Implementing Regulation with Cybersecurity, and Governance, Risk, & Compliance

Chris Green

Manager of Penetration Testing

Structured.com

structured
bridging people, business & technology™

Chris Green

Manager of Penetration Testing

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

- 12 years in Information Security
- Compliance Assessments
- vCISO – Security Program and Policy Development
- Penetration Testing

Agenda

1 News and Trends - 2025

2 Federal Requirements

3 State & Other Requirements

4 Complete Security Program

1

News and Trends - 2025

Food for thought

What Has Not Changed

- National Cybersecurity Strategy
- Sweeping National AI Legislation
- Across the Board Privacy Legislation
- Worldwide Containment of Hacking and Ransomware

Executive Accountability

CISO and Board of Directors

- SEC
- FTC Safeguards
- HIPAA

Executive Accountability

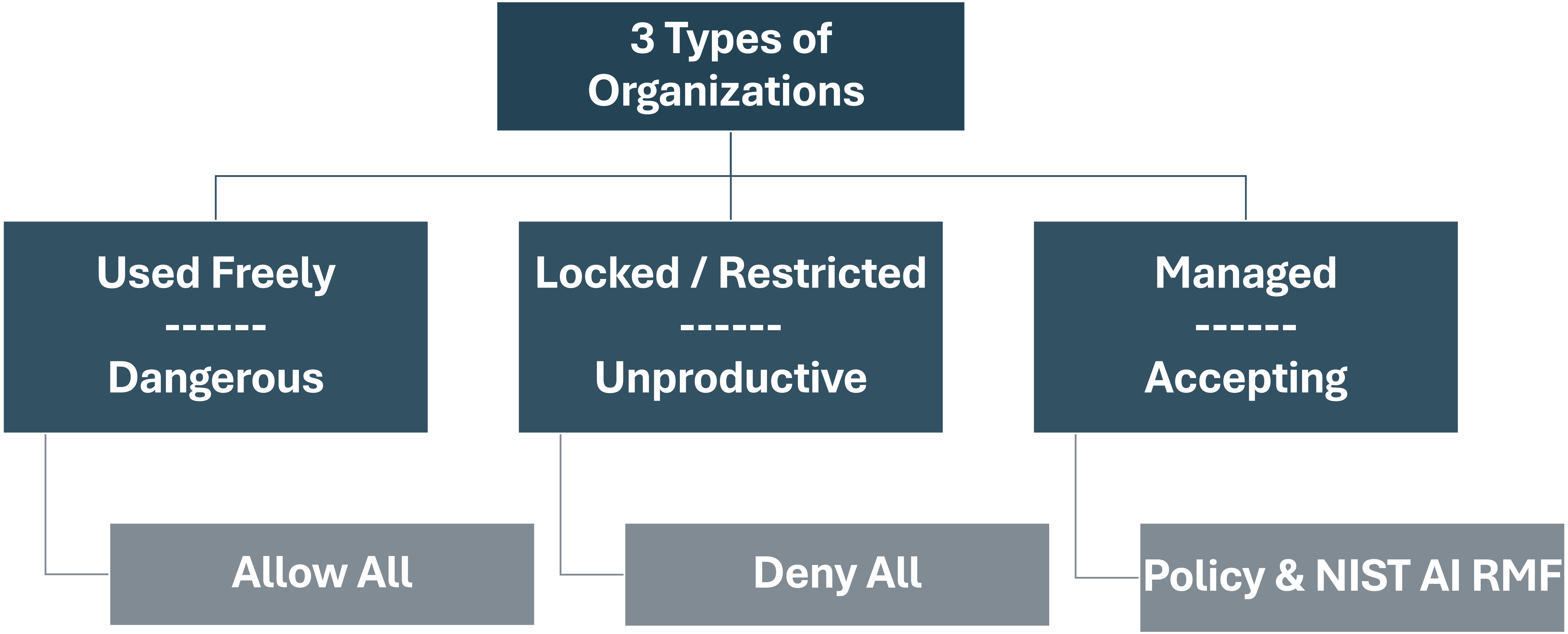
Keep Vendors In Check

- Interview staff
- Review reports
- Vendor management platforms
  - Group monitoring
  - Scanning and dark web artifacts

Artificial Intelligence

- Uses in cybersecurity
  - Policy and procedure creation
  - Threat detection
  - Threat response
  - Risk Prioritization
  - Characteristic recognition

Generative AI Governance



3 Types of Organizations

Used Freely

Dangerous

Locked / Restricted

Unproductive

Managed

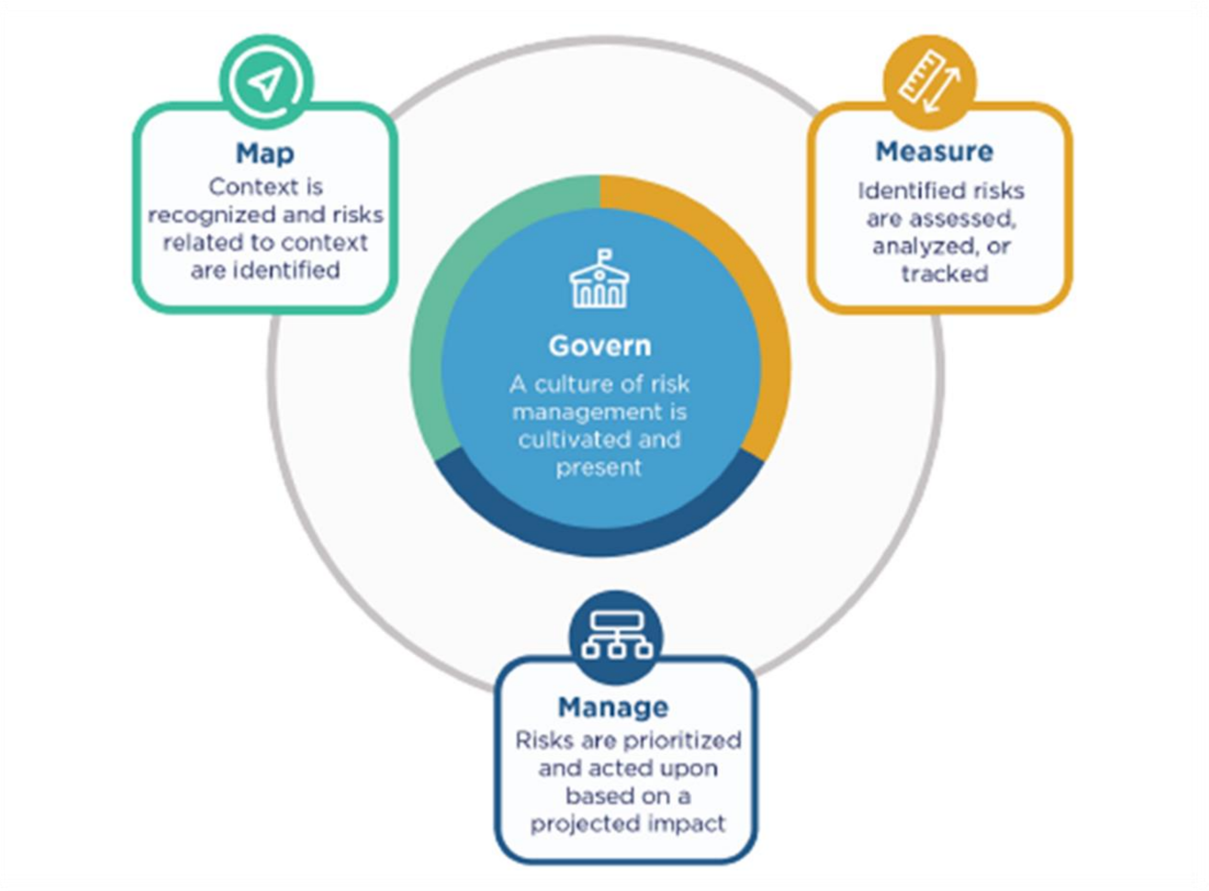
Accepting

Allow All

Deny All

Policy & NIST AI RMF

AI Deployment & Assessment


Map
Context is recognized and risks related to context are identified
Measure
Identified risks are assessed, analyzed, or tracked
Govern
A culture of risk management is cultivated and present
Manage
Risks are prioritized and acted upon based on a projected impact

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

Current Attack Vectors

Trends

- Vulnerability Exploitation
- Third-Party Risk
- Social Engineering
  - As a Service

Highly Evasive Adaptive Threats (HEAT)

  - Zero Trust Principles
    - Enterprise browsers

Current Attack Vectors

- Ransomware

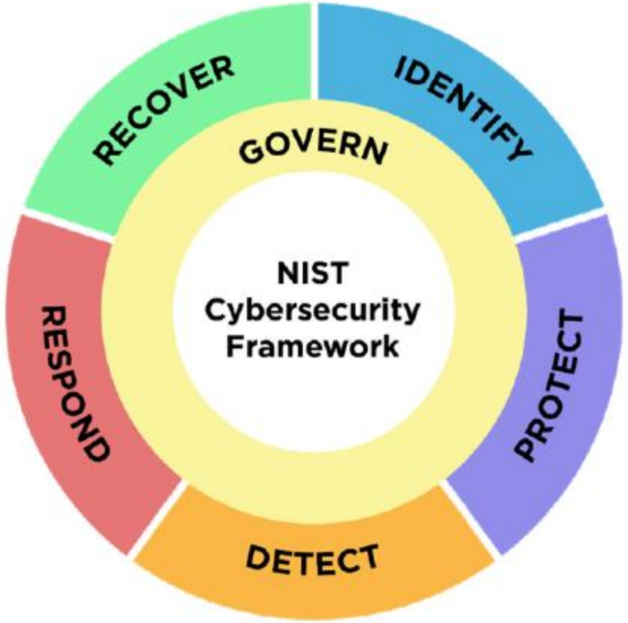
  - 60% of worldwide attacks on North America
  - Fastest movers in ‘25
    - Financial
    - Energy and Utilities
  - Email as a vector
  - External access

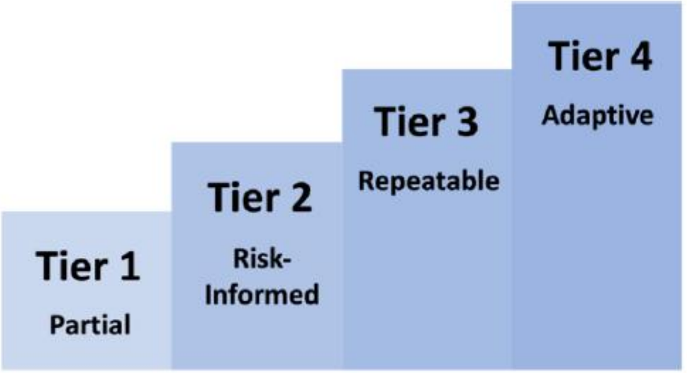
2

Federal Government

Frameworks and regulations

NIST Cybersecurity Framework 2.0





- The latest NIST CSF framework
  - No longer specific to critical infrastructure
  - Core
  - Organizational Profiles
    - Posture, objectives, outcomes
  - Tiers

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

Security Rule Control Areas

Increased Oversight of Business Associates

- Annual written validation
- 24 Hour notification of incidents

Workforce Security and Remote Access

- RBAC
- 1-hour cutoff for termination

Annual Audits

- Security Rule standards

Endpoint Security

- Workstation to include mobile devices

Security Rule Control Areas

Mandatory Implementation of All Controls

- Required unless exempt

Technical Safeguards

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

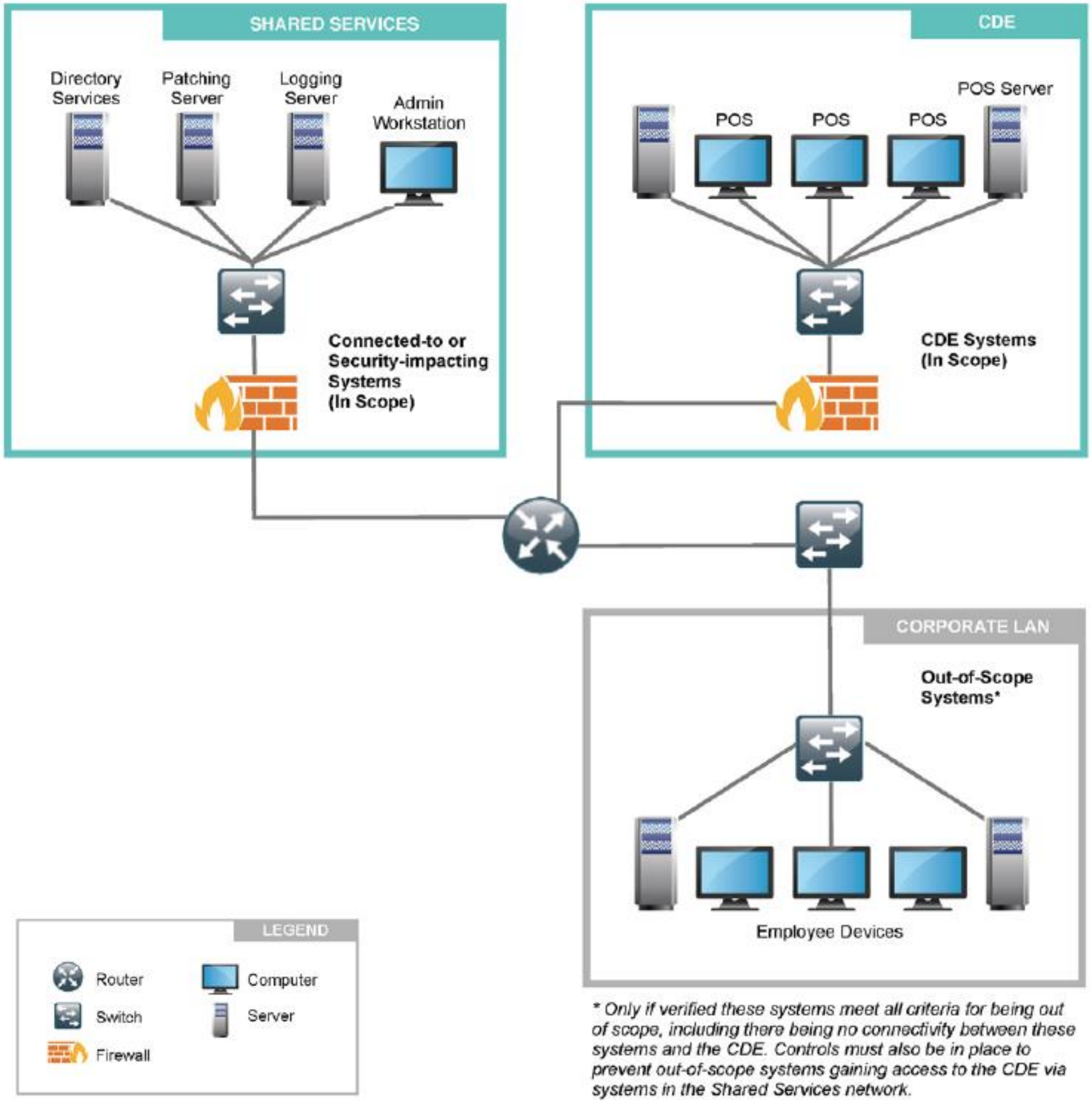
Enhanced Risk Assessment

- Inventory, threats, CIA of ePHI
- Policies

Formal IR and Contingency Planning

- Document plans, 72-hour restoration

Segmentation



* Only if verified these systems meet all criteria for being out of scope, including there being no connectivity between these systems and the CDE. Controls must also be in place to prevent out-of-scope systems gaining access to the CDE via systems in the Shared Services network.

Segmentation

Network or data center

- NAC for network access
  - .1x, CISCO ISE, Aruba ClearPass
- VLAN segmentation
  - With ACL or FW rules
- Microsegmentation
  - Secure Workload, VMWare ESX, Illumio

Cybersecurity Maturity Model Certification

THE CYBER AB

CMMC CERTIFICATION

CMMC applies to the Defense Industrial Base

- Forms the supply chain for the DoD
- 350,000+ prime contractors and subcontractors
  - Manufacturing
  - Staff augmentation
  - Construction
  - Utilities
  - Services

Cybersecurity Maturity Model Certification

Sensitive data must be *identified and protected*

- Federal Contract Information (FCI)
  - Cost/pricing information
  - Project timelines
  - Draft deliverables or reports

- Controlled Unclassified Information (CUI)
  - PII
  - Sensitive business information

Cybersecurity Maturity Model Certification

Cloud Service Providers

- Certification not required
- Azure Government GCC-HIGH
  - FedRAMP Certified

Managed Service Providers

- Will be included in the audit of the organization seeking certification

What To Do Now?

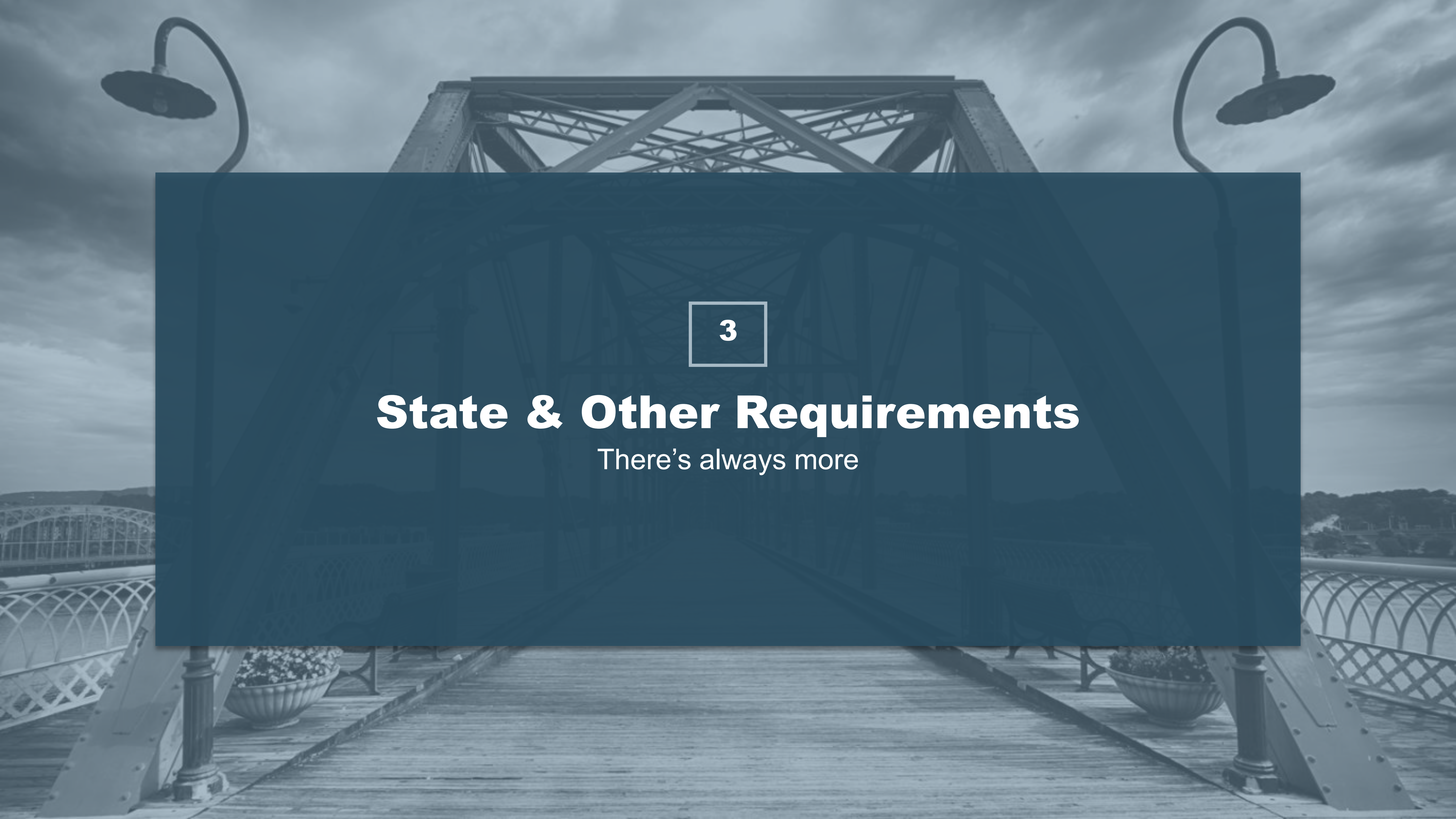
Until CMMC 2.0 is required…

- Become and stay compliant with NIST 800-171v2
- Complete your DoD Assessment Methodology checklist and score
- Complete your SSP/POAM and policies
- File your SPRS status
- Have a pre-assessment

Registered Practitioner

Get assistance within the ecosystem

- Policy development
- System Security Plan/Plan Of Action Milestones
- Tabletop exercises
- Penetration testing
- Pre-assessment and CMMC guidance



3

State & Other Requirements

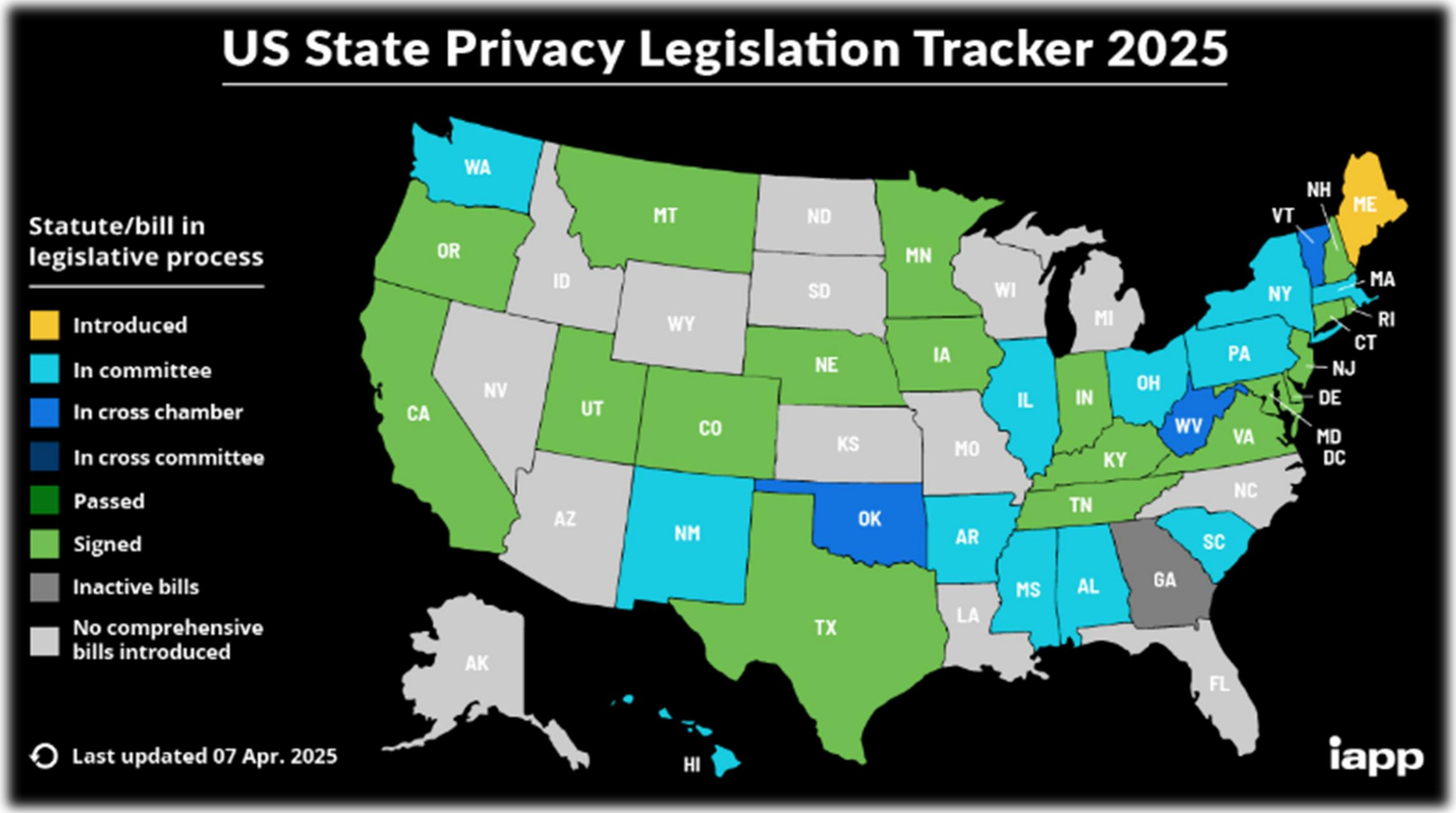
There’s always more

Privacy

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

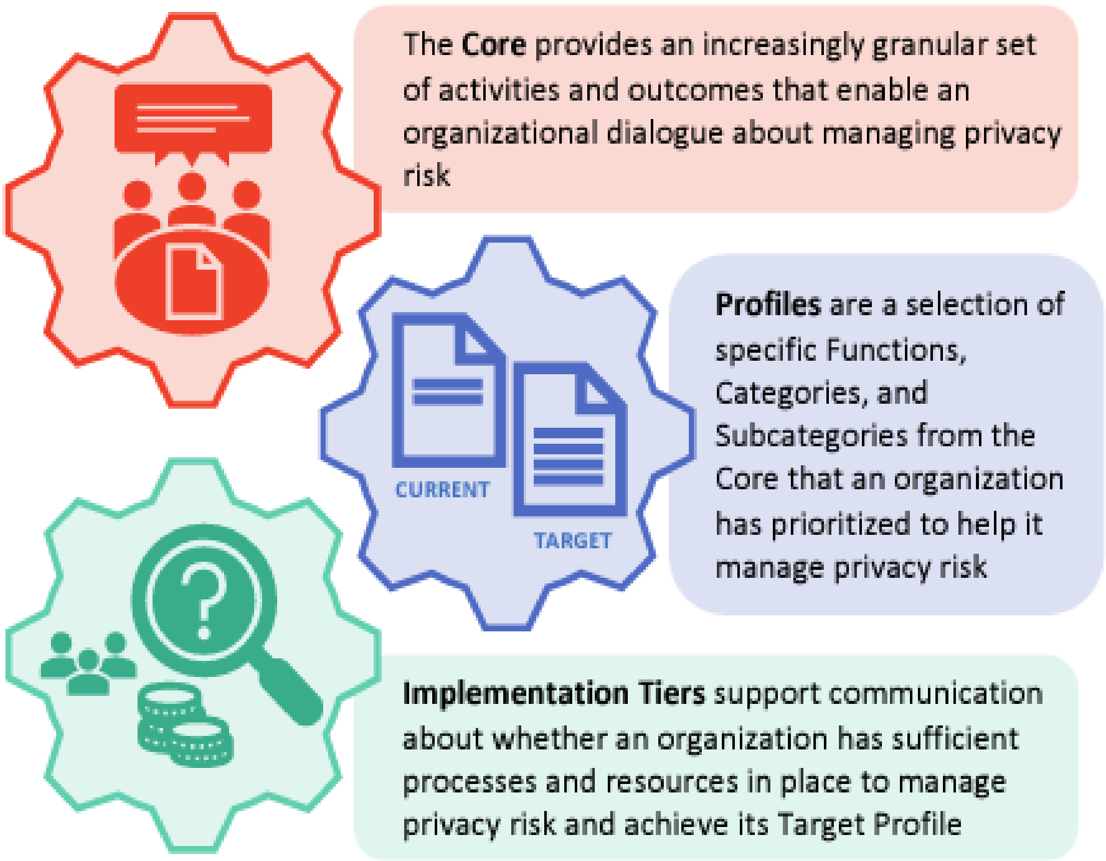
Privacy



US State Privacy Legislation Tracker 2025

Last updated 07 Apr. 2025

Privacy – Build a Program



The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk

Implementation Tiers support communication about whether an organization has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

The NIST Privacy Framework:

Use in conjunction with the NIST Cybersecurity Framework to manage organizational risk.

PCI

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

PCi Security Standards Council®

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

Common Misconceptions

Myth 1

We outsource; therefore, we have no PCI compliance responsibility.

Myth 2

Our e-commerce website links to a gateway/ processor page so it is completely out of scope.

Myth 3

We don't store CHD, so we are not required to comply or report.

Myth 4

We encrypt all CHD, so we are out of scope.

NOTE: It's a requirement to encrypt stored CHD!

Scoping

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.

Scoping

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.

Scoping

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.

DSS v4.0

E-Commerce Requirements in 4.0

- **6.4.3 - Ensure scripts are authorized, integrity checked**
  - Recommendation - Use a vendor solution or Content Security Policy

DSS v4.0

E-Commerce Requirements in 4.0

- **11.6.1 - Ensure HTTP headers and payment pages are authorized, integrity checked**
  - Recommendation – Use a vendor solution or reverse proxy/Content Delivery Network

DSS 4.0 Controls

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

Complete Security Program

Keys to 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

Data Security Posture Management (DSPM)

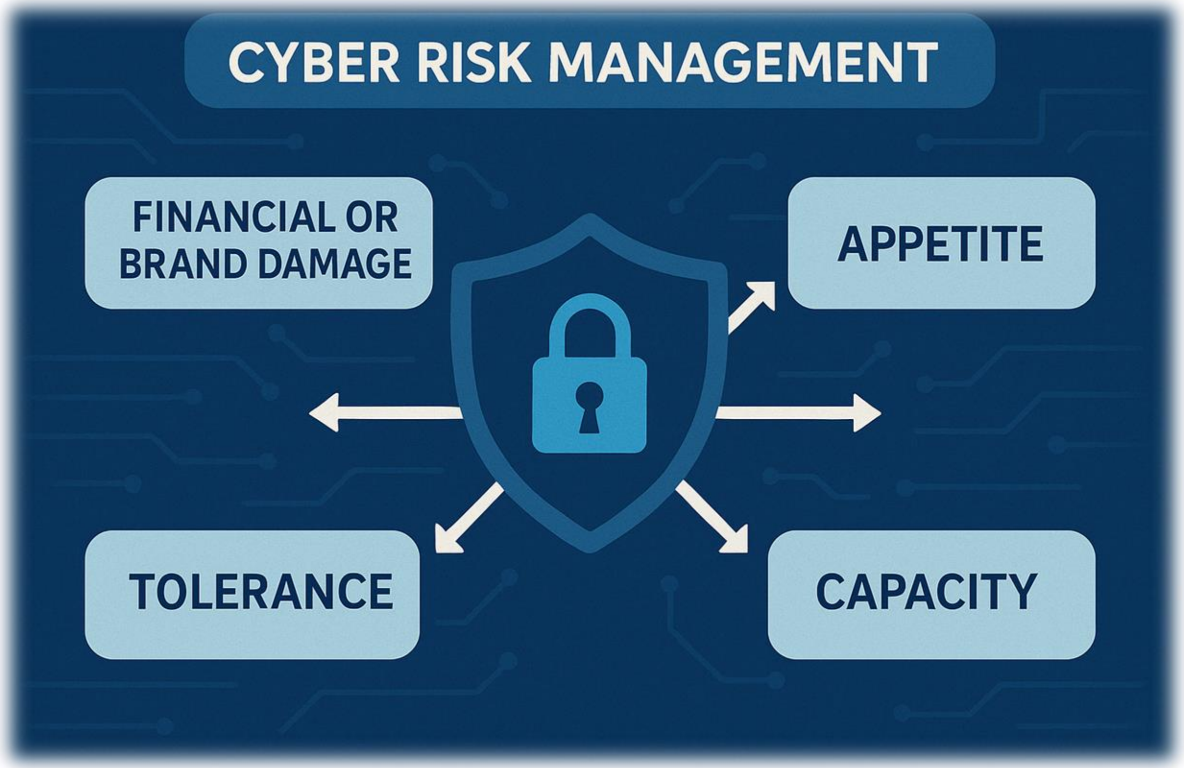
A Foundation for Cybersecurity Maturity

- Builds and maintains a categorized data inventory
- Maps data across systems, cloud, and formats
- Aligns with privacy and compliance needs
- Supports data lifecycle governance
- Enables breach detection and notification

Risk Management

- **Perform recurring risk assessments**

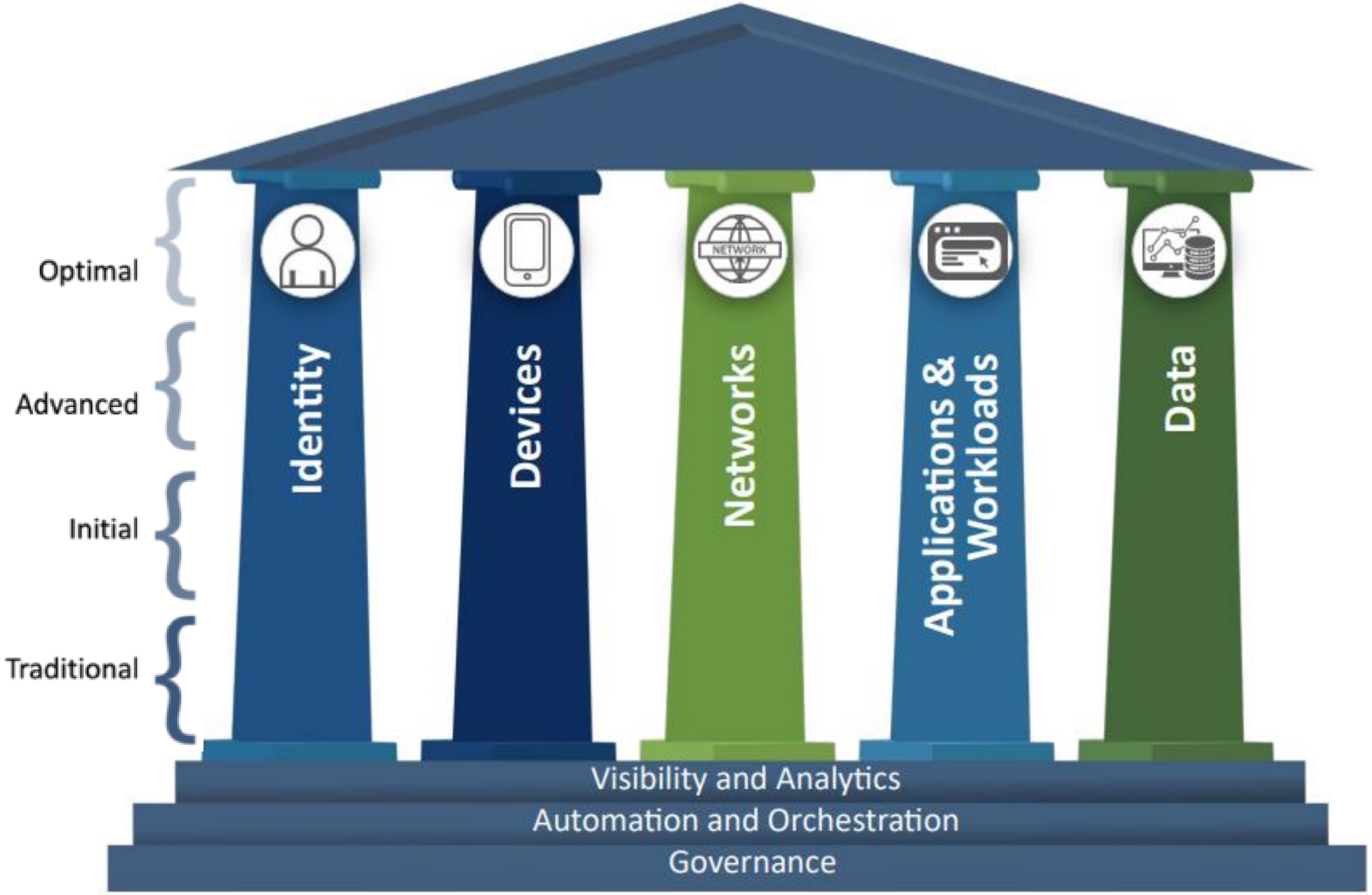
- **Define key objectives –**
  - Financial, brand damage, staff
  - Appetite
  - Tolerance
  - Capacity



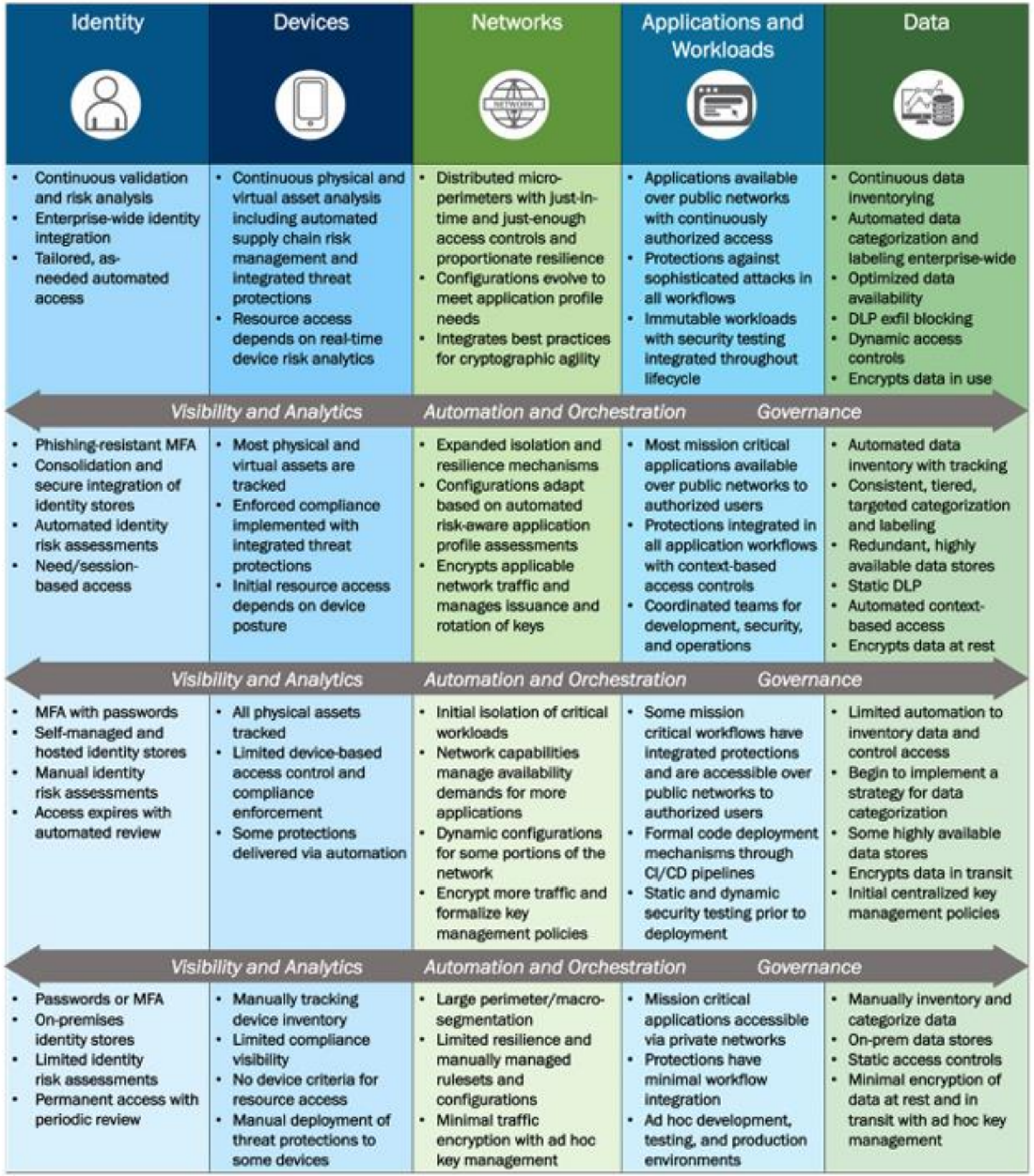
Zero Trust

Zero Trust Effectiveness

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

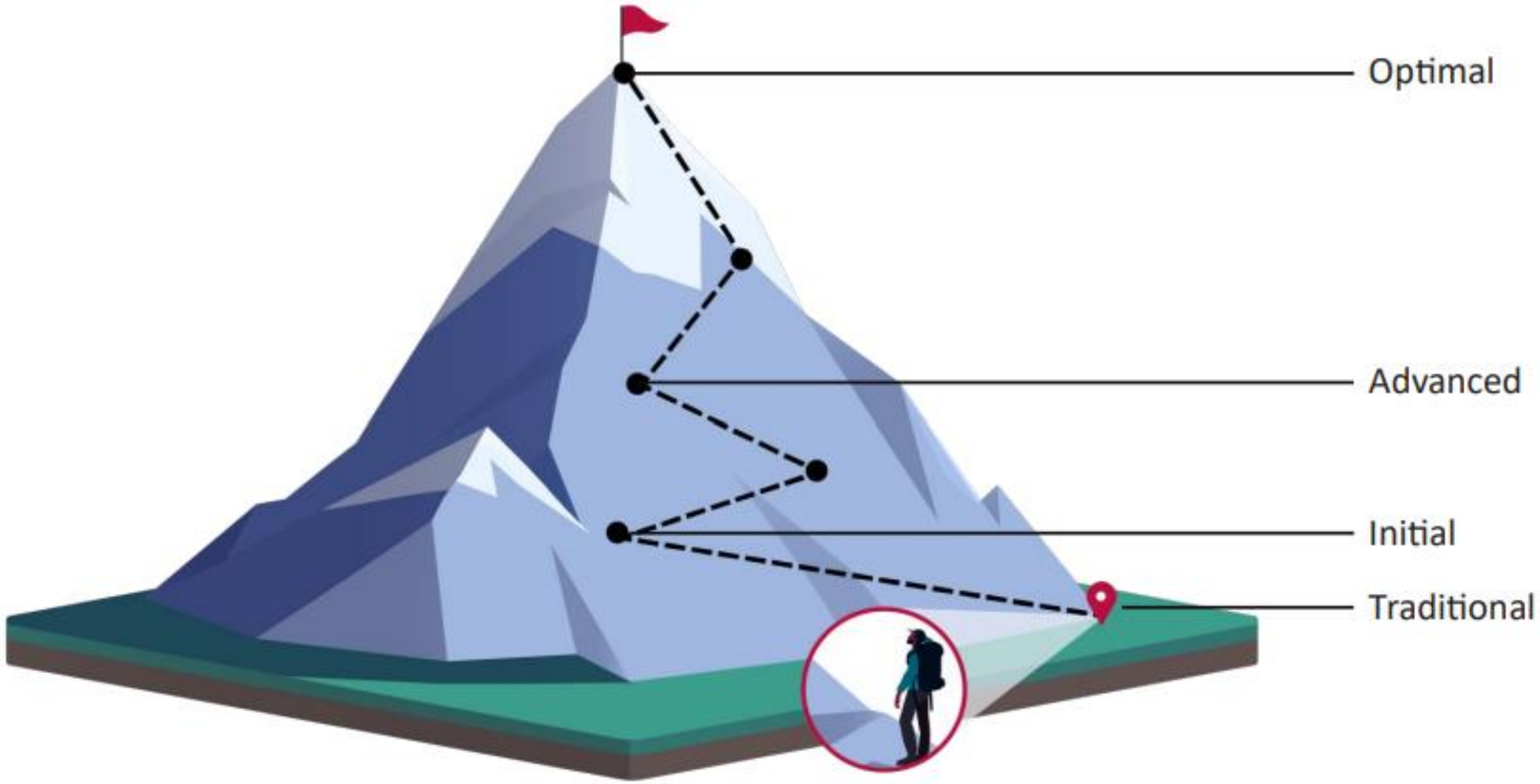


Zero Trust



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		Automation and Orchestration		Governance
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		Automation and Orchestration		Governance
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		Automation and Orchestration		Governance
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

ZTMM Example - Identity



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

Multifactor Authentication (MFA)

Drives Security & Compliance

- Reduces risk of compromise
- Supports cyber insurance qualification

Focus Where It Counts

- External systems (cloud, remote access, customer-facing)
- Admin credentials

Further Resistance

- Leverage FIDO2, PKI, hardware tokens, passkeys

Cloud

Cloud deployments in M365, Azure, AWS and GCP

- Posture management assessment
- Penetration test
  - IaaS
  - PaaS
  - SaaS
  - Don’t forget endpoints

Penetration Testing

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

Summary

- Govern AI
- Segmentation
- Risk Management
- Compliance
  - HIPAA, PCI, CJIS, CMMC
- Penetration Testing

ARE THERE ANY QUESTIONS?

Stay connected!

structured

bridging people, business & technology™

Structured.com