ("Published") and Level 2 ("Limited") data only, as classified in the Information Asset Classification Policy (107-004-050).

Principles
Agencies are to review and act in accordance with the Oregon's Artificial Intelligence Guiding Principles as captured in the Final Recommended Action Plan.

Use Case Recommendations
- Generative AI is permissible for tasks such as drafting documents, summarizing information, and generating creative content.
- For public meetings, users should not use AI-powered translation or transcription services, including those offered by Microsoft Copilot, or Teams Premium for translating speech in real-time, as federal and Oregon laws mandate equal access to government information regardless of language. For public meetings requiring language translation, agencies should continue to use qualified human interpreters to ensure accuracy and compliance with legal requirements.

Mission: Mature enterprise technology governance, optimize investments, ensure transparency, provide oversight, and deliver secure and innovative solutions.

Data Governance Policy

ENTERPRISE information services
DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

STATEWIDE POLICY	**NUMBER** 107-004-160	**SUPERSEDES** New
	EFFECTIVE DATE February 9, 2022	**PAGE NUMBER** Pages 1 of 6
	DATE OF LAST REVIEW February 9, 2022	
Division Enterprise Information Services	**REFERENCE** • ORS 162.305, 192.660, 219.110, 276A.206, 276A.300, 291.037 • OAR 125-800-0005, 125-800-0020	
Policy Owner Data Governance and Transparency		
SUBJECT Data Governance	**APPROVED SIGNATURE** Terrence Woods, State Chief Information Officer (Signature on file with DAS Business Services)	

PURPOSE

Data and information are strategic assets of the state and must be actively governed in order to preserve and enhance their value. This policy sets forth a statewide approach to data governance and establishes a baseline framework and accountability structure for agencies to use in establishing internal data governance programs.

APPLICABILITY

This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division or office within the Oregon Executive Branch. The following agencies and boards are excluded:

- Secretary of State.
- State Treasurer.
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice.
- Oregon State Lottery.
- State Board of Higher Education or any public university listed in ORS 352.002.

https://www.oregon.gov/das/Policies/107-004-160.pdf

Information Asset Classification Policy

ENTERPRISE information services
DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

STATEWIDE POLICY	**NUMBER** 107-004-050	**SUPERSEDES** Policy #107-004-050| January 1, 2008
	EFFECTIVE DATE 7/12/2023	**PAGE NUMBER** Pages 1 of 4
	REVIEWED DATE 7/12/2023	
Division Enterprise Information Services (State CIO)	**REFERENCE** ORS 162.305, 192.660, 276A.200, 276A.206, 276A.300, 291.110	
Policy Owner Data Governance and Transparency	OAR 125-800-0005, 125-800-0020	
SUBJECT Information Asset Classification Policy	**APPROVED SIGNATURE** Terrence Woods, State Chief Information Officer (Signature on file with Strategic Initiatives and Enterprise Accountability Office)	

PURPOSE

This policy defines Oregon state government's approach to identifying, classifying, and protecting state data and information assets throughout their lifecycles. Information, like other assets, must be properly managed from its creation to disposal. For the purpose of this policy, data is incorporated into the definition of "information."

APPLICABILITY

This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division, or office within the Oregon Executive Branch. The following agencies and boards are excluded:

- Secretary of State
- State Treasurer
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice
- Oregon State Lottery
- State Board of Higher Education or any public university listed in ORS 352.002

https://www.oregon.gov/das/Policies/107-004-050.pdf

Questions?

Legislative Fiscal Office

900 Court Street NE, Room H-178, Salem, Oregon 97301

Oregon State Capitol | (503) 986-1828 | www.oregonlegislature.gov/lfo

Contact Information

Sean McSpaden, Principal Legislative IT Analyst

Oregon Legislative Fiscal Office

Committee Administrator:

- Joint Legislative Committee on Information Management and Technology
- Transparency Oregon Advisory Commission

Email: Sean.L.McSpaden@oregonlegislature.gov | Phone: 503-986-1835