

Securing the Mission: Cybersecurity and Compliance For 2025

Chris Green

Manager of Penetration Testing

Chris Green

Manager of Penetration Testing

CISSP, CISA, CRISC, QSA/PCIP, OSCP, CMMC RP

- **12 years in Information Security**
- **Compliance Assessments**
- **Policy & Security Program Development**
- **Penetration Testing**

Structured Practices

Governance, Risk, & Compliance



Cybersecurity



Cloud Services



Data Center Solutions



Networking



Unified Communications & Collaboration



Secure Managed Services

Agenda

- 1 2025: What a Busy Year**
- 2 Federal Government Requirements**
- 3 State & Other Requirements**
- 4 Putting it all Together**

An aerial photograph of a city skyline, likely San Francisco, featuring the Transamerica Pyramid and other skyscrapers. The city is situated along a body of water, with bridges visible in the foreground. The image is overlaid with a semi-transparent blue rectangle containing text.

1

2025: What a Busy Year

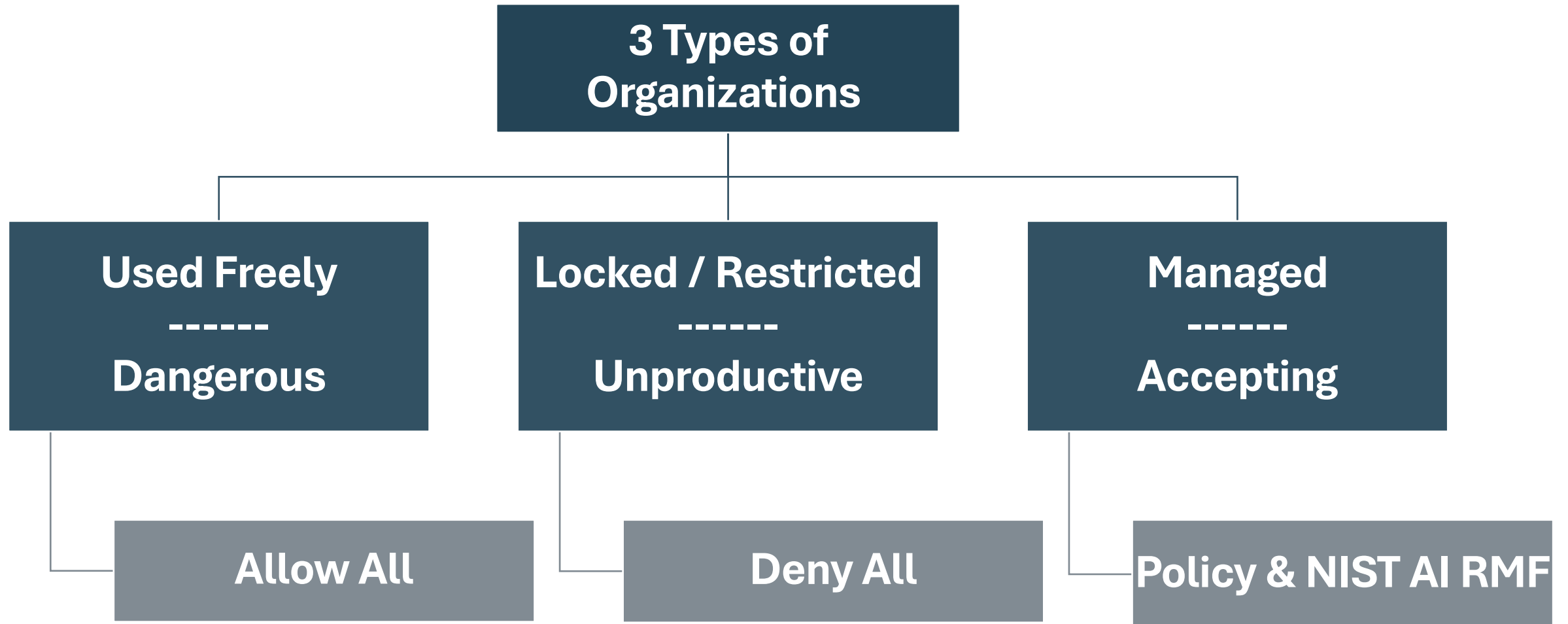
Change begets change



Uses in Cybersecurity

- Policy and procedure creation
- Content generation
- Threat detection
- Threat response
- Agents
- Risk prioritization
- Characteristic recognition

AI Governance – Or Lackthereof



AI Deployment & Assessment



National Institute of Standards and Technology (NIST)

AI Risk Management Framework (RMF) – NIST AI 100-1

- NIST AI RMF Playbook
- NIST AI 600-1
 - Generative AI Profile

Threats to AI for Risk Assessment

MITRE ATLAS

- MITRE ATT&CK for AI
- Adversarial Threat Landscape for AI Systems
- Threats to and from generative AI
- Case studies



Threats to AI for Risk Assessment

MIT AI Risk Repository: 1600+ Risks

7 Domain Classifications

1. Discrimination & Toxicity
2. Privacy & Security
3. Misinformation
4. Malicious Actors & Misuse
5. Human/Computer Interaction
6. Socioeconomic & Environmental Harms
7. AI System Safety, Failures, & Limitations

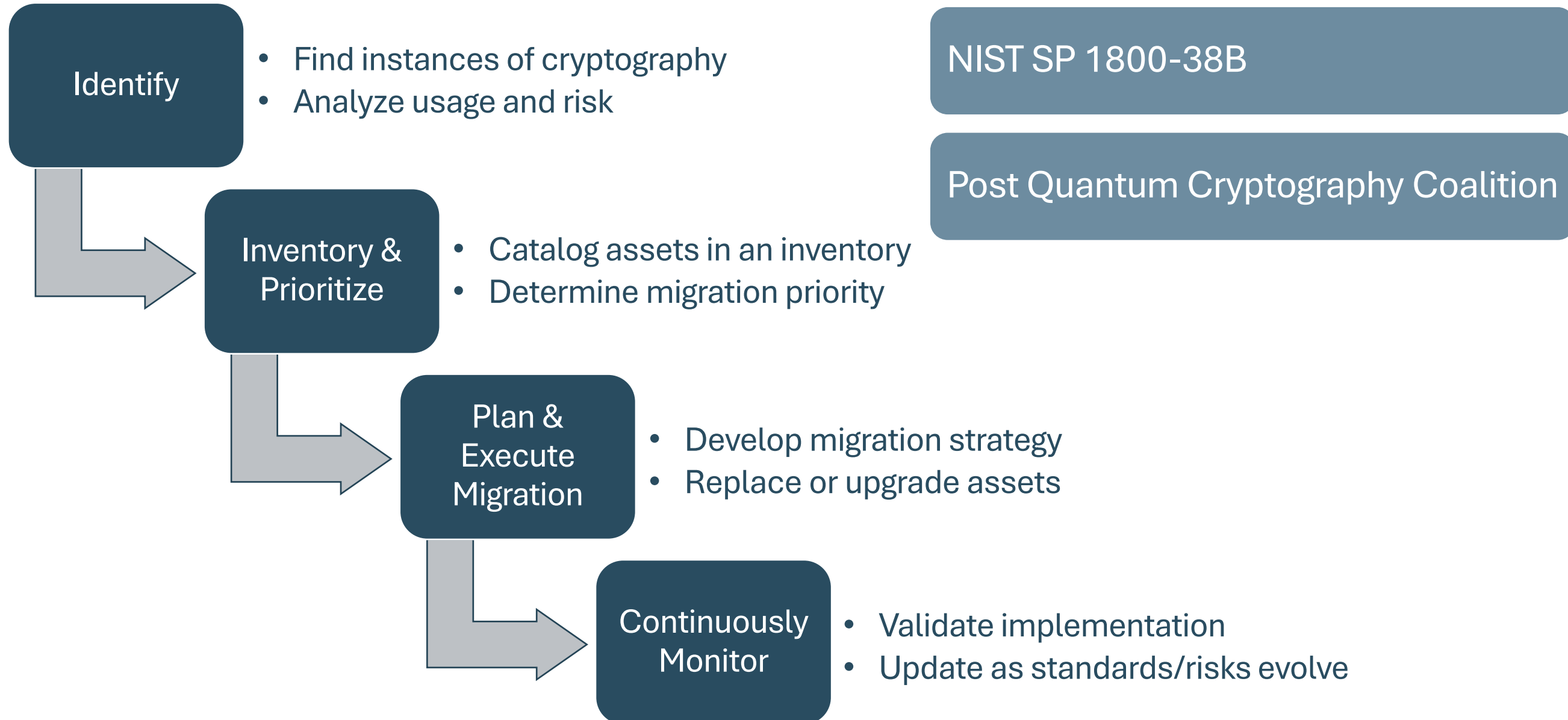


Post Quantum Cryptography (PQC)



- Quantum Computing
 - Could be here in 2 to 4 years
- Impact
 - Can break encrypted data
- PKI
 - Asymmetrical Algorithms
 - Key Exchange

Post Quantum Cryptography





2

Federal Requirements

Frameworks and regulations

Current Security Policy Versions

- 5.9.5 released 9 July 2024
 - ***Effective 1 Oct 2024***
- 6.0 released 27 Dec 2024
 - ***Effective 1 Oct 2025***
- Priority Driven
 - P1 – Immediate implementation
 - P2-4 – Phased, 30 Sept 2027
- ***“CJISSECPOL applies to all entities with access to, or that operate systems which are used to process, store, or transmit CJI.”***



CJIS Security Policy v6.0 Priority 1



Control Name	Control ID	Control Name	Control ID
Account Management	AC-2	Least Functionality	CM-7
Access Enforcement	AC-3	System Component Inventory	CM-8
Information Flow Enforcement	AC-4	Identification and Authentication (Org. Users)	IA-2
Separation of Duties	AC-5	Authenticator Management	IA-5
Least Privilege	AC-6	Vulnerability Monitoring and Scanning	RA-5
Remote Access	AC-17	Boundary Protection	SC-7
Use of External Systems	AC-20	Flaw Remediation	SI-2
Continuous Monitoring	CA-7	Malicious Code Protection	SI-3
Baseline Configuration	CM-2	System Monitoring	SI-4
Access Restrictions for Change	CM-5	Software, Firmware, and Information Integrity	SI-7
Configuration Settings	CM-6	Information Input Validation	SI-10

Access Control & ID Management

- Enforce RBAC
- Require MFA for remote logins
- Restrict external systems/media
- Disable inactive accounts

Configuration & Asset Management

- Apply secure baselines
- Remove unnecessary software
- Restrict change privileges
- Maintain device inventory

CJIS - Criminal Justice Information Services

Monitoring & Vulnerability Management

- Monitor logs/network activity
- Conduct vulnerability scans/tests
- Remediate vulnerabilities quickly
- Block malicious code

System Integrity & Data Protection

- Enforce network segmentation
- Validate all inputs
- Protect firmware/software integrity
- Secure CJI in storage/transit

Health Insurance Portability and Accountability Act



U.S. Department of
Health and Human Services

Enhancing the health and well-being of all Americans

Who Must Comply?

- Covered Entities
 - Healthcare Providers
 - Health Plans
 - Clearing Houses
- Business Associates
 - Vendors & Subcontractors

HIPAA Omnibus Rule (2013)

- Business associates directly liable
- Broader breach notification
 - Subcontractor liability

Security Rule Revisions

- Proposed by HHS OCR in 2021
- Expect final in 2025/2026

Security Rule Control Areas

Increased Oversight of Business Associates

- Annual written validation
- 24 Hour notification of incidents

Annual Audits

- Security Rule standards

Workforce Security and Remote Access

- RBAC
- 1-hour cutoff for termination

Endpoint Security

- Workstation to include mobile devices

Security Rule Control Areas

Mandatory Implementation of All Controls

- Required unless exempt

Formal IR & Contingency Planning

- Document plans, 72-hour restoration

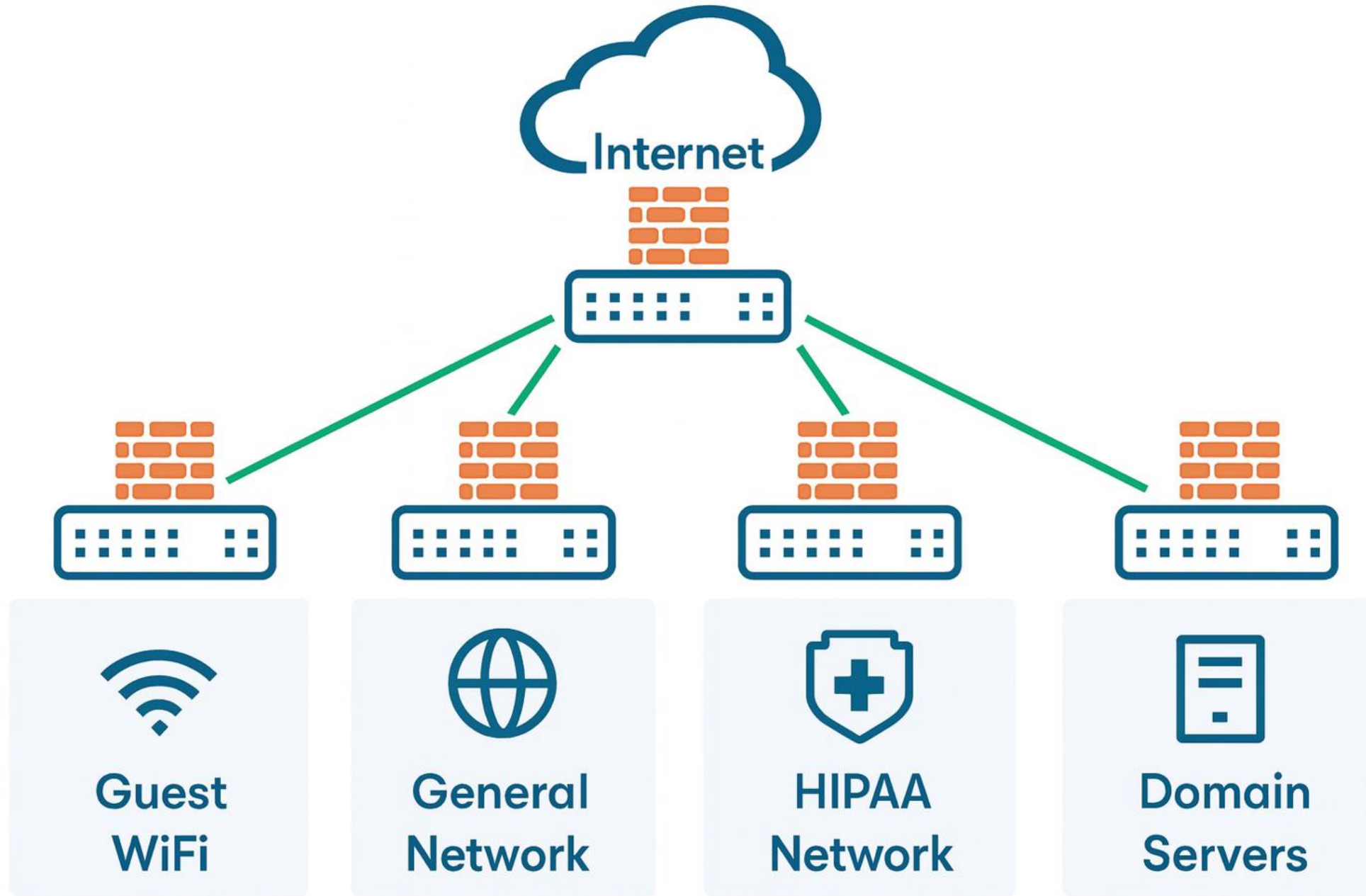
Enhanced Risk Assessment

- Inventory, threats, CIA of ePHI
- Policies

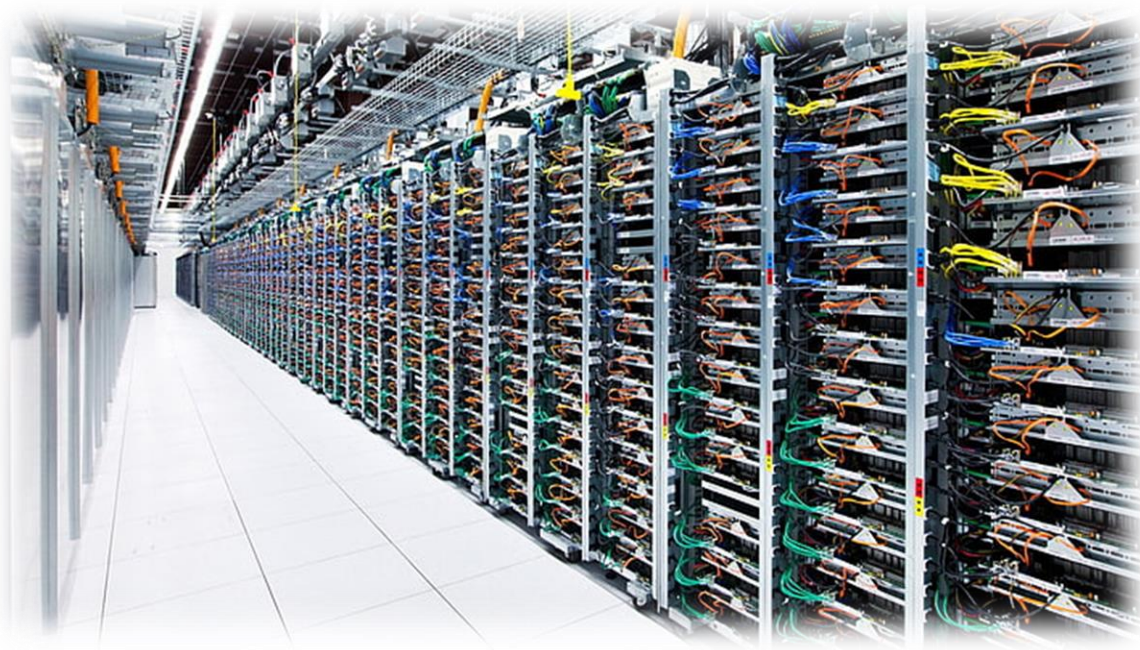
Technical Safeguards

- Encryption, MFA, vuln scanning, and annual pen testing
- Segmentation

Segmentation



Segmentation



Network or Data Center

VLAN Segmentation

- With ACL or FW rules

NAC for Network Access

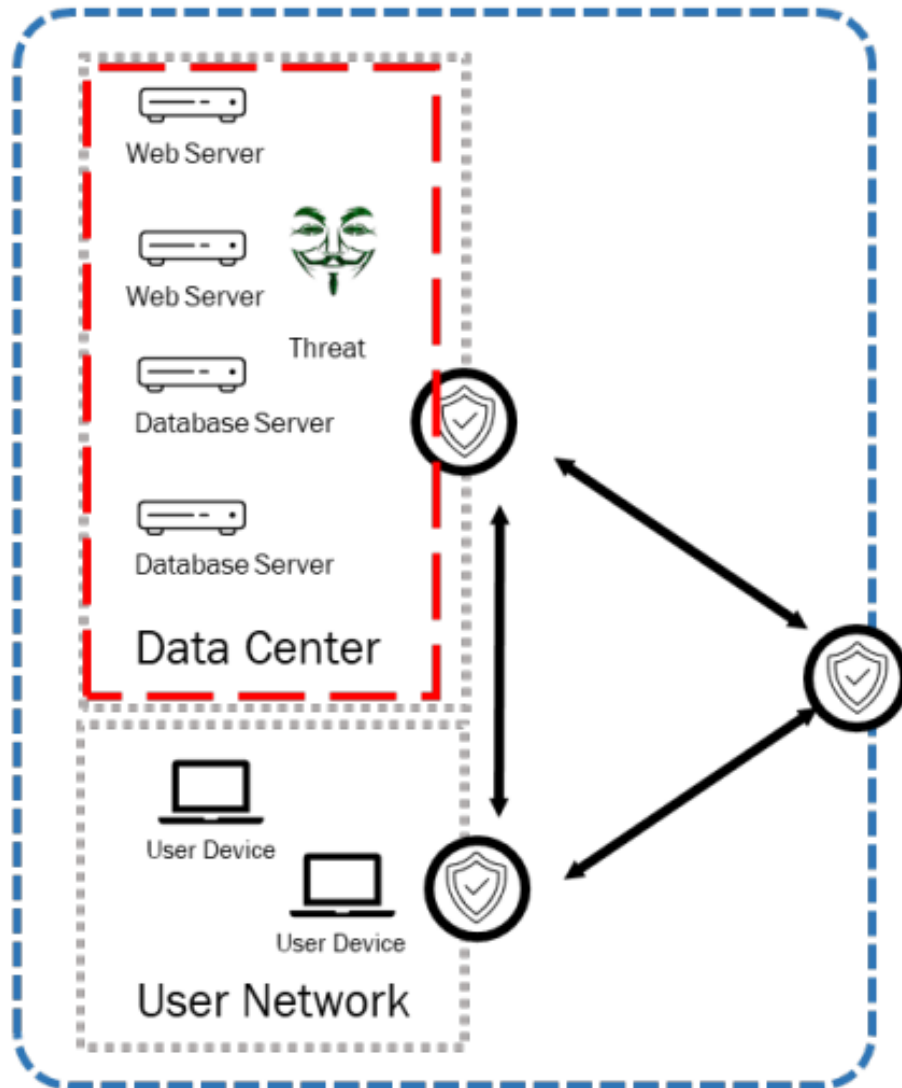
- .1x, Cisco ISE, Aruba ClearPass

Microsegmentation

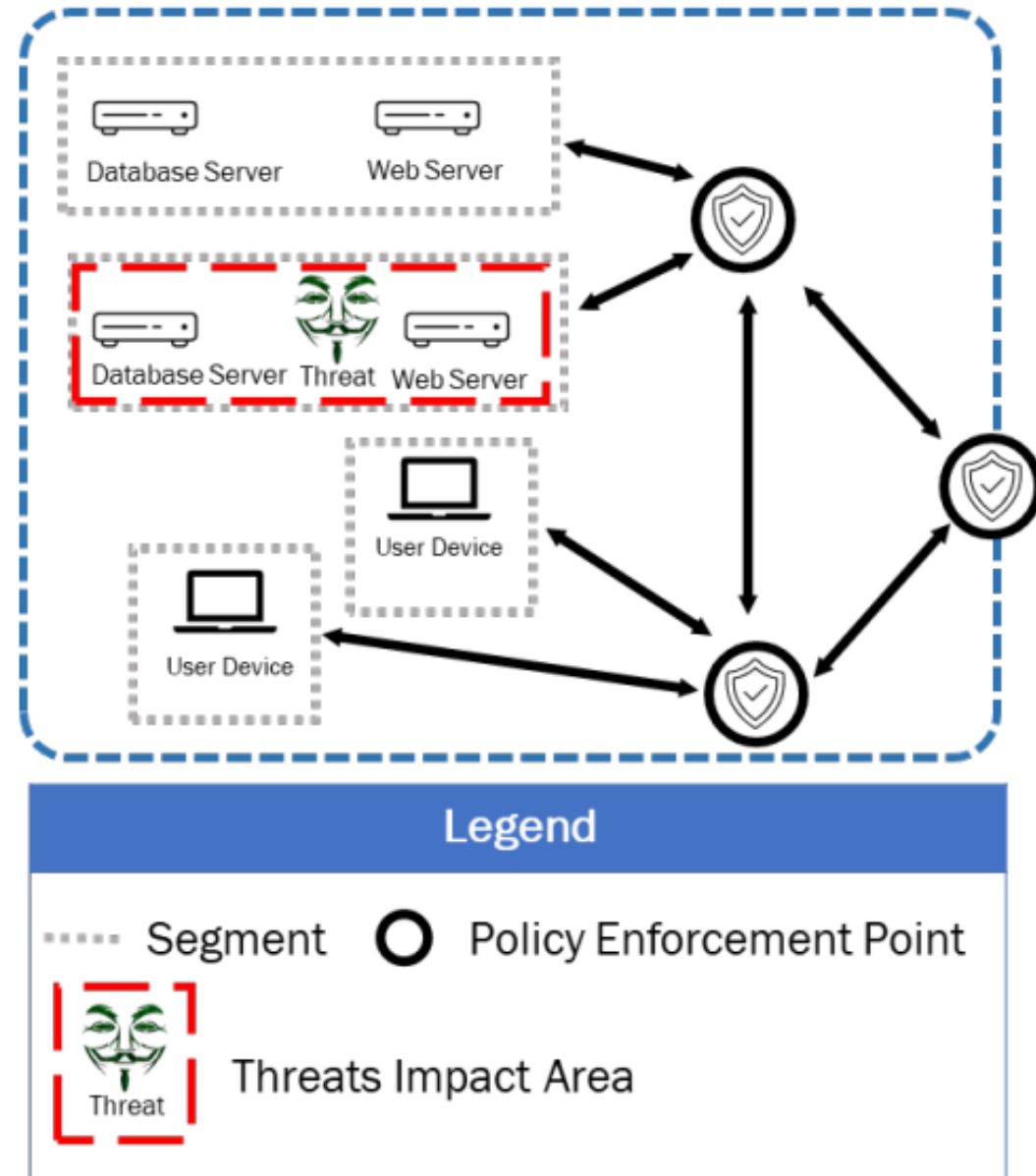
- Secure Workload, VMWare ESX, Illumio

Microsegmentation

Traditional Segmentation



Microsegmentation



The background is a grayscale photograph of a bridge deck, looking down the length of the bridge. The bridge has a steel truss structure. On either side of the walkway, there are ornate metal light fixtures and planters. A dark blue semi-transparent rectangle is centered over the image, containing the number 3 and the title text.

3

State & Other Requirements

More fun!

Legislation is here and more is coming

- Right to know
- Right to correction
- Right to be forgotten
- Right to data portability
- Right to restrict processing
- Right to no discrimination

Oregon Consumer Privacy Act (OCPA)

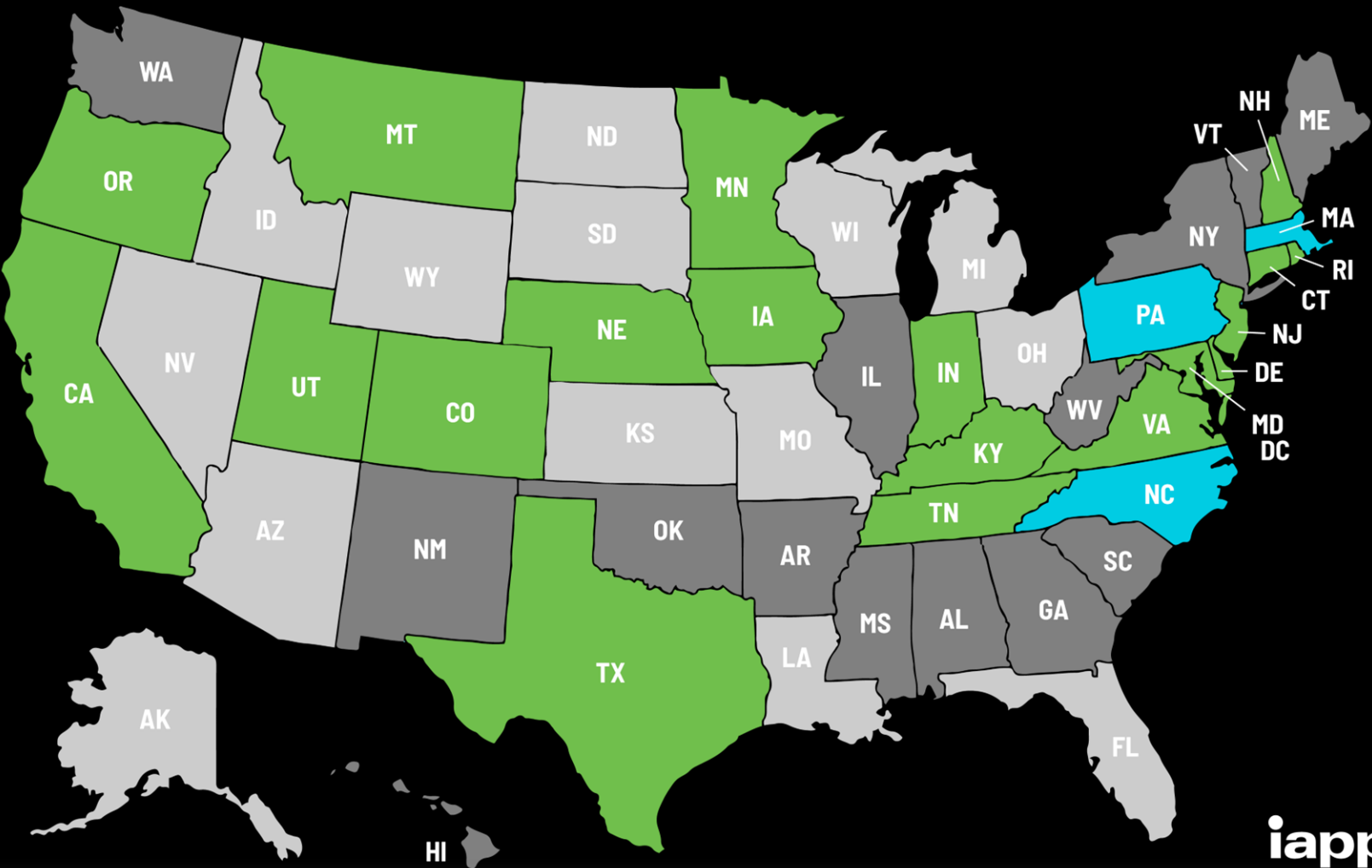
- Effective 1 July 2024
- **Consumer Rights**
 - Access/Correction/Deletion
 - Portability
 - Universal Opt-Out (1 January 2026)
- **Agency Obligations**
 - Privacy Notifications
 - Data Security/Minimization
 - Consent for Sensitive Data



US State Privacy Legislation Tracker 2025

Statute/bill in legislative process

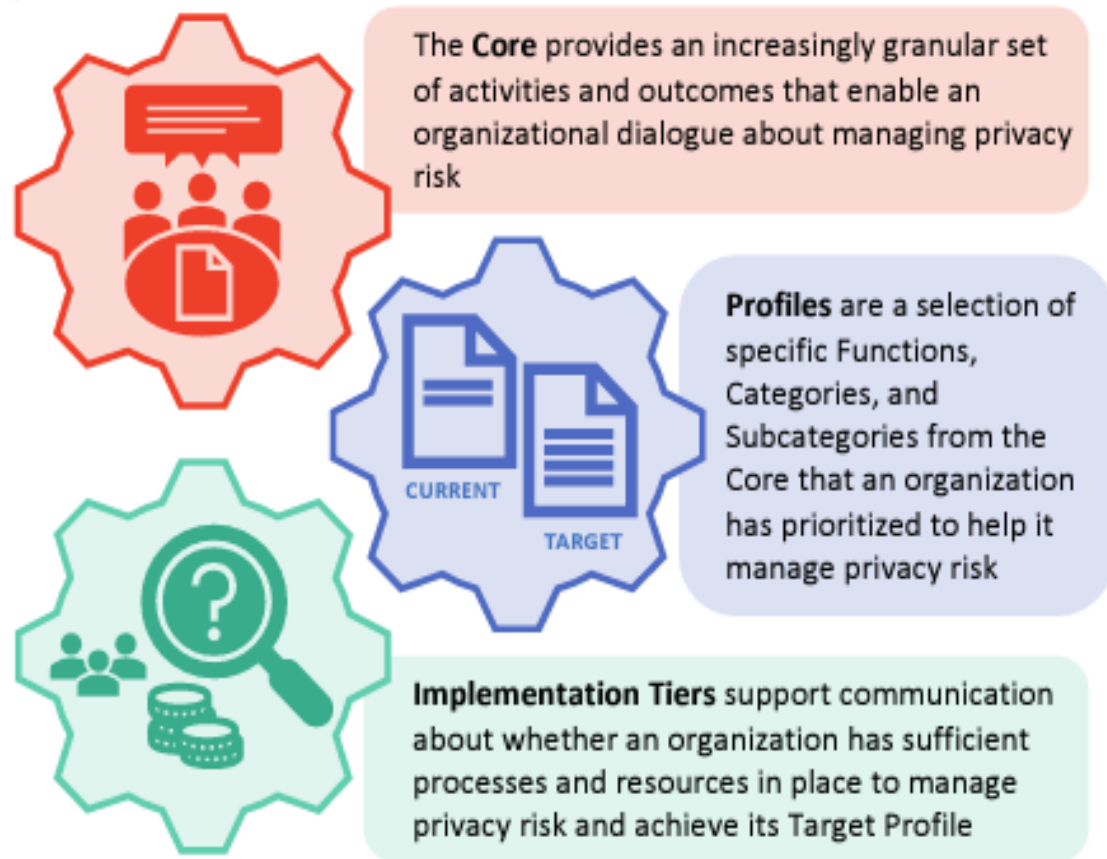
- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bills introduced



Last updated 7 July. 2025

iapp

Privacy – Build a Program



The NIST Privacy Framework

Use with NIST CSF to manage risk

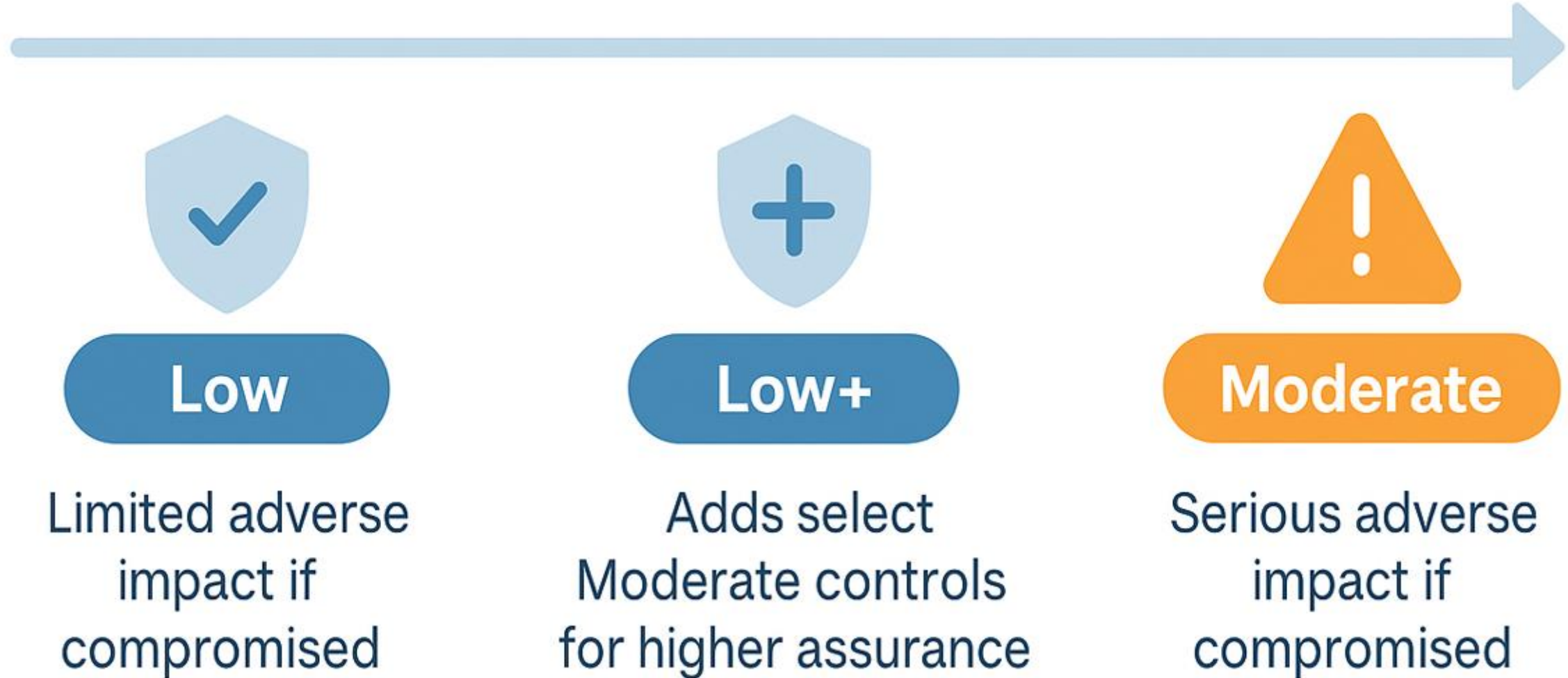
- v1.1 draft released 14 April 2025
- Final in late 2025, early 2026

- **Third-Party Risk Management**

-

GovRAMP Security Categories

Agencies determine impact level based on data sensitivity and potential risk



Individual Government Membership

Stay Informed. Stay Connected.

For government professionals in IT, procurement, risk, or compliance roles. Get insights, resources, and peer collaboration to support secure technology adoption.

FREE

View Benefits

Join Now

Participating Government Membership

Modernize Procurement. Strengthen Security.

Designed for state, local, tribal, and territorial agencies adopting GovRAMP to standardize secure cloud procurement and reduce third-party risk.

FREE

View Benefits

Apply Now

The Payment Card Industry Security Standards Council (PCI SSC) is the governing body.

- PCI is a comprehensive security program for how merchants and service providers must handle card holder data (CHD).
- Sanctioned by the 6 major card brands:
 - Visa
 - Mastercard
 - Discover
 - JCB
 - American Express
 - Union Pay



Does PCI Apply to You?



ANY merchant that while conducting
credit card transactions
“Stores, Processes, or Transmits”
cardholder data
MUST comply with the
**Payment Card Industry Data Security
Standard (PCI-DSS).**

That includes Service Providers

It's all about the Scope.

Scope for PCI is all people, systems and processes that store, transmit, or process credit card information.

This also includes security systems.

Follow the Merchant ID

- A Merchant ID (MID) is usually issued by the acquiring bank to the merchant entity.
- Where and how the MID is used is the first step to determining scope.

Not your MID? PCI might not apply.



Use validated Point to Point Encryption



Validated P2PE is not infectious to other network devices.

This is the easiest, most cost-effective way to reduce scope.

E-Commerce Requirements in 4.0

- **6.4.3 - Ensure scripts are authorized, integrity checked**
 - Use a Content Security Policy
- **11.6.1 - Ensure HTTP headers and payment pages are authorized, integrity checked**
 - Use a reverse proxy/CDN
- **Outsource!**



6.4.2

- Real time monitoring - Use a WAF

11.3.1.2

- Use authenticated internal vulnerability scans

12.5.2.1 Service Providers Only

- Document and confirm scope every 12 months, validated every 6 months



4

Putting it all Together

Best practices and solutions for security and risk reduction.

Define Your Security Program

- **Who** – Responsible party
- **What** – Sensitive data and operational technology
- **When** – Key dates and objectives
- **Where** – Locations and topology
- **Why** – Compliance, regulatory requirements, and risk
- **How** – Architecture & security tech, policy, IR plans

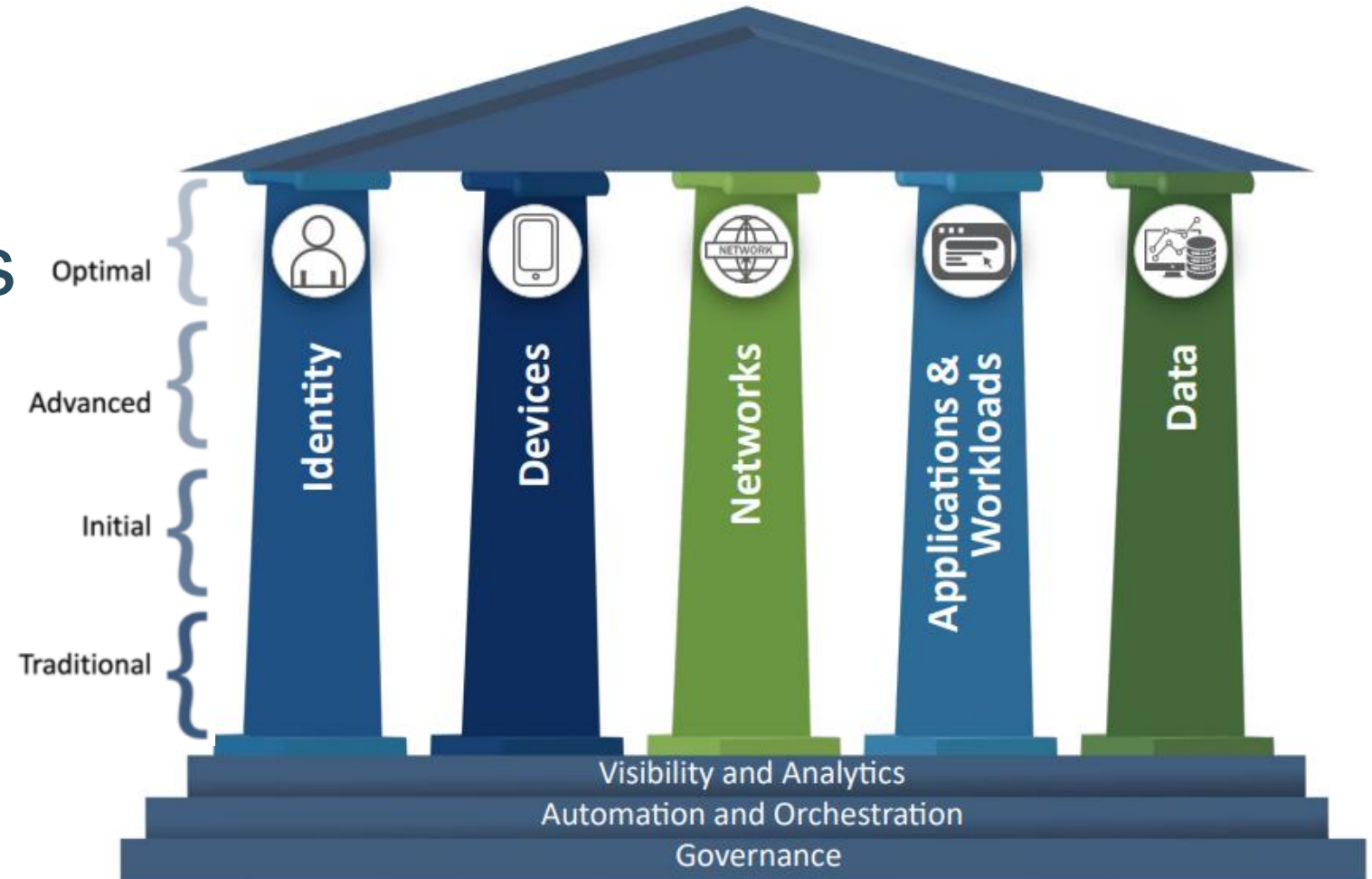


SCF – Not the CSF

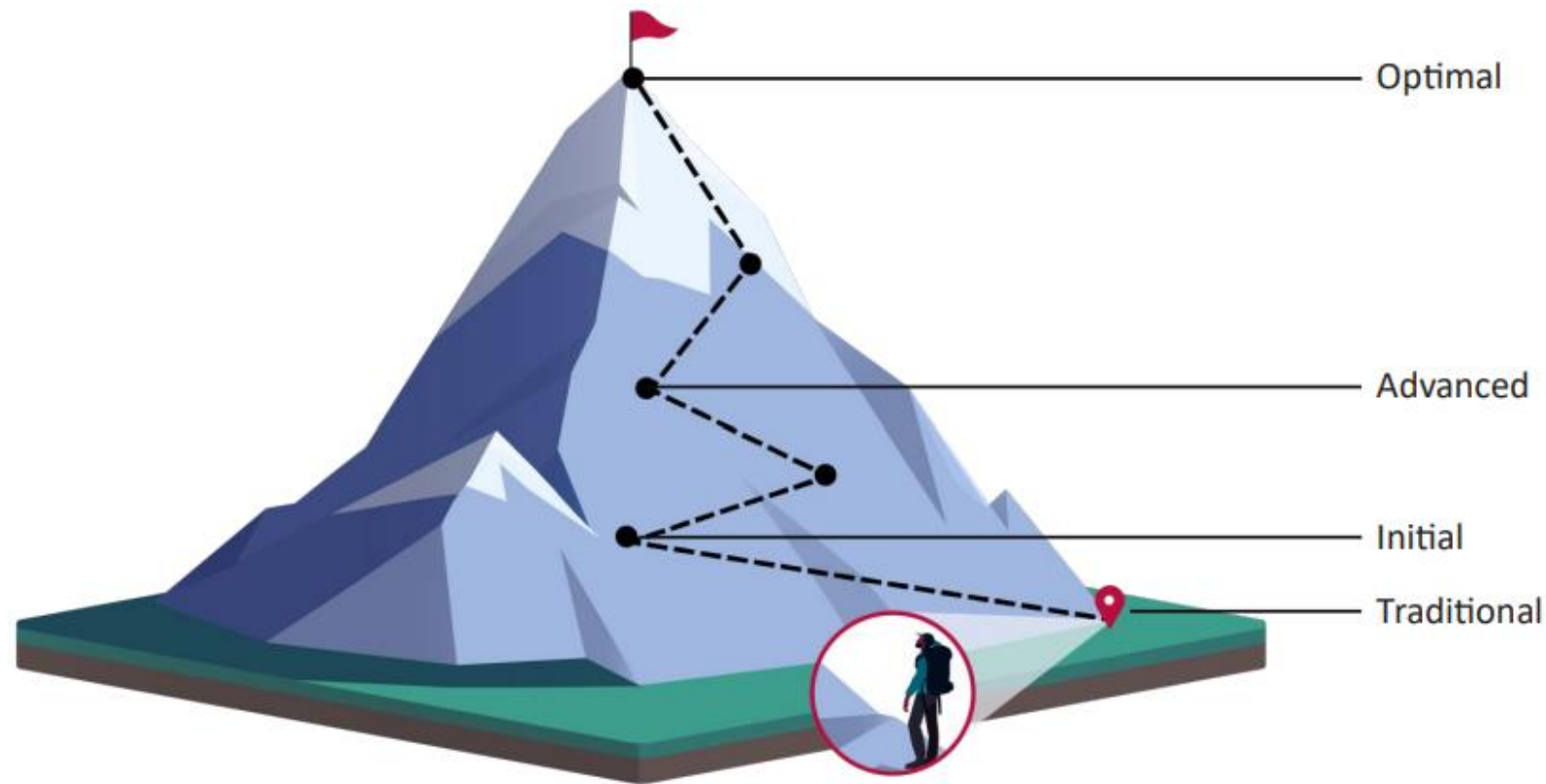
- Maps to all control frameworks
 - NIST, PCI, HIPAA, CJIS
- Provides an enterprise crosswalk of controls
- Security and privacy controls


Zero Trust Effectiveness

- CISA Zero Trust Maturity Model v2.0 (ZTMM)
- Internal or 3rd Party Assessment



ZTMM Example - Identity



Identity	Traditional	Initial	Advanced	Optimal
	Passwords or MFA	MFA with passwords	Phishing-resistant MFA	Continuous validation and risk analysis

Penetration Testing



- External
- Internal
- **Social Engineering**
- Physical
- Applications and API
- On-premises and in the Cloud
- **MFA Replay & Phish Resistance**
- Change-Based

Summary



- Govern AI
- Post Quantum Cryptography
- Compliance
 - HIPAA, PCI, CJIS, CMMC
- Segmentation
- Penetration Testing

Stay connected/More info!



Structured.com