Vendor Risk Management (VRM) system

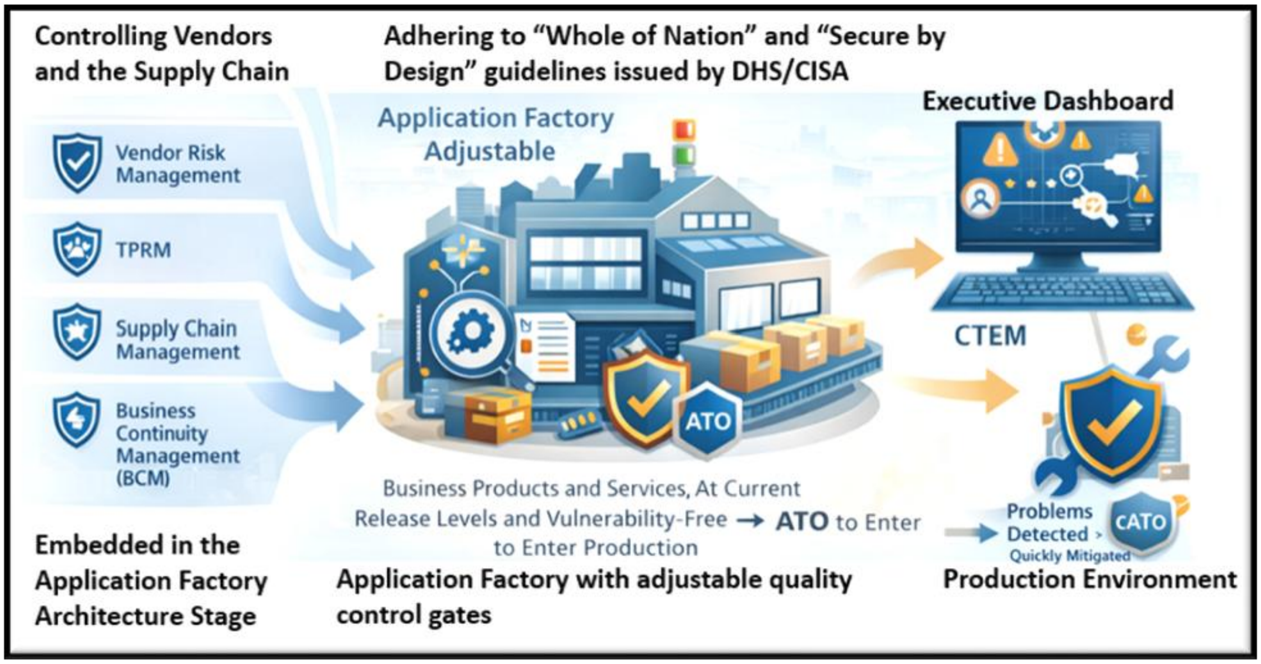

Controlling Vendors and the Supply Chain
Adhering to "Whole of Nation" and "Secure by Design" guidelines issued by DHS/CISA
Executive Dashboard
Application Factory Adjustable
Vendor Risk Management
TPRM
Supply Chain Management
Business Continuity Management (BCM)
CTEM
ATO
Business Products and Services, At Current Release Levels and Vulnerability-Free → ATO to Enter to Enter Production
Problems Detected › Quickly Mitigated
CATO
Embedded in the Application Factory Architecture Stage
Application Factory with adjustable quality control gates
Production Environment

Figure 1: Vendor Risk Management (VRM) through Application Factory to achieve ATO and using CTEM to achieve cATO.

A complete perspective of implementing VRM and protecting your environment through an Application Factory with adjustable quality control gates is provided within this document.

This document provides a plan for implementing Cybersecurity – Supply Chain Risk Management (C-SCRM), Vendor Risk Management (VRM), Third-Party Risk Management (TPRM), Supply Chain Management (SCM), Vulnerability Management, and Business Continuity Management (BCM) through an Application Factory (AP) with adjustable quality control gates (AQCGs) to achieve Authorization to Operate (ATO) within the Production Operations Environment.

It then describes implementing Continuous Threat Exposure Management (CTEM) to quickly identify problems and support rapid mitigations prior to being attacked by Hackers. The document illustrates how an executive Dashboard can monitor and report on exceptions to appropriate personnel as rapidly as possible, so that they can monitor the environment and take rapid corrective actions to protect business products and services and adhere to Board Compliance requirements. Domestic and International Laws and Regulations are provided and an overview of the Application Factory with adjustable quality control gates is provided. The document supports applying automation whenever possible to improve efficiency and reliability.

Thomas Bronack, Founder and CEO

Data Center Assistance Group, LLC

bronackt@dcag.com | bronackt@gmail.com | www.dcag.com } (917) 673-6992

Contents

Board Brief

Why Integrated Asset Management, Infrastructure Management, Vendor Risk Management, Supply Chain Management, Security, Compliance, Resilience, and Business Continuity Management Programs Are Now Mandatory because of enhanced Board Due Diligence requirements.

Executive Summary

Every Organization Must Implement Integrated Risk, Resilience, Security, and Compliance Programs

In today's operating environment, organizational success and survival are inseparable from third-party risk, supply chain integrity, cybersecurity resilience, and regulatory compliance. Companies no longer fail solely due to internal weaknesses; they fail because external dependencies introduce unmanaged risk that leadership cannot see, measure, or control.

Vendor Risk Management (VRM), Third-Party Risk Management (TPRM), Supply Chain Management (SCM), Business Continuity Management (BCM), cybersecurity (pre- and post-quantum), plus domestic and international compliance must be treated as one integrated executive discipline, not siloed initiatives.

C-SCRM Policy – Executive Definition

Cybersecurity - Supply Chain Risk Management (C-SCRM) Policy establishes the governance framework for identifying, assessing, mitigating, and continuously monitoring cybersecurity risks introduced by third-party vendors, suppliers, and service providers across the enterprise (see Link).

The policy ensures that all products, services, and technologies entering the organization meet defined **security, resilience, and compliance standards** before deployment and throughout their lifecycle. It mandates:

- Inventory of all present vendors and suppliers.
- Identify and Rate Risk-based supplier classification.
- Security requirements are embedded in contracts and procurement.
- Continuous monitoring of vendor cyber posture
- Executive oversight and accountability

Purpose:
To protect mission operations, data, and enterprise value by preventing supply-chain vulnerabilities from becoming systemic business failures.

An overview of the problem.

Vendors include Suppliers, Vendors, and Transportation organizations – all classified as Manufacturing.

Raw materials are mined all over the world, then transported to Factories for smelting, manufacturing, assembly, transportation to warehouses, and client location for sale to the public as business products or services. Overhead related to manufacturing is offset by profits made through client sales for business products or services.

Supply Chains must provide products and services when needed to support operations efficiency. Coordination between vendors and clients must be maintained should a disaster event cause the relocation of a facility or department. This occurs when a fire, natural event, or human caused event, causes a disaster interruption to be experienced. Recovery actions must be taken when business interruptions occur. Suppliers must be notified to deliver their supplies to a new location during a disaster event if relocation occurs.

Business operations is therefore dependent on a Vendor Risk Management system that includes Vendors, Suppliers, and Transportation of components to support client demands an uninterrupted service.

Additional ingredients in Vendor Risk Management are the quality of the components, their adherence to contract and service level agreements, their compliance to standards, their release management as it applies to the environment (to avoid vulnerabilities being injected through out-of-date vendor components), their security adherence ("Secure by Design" adherence), and finally their ability to provide excellent service in support of client requirements and time demands.

The use of SBOMs (Software Bill of Materials), RBOMs (Runtime Bill of Materials), and other BOMs like AIBOMs (Artificial Intelligence Bill of Materials, which are now included in SBOMs) can identify weaknesses that require patches or new releases. Their use can support Vulnerability Management and keep your systems running at peak performance.

Why This Matters to the Board

1. Vendor Risk Management in a world full of turmoil

This illustration shows the issues associated with getting supplies to your company in support of continued uninterrupted operations. World events can be out of your control, so alternative routes and problem circumventions should be included in the Vendor Risk Management process.

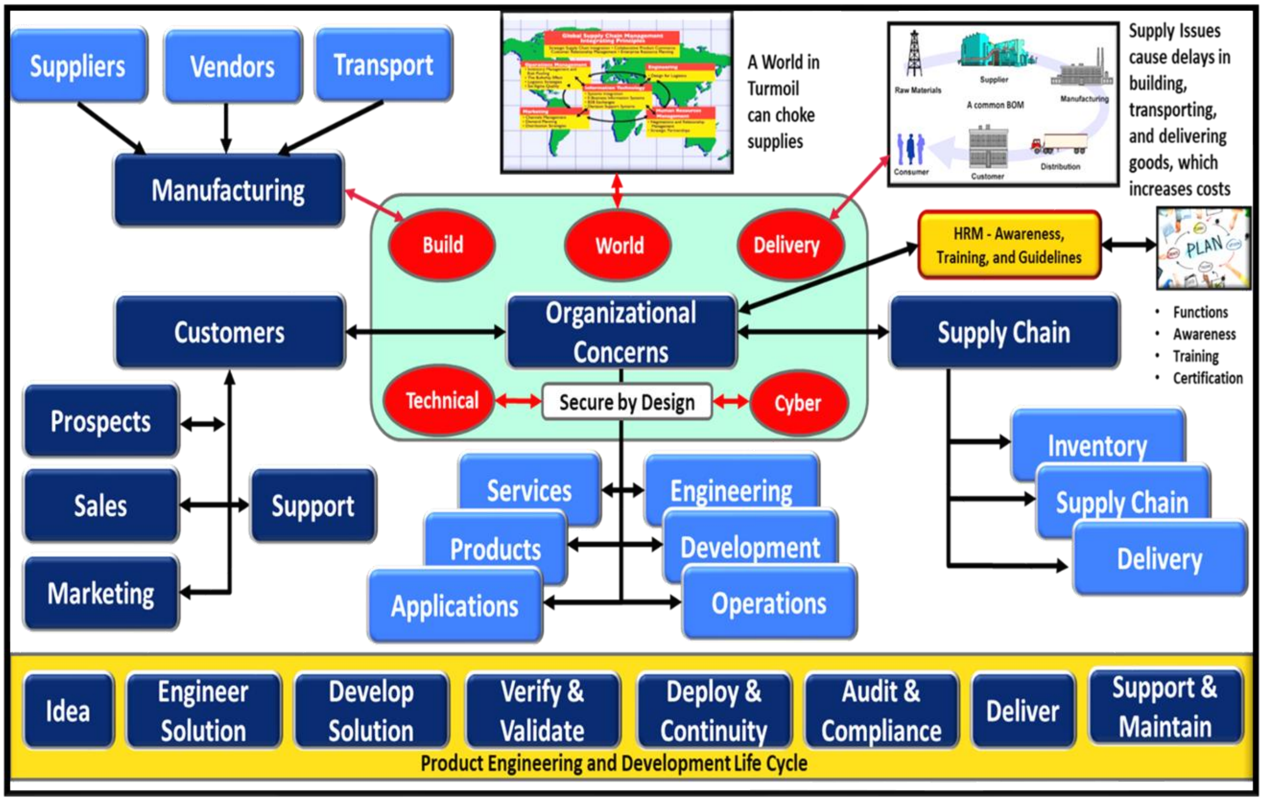


Figure 2: Overview of the Vendor Risk Management (VRM) Problem

- ## Third-Party Risk Is Enterprise Risk

  - Vendors and suppliers operate inside core business processes and data flows.
  - A single vendor failure can trigger operational outages, data breaches, and regulatory action.
  - Without VRM and TPRM, leadership lacks visibility into who supports critical services and where risk is being accepted unknowingly.
  - Identification of component owners delays the resolution process.

  Board implication:
  Risk decisions are being made without sufficient information.

- ## Supply Chain Disruptions Are Value-Destroying Events

  - Supply chains now represent cyber-attack vectors, geopolitical exposure, and single points of failure.
  - Boards are increasingly expected to understand dependency concentration and recovery capability.
  - Rules governing countries where supplies are obtained are being tightened.

  Board implication:
  Unmanaged supply chains can stop revenue generation overnight and can even cause loss revenue in fines and exposures.

Business Continuity Is a Governance Obligation

- BCM ensures the organization can continue delivering products and services under stress.
- Disruptions without prepared recovery plans escalate into reputational and financial crises.

Board implication:
BCM protects revenue, customer trust, and executive credibility.

Cybersecurity Must Address Both Today and Tomorrow

- **Today:** Vendors and supply chains are primary attack targets.
- **Tomorrow:** Data stolen today may be decrypted in the future using quantum computing.
- **Long-lived** data (financial, personal, intellectual property) is already at risk.
- **AI and Quantum computing** will introduce new exposures not fully recognized yet.

Board implication:
Cybersecurity strategy must protect both current operations and future data value.

Compliance Is Now Strategic, Not Administrative

- Regulations increasingly require demonstrable governance over third-party risk, cyber resilience, and data protection.
- Failure results in fines, litigation, loss of market access, and investor distrust.

Board implication:
Weak compliance directly exposes directors and executives to liability.

Why Cybersecurity Must Address Both Pre- and Post-Quantum Risk

Today's Reality (Pre-Quantum)

- Cyber-attacks target vendors and supply chains first.
- Ransomware, data exfiltration, and service disruption are daily events.
- Regulators now treat cyber risk as a governance issue.
- Harvest Now, Decrypt Later (HNDL) is a real problem today and must be addressed.

Tomorrow's Reality (Post-Quantum)

- Data stolen today can be decrypted in the future (HNDL).
- Cryptographic systems in use today will become obsolete.
- Long-lived data (financial, healthcare, IP, PII) is already at risk.
- File transfers must use TLS to safeguard data and provide cryptography in motion.

Organizations must:

- Know where cryptography is used.
- Protect sensitive data against future decryption.
- Plan orderly transitions to quantum-resistant algorithms.

Bottom line:
Security strategy must protect both current operations and future data value.

The Executive Requirement: Integration

Organizations that succeed:

- Integrate VRM, TPRM, supply chain management, BCM, security, and compliance.
- Use executive dashboards and metrics to monitor risk.
- Make informed risk-acceptance decisions.
- Demonstrate governance, not reaction (use "Left of Boom" guidelines).

Organizations that do not:

- Operate blindly.
- React to incidents instead of preventing them.
- Accumulate silent risk until failure occurs.
- Do not use "Left of Boom" guidelines for proactive safety.

Board-Level Conclusion

- Integrated risk, resilience, security, and compliance programs are no longer best practices. They are requirements for responsible oversight and long-term enterprise value protection.

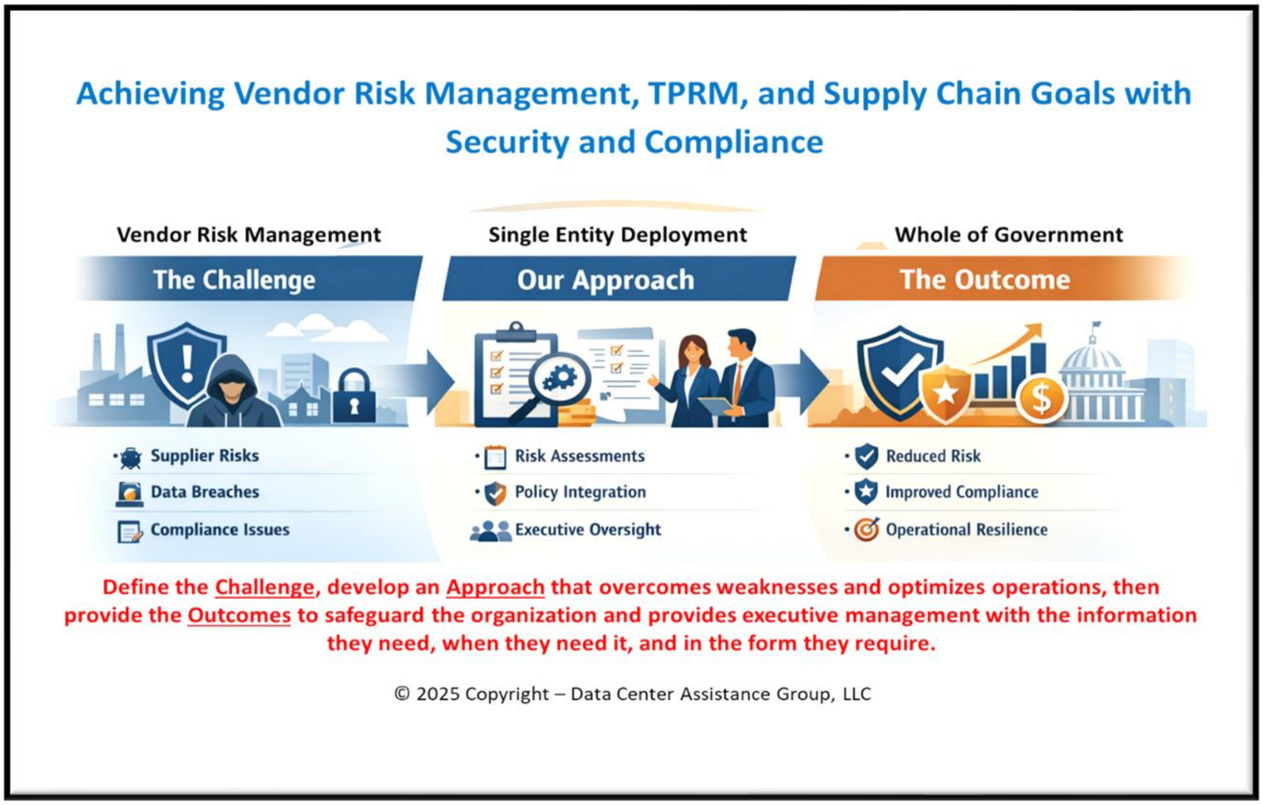
One-Sentence Board Takeaway

- If third-party, supply chain, cyber, resilience, and compliance risks are not managed as a single executive system, the organization is accepting preventable enterprise-level failure. Consider the use of an Application Factory (SecDevOps) with adjustable quality control gates to ensure adherence to security, compliance, and efficiency requirements (an all-in-one solution).

Resolving the problem

• Develop a Pilot System as Proof of Concept.

Achieving a Pilot environment that delivers Vendor Risk Management (VRM), Third-Part Risk Management (TPRM), Supply Chain Management (SCM), Business Continuity Management (BCM), Security, Compliance, Monitoring and Reporting support, and a maintenance system. Utilize monitoring and feedback loops to continuously optimize operations and reduce technical problems and cybercrimes.



Achieving Vendor Risk Management, TPRM, and Supply Chain Goals with Security and Compliance

Vendor Risk Management

The Challenge

- Supplier Risks
- Data Breaches
- Compliance Issues

Single Entity Deployment

Our Approach

- Risk Assessments
- Policy Integration
- Executive Oversight

Whole of Government

The Outcome

- Reduced Risk
- Improved Compliance
- Operational Resilience

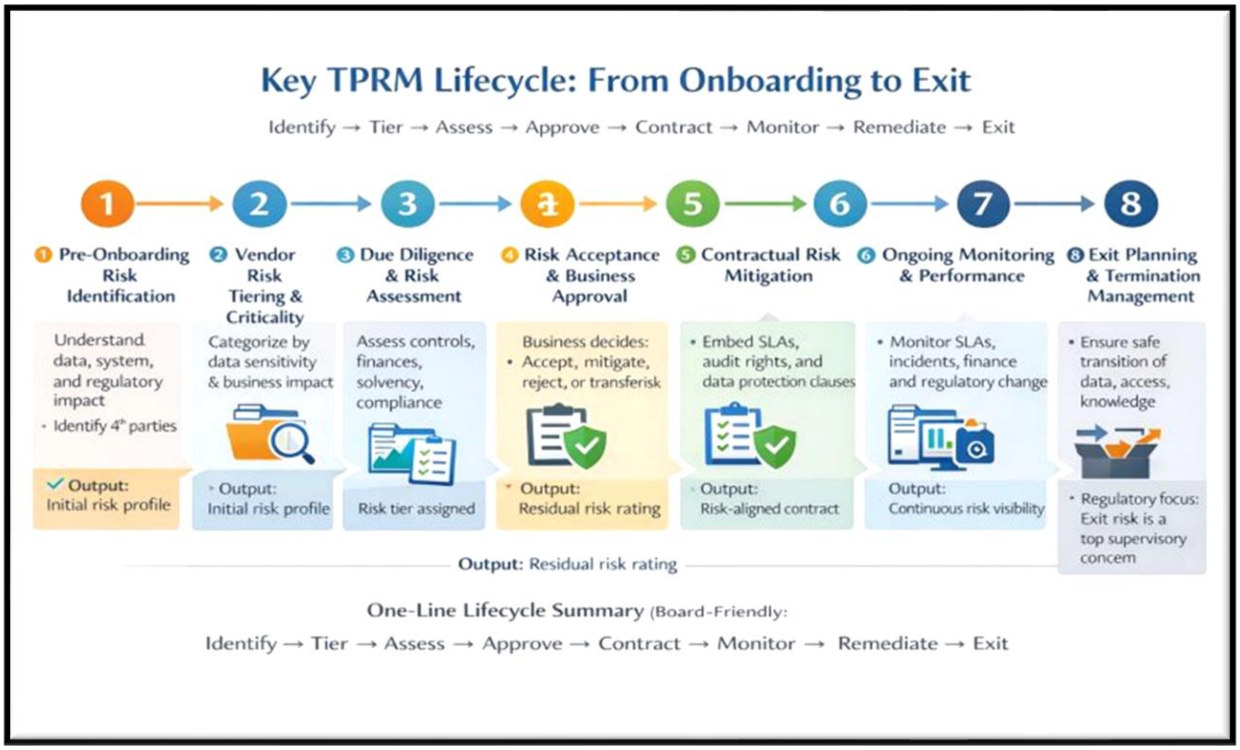
Define the Challenge, develop an Approach that overcomes weaknesses and optimizes operations, then provide the Outcomes to safeguard the organization and provides executive management with the information they need, when they need it, and in the form they require.

Figure 3: Creating a Pilot System for Proof of Concept

• POA&M for Pilot System

The pilot systems should be based on improvements to current operations, so the following should be completed.

1. **Management Direction Statement:** defining goals and objectives with funding and support -" Where do we want to be at the end of the project."
2. **Review the existing environment** – "Where we are today."
3. **Conduct a Needs Analysis** and produce a **Statement of Work** defining how to best go from where you are to where you want to be.
4. **Gain approval**, form a team, and conduct the project work, providing status reports and obstacles to overcome with action items to resolve issues.
5. **Formulate team and Conduct awareness and training sessions** as deemed necessary.
6. **Maintain schedule and costs**, requesting project changes, as necessary.
7. **Complete**, test, accept, deploy, support, and maintain product using an Executive Dashboard to monitor and report on product operations, weaknesses, and areas of improvement.
8. **Mitigate failures** (technical and cyber) and continuously improve operations.
9. **Roll-Out system** to other areas in priority order. Gains in efficiency should be realized as the team matures.



Key TPRM Lifecycle: From Onboarding to Exit

Identify → Tier → Assess → Approve → Contract → Monitor → Remediate → Exit

1 Pre-Onboarding Risk Identification
Understand data, system, and regulatory impact
- Identify 4th parties
✓ Output: Initial risk profile

2 Vendor Risk Tiering & Criticality
Categorize by data sensitivity & business impact
- Output: Initial risk profile

3 Due Diligence & Risk Assessment
Assess controls, finances, solvency, compliance
Risk tier assigned

4 Risk Acceptance & Business Approval
Business decides:
- Accept, mitigate, reject, or transferisk
- Output: Residual risk rating

5 Contractual Risk Mitigation
- Embed SLAs, audit rights, and data protection clauses
Output: Risk-aligned contract

6 Ongoing Monitoring & Performance
- Monitor SLAs, incidents, finance and regulatory change
Output: Continuous risk visibility

8 Exit Planning & Termination Management
- Ensure safe transition of data, access, knowledge
- Regulatory focus: Exit risk is a top supervisory concem

Output: Residual risk rating

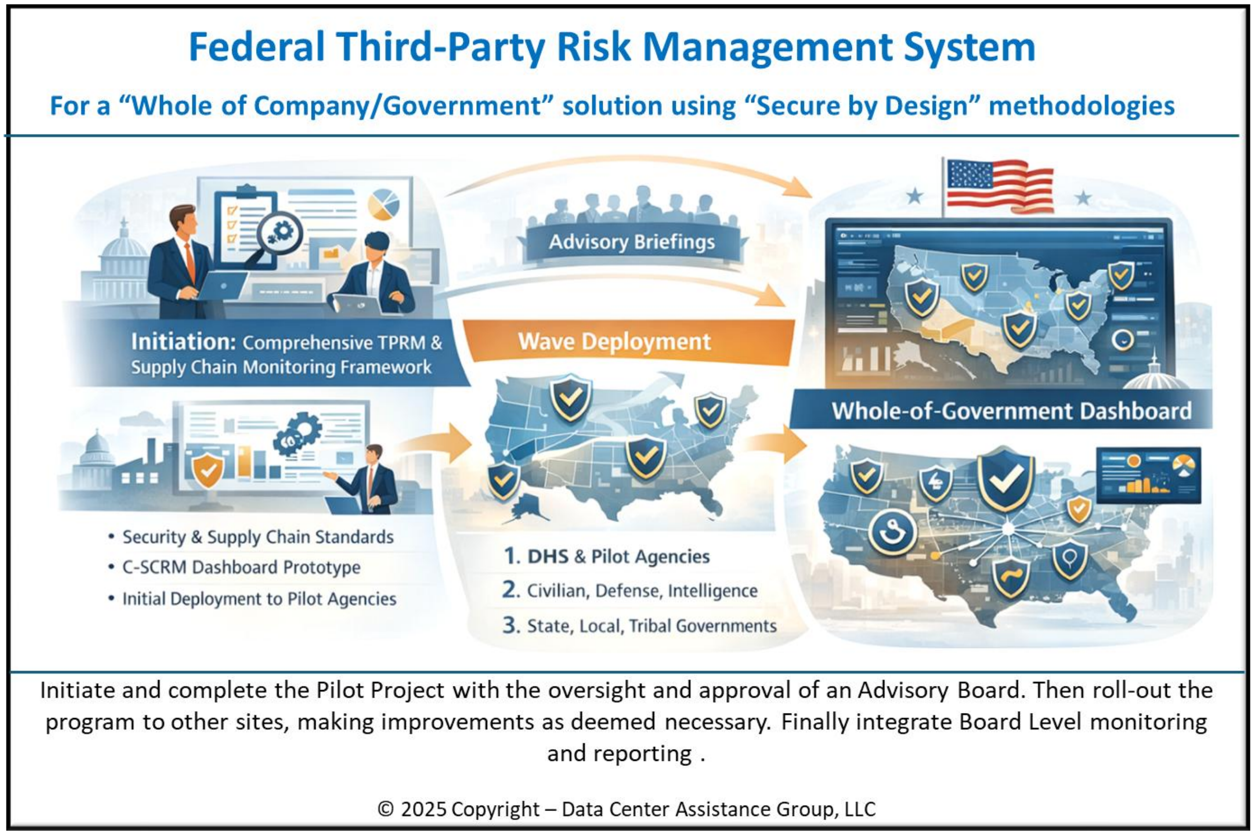
One-Line Lifecycle Summary (Board-Friendly:

Identify → Tier → Assess → Approve → Contract → Monitor → Remediate → Exit

Figure 4: TPRM Lifecycle and stages.

• Roll the Pilot System out to other locations.

Once the proof of concept has been accomplished through a well-documented pilot system, you can roll the system out to other locations as deemed necessary and in priority order. A wave approach to roll-out is recommended. Implementing these systems should be accomplished more quickly and with fewer delays because your team will be better aware of anticipated problems and well trained in system implementation. As the team’s experience increases, the amount of time to deploy is decreased and efficiency is improved.



Federal Third-Party Risk Management System

For a "Whole of Company/Government" solution using "Secure by Design" methodologies

Advisory Briefings
Initiation: Comprehensive TPRM & Supply Chain Monitoring Framework
Wave Deployment
Whole-of-Government Dashboard
• Security & Supply Chain Standards
• C-SCRM Dashboard Prototype
• Initial Deployment to Pilot Agencies
1. DHS & Pilot Agencies
2. Civilian, Defense, Intelligence
3. State, Local, Tribal Governments

Initiate and complete the Pilot Project with the oversight and approval of an Advisory Board. Then roll-out the program to other sites, making improvements as deemed necessary. Finally integrate Board Level monitoring and reporting .

© 2025 Copyright – Data Center Assistance Group, LLC

Figure 5: Rolling the Pilot System Out to other locations.

• The final product

After rolling the system out to all desired locations, your organizations will have achieved Vendor Risk and Third-Part Risk Management (TPRM), Supply Chain Management (SCM), Business Continuity Management (BCM), with adherence to all required Governance Risk and Compliance (GRC) requirements embedded in the process. Contracts with Service Level Agreements will be implemented and a metrics system of Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) that support monitoring and reporting to judge performance and operational issues will be utilized to construct an executive dashboard.

Now the problem arises of where and how to integrate this accomplishment into the everyday functions performed by personnel through systems development, deployment, and change cycles. That is where an Application Factory with adjustable quality control gates that ensures compliance with these systems.

• Continuous Monitoring, analysis, reporting, and mitigation

Once the C-SCRM system is initially implemented and during the roll-out period, the VRM system must continuously monitor vendor status via an executive dashboard, whose contents will be decided upon during this project. The purpose of the executive dashboard is to identify weaknesses in the Vendor Management System, TPRM, SCM, Problem and Incident management, and activation of recovery plans as required. The dashboard will direct activities and provide feedback so improvements can be made. This feedback loop will continue until no further improvements can be made and the system is optimized.

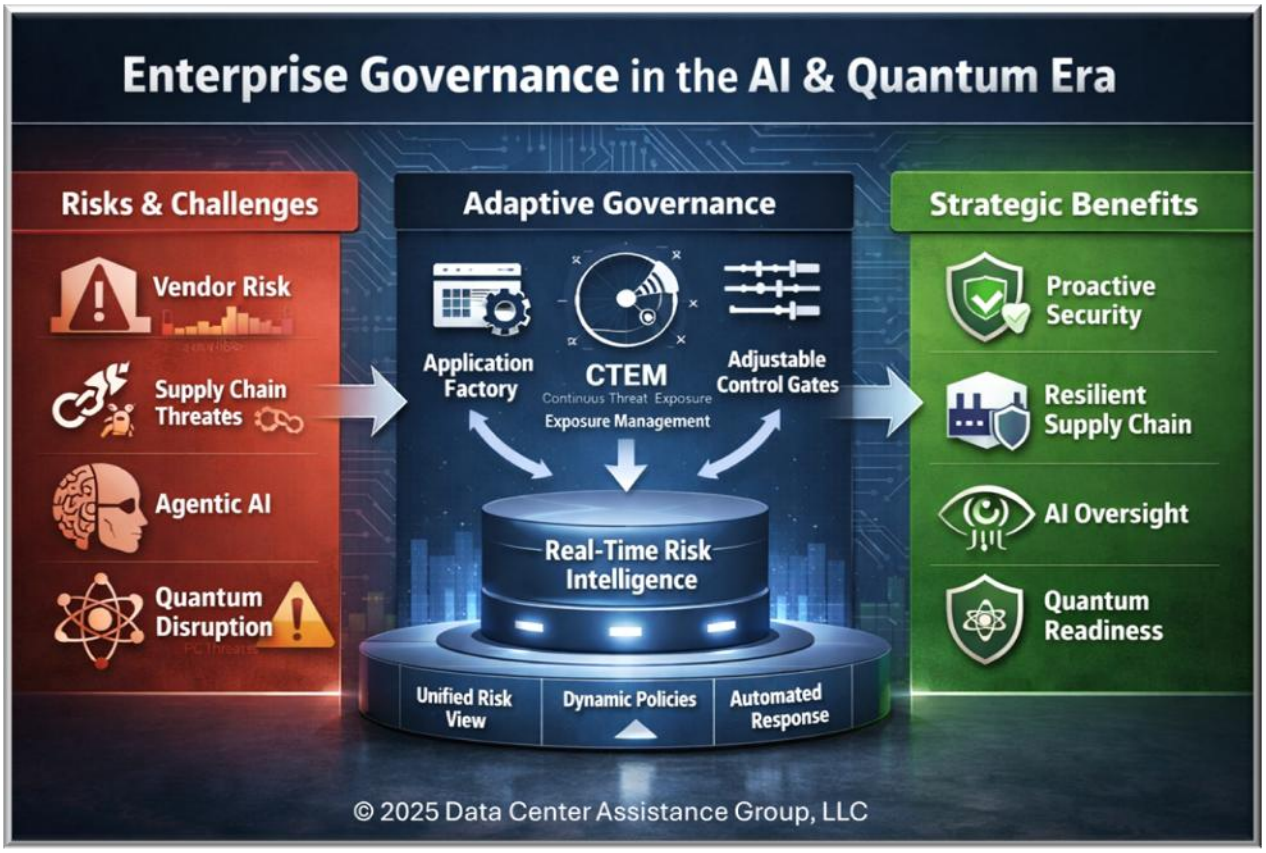


Figure 6: Fully implemented Vendor Risk Management System

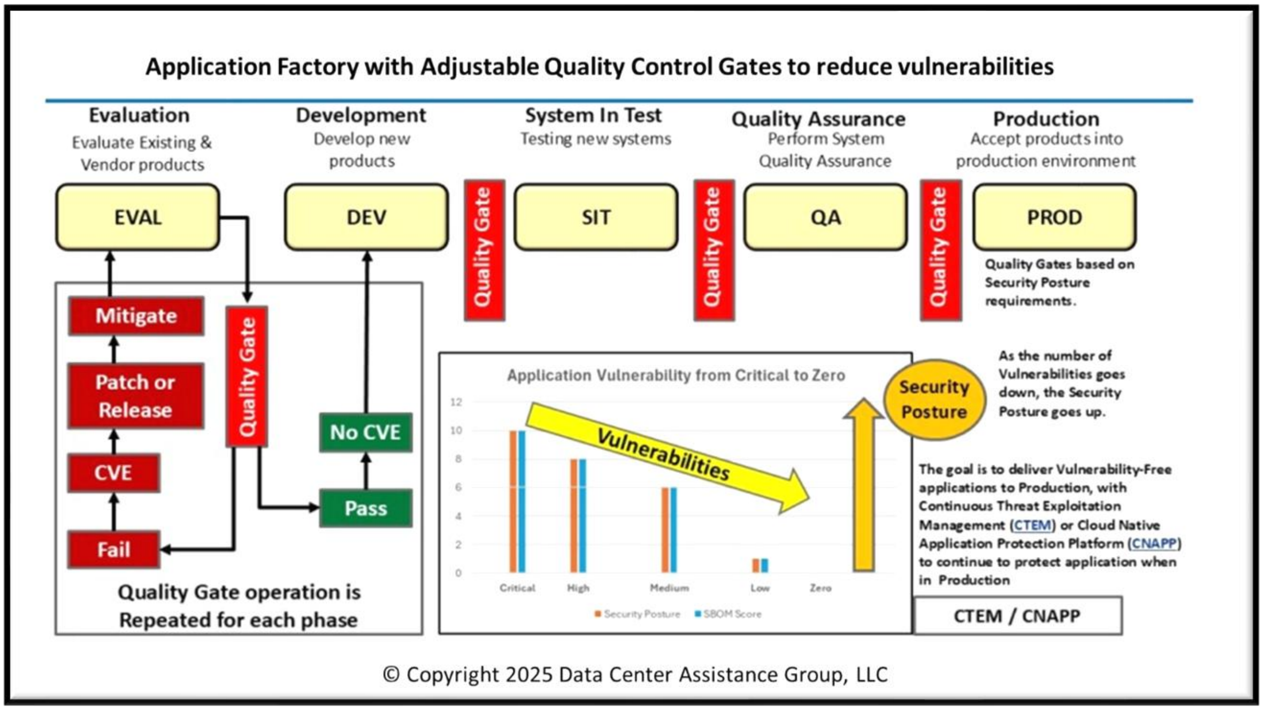
Remove Risks & Challenges concerning Vendor Risk Management by utilizing an Adaptive Governance control system through an Application Factory to achieve Strategic Benefits.

This illustration demonstrates how the project goals would be achieved in one location and then rolled out to all other locations in waves, with improvements and upgrades added as needed. In the end, a dashboard system will display vendor and supply chain activity and rate performance through metrics. Each location would generate a summary report on vendor and supply chain activity and forward the information to headquarters for analysis. Headquarters would then generate a “Whole of Company” report identifying and rating vendor and supply chain actions in a “Worse Case” report that identifies the most impactful problems in descending order from most impactful down. Supply chain problems can be rectified through alternate paths while poorly performing vendors can be replaced with vendors better suited to meet the needs of the company.

The Application Factory

Integration of the Vendor Risk Management system should be embedded into the systems development, deployment and change cycles within an Application Factory with adjustable quality control gates.

Before an application can be built, it needs resources to store data, process information, and deliver results to clients through network services. If implemented correctly, the adjustable quality control gates of the application factory will ensure you deliver products whose components are at current release levels and free of any vulnerabilities. Once implemented in production and an Authorization to Operate (ATO) received, Continuous Threat Exposure Management (CTEM) should be utilized to rapidly identify and mitigate problems before hackers can take advantage of vulnerabilities to attack your system. When achieved, your environment will achieve continuous Authorization to Operate (cATO), which is every production data center’s goal.


Application Factory with Adjustable Quality Control Gates to reduce vulnerabilities

Quality Gates based on Security Posture requirements.

As the number of Vulnerabilities goes down, the Security Posture goes up.

The goal is to deliver Vulnerability-Free applications to Production, with Continuous Threat Exploitation Management (CTEM) or Cloud Native Application Protection Platform (CNAPP) to continue to protect application when in Production

Quality Gate operation is Repeated for each phase

© Copyright 2025 Data Center Assistance Group, LLC

Figure 7: Application Factory with Quality Control Gates.

• Fully developed Application Factory

A fully implemented Application Factory controls the progression of ideas through brainstorming, collaboration, innovations, Requirements Transparency Matrix (RTM), architecture with vendor risk management, engineering, development, testing, quality assurance, acceptance, ATO, CTEM, and cATO.

This complete cycle for conceiving, building, deploying, and protecting business products and services orchestrates the production environment and can implement an executive dashboard that monitors and reports on status indicators needed to identify success and weaknesses that allow for rapid mitigation prior to impacting production business products and services provided to clients.

Completing VRM, TPRM, SCM, BCM, Security, and Compliance can be best controlled when utilizing “Whole of Nation” and “Secure by Design” guidelines produces by DHS/CISA and adhering to all domestic and international laws and regulations governing your business environment.

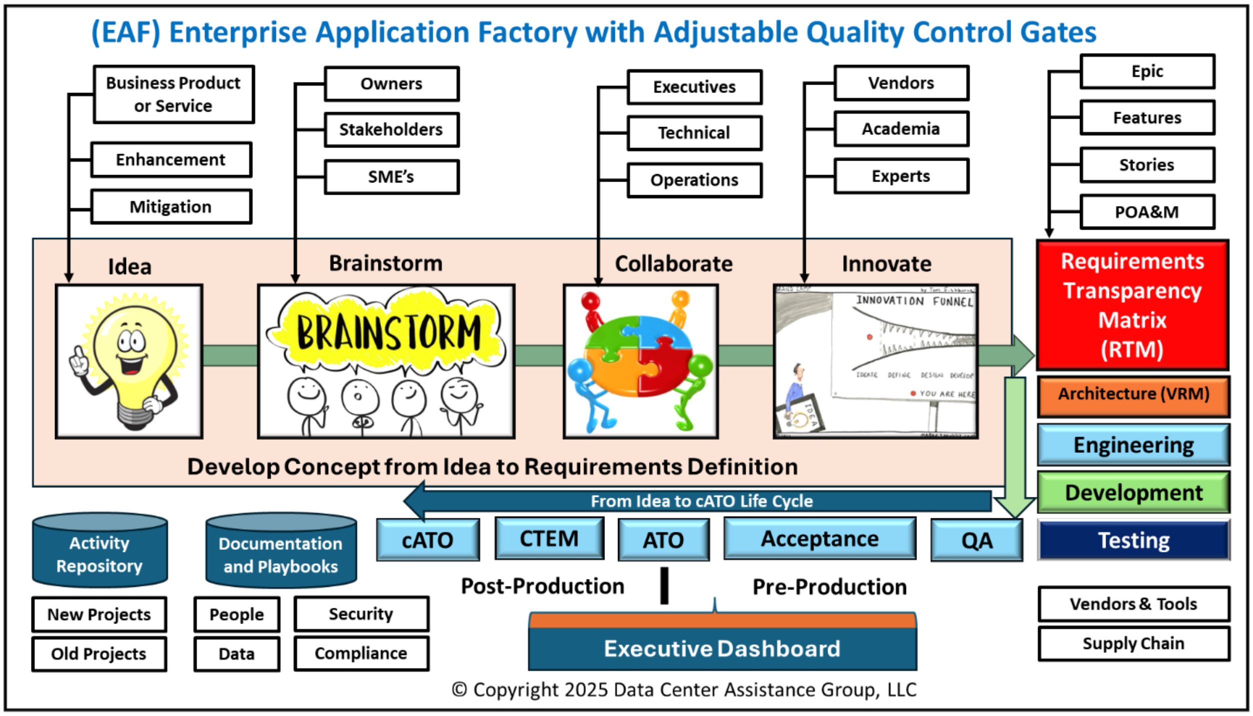
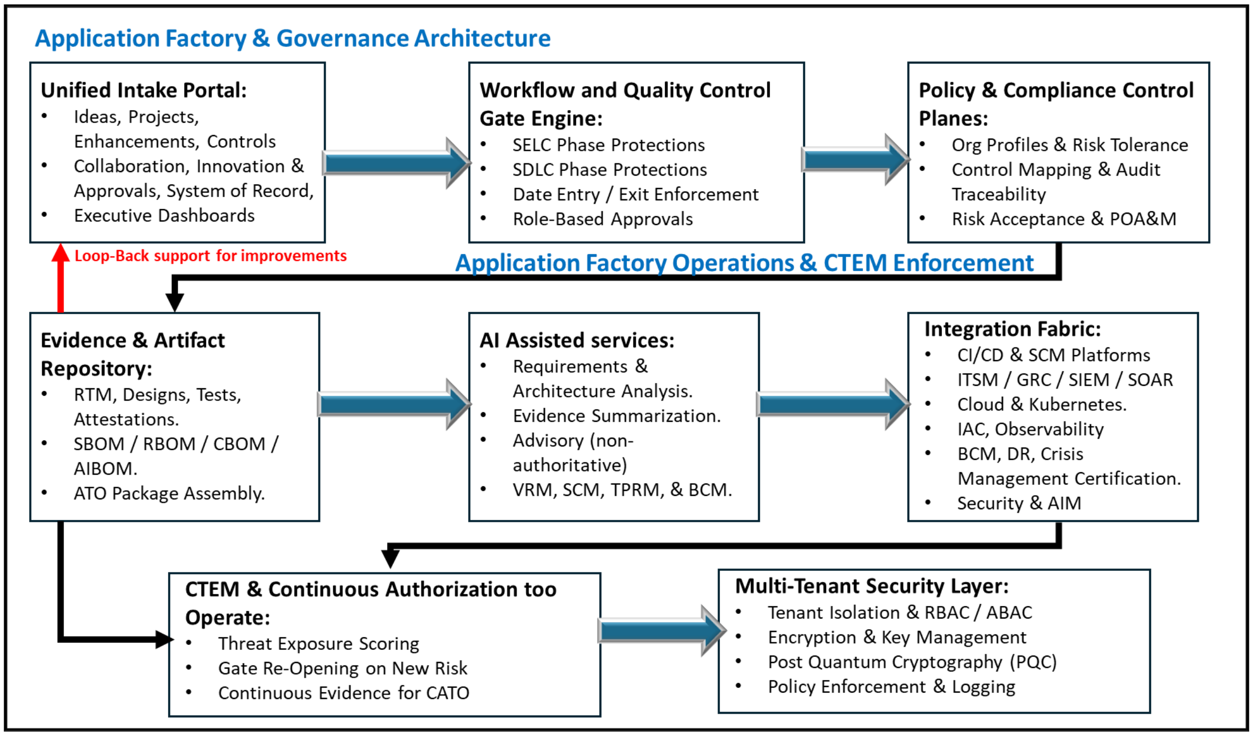


Figure 8: Fully implemented Application Factory with adjustable quality control gates.

• Application Factory Flow Chart, by step



Application Factory & Governance Architecture

Unified Intake Portal:
- Ideas, Projects, Enhancements, Controls
- Collaboration, Innovation & Approvals, System of Record,
- Executive Dashboards

Workflow and Quality Control Gate Engine:
- SELC Phase Protections
- SDLC Phase Protections
- Date Entry / Exit Enforcement
- Role-Based Approvals

Policy & Compliance Control Planes:
- Org Profiles & Risk Tolerance
- Control Mapping & Audit Traceability
- Risk Acceptance & POA&M

Loop-Back support for improvements

Application Factory Operations & CTEM Enforcement

Evidence & Artifact Repository:
- RTM, Designs, Tests, Attestations.
- SBOM / RBOM / CBOM / AIBOM.
- ATO Package Assembly.

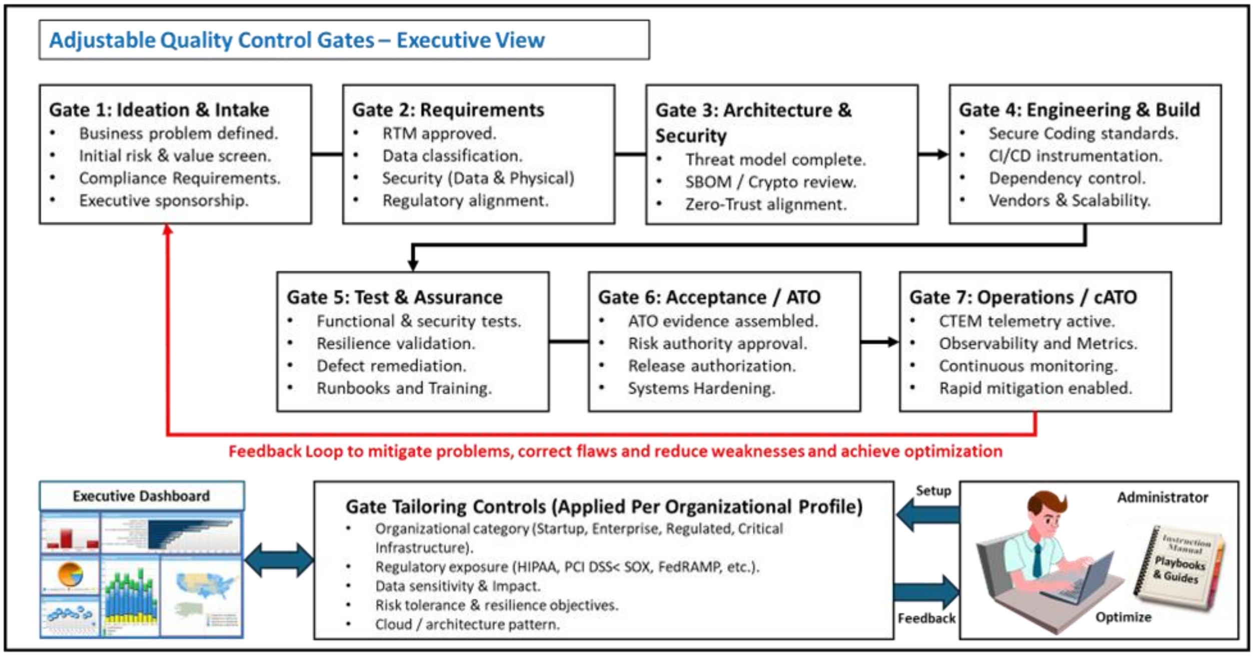
AI Assisted services:
- Requirements & Architecture Analysis.
- Evidence Summarization.
- Advisory (non-authoritative)
- VRM, SCM, TPRM, & BCM.

Integration Fabric:
- CI/CD & SCM Platforms
- ITSM / GRC / SIEM / SOAR
- Cloud & Kubernetes.
- IAC, Observability
- BCM, DR, Crisis Management Certification.
- Security & AIM

CTEM & Continuous Authorization too Operate:
- Threat Exposure Scoring
- Gate Re-Opening on New Risk
- Continuous Evidence for CATO

Multi-Tenant Security Layer:
- Tenant Isolation & RBAC / ABAC
- Encryption & Key Management
- Post Quantum Cryptography (PQC)
- Policy Enforcement & Logging

- ### Application Factory adjustable quality control gates



Adjustable Quality Control Gates – Executive View

Gate 1: Ideation & Intake
- Business problem defined.
- Initial risk & value screen.
- Compliance Requirements.
- Executive sponsorship.

Gate 2: Requirements
- RTM approved.
- Data classification.
- Security (Data & Physical)
- Regulatory alignment.

Gate 3: Architecture & Security
- Threat model complete.
- SBOM / Crypto review.
- Zero-Trust alignment.

Gate 4: Engineering & Build
- Secure Coding standards.
- CI/CD instrumentation.
- Dependency control.
- Vendors & Scalability.

Gate 5: Test & Assurance
- Functional & security tests.
- Resilience validation.
- Defect remediation.
- Runbooks and Training.

Gate 6: Acceptance / ATO
- ATO evidence assembled.
- Risk authority approval.
- Release authorization.
- Systems Hardening.

Gate 7: Operations / cATO
- CTEM telemetry active.
- Observability and Metrics.
- Continuous monitoring.
- Rapid mitigation enabled.

Feedback Loop to mitigate problems, correct flaws and reduce weaknesses and achieve optimization

Gate Tailoring Controls (Applied Per Organizational Profile)
- Organizational category (Startup, Enterprise, Regulated, Critical Infrastructure).
- Regulatory exposure (HIPAA, PCI DSS< SOX, FedRAMP, etc.).
- Data sensitivity & Impact.
- Risk tolerance & resilience objectives.
- Cloud / architecture pattern.

- ### Mindful Modernization, five step approach.

1. Align Vision and Organization.
2. Implement an Agile Phased Approach.
3. Manage Risks Proactively.
4. Foster Transparency and Stakeholder Engagement.
5. Encourage Continuous Learning and Improvement.

All five of these goals is achieved through the Application Factory with its adjustable quality control gates that ensure all precautions needed to validate and verify application development, support, and maintenance is achieved in an optimized manner.

Laws and Regulations governing Vendor Risk Management

- ### Domestic Laws & Regulations Governing Vendor Risk Management

Law / Regulation	Governing Body	Scope & Applicability	VRM / TPRM Implications
NIST SP 800-161 Rev. 1	NIST	Federal agencies & contractors	Primary federal standard for Cyber Supply Chain Risk Management (C-SCRM); requires supplier risk identification, monitoring, and mitigation
NIST SP 800-53 Rev. 5	NIST	Federal systems & regulated enterprises	Controls for third-party access, system interconnections, vendor monitoring, and continuous assessment

Law / Regulation	Governing Body	Scope & Applicability	VRM / TPRM Implications
FISMA	OMB / DHS / NIST	Federal agencies & contractors	Requires risk management across systems and vendors supporting federal information
Executive Order 14028	White House	Federal government & software suppliers	Mandates supply chain security, SBOMs, vendor accountability, and secure-by-design practices
FAR / DFARS	DoD / GSA	Federal procurement	Requires vendor cybersecurity controls, reporting, and contractual risk obligations
CMMC	DoD	Defense Industrial Base	Vendor and subcontractor cybersecurity maturity and ongoing compliance
FedRAMP	GSA / OMB	Cloud service providers	Continuous monitoring and risk management of cloud vendors used by government
SEC Cybersecurity Disclosure Rules (2023)	SEC	Public companies	Requires disclosure of material third-party cyber risks and governance oversight
GLBA	FTC / Federal Banking Regulators	Financial institutions	Requires oversight of service providers overseeing customer data
HIPAA / HITECH	HHS	Healthcare & business associates	Requires vendor safeguards for protected health information (PHI)
SOX	SEC	Public companies	Internal controls extend to outsourced and third-party services
NYDFS 23 NYCRR 500	NYDFS	Financial institutions (NY)	Explicit third-party cybersecurity risk management requirements
State Privacy Laws (CCPA/CPRA, etc.)	State Attorneys General	Companies overseeing personal data	Vendor due diligence, contractual controls, and ongoing monitoring

- ## International Laws & Regulations Governing Vendor Risk Management

Law / Regulation	Authorities	Scope & Applicability	VRM / TPRM Implications
GDPR	European Union	Any organization processing EU personal data	Requires vendor due diligence, data processing agreements, and continuous oversight
NIS2 Directive	European Union	Essential & important entities	Mandates supply chain and third-party cybersecurity risk management
DORA	European Union	Financial institutions	Requires ICT third-party risk management, testing, and reporting

Law / Regulation	Authorities	Scope & Applicability	VRM / TPRM Implications
ISO/IEC 27001 & 27036	International	Global standard	Supplier security controls and formal third-party risk governance
UK GDPR & UK NIS Regulations	United Kingdom	Data controllers & critical services	Vendor accountability and resilience requirements
APRA CPS 231 / CPS 234	Australia	Financial services	Outsourcing and third-party cyber risk governance
MAS TRM Guidelines	Singapore	Financial institutions	Vendor risk assessment, monitoring, and board accountability
PIPEDA	Canada	Organizations overseeing personal data	Requires vendor safeguards and accountability
PDPA	Singapore	Data processors & controllers	Vendor oversight and contractual obligations
Cybersecurity Law of the PRC	China	Operators of networked systems	Vendor security controls and supply chain accountability
Brazil LGPD	Brazil	Organizations processing personal data	Vendor due diligence and risk management
Japan APPI	Japan	Personal data handlers	Third-party data processing risk controls
South Africa POPIA	South Africa	Data controllers & processors	Vendor accountability and security safeguards
OECD Supply Chain Due Diligence Guidance	Multinational	Multinational enterprises	Ethical, operational, and risk governance expectations

- ### Executive Interpretation (Board-Level Takeaway)

Authorities and regulators are converging on **four non-negotiable expectations**:

1. You are accountable for your vendors' actions.
2. Risk must be continuously monitored—not assessed once.
3. Contracts must enforce security, resilience, and compliance.
4. Boards and executives are responsible for oversight.

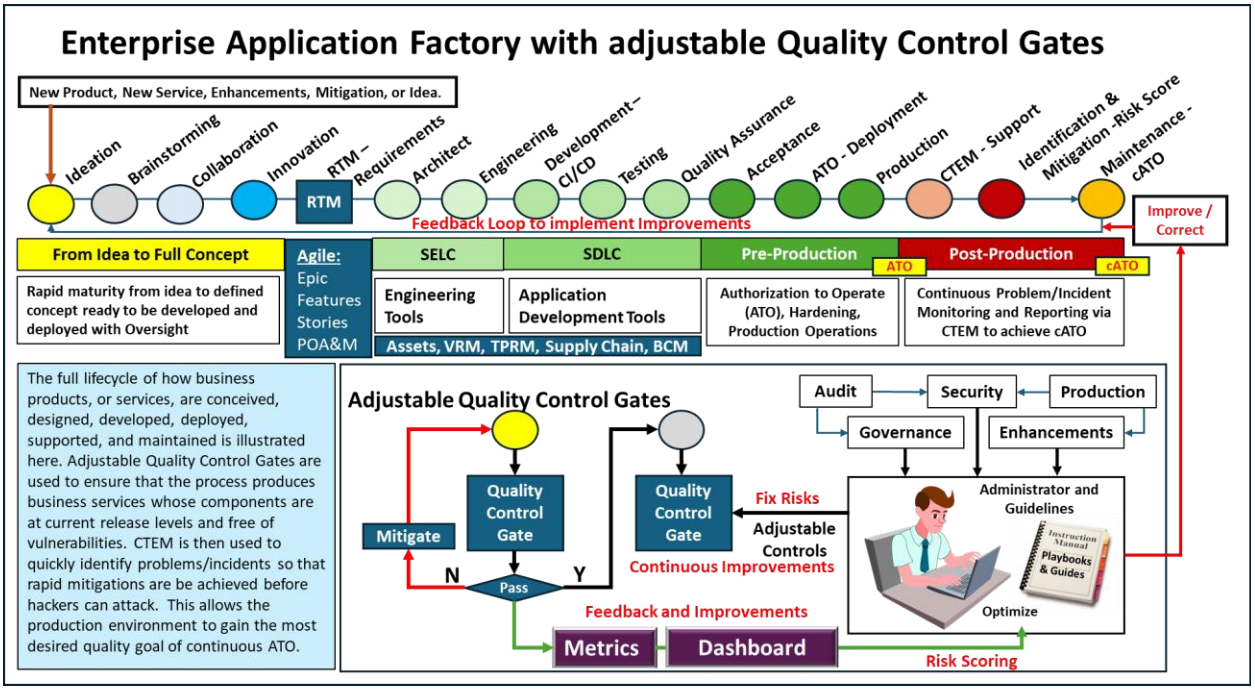
Failure to implement structured VRM / TPRM programs is now viewed as a **governance failure**, not an operational oversight. Board members will be deemed to lack their performance of due diligence and can be fined and sued (both the business and them personally).

Vendor Risk Management system and Application Factory relationship

The Vendor Risk Management system is part of the overall DevSecOps process being employed by IT Organizations today. To illustrate where Vendor Risk Management resides within the business product/service creation process, I have included an overview of the Application Factory with quality control gates concept I developed to enhance the DevSecOps process. This system provided continuous monitoring, reporting, and a feedback loop to implement continuous improvements or mitigate encountered technical problems and cybercrimes.

- ## Enterprise Application Factory,

with adjustable Quality Control Gates

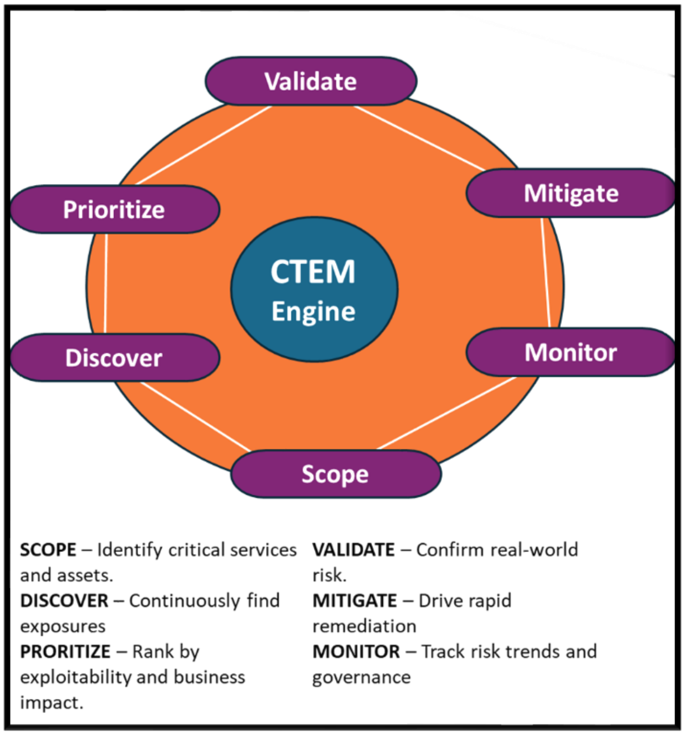

Enterprise Application Factory with adjustable Quality Control Gates
New Product, New Service, Enhancements, Mitigation, or Idea.
Ideation
Brainstorming
Collaboration
Innovation
RTM – Requirements
RTM
Architect
Engineering
Development – CI/CD
Testing
Quality Assurance
Acceptance
ATO - Deployment
Production
CTEM - Support
Identification & Mitigation -Risk Score
Maintenance - cATO
Feedback Loop to implement Improvements
Improve / Correct
From Idea to Full Concept
Agile:
Epic
Features
Stories
POA&M
SELC
SDLC
Pre-Production
Post-Production
ATO
cATO
Rapid maturity from idea to defined concept ready to be developed and deployed with Oversight
Engineering Tools
Application Development Tools
Assets, VRM, TPRM, Supply Chain, BCM
Authorization to Operate (ATO), Hardening, Production Operations
Continuous Problem/Incident Monitoring and Reporting via CTEM to achieve cATO
The full lifecycle of how business products, or services, are conceived, designed, developed, deployed, supported, and maintained is illustrated here. Adjustable Quality Control Gates are used to ensure that the process produces business services whose components are at current release levels and free of vulnerabilities. CTEM is then used to quickly identify problems/incidents so that rapid mitigations are be achieved before hackers can attack. This allows the production environment to gain the most desired quality goal of continuous ATO.
Adjustable Quality Control Gates
Quality Control Gate
Mitigate
N
Pass
Y
Quality Control Gate
Fix Risks
Adjustable Controls
Continuous Improvements
Audit
Security
Production
Governance
Enhancements
Administrator and Guidelines
Instruction Manual
Playbooks & Guides
Optimize
Feedback and Improvements
Metrics
Dashboard
Risk Scoring

The Enterprise Application Factory was designed with DevSecOps in mind, but includes a user-friendly interface that best helps build designs from a range of inputs (New Product, New Service, Enhancement, Mitigation, etc.):

1. **Supervised advancements** and improvements through controlled process including:
    a. Ideas that have been approved through supervisory board for investigation,
    b. Brainstorming,
    c. Collaboration, and
    d. Innovation under supervisory control, to produce a secure and compliant framework.
2. **Requirements Transparency Matrix (RTM)** used to define Agile Epics, Features, Stories, and Tasks (like Asset Management, Third-Party Risk Management, Supply Chain Management, Business Continuity Management, Security, and Compliance) ready to be satisfied through the,
3. **Engineering phase** including:
    a. Architecture design (i.e., TOGAF, etc.), and
    b. Engineering phase (Systems Engineering Life Cycle - SELC),
4. **Development phase** (Systems Development Life Cycle – SDLC), including Testing, Quality Assurance, and

5. **Production Acceptance** of business products or services whose components are all at current release level and free of vulnerabilities. This supports the Authorization to Operate (ATO) approval function with device Hardening to optimize protections,
6. **Support and Maintenance** through Continuous Threat Exposure Management (**CTEM**), Identification and Mitigation of detected problems before hackers can attack, then the achievement of continuous ATO (cATO) can be approved, which is the goal of every organization's production environment.
7. **Executive Dashboard** fed through system metrics displaying actions and status of products and services, being created, in operations, and being supported, so that continuous improvements through mitigations and enhancement can optimize the creation, operation, and support provided to the company clients in a continuous manner that is constantly being optimized in response to environmental sensing and technology change evolutions.

CTEM (CONTINUOUS THREAT EXPOSURE MANAGEMENT) – EXECUTIVE DEFINITION



SCOPE – Identify critical services and assets.
DISCOVER – Continuously find exposures
PRORITIZE – Rank by exploitability and business impact.
VALIDATE – Confirm real-world risk.
MITIGATE – Drive rapid remediation
MONITOR – Track risk trends and governance

Continuous Threat Exposure Management (CTEM) is a **systematic, business-aligned process** used to **continuously identify, prioritize, validate, and mitigate cyber risk** based on *real exploitability and business impact* — not theoretical vulnerability scores.

CTEM shifts security from **periodic scanning** to **continuous risk governance**.

How to read this visual (for executives)

CTEM is shown as a continuous engine, not a tool.

At the center:

CTEM ENGINE
This reinforces governance, not scanning.

Around the loop:

SCOPE, DISCOVERY, PRIORITIZE, VALIDATE, MITIGATE, MONITOR. The arrows show:

CTEM never stops — it learns and adjusts.

Why this works

Circular motion = **continuous process**

No technical clutter

Executives can explain it without notes.

Aligns directly to **cATO.**

Reinforces **risk governance vs. vulnerability scanning.**

• CTEM PROCESS MODEL

CTEM operates as a **continuous loop**, not a linear program:

1. SCOPE

Define what matters to the business.

- Identify critical business services.
- Map:
  - Applications
  - Data flows
  - Dependencies
  - Third parties
- Align exposure management to:
  - Revenue
  - Safety
  - Regulatory obligations

Executive value:
Security effort is aligned to business priorities, not tool outputs.

2. DISCOVER

Continuously identify exposures.

Includes:

- Vulnerabilities (CVE, KEV, zero-days)
- Misconfigurations
- Identity weaknesses
- Cloud & API exposures
- Supply chain risk (SBOM, CBOM)
- Data exposure
- Shadow IT

Sources:

- Scanners
- EDR/XDR
- Cloud posture tools
- Threat intelligence
- SBOM monitoring

Executive value:
You know what is exposed right now — not last quarter.

3. PRIORITIZE

Determine what truly matters.

Instead of CVSS alone, prioritize by:

- Exploitability (active exploitation)
- Asset criticality
- Data sensitivity
- Regulatory impact
- Business disruption potential
- Lateral movement risk

This creates a risk-based exposure score.

Executive value:
Teams fix what threatens the business — not what scores highest.

4. VALIDATE

Confirm real-world risk.

- Pen testing
- Red team simulation
- Attack path modeling.
- Exploit verification
- Control effectiveness testing.

This prevents:

- False positives
- Noise-driven remediation

Executive value:
You only spend money fixing real risk.

5. MOBILIZE (MITIGATE)

Drive rapid remediation.

Actions include:

- Patching
- Configuration hardening
- Access restriction
- Architecture changes
- Compensation controls
- Temporary containment

This phrase:

- Re-opens Application Factory gates if needed.
- Triggers engineering change requests
- Updates ATO evidence

Executive value:
Security becomes operationally effective, not advisory.

6. MONITOR & GOVERN

Sustain continuous protection.

Track:

- SLA to remediate.
- Risk trend lines.
- Repeat exposures.

Update:

- Risk posture
- Board dashboards
- Compliance evidence

Feeds directly into:

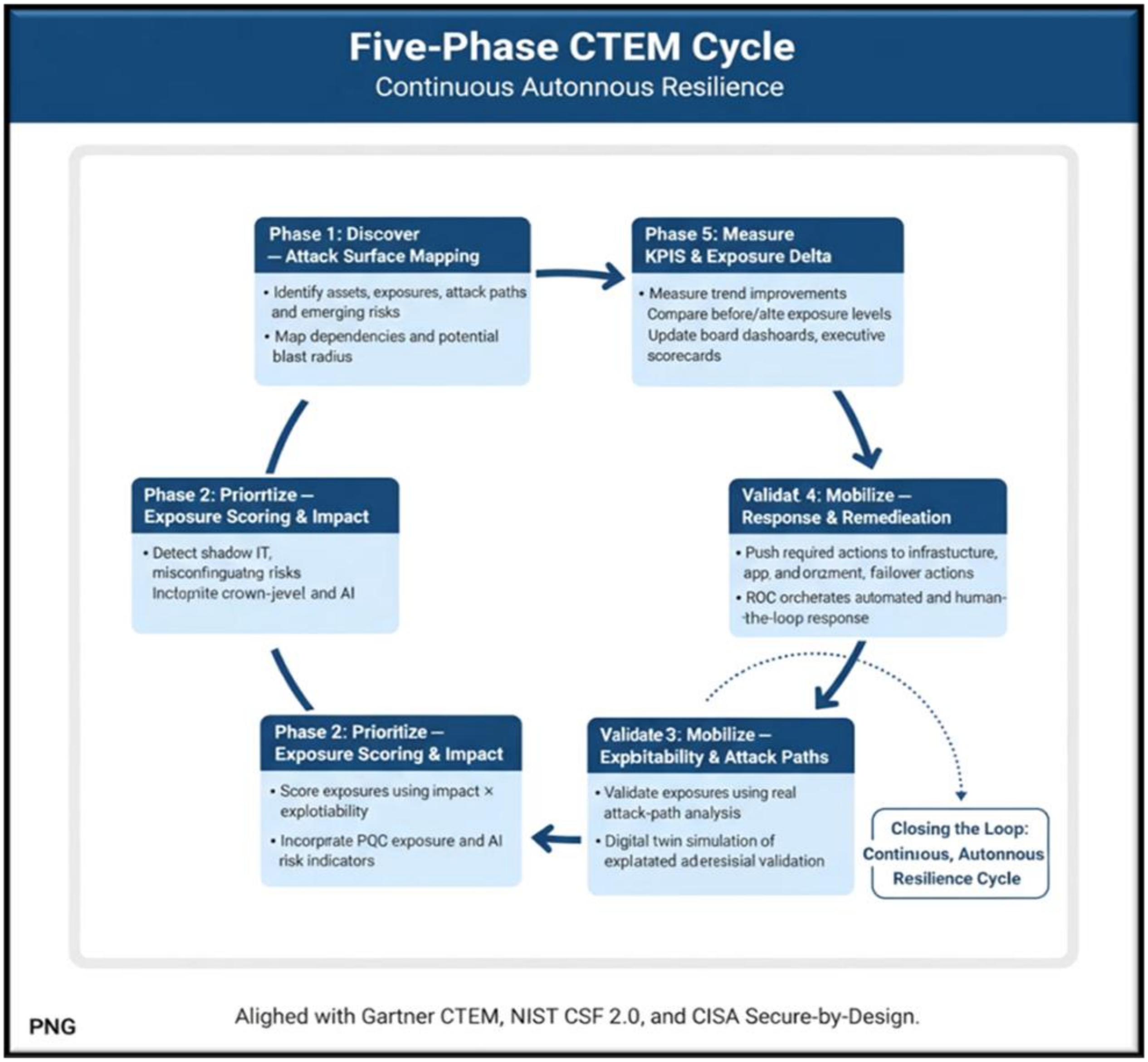
- cATO
- Audit readiness
- Board reporting

Executive value:
You see risk trending, not isolated events.

CTEM LIFECYCLE VISUAL

SCOPE → DISCOVER → PRIORITIZE → VALIDATE → MITIGATE → MONITOR ->.↺ (Continuous loop)

The CTEM Five-Phase Cycle



Five-Phase CTEM Cycle

Continuous Autonnous Resilience

Phase 1: Discover — Attack Surface Mapping

- Identify assets, exposures, attack paths and emerging risks
- Map dependencies and potential blast radius

Phase 5: Measure KPIS & Exposure Delta

- Measure trend improvements Compare before/alte exposure levels Update board dashoards, executive scorecards

Validat 4: Mobilize — Response & Remedieation

- Push required actions to infrastucture, app, and orzment, failover actions
- ROC orchetates automated and human--the-loop response

Validate 3: Mobilize — Expbitability & Attack Paths

- Validate exposures using real attack-path analysis
- Digital twin simulation of explatated aderesisial validation

Phase 2: Prioritize — Exposure Scoring & Impact

- Score exposures using impact × explotiability
- Incorprate PQC exposure and AI risk indicators

Phase 2: Priorrtize — Exposure Scoring & Impact

- Detect shadow IT, misconfinguatng risks Inctopite crown-jevel and AI

Closing the Loop: Continıous, Autonnous Resilience Cycle

PNG

Alighed with Gartner CTEM, NIST CSF 2.0, and CISA Secure-by-Design.

WHY CTEM IS DIFFERENT FROM TRADITIONAL VULNERABILITY MANAGEMENT

Traditional VM	CTEM
Periodic scans	Continuous discovery
CVSS driven	Business risk driven
Tool-centric	Process & governance driven
Patch-focused	Risk mitigation focused
Technical	Business-aligned
Reactive	Proactive

CTEM IN YOUR APPLICATION FACTORY MODEL

CTEM is the enforcement engine for:

- Continuous ATO (cATO)
- Gate re-opening
- Engineering change control
- Regulatory assurance
- Board-level risk governance.

Key concept:

> CTEM does not “find problems.”
> CTEM governs risk.

EXECUTIVE ONE-LINER

CTEM ensures authorization never goes stale by continuously measuring real-world threat exposure and forcing remediation before risk becomes a business incident.

Call to Action

Should you find this approach interesting and want to explore how you can achieve it, please contact us to discuss how we can assist you achieve this goal.

Thomas Bronack, President
Data Center Assistance Group, LLC
bronackt@dcag.com | bronackt@gmail.com } www.dcag.com | (917) 673-6992

Appendices:

• Government Bodies Defining C-SCRM (U.S.)

1. National Institute of Standards and Technology (**NIST)**

- **Primary Federal Authority** on C-SCRM guidance. NIST develops the foundational standards and frameworks used by federal agencies and industry for Cyber Supply Chain Risk Management.
- **NIST's Cybersecurity Supply Chain Risk Management program** produces guidance documents such as *SP 800-161*, related special publications, and best practice references that define C-SCRM practices across the lifecycle of systems, products, and services.

2. Federal Acquisition Security Council (**FASC**)

- Created by the **Federal Acquisition Supply Chain Security Act** (FASCSA).
- This **interagency council** coordinates supply chain risk priorities government-wide and integrates policy with acquisition risk objectives for federal executive agencies. It helps harmonize C-SCRM implementation across agencies.

3. Office of Management and Budget (**OMB**) & Executive Office of the President

- Through executive orders and policy guidance (e.g., **Executive Order 14028** on Improving the Nation's Cybersecurity), the OMB and White House set priorities and expectations for supply chain security and secure software practices across all federal civilian agencies — which directly influence C-SCRM strategy and implementation.

4. **Cybersecurity and Infrastructure Security Agency (CISA)**

- Provides operational guidance and implementation support for federal and critical infrastructure C-SCRM efforts.
- While not a standards author, CISA translates policy into practice and drives coordination with the private sector on threats that arise through supply chain compromise.

• Working Groups and Collaborative Forums

1. Federal C-SCRM Forum (NIST Hosted)

- An ongoing government-industry collaborative forum where federal agencies, industry partners, and academic experts share insights, best practices, and updates related to supply chain risk.
- It supports the dissemination and evolution of C-SCRM practices and offers a common place to align implementation on scale.

2. Interagency Bodies Supporting C-SCRM

- FASC Working Groups: Within the Federal Acquisition Security Council, various working groups bring together representatives from DoD, DHS, OMB, GSA, and others to align federal acquisition and supply chain risk approaches. This is part of the FASCSA implementation ecosystem.

3. Cross-Agency and Public-Private Collaboration

Although not formal *government law-making bodies*, use collaborative mechanisms support C-SCRM coordination:

- National Cybersecurity Center of Excellence (NCCoE) (NIST) — brings public-private teams together to prototype and publish example solutions that address complex cybersecurity problems, including supply chain concerns.
- Sector-Specific Information Sharing and Analysis Centers (ISACs) — support sharing of supply chain risks and threat intelligence between government and private sector critical infrastructure sectors (electricity, finance, defense, etc.).
- Global Research/Standards Bodies (e.g., CSA, ISO) — while outside direct government authority, these organizations provide interoperable frameworks that influence federal expectations via NIST and OMB guidance.

• How These Bodies Work Together

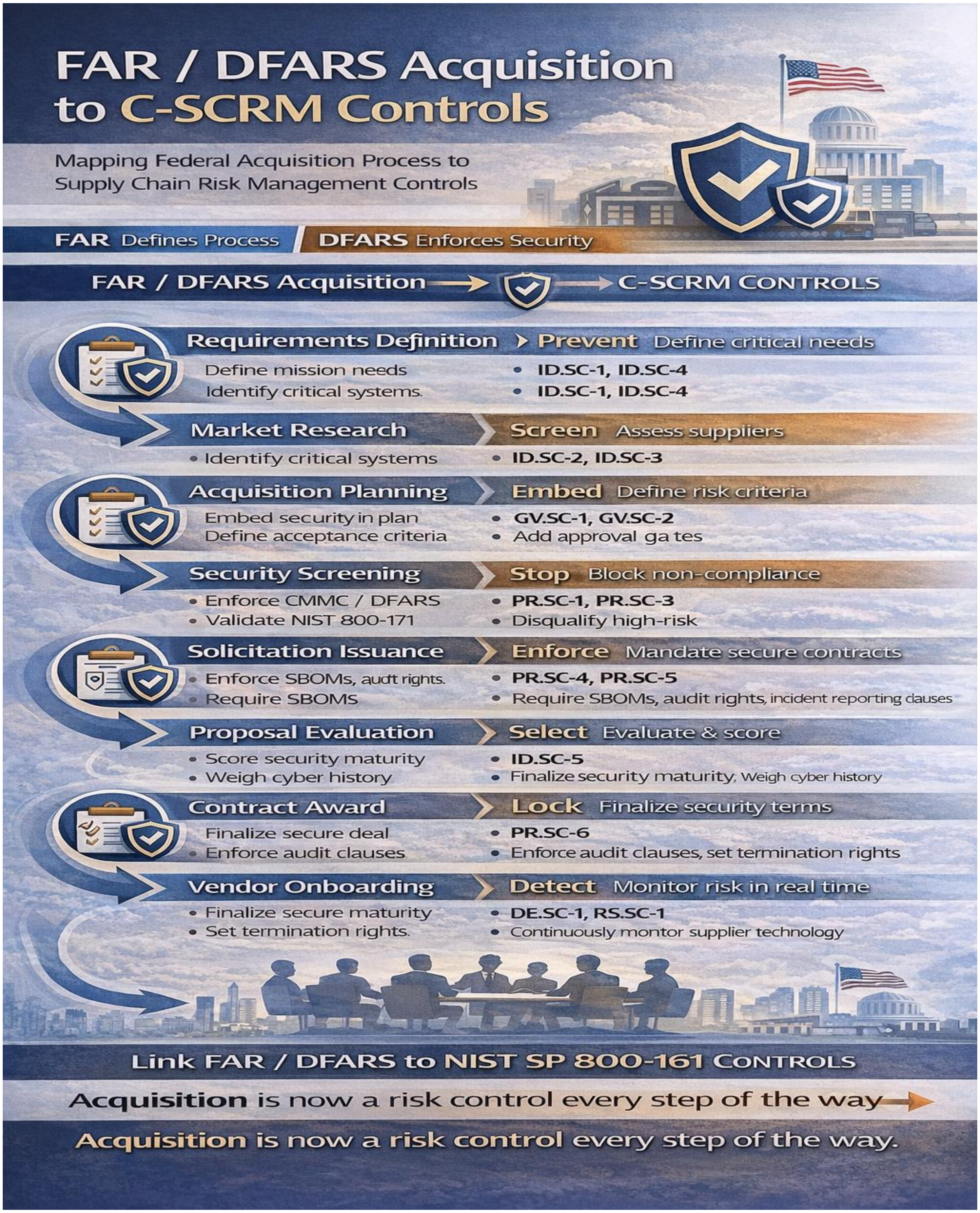
Role / Activity	Responsible Group(s)
Standards & Definitions	NIST (SP 800-161, supplemental publications)
Government-wide Policy & Mandates	White House / OMB (Executive Orders)
Acquisition Security Oversight	Federal Acquisition Security Council (FASC)
Operational Implementation Support	CISA & agency CISO/CFO teams
Cross-agency Coordination	Federal C-SCRM Forum; ISACs
Public-Private Best Practice Development	NCCoE; industry bodies (CSA, standards consortia)

• Executive Synopsis of Governing bodies working together.

C-SCRM in the U.S. is defined by a combination of standards, policy mandates, and interagency coordination:

- **NIST** provides the technical and lifecycle frameworks that shape how organizations manage supply chain cyber risk.
- **FASC** ensures that federal acquisition and procurement integrate those risk priorities enterprise wide.
- **OMB** and executive orders set the strategic national priorities that drive adoption at agency and contractor levels.
- **Collaborative forums and working groups** ensure the approach evolves as threats and best practices change — bringing together government and private sector stakeholders to align strategy and execution.

- ## Infographic - Navigating DAR/DFARS to C-SCRM Controls



FAR / DFARS Acquisition to C-SCRM Controls

Mapping Federal Acquisition Process to Supply Chain Risk Management Controls

FAR Defines Process / **DFARS** Enforces Security

FAR / DFARS Acquisition → C-SCRM CONTROLS

Requirements Definition › **Prevent** Define critical needs
Define mission needs
Identify critical systems.
- ID.SC-1, ID.SC-4
- ID.SC-1, ID.SC-4

Market Research › **Screen** Assess suppliers
- Identify critical systems
- ID.SC-2, ID.SC-3

Acquisition Planning › **Embed** Define risk criteria
Embed security in plan
Define acceptance criteria
- GV.SC-1, GV.SC-2
- Add approval ga tes

Security Screening › **Stop** Block non-compliance
- Enforce CMMC / DFARS
- Validate NIST 800-171
- PR.SC-1, PR.SC-3
- Disqualify high-risk

Solicitation Issuance › **Enforce** Mandate secure contracts
- Enforce SBOMs, audt rights.
- Require SBOMS
- PR.SC-4, PR.SC-5
- Require SBOMs, audit rights, incident reporting dauses

Proposal Evaluation › **Select** Evaluate & score
- Score security maturity
- Weigh cyber history
- ID.SC-5
- Finalize security maturity; Weigh cyber history

Contract Award › **Lock** Finalize security terms
Finalize secure deal
- Enforce audit clauses
- PR.SC-6
- Enforce audit clauses, set termination rights

Vendor Onboarding › **Detect** Monitor risk in real time
- Finalize secure maturity
- Set termination rights.
- DE.SC-1, RS.SC-1
- Continuously montor supplier technology

Link FAR / DFARS to NIST SP 800-161 CONTROLS

Acquisition is now a risk control every step of the way →

Acquisition is now a risk control every step of the way.

• Cyber Supply Chain Risk Management (C-SCRM)

Acquisition Policy & Operational Playbook

(FAR / DFARS Aligned)

1. Purpose

This policy establishes mandatory governance and operational controls for managing cybersecurity risks introduced through suppliers, vendors, integrators, and service providers across the federal acquisition lifecycle.

C-SCRM is embedded directly into FAR and DFARS acquisition processes to ensure that:

- Risk is prevented before purchase.
- Security is contractually enforced.
- Suppliers are continuously monitored.
- Executive oversight is maintained.

2. Scope

This policy applies to:

- All acquisitions involve IT, OT, cloud services, software, hardware, and managed services.
- All prime contractors and subcontractors
- All systems process federal data (CUI, FOUO, mission data)
- All program offices and contracting activities

3. Governance Model

Role	Responsibilities
Executive Sponsor	Risk acceptance authority
CISO	Cyber risk oversight
Contracting Officer	FAR/DFARS enforcement
Program Manager	Mission risk ownership
Legal	Contract language
Security Team	Technical validation
Risk Committee	Escalation authority

4. Acquisition Lifecycle Playbook

Phase 1 – Requirements Definition

C-SCRM Objective: PREVENT

Policy Requirements

- Mission criticality classification required.
- Data sensitivity identified (CUI, ITAR, etc.)
- Minimum supplier security baseline defined.

Operational Actions

- Identify critical systems.
- Define acceptable supplier risk.
- Establish security requirements upfront.

Artifacts

- System categorization
- Risk tolerance statement.
- Security requirements matrix

Phase 2 – Market Research (FAR 10)

C-SCRM Objective: SCREEN

Policy Requirements

- Supplier background checks mandatory
- Country-of-origin analysis required.
- FASC prohibited vendors from being blocked.

Operational Actions

- Screen Section 889 vendors
- Review ownership structure.
- Analyze geopolitical exposure.

Artifacts

- Market research report
- Supplier risk profiles
- Screening evidence

Phase 3 – Acquisition Planning (FAR 7)

C-SCRM Objective: EMBED

Policy Requirements

- Security weighting in evaluation criteria
- Executive risk rates defined.
- Mandatory DFARS clauses selected.

Operational Actions

- Define risk acceptance thresholds.
- Identify approval checkpoints.
- Integrate security into scoring.

Artifacts

- Acquisition Plan
- Risk governance workflow.
- Evaluation scorecard

Phase 4 – Security & Compliance Screening

C-SCRM Objective: STOP

Policy Requirements

- DFARS 7012/7020/7021 enforced
- CMMC validation required
- NIST 800-171 evidence verified.

Operational Actions

- Validate SSPs & POA&Ms
- Confirm certification status.
- Disqualify non-compliant vendors.

Artifacts

- Compliance attestation
- CMMC evidence
- Risk acceptance memo.

Phase 5 – Solicitation Issuance

C-SCRM Objective: ENFORCE

Policy Requirements

- Security clauses mandatory
- SBOM requirements included
- Audit rights enforced

Operational Actions

- Embed incident reporting SLAs.
- Require vulnerability disclosure.
- Include termination clauses.

Artifacts

- RFP language
- Contract clause library.
- Supplier obligations matrix

Phase 6 – Proposal Evaluation

C-SCRM Objective: SELECT

Policy Requirements

- Cyber posture scored
- Risk-adjusted pricing applied.
- High-risk bids escalated

Operational Actions

- Score security maturity.
- Review of breach history
- Apply risk weighting.

Artifacts

- Evaluation results
- Risk scoring worksheet.
- Source selection decision.

Phase 7 – Contract Award

C-SCRM Objective: LOCK

Policy Requirements

- Security obligations contractually binding.
- Audit & termination rights enforced.

Operational Actions

- Finalize compliance clauses.
- Define SLA penalties.
- Obtain executive signoff.

Artifacts

- Executed contract.
- Compliance appendix
- Governance approval

Phase 8 – Vendor Onboarding

C-SCRM Objective: VERIFY

Policy Requirements

- Integrity validation required
- Secure configuration enforced

Operational Actions

- Validate firmware integrity.
- Conduct security testing.
- Apply Zero Trust controls.

Artifacts

- Acceptance testing report
- Configuration baseline
- Risk acceptance record.

Phase 9 – Deployment & Continuous Monitoring

C-SCRM Objective: DETECT

Policy Requirements

- Continuous monitoring mandatory
- Threat intelligence integration required.

Operational Actions

- Monitor CVEs
- Track supplier advisories.
- Integrate CTEM

Artifacts

- Risk dashboards
- Incident reports
- Vendor scorecards

Phase 10 – Contract Closeout & Offboarding

C-SCRM Objective: ELIMINATE

Policy Requirements

- Data destruction verified
- Access revoked

Operational Actions

- Revoke credentials
- Confirm data return/destruction.
- Update supplier risk profile.

Artifacts

- Closeout report
- Lessons learned
- Risk model updates.

5. Metrics & Reporting

Mandatory executive KPIs:

- % of suppliers risk-assessed
- # of high-risk suppliers
- Mean time to remediate.
- # of DFARS non-compliance events
- # of supply chain incidents

6. Enforcement

Non-compliance results in:

- Procurement suspension
- Contract termination
- Executive escalation
- Regulatory reporting

7. Continuous Improvement

Annual reviews required:

- Threat landscape updates
- Policy updates
- Training refresh
- Technology assessment

8. Executive Summary

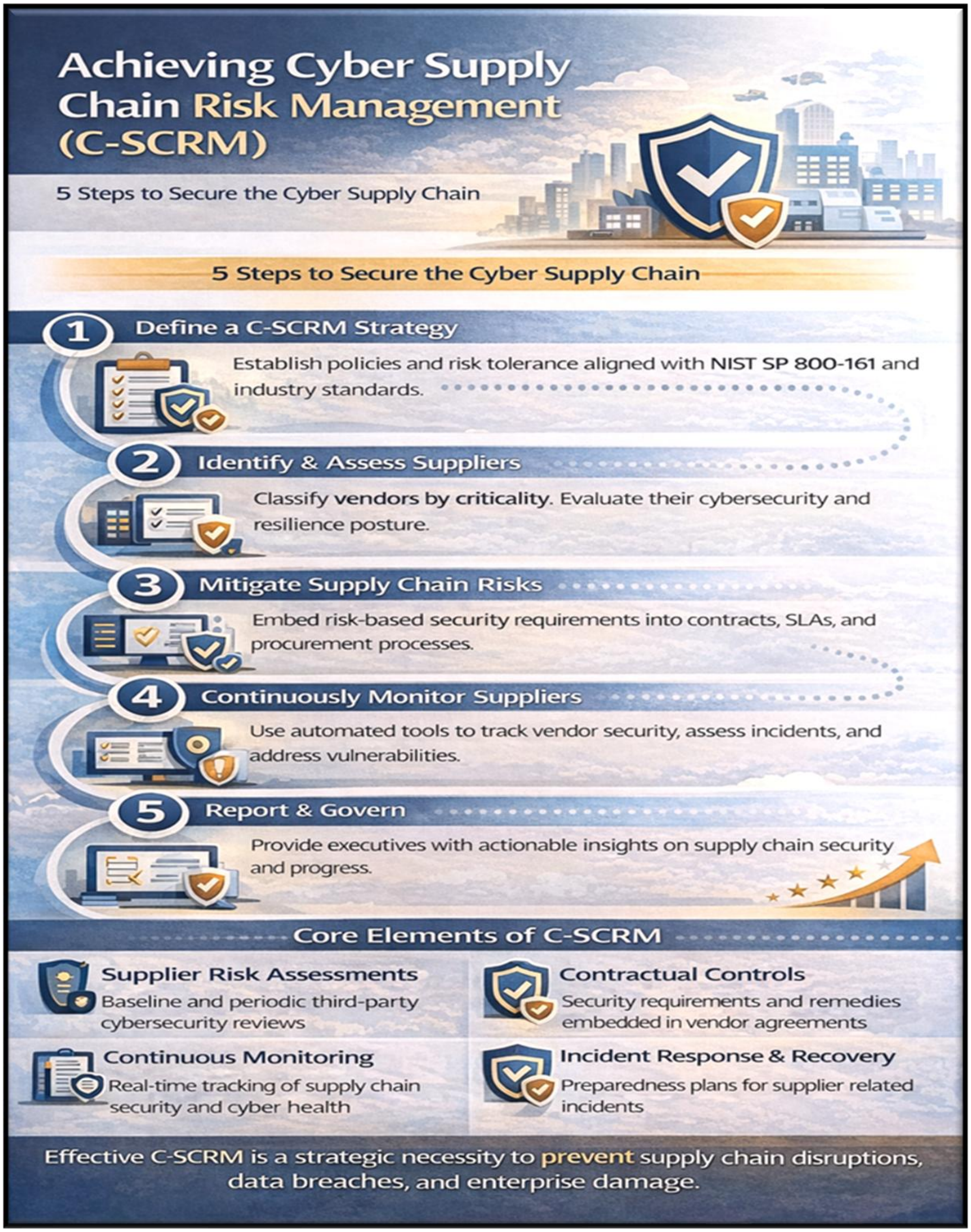
This policy ensures:

- Acquisition is security control.
- Supply chain risk is governed.
- Vendors are continuously monitored.
- Executives retain accountability.

Board-Level Statement

If C-SCRM is not embedded in procurement, it does not exist.
Acquisition is now a frontline cybersecurity control.

- **Infographic - Achieving C-SCRM (Cybercrime Supply Chain Risk Management)**



Achieving Cyber Supply Chain Risk Management (C-SCRM)

5 Steps to Secure the Cyber Supply Chain

5 Steps to Secure the Cyber Supply Chain

1. **Define a C-SCRM Strategy**

   Establish policies and risk tolerance aligned with **NIST SP 800-161** and industry standards.

2. **Identify & Assess Suppliers**

   Classify **vendors by criticality**. Evaluate their cybersecurity and resilience posture.

3. **Mitigate Supply Chain Risks**

   Embed risk-based security requirements into contracts, SLAs, and procurement processes.

4. **Continuously Monitor Suppliers**

   Use automated tools to track vendor security, assess incidents, and address vulnerabilities.

5. **Report & Govern**

   Provide executives with actionable insights on supply chain security and progress.

Core Elements of C-SCRM

Supplier Risk Assessments
Baseline and periodic third-party cybersecurity reviews

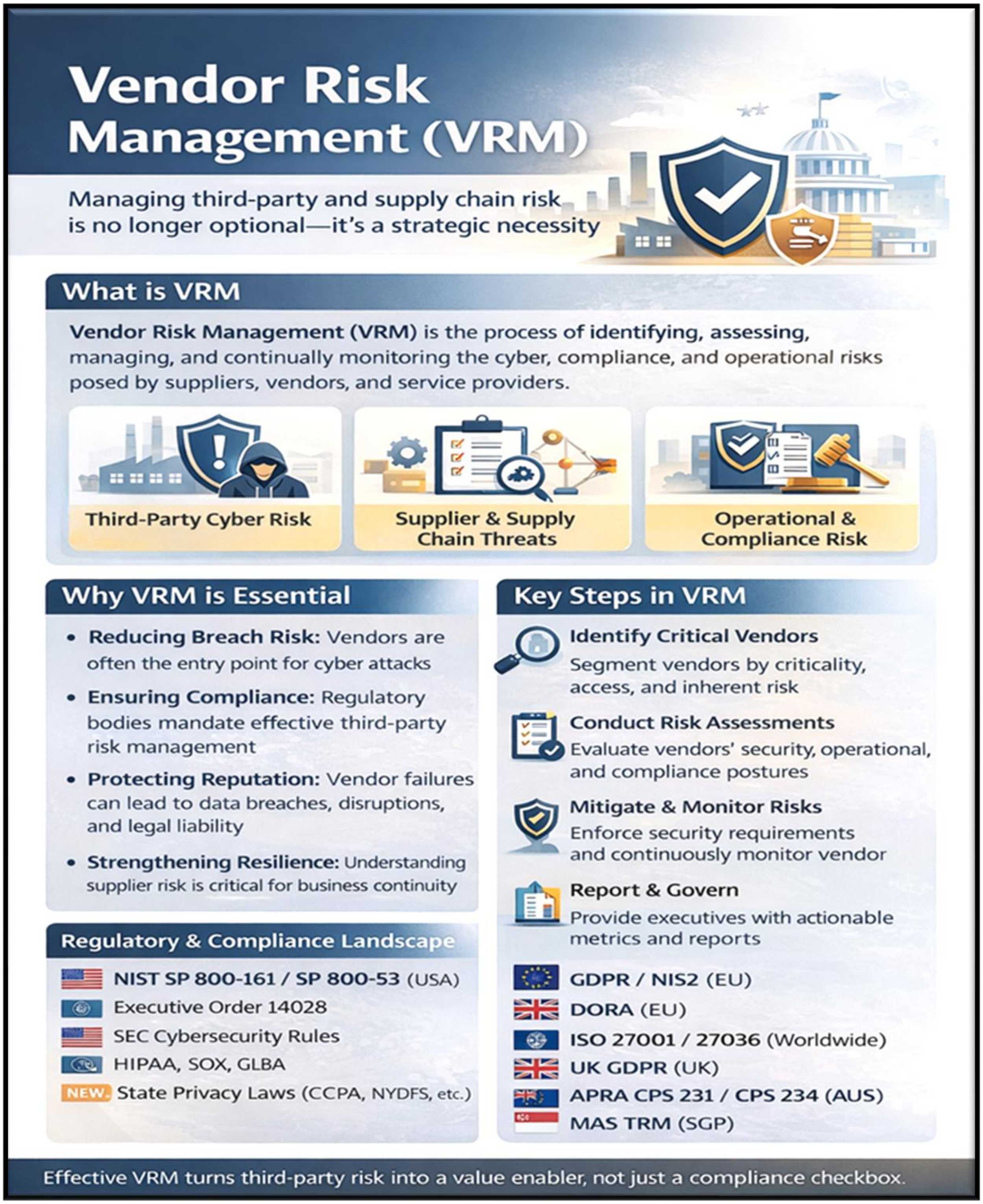
Contractual Controls
Security requirements and remedies embedded in vendor agreements

Continuous Monitoring
Real-time tracking of supply chain security and cyber health

Incident Response & Recovery
Preparedness plans for supplier related incidents

Effective C-SCRM is a strategic necessity to prevent supply chain disruptions, data breaches, and enterprise damage.

- **Infographic - Vendor Risk Management process overview**



Vendor Risk Management (VRM)

Managing third-party and supply chain risk is no longer optional—it's a strategic necessity

What is VRM

Vendor Risk Management (VRM) is the process of **identifying, assessing,** managing, and continually monitoring the cyber, compliance, and operational risks posed by suppliers, vendors, and service providers.

Third-Party Cyber Risk

Supplier & Supply Chain Threats

Operational & Compliance Risk

Why VRM is Essential

- **Reducing Breach Risk:** Vendors are often the entry point for cyber attacks
- **Ensuring Compliance:** Regulatory bodies mandate effective third-party risk management
- **Protecting Reputation:** Vendor failures can lead to data breaches, disruptions, and legal liability
- **Strengthening Resilience:** Understanding supplier risk is critical for business continuity

Key Steps in VRM

Identify Critical Vendors
Segment vendors by criticality, access, and inherent risk

Conduct Risk Assessments
Evaluate vendors' security, operational, and compliance postures

Mitigate & Monitor Risks
Enforce security requirements and continuously monitor vendor

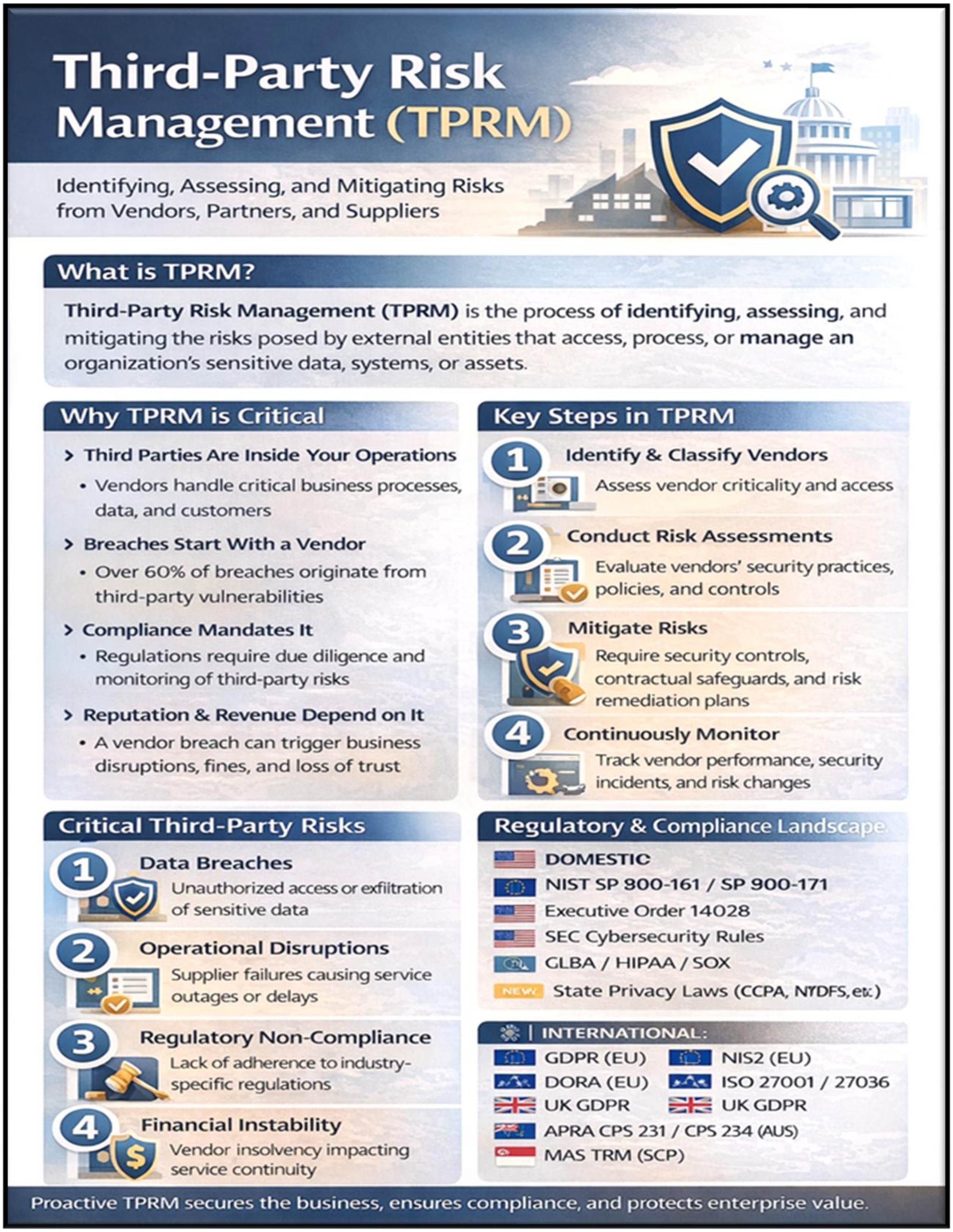
Report & Govern
Provide executives with actionable metrics and reports

Regulatory & Compliance Landscape

- **NIST SP 800-161 / SP 800-53** (USA)
- Executive Order 14028
- SEC Cybersecurity Rules
- HIPAA, SOX, GLBA
- NEW State Privacy Laws (CCPA, NYDFS, etc.)
- **GDPR / NIS2** (EU)
- **DORA** (EU)
- **ISO 27001 / 27036** (Worldwide)
- **UK GDPR** (UK)
- **APRA CPS 231 / CPS 234** (AUS)
- **MAS TRM** (SGP)

Effective VRM turns third-party risk into a value enabler, not just a compliance checkbox.

- **Infographic - Third-Party Risk Management Lifecycle and description**



Third-Party Risk Management (TPRM)

Identifying, Assessing, and Mitigating Risks
from Vendors, Partners, and Suppliers

What is TPRM?

Third-Party Risk Management (TPRM) is the process of **identifying, assessing**, and mitigating the risks posed by external entities that access, process, or **manage an** organization's sensitive data, systems, or assets.

Why TPRM is Critical

> **Third Parties Are Inside Your Operations**

- Vendors handle critical business processes, data, and customers

> **Breaches Start With a Vendor**

- Over 60% of breaches originate from third-party vulnerabilities

> **Compliance Mandates It**

- Regulations require due diligence and monitoring of third-party risks

> **Reputation & Revenue Depend on It**

- A vendor breach can trigger business disruptions, fines, and loss of trust

Key Steps in TPRM

1 **Identify & Classify Vendors**
Assess vendor criticality and access

2 **Conduct Risk Assessments**
Evaluate vendors' security practices, policies, and controls

3 **Mitigate Risks**
Require security controls, contractual safeguards, and risk remediation plans

4 **Continuously Monitor**
Track vendor performance, security incidents, and risk changes

Critical Third-Party Risks

1 **Data Breaches**
Unauthorized access or exfiltration of sensitive data

2 **Operational Disruptions**
Supplier failures causing service outages or delays

3 **Regulatory Non-Compliance**
Lack of adherence to industry-specific regulations

4 **Financial Instability**
Vendor insolvency impacting service continuity

Regulatory & Compliance Landscape

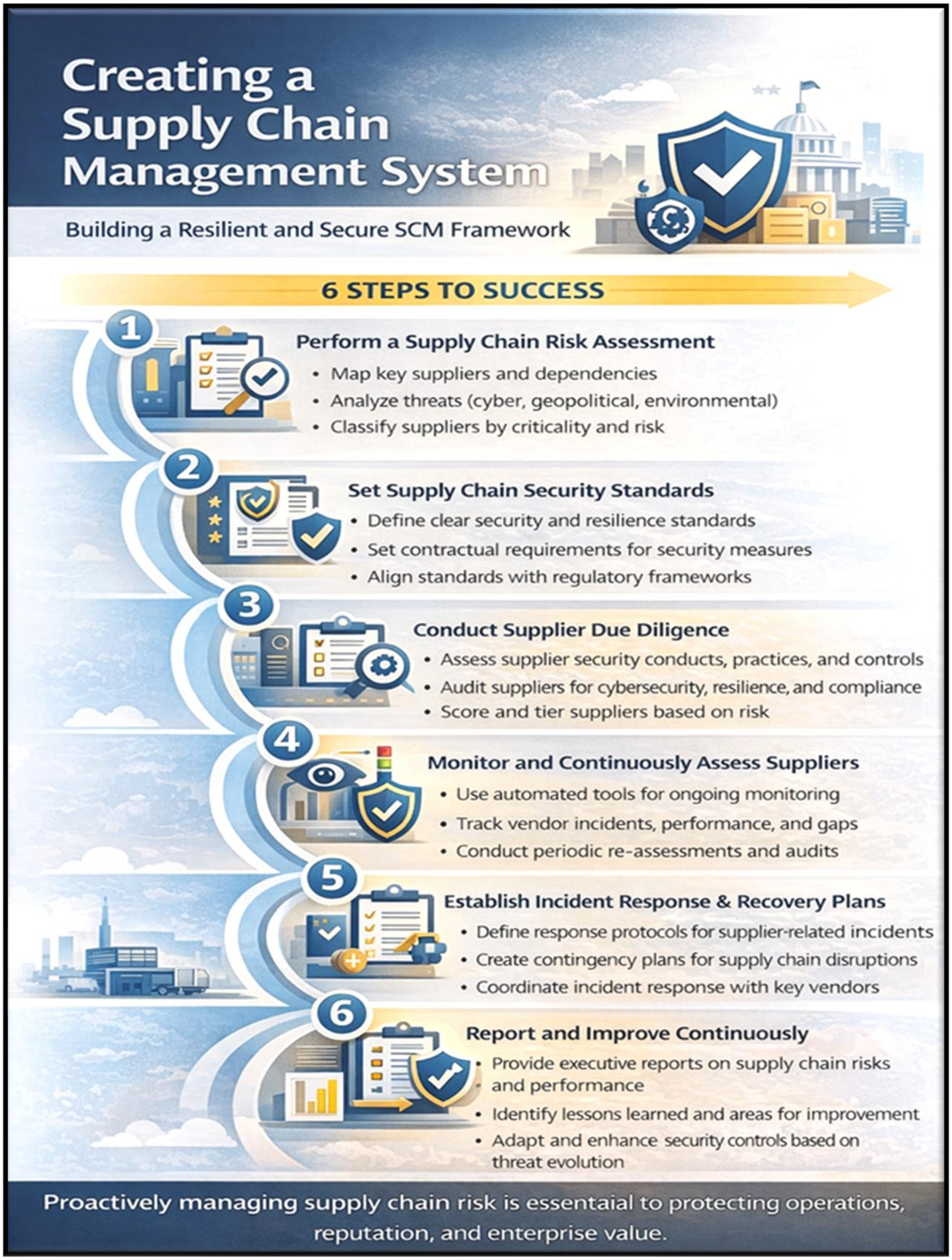
DOMESTIC
NIST SP 800-161 / SP 900-171
Executive Order 14028
SEC Cybersecurity Rules
GLBA / HIPAA / SOX
NEW State Privacy Laws (CCPA, NYDFS, etc.)

INTERNATIONAL:

GDPR (EU)	NIS2 (EU)
DORA (EU)	ISO 27001 / 27036
UK GDPR	UK GDPR
APRA CPS 231 / CPS 234 (AUS)	
MAS TRM (SCP)	

Proactive TPRM secures the business, ensures compliance, and protects enterprise value.

- **Infographic - Supply Chain Management System Development Lifecycle**



Creating a Supply Chain Management System

Building a Resilient and Secure SCM Framework

6 STEPS TO SUCCESS

1 Perform a Supply Chain Risk Assessment

- Map key suppliers and dependencies
- Analyze threats (cyber, geopolitical, environmental)
- Classify suppliers by criticality and risk

2 Set Supply Chain Security Standards

- Define clear security and resilience standards
- Set contractual requirements for security measures
- Align standards with regulatory frameworks

3 Conduct Supplier Due Diligence

- Assess supplier security conducts, practices, and controls
- Audit suppliers for cybersecurity, resilience, and compliance
- Score and tier suppliers based on risk

4 Monitor and Continuously Assess Suppliers

- Use automated tools for ongoing monitoring
- Track vendor incidents, performance, and gaps
- Conduct periodic re-assessments and audits

5 Establish Incident Response & Recovery Plans

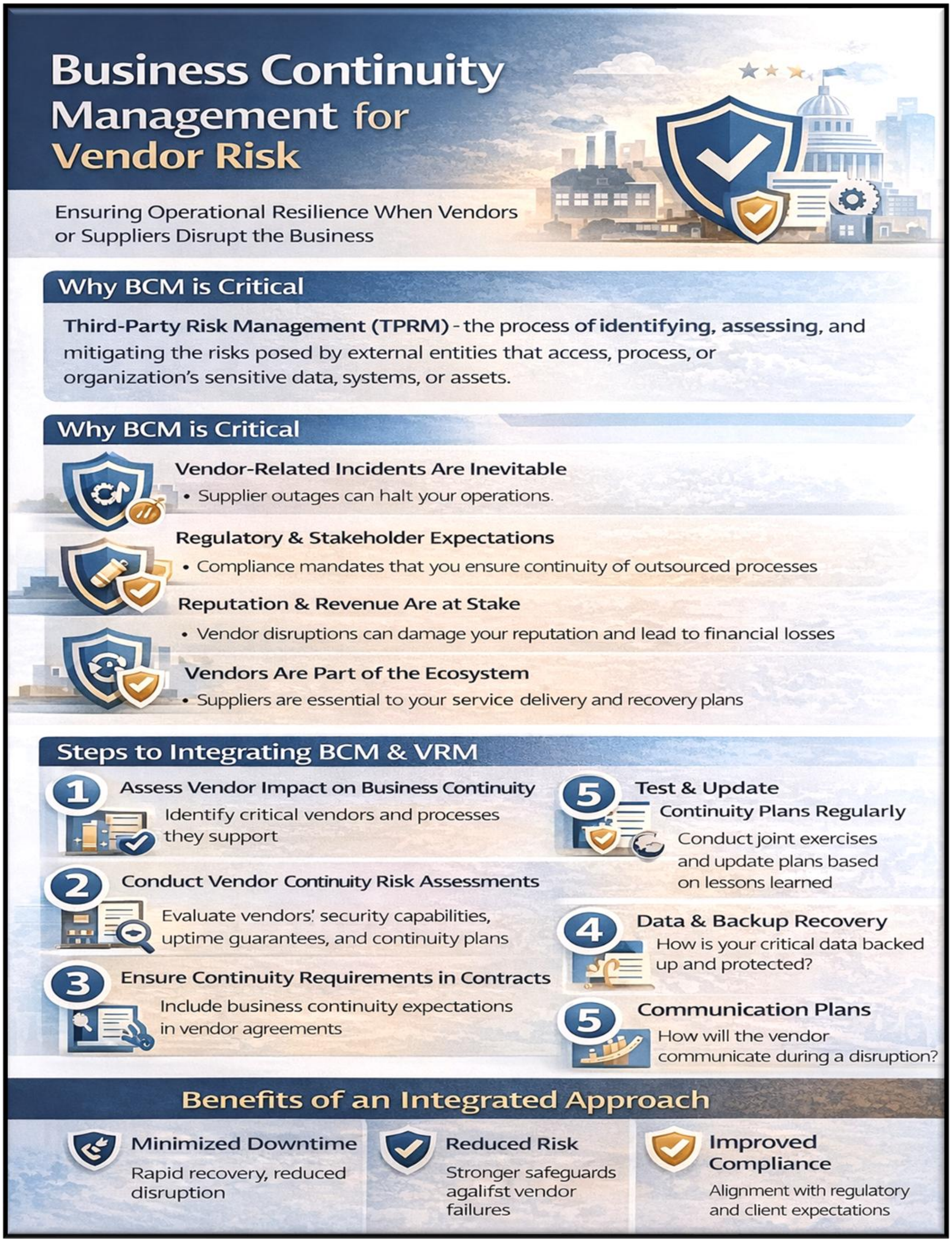
- Define response protocols for supplier-related incidents
- Create contingency plans for supply chain disruptions
- Coordinate incident response with key vendors

6 Report and Improve Continuously

- Provide executive reports on supply chain risks and performance
- Identify lessons learned and areas for improvement
- Adapt and enhance security controls based on threat evolution

Proactively managing supply chain risk is essentaial to protecting operations, reputation, and enterprise value.

- **Infographic - Business Continuity Management with Vendor Risk Management**



Business Continuity Management for Vendor Risk

Ensuring Operational Resilience When Vendors or Suppliers Disrupt the Business

Why BCM is Critical

Third-Party Risk Management (TPRM) - the process **of identifying, assessing**, and mitigating the risks posed by external entities that access, process, or organization's sensitive data, systems, or assets.

Why BCM is Critical

Vendor-Related Incidents Are Inevitable

- Supplier outages can halt your operations.

Regulatory & Stakeholder Expectations

- Compliance mandates that you ensure continuity of outsourced processes

Reputation & Revenue Are at Stake

- Vendor disruptions can damage your reputation and lead to financial losses

Vendors Are Part of the Ecosystem

- Suppliers are essential to your service delivery and recovery plans

Steps to Integrating BCM & VRM

1 **Assess Vendor Impact on Business Continuity**
Identify critical vendors and processes they support

2 **Conduct Vendor Continuity Risk Assessments**
Evaluate vendors' security capabilities, uptime guarantees, and continuity plans

3 **Ensure Continuity Requirements in Contracts**
Include business continuity expectations in vendor agreements

5 **Test & Update Continuity Plans Regularly**
Conduct joint exercises and update plans based on lessons learned

4 **Data & Backup Recovery**
How is your critical data backed up and protected?

5 **Communication Plans**
How will the vendor communicate during a disruption?

Benefits of an Integrated Approach

Minimized Downtime
Rapid recovery, reduced disruption

Reduced Risk
Stronger safeguards agalifst vendor failures

Improved Compliance
Alignment with regulatory and client expectations

- ## Infographic - Achieving CMMC Level 3 Certification

Achieving CMMC Level 3 Certification

6 Steps to Get CMMC Level 3 Certification (Expert)

CMMC LEVEL 3
CERTIFIED

6 Steps to Get CMMC Level 3 Certification

1 Understand CMMC Level 3 Requirements

Review the 130 security controls required .2 for Level 3 in alignment with NIST SP 800-171 and additional requirements for protecting Controlled Unclassified Information (CUI).

2 Conduct a GAP Analysis

Assess your current cybersecurity practices against CMMC Level 3 controls. identify gaps and create a remediation plan.

3 Implement Security Controls

Deploy robust security measures including multi-factor authentication (MFA), encryption, incident response plans, and continuous monitoring.

4 Prepare Documentation

Develop thorough policies, plans, and evidence of implemented security controls. Maintain an SSP, POA&M, incident response plans, and training records.

5 Conduct Internal Assessments

Perform internal audits to validate the effectiveness of security controls and readiness for the Level 3 external assessment.

6 Pass the Third-Party CMMC Assessment

Engage a Certified Third-Party Assessor Organization (C3PAO) to evaluate your security controls. Pass the assessment to become CMMC Level 3 certified

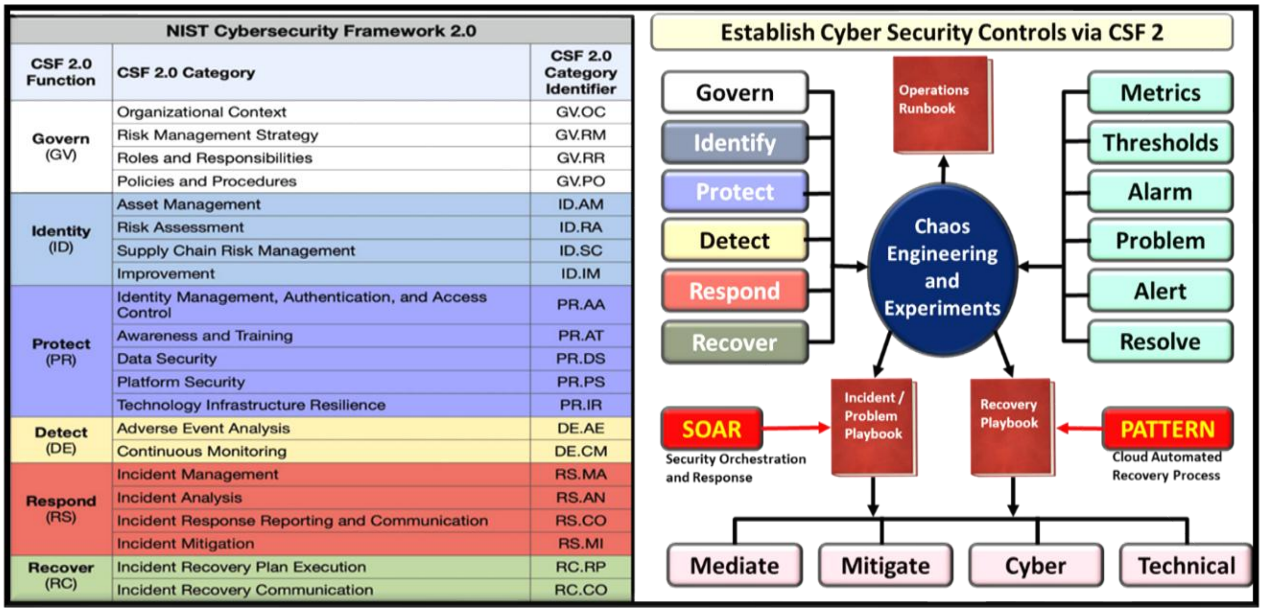
Why It Matters:

- ✓ Eligible for DoD contracts involving CUI
- ✓ Demonstrates superior cybersecurity maturity
- ✓ Protects sensitive defense information

- ✓ Protects sensitive defense
- ✓ Strengthens business competitiveness

Effective BCM ensures that vendor risk is not a single point of failure for your

• CSF 2.0 (Cybersecurity Framework 2.0) and its implementation



NIST Cybersecurity Framework 2.0

CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Establish Cyber Security Controls via CSF 2

Govern
Identify
Protect
Detect
Respond
Recover

Operations Runbook

Chaos Engineering and Experiments

Metrics
Thresholds
Alarm
Problem
Alert
Resolve

SOAR
Security Orchestration and Response

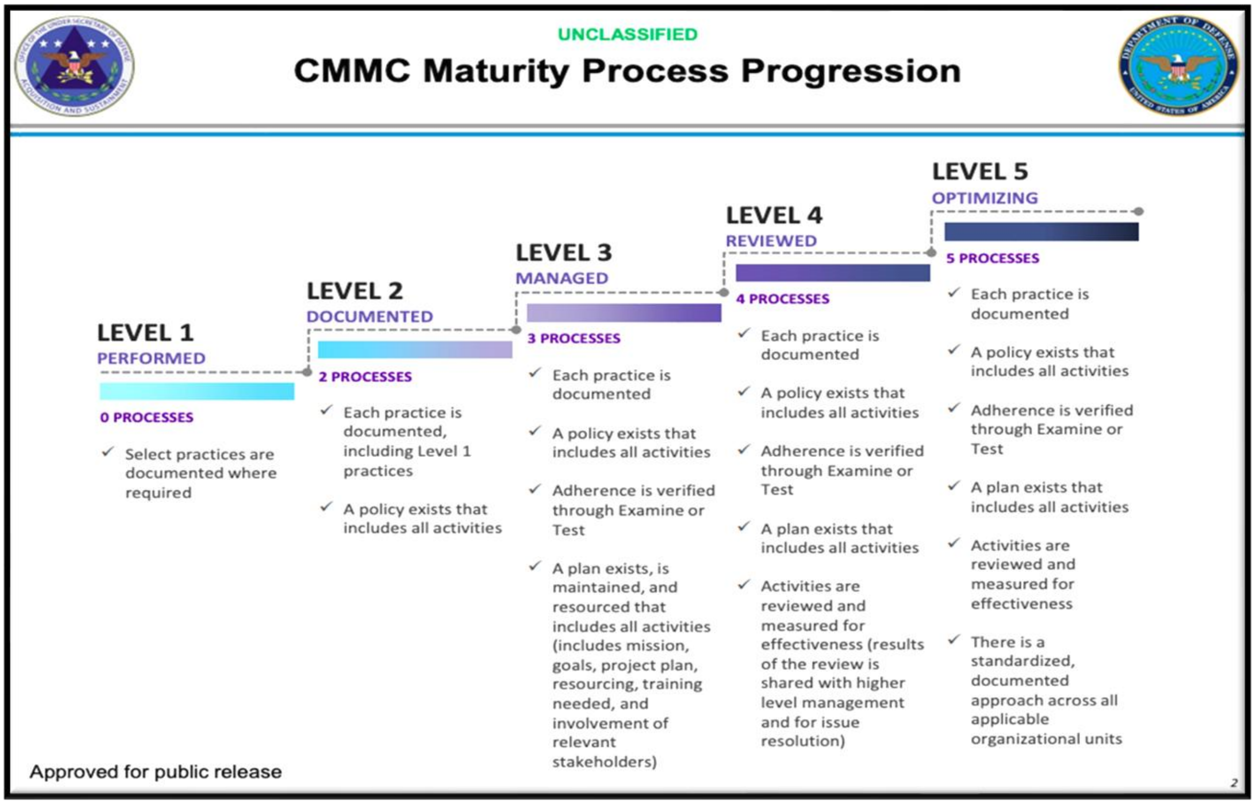
Incident / Problem Playbook

Recovery Playbook

PATTERN
Cloud Automated Recovery Process

Mediate
Mitigate
Cyber
Technical

• CMMC Overview of Levels and their requirements



UNCLASSIFIED

CMMC Maturity Process Progression

LEVEL 1
PERFORMED
0 PROCESSES
- ✓ Select practices are documented where required

LEVEL 2
DOCUMENTED
2 PROCESSES
- ✓ Each practice is documented, including Level 1 practices
- ✓ A policy exists that includes all activities

LEVEL 3
MANAGED
3 PROCESSES
- ✓ Each practice is documented
- ✓ A policy exists that includes all activities
- ✓ Adherence is verified through Examine or Test
- ✓ A plan exists, is maintained, and resourced that includes all activities (includes mission, goals, project plan, resourcing, training needed, and involvement of relevant stakeholders)

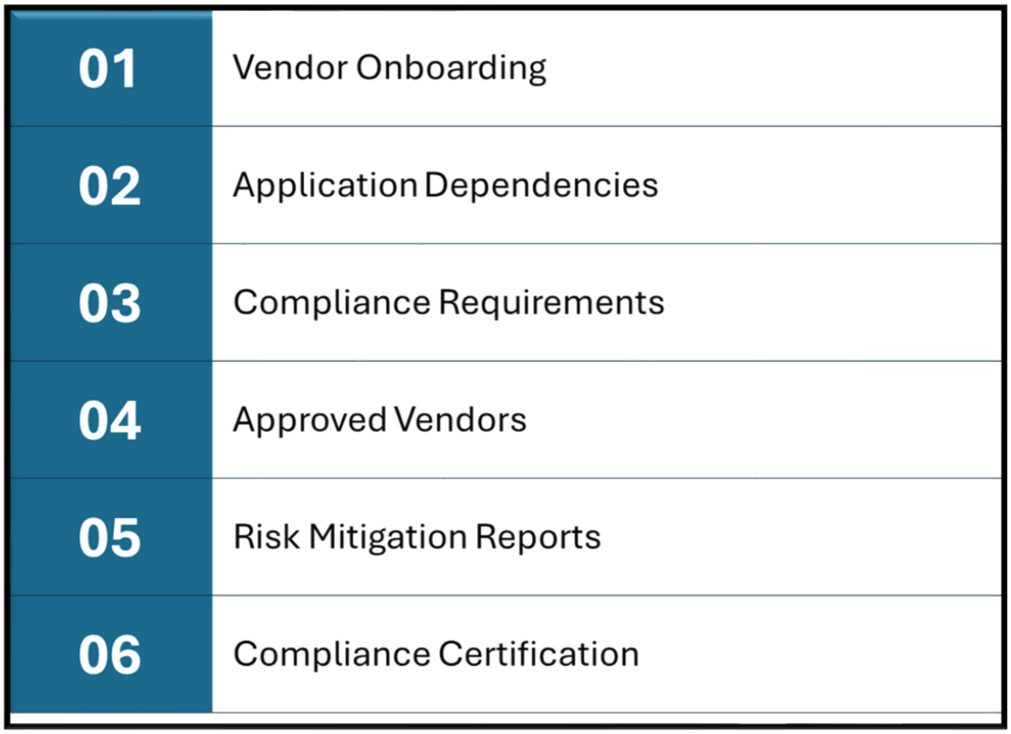
LEVEL 4
REVIEWED
4 PROCESSES
- ✓ Each practice is documented
- ✓ A policy exists that includes all activities
- ✓ Adherence is verified through Examine or Test
- ✓ A plan exists that includes all activities
- ✓ Activities are reviewed and measured for effectiveness (results of the review is shared with higher level management and for issue resolution)

LEVEL 5
OPTIMIZING
5 PROCESSES
- ✓ Each practice is documented
- ✓ A policy exists that includes all activities
- ✓ Adherence is verified through Examine or Test
- ✓ A plan exists that includes all activities
- ✓ Activities are reviewed and measured for effectiveness
- ✓ There is a standardized, documented approach across all applicable organizational units

Approved for public release

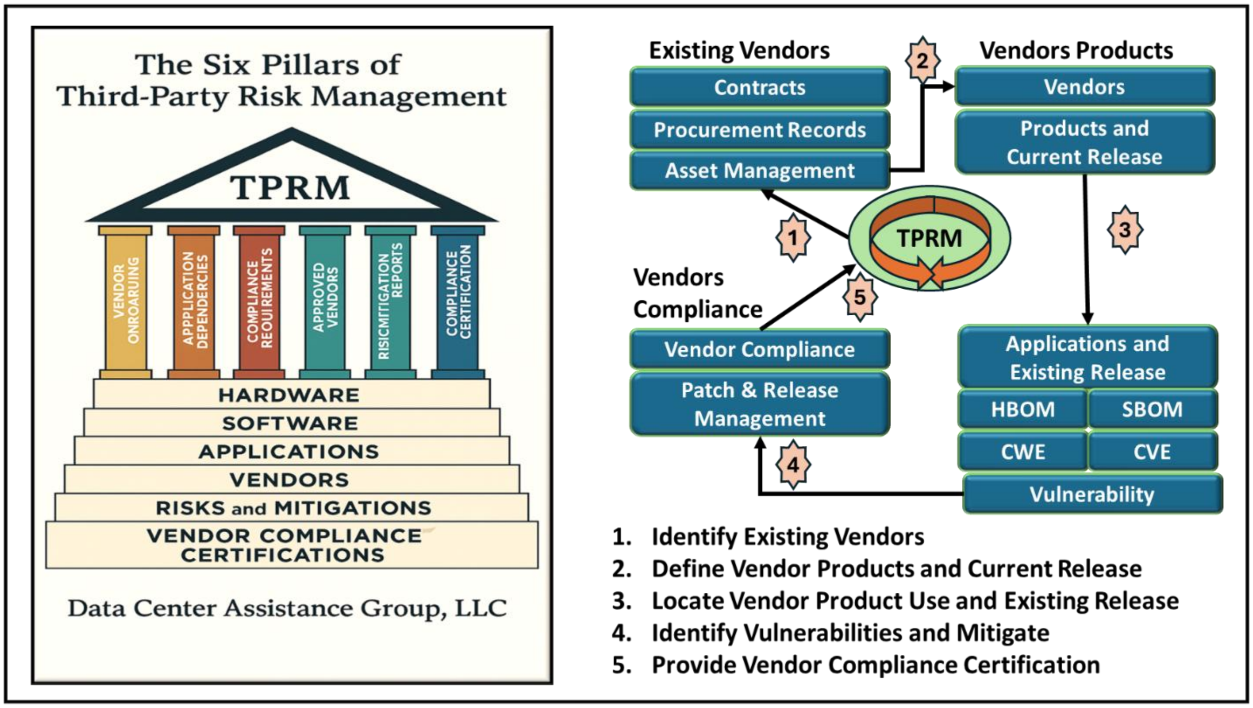
2

- ## Third-Party Risk Management Onboarding



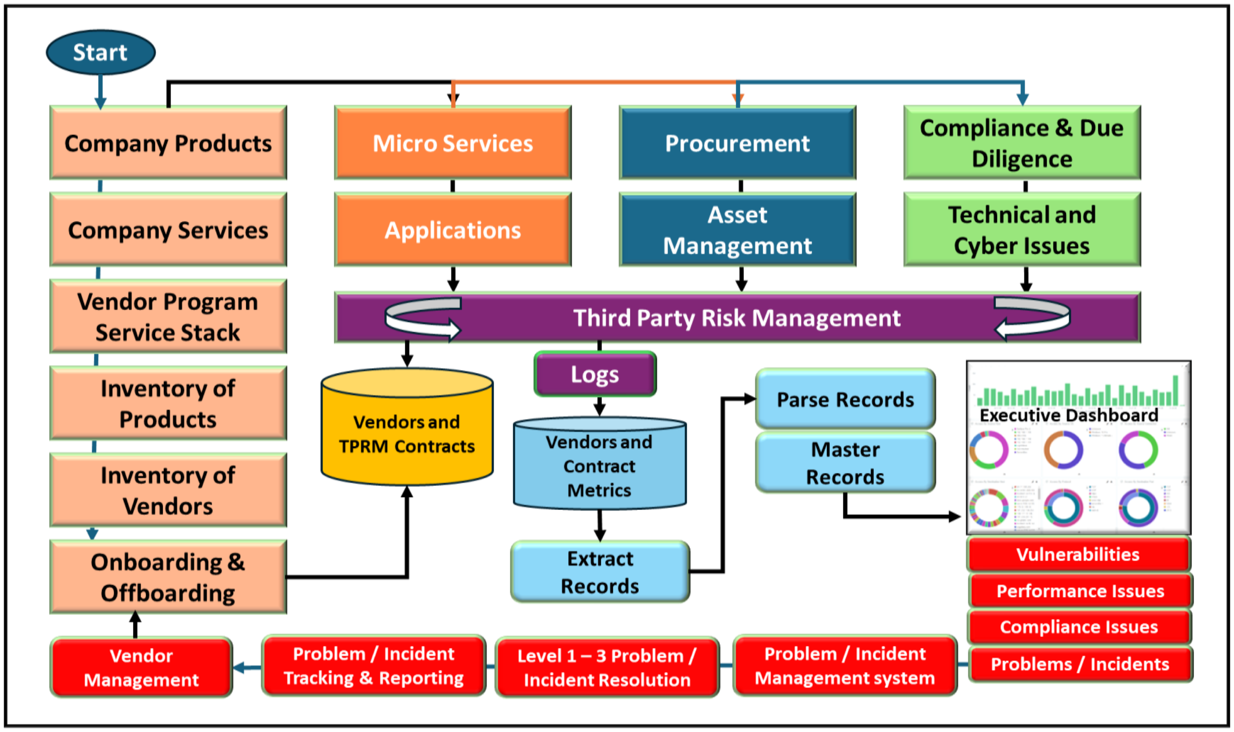
01	Vendor Onboarding
02	Application Dependencies
03	Compliance Requirements
04	Approved Vendors
05	Risk Mitigation Reports
06	Compliance Certification

- ## Third-Party Risk Management overview



1. **Identify Existing Vendors**
2. **Define Vendor Products and Current Release**
3. **Locate Vendor Product Use and Existing Release**
4. **Identify Vulnerabilities and Mitigate**
5. **Provide Vendor Compliance Certification**

• Third-Part Risk Management Project Overview



Start

Company Products

Company Services

Vendor Program Service Stack

Inventory of Products

Inventory of Vendors

Onboarding & Offboarding

Micro Services

Applications

Procurement

Asset Management

Compliance & Due Diligence

Technical and Cyber Issues

Third Party Risk Management

Vendors and TPRM Contracts

Logs

Vendors and Contract Metrics

Extract Records

Parse Records

Master Records

Executive Dashboard

Vulnerabilities

Performance Issues

Compliance Issues

Problems / Incidents

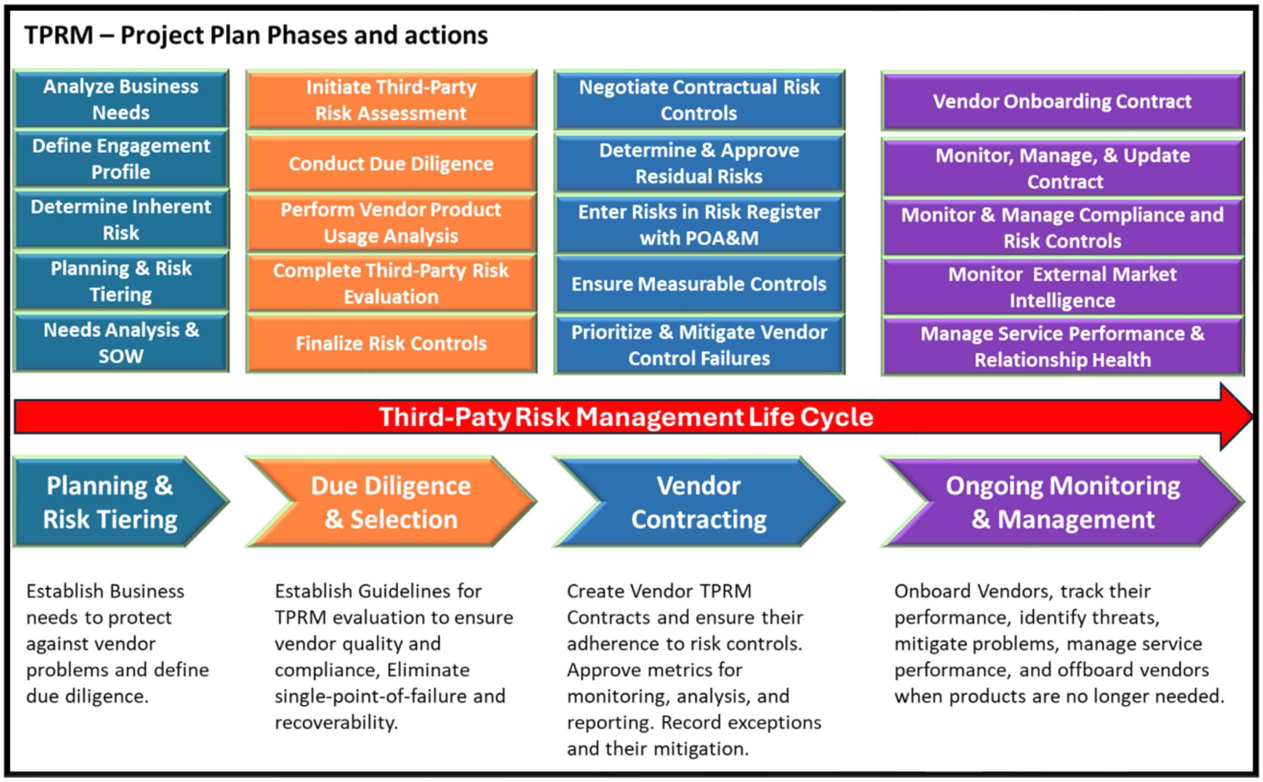
Problem / Incident Management system

Level 1 – 3 Problem / Incident Resolution

Problem / Incident Tracking & Reporting

Vendor Management

• Building the VRM System



TPRM – Project Plan Phases and actions

Analyze Business Needs

Define Engagement Profile

Determine Inherent Risk

Planning & Risk Tiering

Needs Analysis & SOW

Initiate Third-Party Risk Assessment

Conduct Due Diligence

Perform Vendor Product Usage Analysis

Complete Third-Party Risk Evaluation

Finalize Risk Controls

Negotiate Contractual Risk Controls

Determine & Approve Residual Risks

Enter Risks in Risk Register with POA&M

Ensure Measurable Controls

Prioritize & Mitigate Vendor Control Failures

Vendor Onboarding Contract

Monitor, Manage, & Update Contract

Monitor & Manage Compliance and Risk Controls

Monitor External Market Intelligence

Manage Service Performance & Relationship Health

Third-Paty Risk Management Life Cycle

Planning & Risk Tiering

Due Diligence & Selection

Vendor Contracting

Ongoing Monitoring & Management

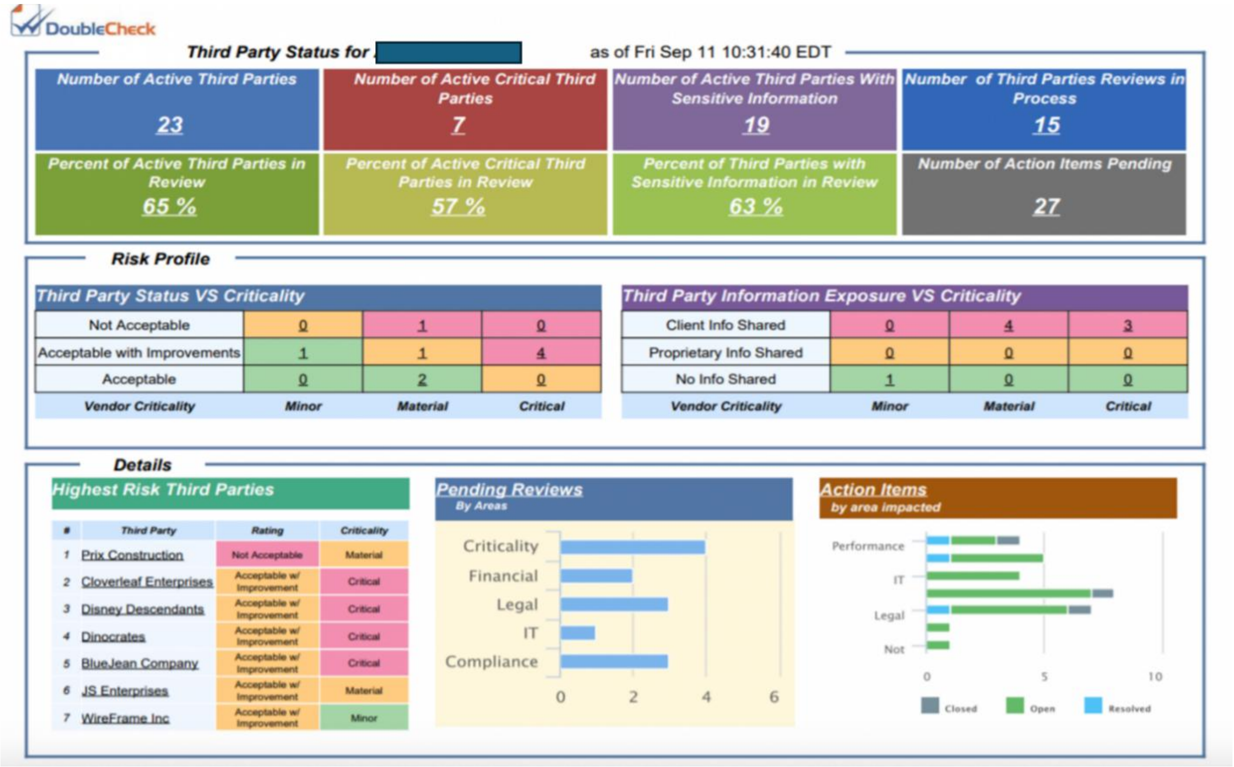
Establish Business needs to protect against vendor problems and define due diligence.

Establish Guidelines for TPRM evaluation to ensure vendor quality and compliance, Eliminate single-point-of-failure and recoverability.

Create Vendor TPRM Contracts and ensure their adherence to risk controls. Approve metrics for monitoring, analysis, and reporting. Record exceptions and their mitigation.

Onboard Vendors, track their performance, identify threats, mitigate problems, manage service performance, and offboard vendors when products are no longer needed.

- ## Sample Vendor Riks Management Executive Dashboard



DoubleCheck

Third Party Status for [redacted] as of Fri Sep 11 10:31:40 EDT

Number of Active Third Parties	Number of Active Critical Third Parties	Number of Active Third Parties With Sensitive Information	Number of Third Parties Reviews in Process
23	7	19	15
Percent of Active Third Parties in Review	**Percent of Active Critical Third Parties in Review**	**Percent of Third Parties with Sensitive Information in Review**	**Number of Action Items Pending**
65 %	57 %	63 %	27

Risk Profile

Third Party Status VS Criticality

Not Acceptable	0	1	0
Acceptable with Improvements	1	1	4
Acceptable	0	2	0
Vendor Criticality	**Minor**	**Material**	**Critical**

Third Party Information Exposure VS Criticality

Client Info Shared	0	4	3
Proprietary Info Shared	0	0	0
No Info Shared	1	0	0
Vendor Criticality	**Minor**	**Material**	**Critical**

Details

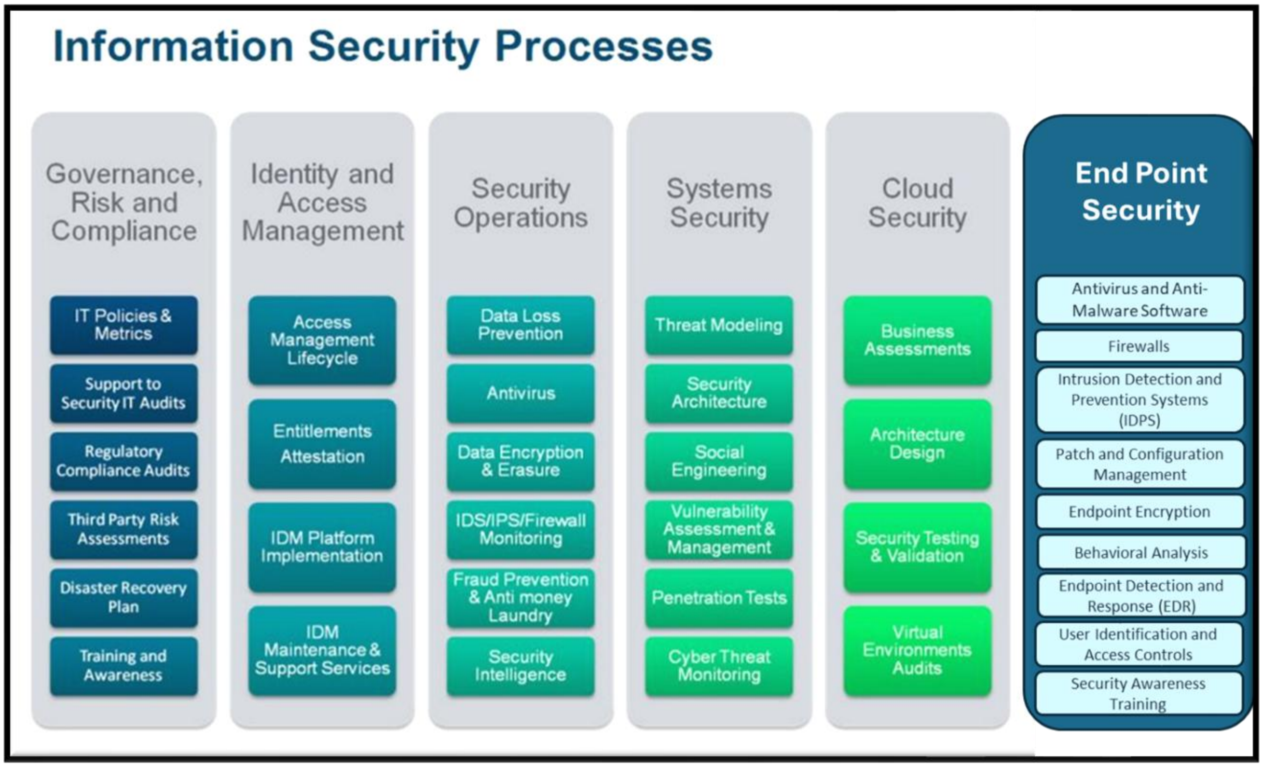
Highest Risk Third Parties

#	Third Party	Rating	Criticality
1	Prix Construction	Not Acceptable	Material
2	Cloverleaf Enterprises	Acceptable w/ Improvement	Critical
3	Disney Descendants	Acceptable w/ Improvement	Critical
4	Dinocrates	Acceptable w/ Improvement	Critical
5	BlueJean Company	Acceptable w/ Improvement	Critical
6	JS Enterprises	Acceptable w/ Improvement	Material
7	WireFrame Inc	Acceptable w/ Improvement	Minor

Pending Reviews
By Areas

Action Items
by area impacted

- ## Information Security



Information Security Processes

Governance, Risk and Compliance
- IT Policies & Metrics
- Support to Security IT Audits
- Regulatory Compliance Audits
- Third Party Risk Assessments
- Disaster Recovery Plan
- Training and Awareness

Identity and Access Management
- Access Management Lifecycle
- Entitlements Attestation
- IDM Platform Implementation
- IDM Maintenance & Support Services

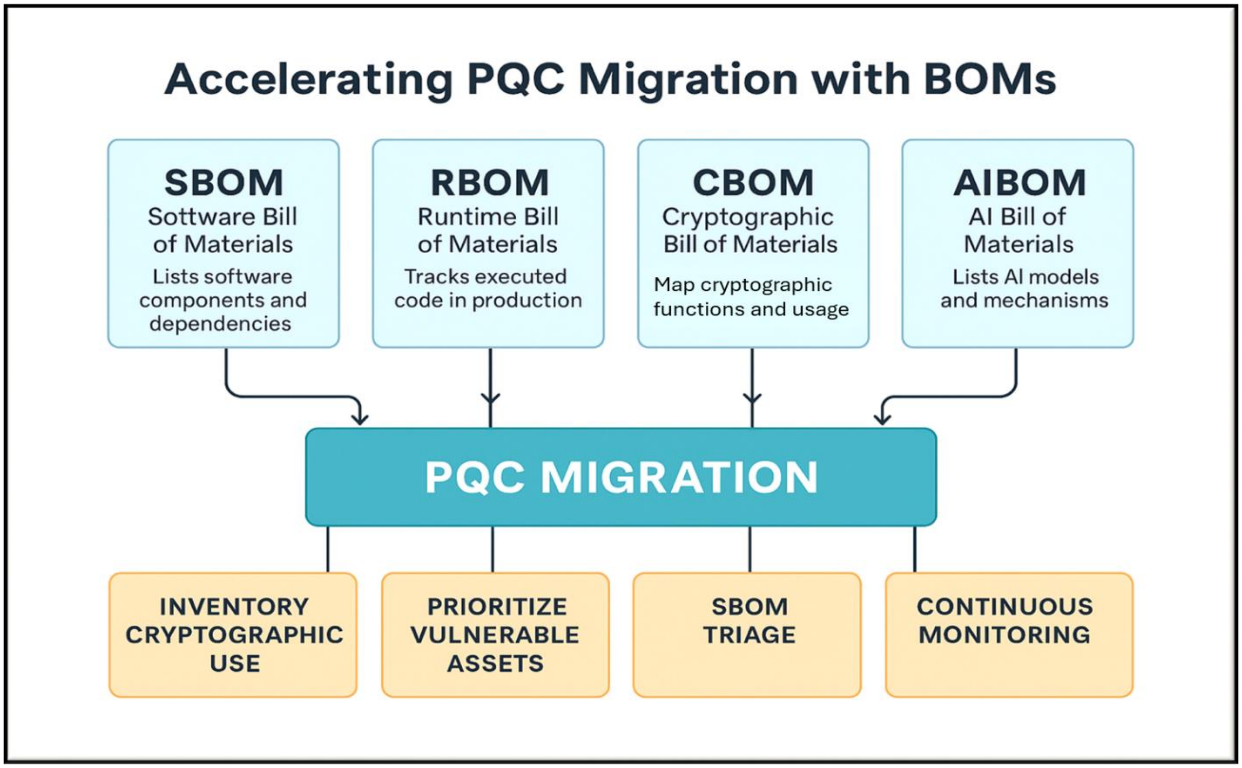
Security Operations
- Data Loss Prevention
- Antivirus
- Data Encryption & Erasure
- IDS/IPS/Firewall Monitoring
- Fraud Prevention & Anti money Laundry
- Security Intelligence

Systems Security
- Threat Modeling
- Security Architecture
- Social Engineering
- Vulnerability Assessment & Management
- Penetration Tests
- Cyber Threat Monitoring

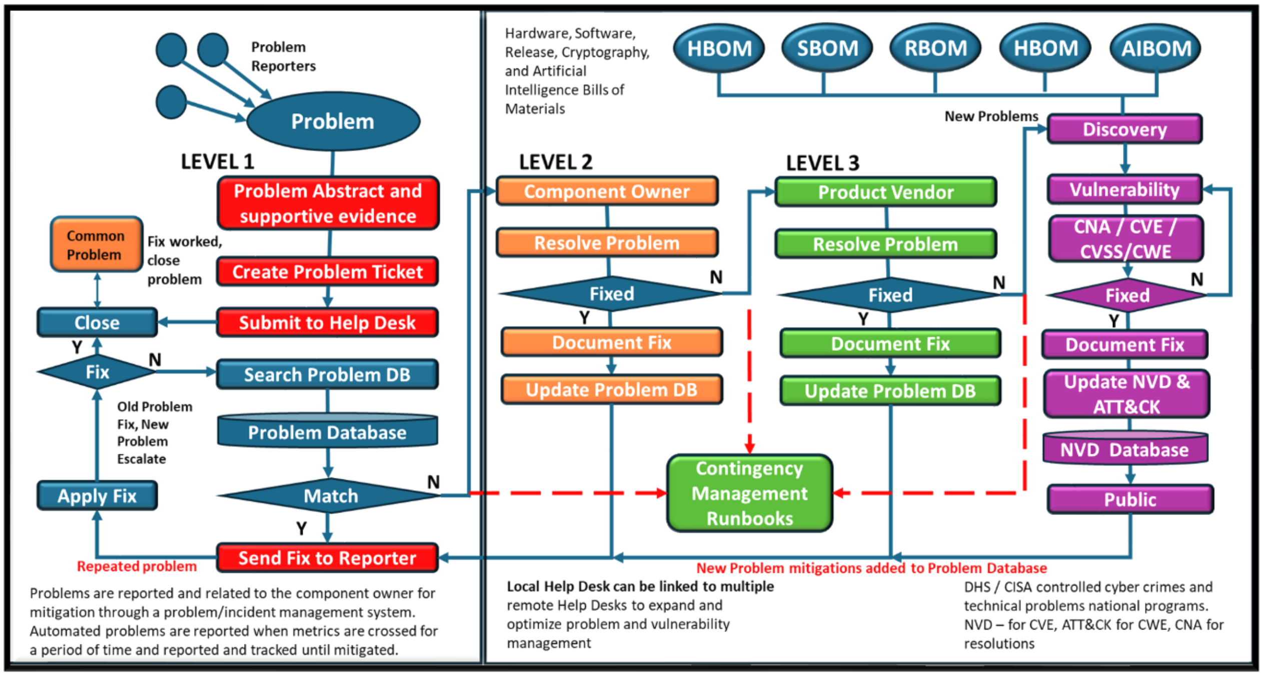
Cloud Security
- Business Assessments
- Architecture Design
- Security Testing & Validation
- Virtual Environments Audits

End Point Security
- Antivirus and Anti-Malware Software
- Firewalls
- Intrusion Detection and Prevention Systems (IDPS)
- Patch and Configuration Management
- Endpoint Encryption
- Behavioral Analysis
- Endpoint Detection and Response (EDR)
- User Identification and Access Controls
- Security Awareness Training

• Accelerating PQC Migration and the use of BOMs


Accelerating PQC Migration with BOMs
SBOM
Sottware Bill of Materials
Lists software components and dependencies
RBOM
Runtime Bill of Materials
Tracks executed code in production
CBOM
Cryptographic Bill of Materials
Map cryptographic functions and usage
AIBOM
AI Bill of Materials
Lists AI models and mechanisms
PQC MIGRATION
INVENTORY CRYPTOGRAPHIC USE
PRIORITIZE VULNERABLE ASSETS
SBOM TRIAGE
CONTINUOUS MONITORING

• Problem / Incident Management with the use of BOMs

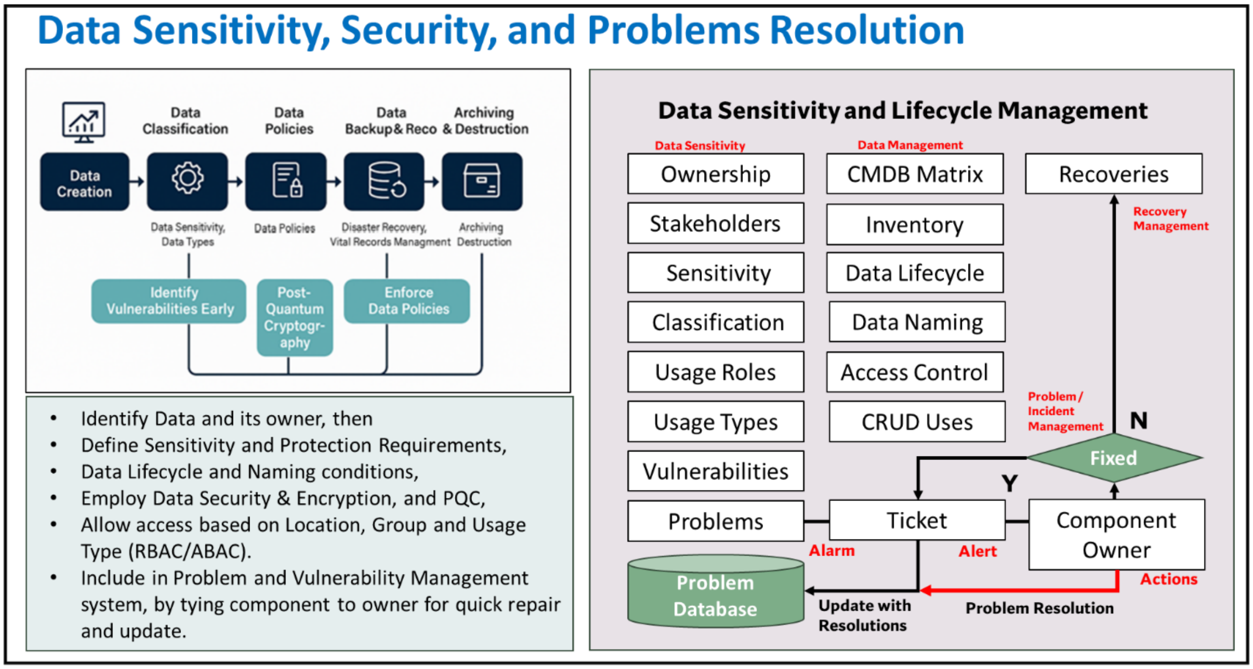


Problems are reported and related to the component owner for mitigation through a problem/incident management system. Automated problems are reported when metrics are crossed for a period of time and reported and tracked until mitigated.

Local Help Desk can be linked to multiple remote Help Desks to expand and optimize problem and vulnerability management

DHS / CISA controlled cyber crimes and technical problems national programs. NVD – for CVE, ATT&CK for CWE, CNA for resolutions

- ## Data Sensitivity, Security, and Problem Management



Data Sensitivity, Security, and Problems Resolution

Data Classification
Data Policies
Data Backup& Reco
Archiving & Destruction
Data Creation
Data Sensitivity, Data Types
Data Policies
Disaster Recovery, Vital Records Managment
Archiving Destruction
Identify Vulnerabilities Early
Post-Quantum Cryptogr-aphy
Enforce Data Policies

- Identify Data and its owner, then
- Define Sensitivity and Protection Requirements,
- Data Lifecycle and Naming conditions,
- Employ Data Security & Encryption, and PQC,
- Allow access based on Location, Group and Usage Type (RBAC/ABAC).
- Include in Problem and Vulnerability Management system, by tying component to owner for quick repair and update.

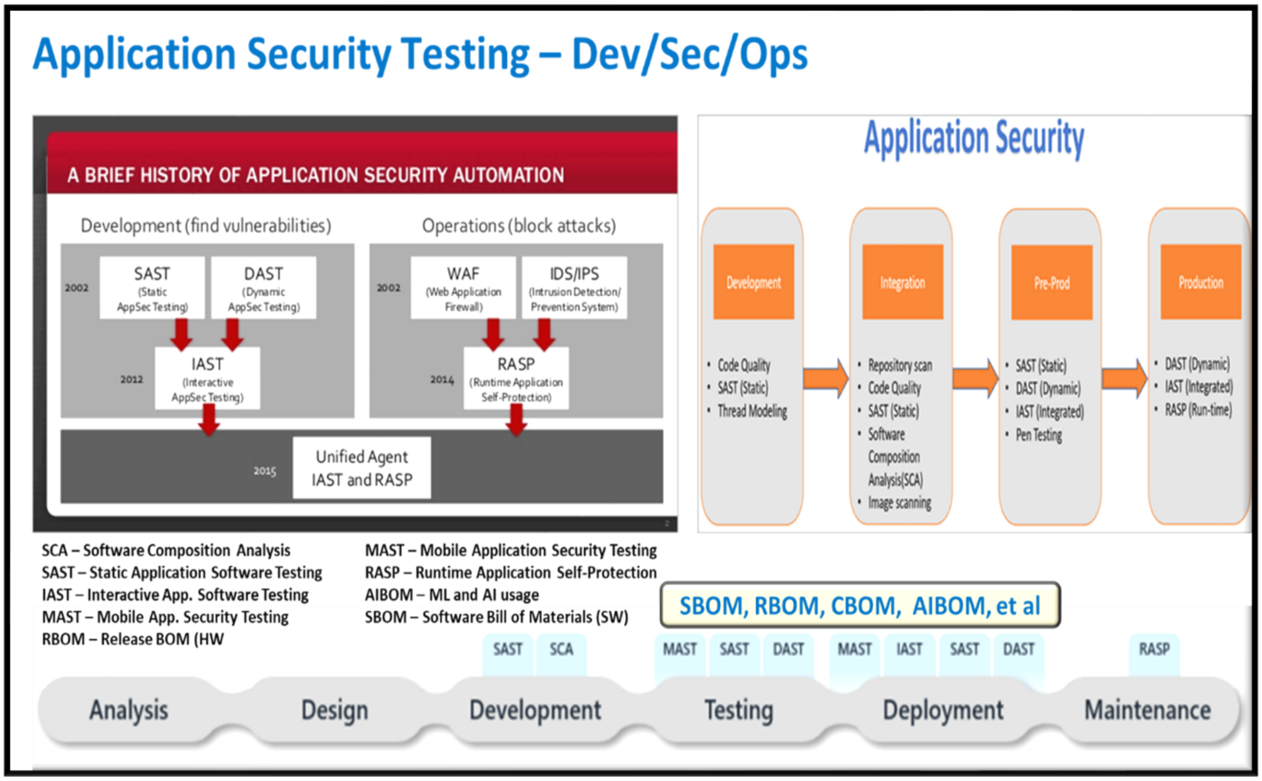
Data Sensitivity and Lifecycle Management

Data Sensitivity
Ownership
Stakeholders
Sensitivity
Classification
Usage Roles
Usage Types
Vulnerabilities
Problems

Data Management
CMDB Matrix
Inventory
Data Lifecycle
Data Naming
Access Control
CRUD Uses

Recoveries
Recovery Management
Problem / Incident Management
N
Fixed
Y
Ticket
Component Owner
Alarm
Alert
Actions
Problem Database
Update with Resolutions
Problem Resolution

- ## Application Security Testing - DevSecOps



Application Security Testing – Dev/Sec/Ops

A BRIEF HISTORY OF APPLICATION SECURITY AUTOMATION

Development (find vulnerabilities)
2002 SAST (Static AppSec Testing) DAST (Dynamic AppSec Testing)
2012 IAST (Interactive AppSec Testing)

Operations (block attacks)
2002 WAF (Web Application Firewall) IDS/IPS (Intrusion Detection/ Prevention System)
2014 RASP (Runtime Application Self-Protection)

2015 Unified Agent IAST and RASP

Application Security

Development
- Code Quality
- SAST (Static)
- Thread Modeling

Integration
- Repository scan
- Code Quality
- SAST (Static)
- Software Composition Analysis(SCA)
- Image scanning

Pre-Prod
- SAST (Static)
- DAST (Dynamic)
- IAST (Integrated)
- Pen Testing

Production
- DAST (Dynamic)
- IAST (Integrated)
- RASP (Run-time)

SCA – Software Composition Analysis
SAST – Static Application Software Testing
IAST – Interactive App. Software Testing
MAST – Mobile App. Security Testing
RBOM – Release BOM (HW

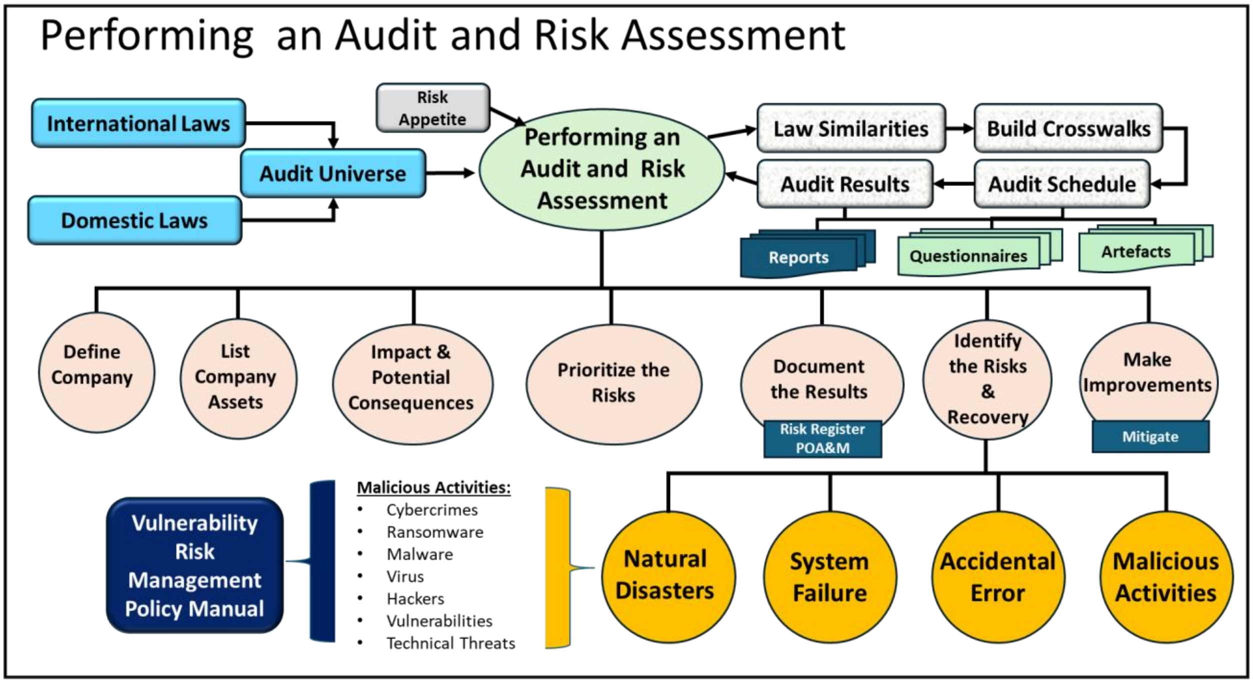
MAST – Mobile Application Security Testing
RASP – Runtime Application Self-Protection
AIBOM – ML and AI usage
SBOM – Software Bill of Materials (SW)

SBOM, RBOM, CBOM, AIBOM, et al

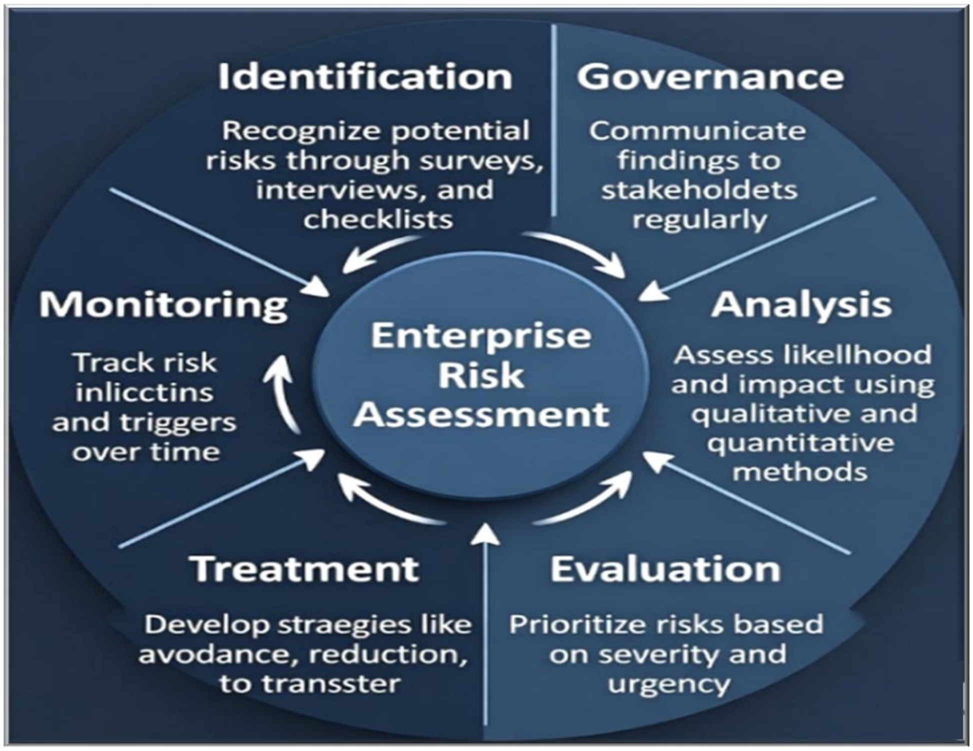
SAST SCA MAST SAST DAST MAST IAST SAST DAST RASP

Analysis Design Development Testing Deployment Maintenance

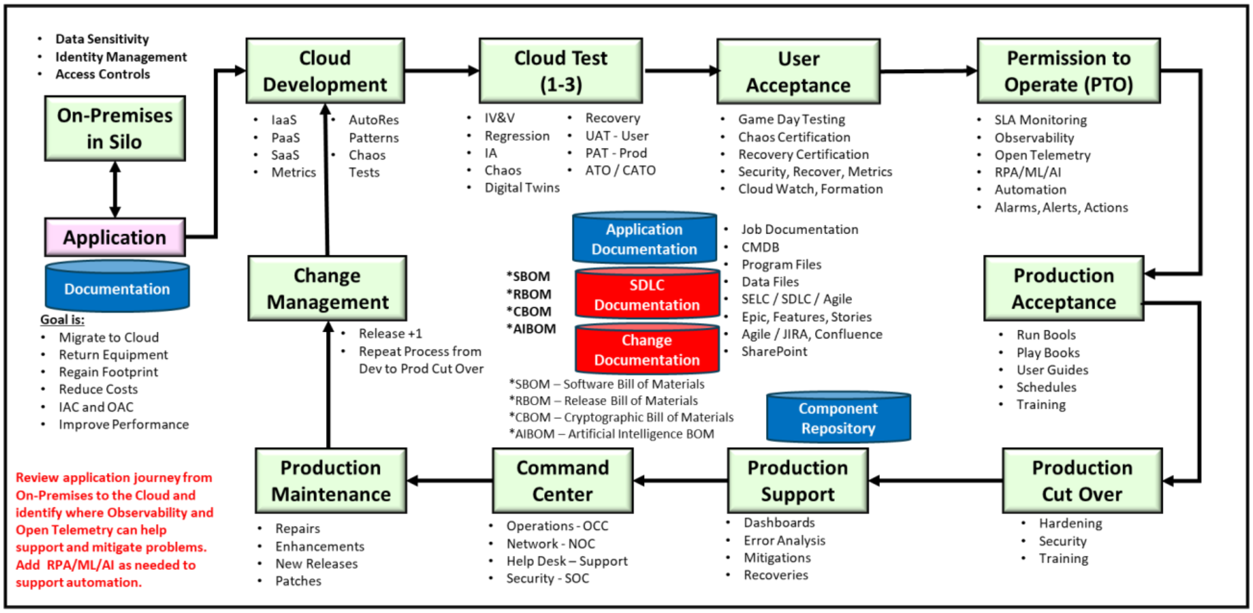
- **Performing an Audit and Risk Assessment**



- **Enterprise Risk Assessments**


Identification
Recognize potential risks through surveys, interviews, and checklists
Governance
Communicate findings to stakeholdets regularly
Monitoring
Track risk inlicctins and triggers over time
Enterprise Risk Assessment
Analysis
Assess likellhood and impact using qualitative and quantitative methods
Treatment
Develop straegies like avodance, reduction, to transster
Evaluation
Prioritize risks based on severity and urgency

Migrating Applications to the Cloud



- Data Sensitivity
- Identity Management
- Access Controls

On-Premises in Silo

Application

Documentation

Goal is:

- Migrate to Cloud
- Return Equipment
- Regain Footprint
- Reduce Costs
- IAC and OAC
- Improve Performance

Review application journey from On-Premises to the Cloud and identify where Observability and Open Telemetry can help support and mitigate problems. Add RPA/ML/AI as needed to support automation.

Cloud Development

- IaaS
- PaaS
- SaaS
- Metrics
- AutoRes
- Patterns
- Chaos
- Tests

Cloud Test (1-3)

- IV&V
- Regression
- IA
- Chaos
- Digital Twins
- Recovery
- UAT - User
- PAT - Prod
- ATO / CATO

User Acceptance

- Game Day Testing
- Chaos Certification
- Recovery Certification
- Security, Recover, Metrics
- Cloud Watch, Formation

Permission to Operate (PTO)

- SLA Monitoring
- Observability
- Open Telemetry
- RPA/ML/AI
- Automation
- Alarms, Alerts, Actions

Change Management

- Release +1
- Repeat Process from Dev to Prod Cut Over

Application Documentation

SDLC Documentation

Change Documentation

*SBOM
*RBOM
*CBOM
*AIBOM

- Job Documentation
- CMDB
- Program Files
- Data Files
- SELC / SDLC / Agile
- Epic, Features, Stories
- Agile / JIRA, Confluence
- SharePoint

*SBOM – Software Bill of Materials
*RBOM – Release Bill of Materials
*CBOM – Cryptographic Bill of Materials
*AIBOM – Artificial Intelligence BOM

Component Repository

Production Acceptance

- Run Bools
- Play Books
- User Guides
- Schedules
- Training

Production Maintenance

- Repairs
- Enhancements
- New Releases
- Patches

Command Center

- Operations - OCC
- Network - NOC
- Help Desk – Support
- Security - SOC

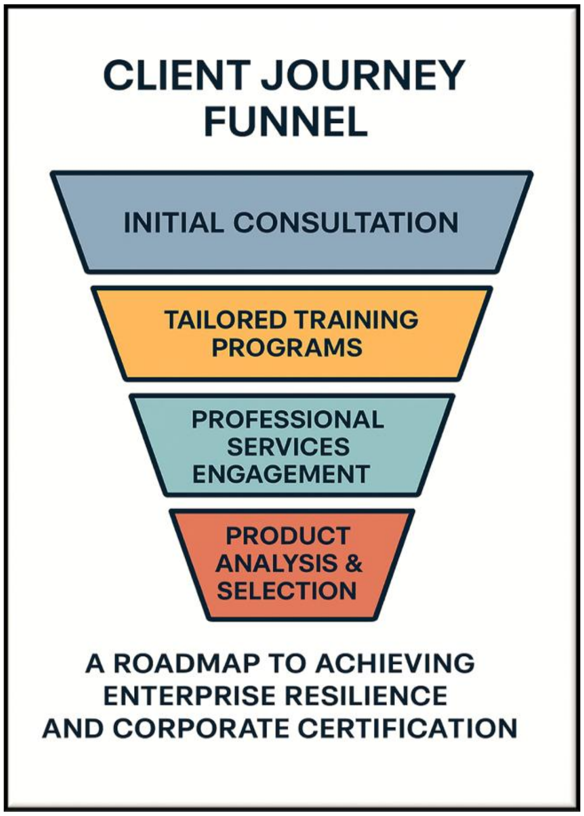
Production Support

- Dashboards
- Error Analysis
- Mitigations
- Recoveries

Production Cut Over

- Hardening
- Security
- Training

• Services provided by DCAG



CLIENT JOURNEY FUNNEL

INITIAL CONSULTATION

TAILORED TRAINING PROGRAMS

PROFESSIONAL SERVICES ENGAGEMENT

PRODUCT ANALYSIS & SELECTION

A ROADMAP TO ACHIEVING ENTERPRISE RESILIENCE AND CORPORATE CERTIFICATION

DCAG SERVICES

Business Continuity Management
Ensuring readiness for disruptions to sustain critical operations

Disaster Recovery
Planning for the restoration of IT systems an I data following an incident

Risk Management
Identifying, assessing, and mitigating potential threats

Vulnerability Management
Detecting and addressing weaknessees in systems and software

Operations Management
Optimizing processes for effective and efficient through a structured approach

Systems Development Life Cycle (SDLC)
Guiding the cration and maintenances systems through a structured approach

Production Operations Support (ATO, CATO)
Enabling secure and compliant systems deployment and operation

Software Supply Chain Management (SBOM)
Managing the integrity of software components. and their dependencies

Corporate Certification
Achieving standards and certifications for organizational excellence

Helping organizations enhance resilience, manage risk, and maintain compliance