Vendor Risk Management (VRM) system

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 Vendor Risk Management (VRM), Third-Party Risk Management (TPRM), Supply Chain Management (SCM), and Business Continuity Management (BCM) through an Application Factory (AP) with adjustable quality control gates (QCGs) 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 then illustrates how an executive Dashboard can monitor and report on exceptions to appropriate personnel as rapidly as possible, so that corrective action can be taken 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.

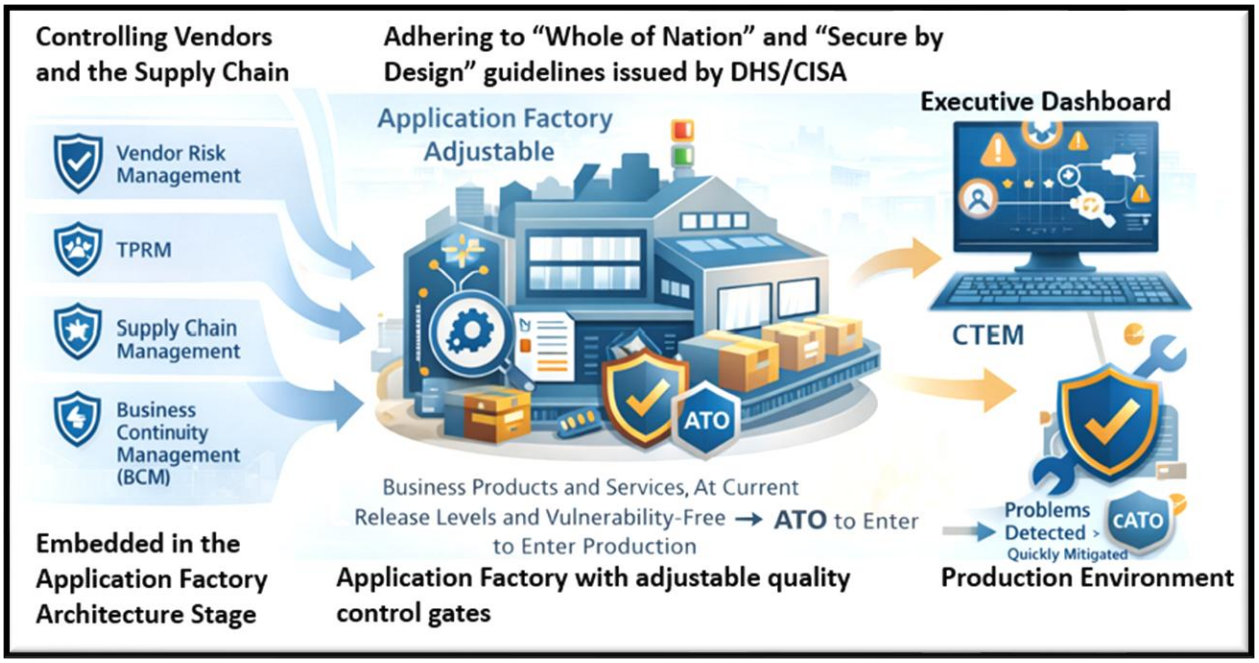


Figure 1: Vendor Risk Management through Application Factory to achieve ATO and using CTEM to achieve cATO.

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

Executive Summary

Why 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.

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, and the suppliers must be notified so that they can deliver their supplies to the new location during a disaster event.

Business operations is dependent on customers being supported and business products or services, provided through a Vendor Risk Management system that includes Vendors, Suppliers, and Transportation of components to support client demands.

One additional ingredient in Vendor Risk Management is 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) can identify weaknesses that require patches or new

releases. Their use can support Vulnerability Management and keep your systems running at peak performance.

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.

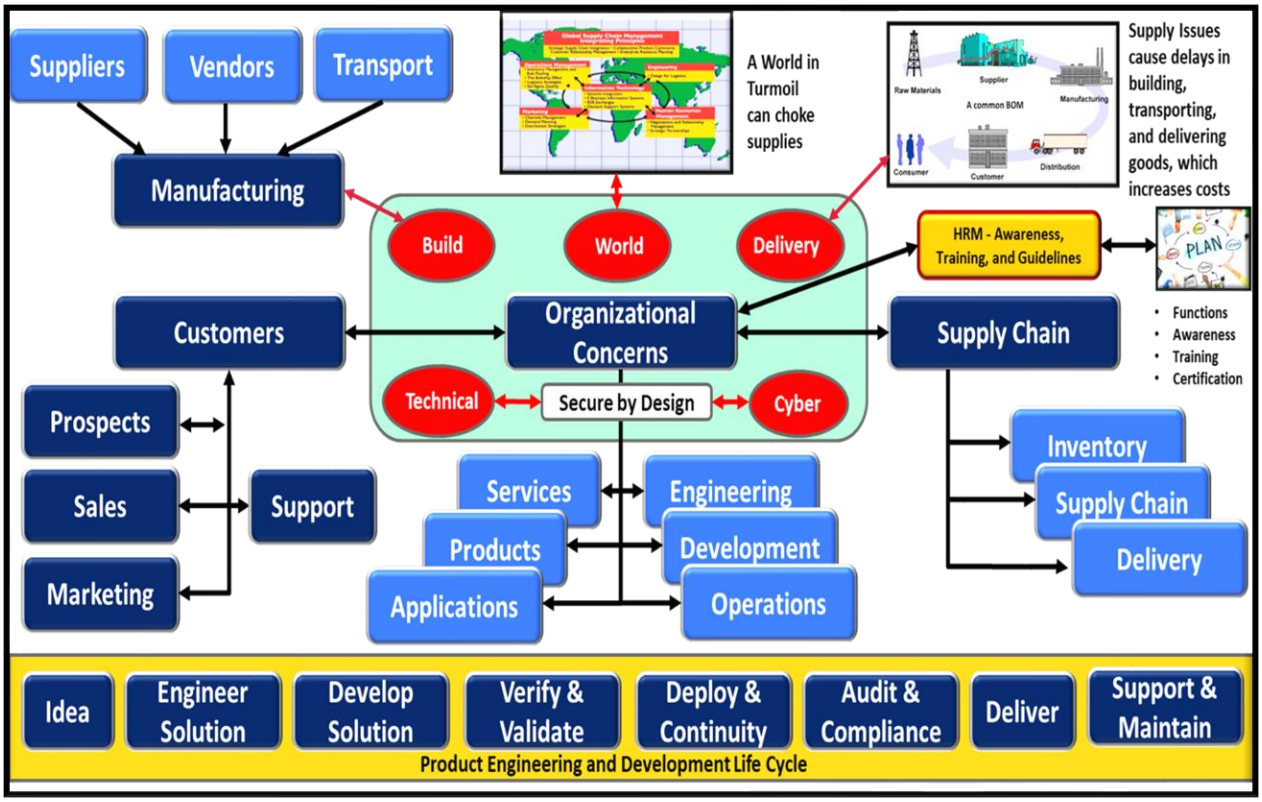


Figure 2: Overview of the Vendor Risk Management (VRM) Problem

Why This Matters to the Board

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

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.

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.

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.

Figure 3: Creating a Pilot System for Proof of Concept

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. Perform a review of 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. 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 system out to other areas in priority order. Gains in efficiency should be realized as the team matures.

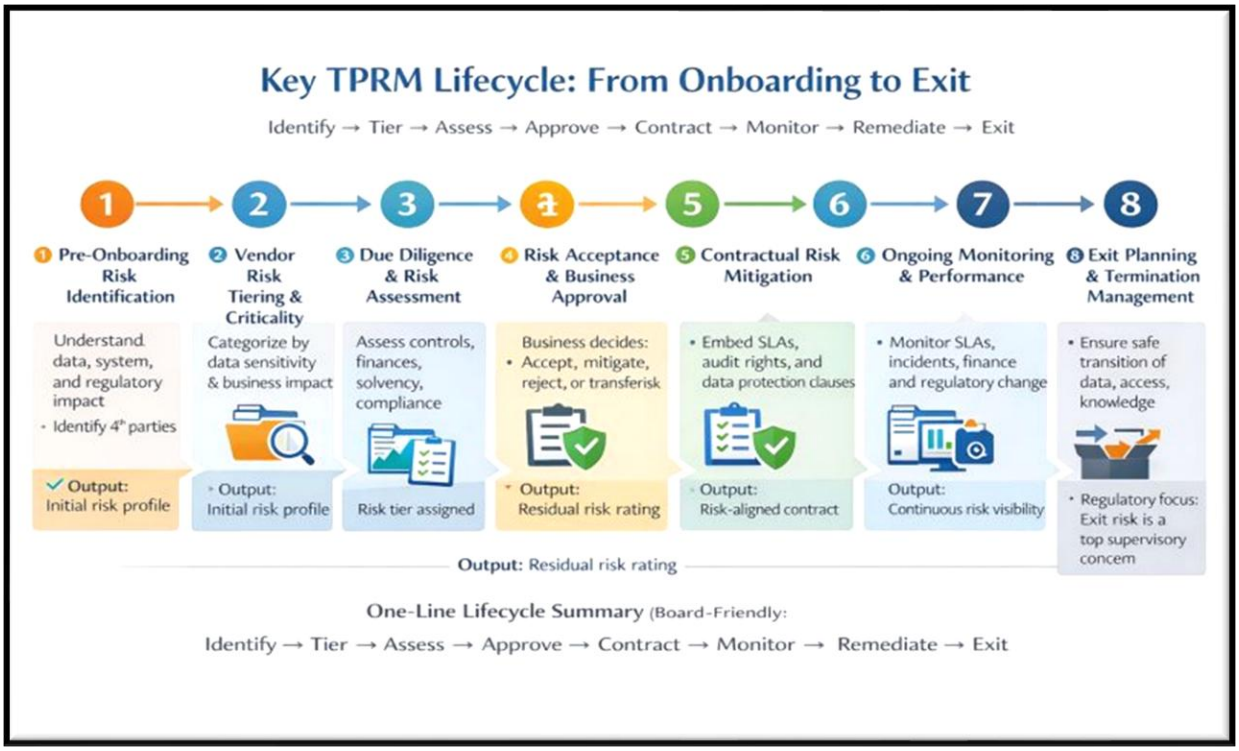


Figure 4: TPRM Lifecycle and stages.

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.

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 Supply Chain Management, with Supply Chain cybersecurity and 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) 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.

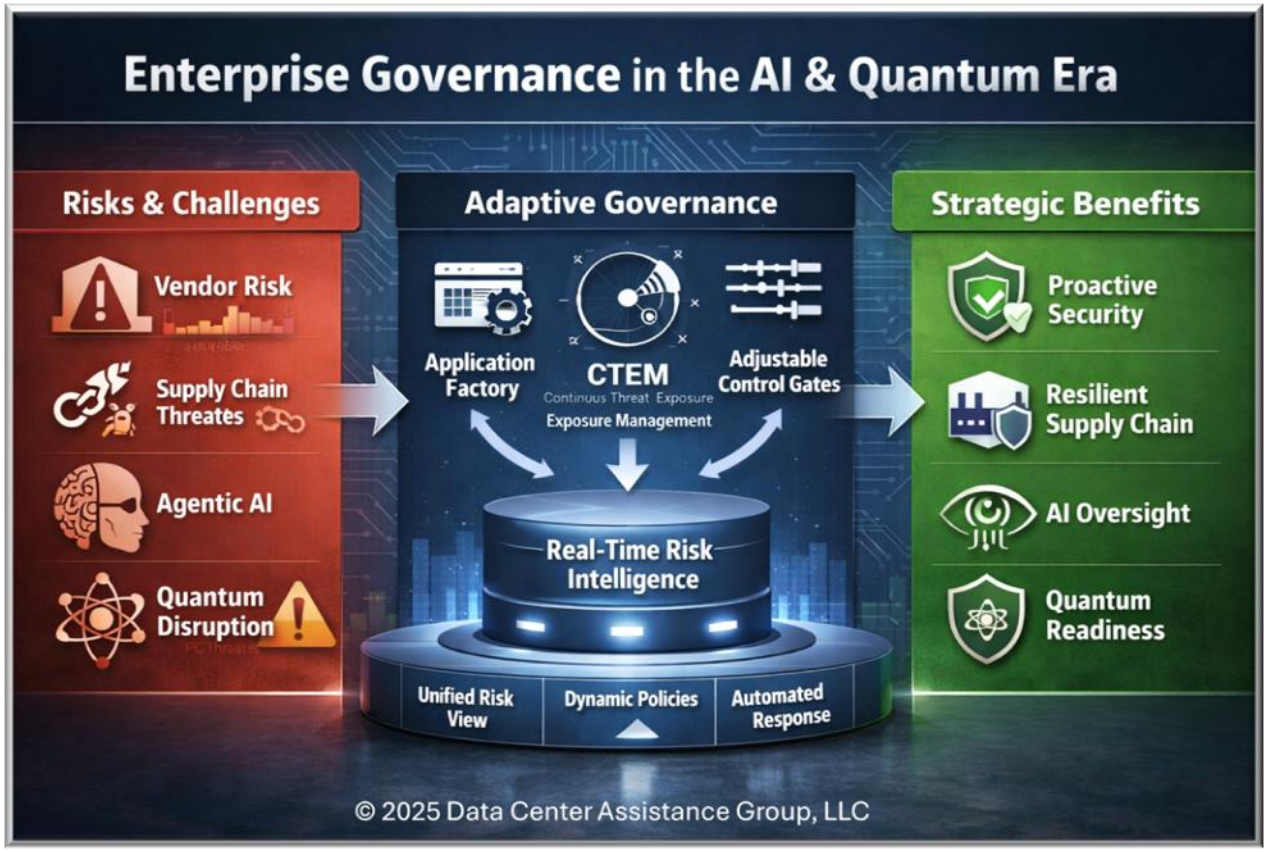


Figure 6: Fully implemented Vendor Risk Management System

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.

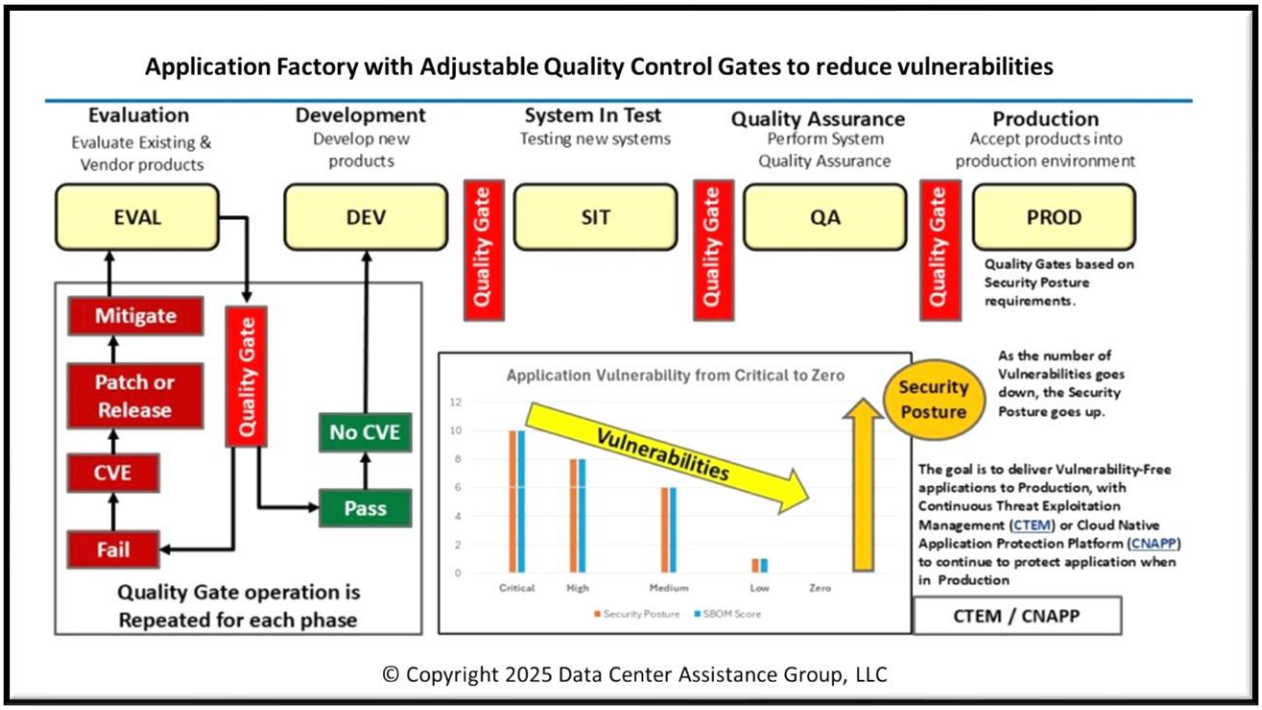


Figure 7: Application Factory with Quality Control Gates.

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 weaknesses and allow for rapid mitigation prior to impacting production business products and services provided to clients.

Completing VRN, 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.

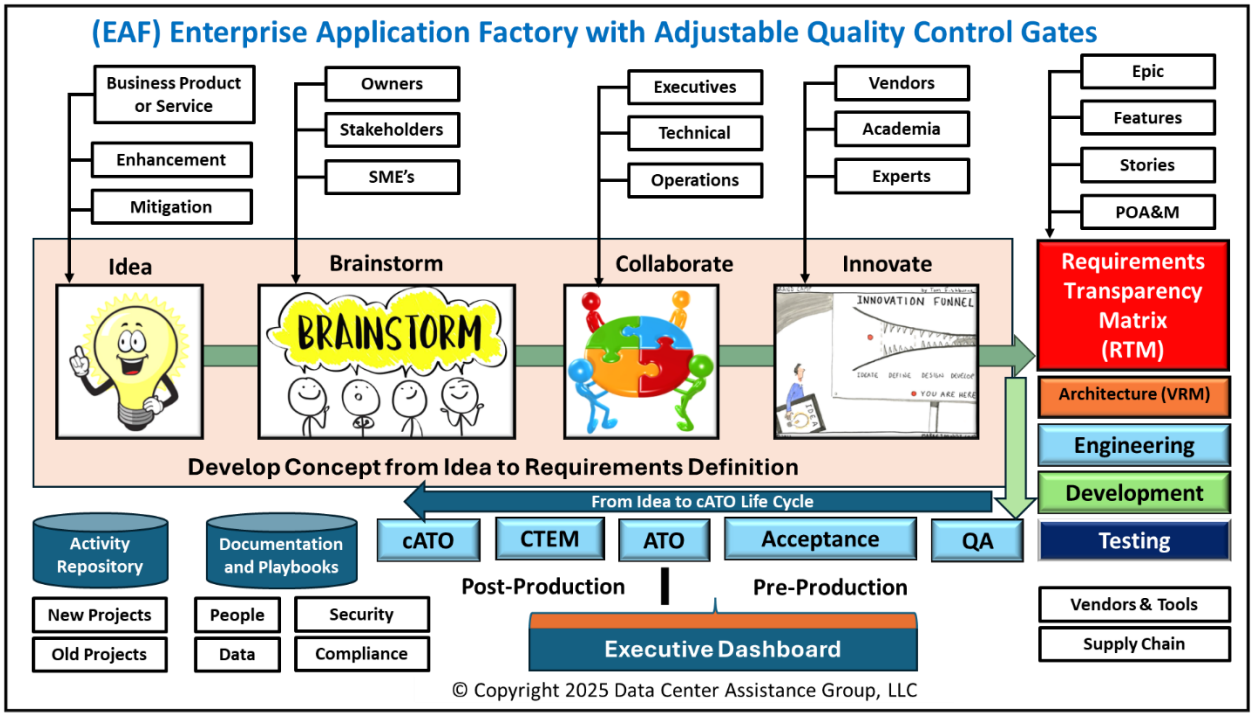


Figure 8: Fully implemented Application Factory with adjustable quality control gates.

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
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

Law / Regulation	Governing Body	Scope & Applicability	VRM / TPRM Implications
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
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

Law / Regulation	Authorities	Scope & Applicability	VRM / TPRM Implications
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.

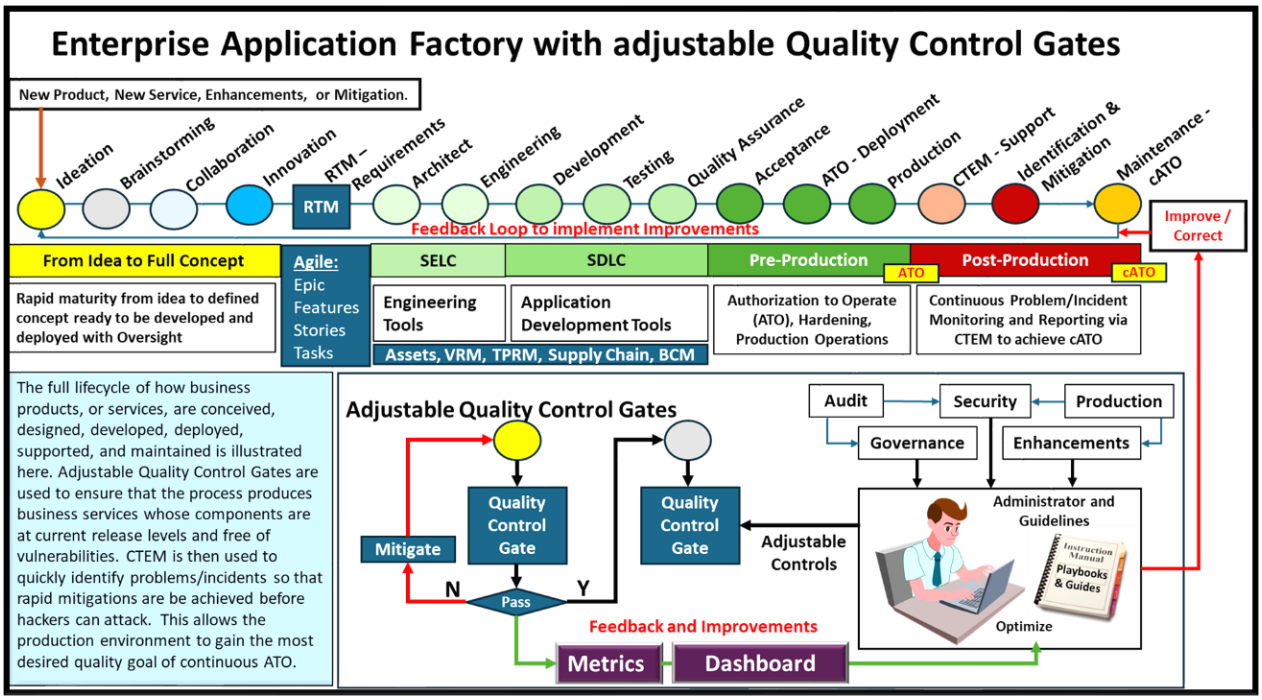
Failure to implement structured VRM / TPRM programs is now viewed as a **governance failure**, not an operational oversight. Board members will be deemed to lack their performance of due diligence and can be fined and sued (both the business and them personally).

Vendor Risk Management system and Application Factory relationship

The Vendor Risk Management system is part of the overall DevSecOps process being employed by many 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



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) which is the goal of every organization's production environment.
7. **Executive Dashboard** feed through system metrics displaying actions and status of products create, operations, and support, 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.

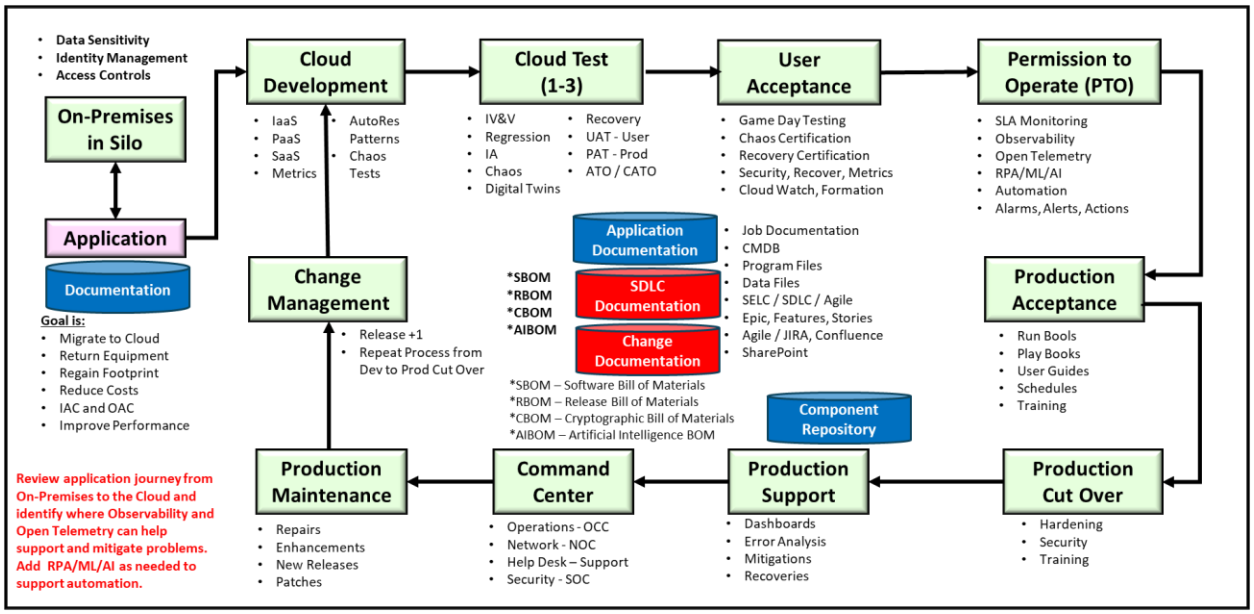
Call to Action

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:

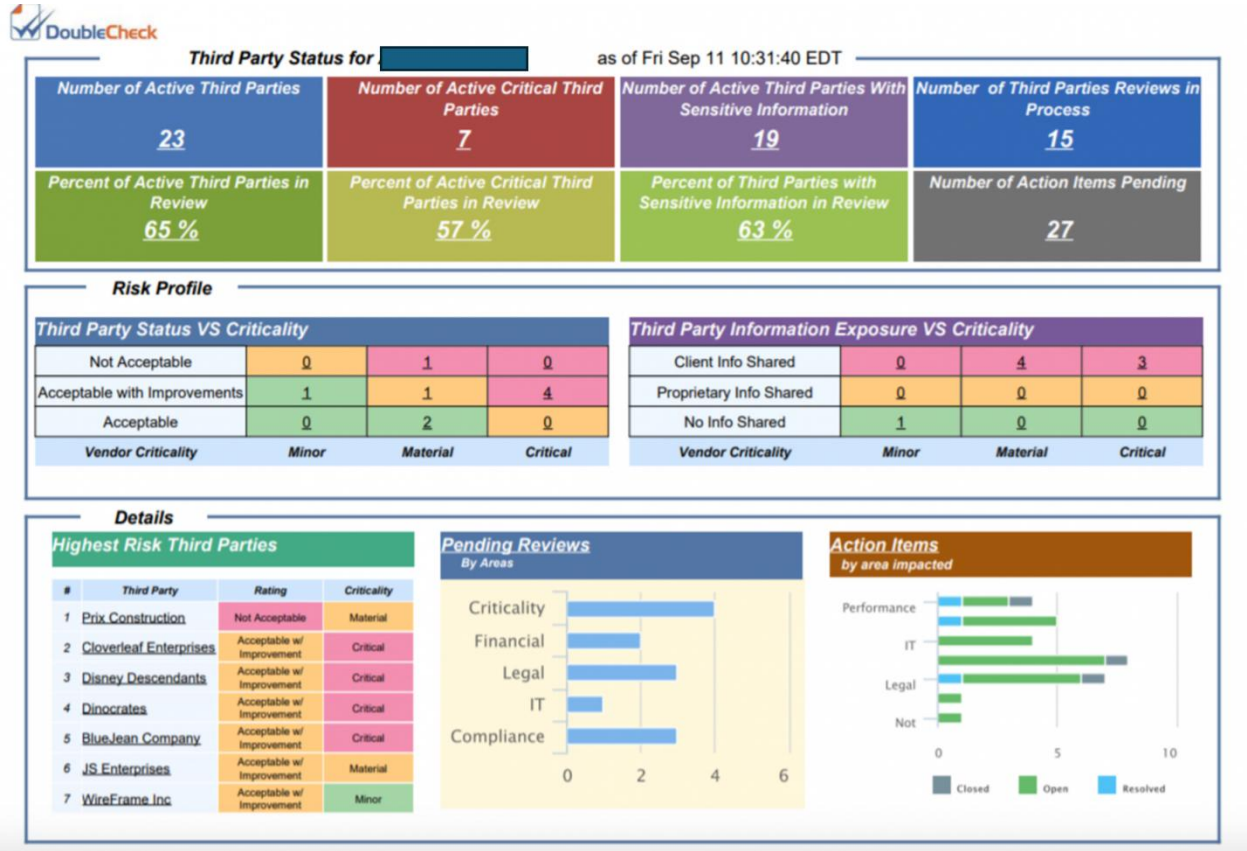
Migrating Applications to the Cloud



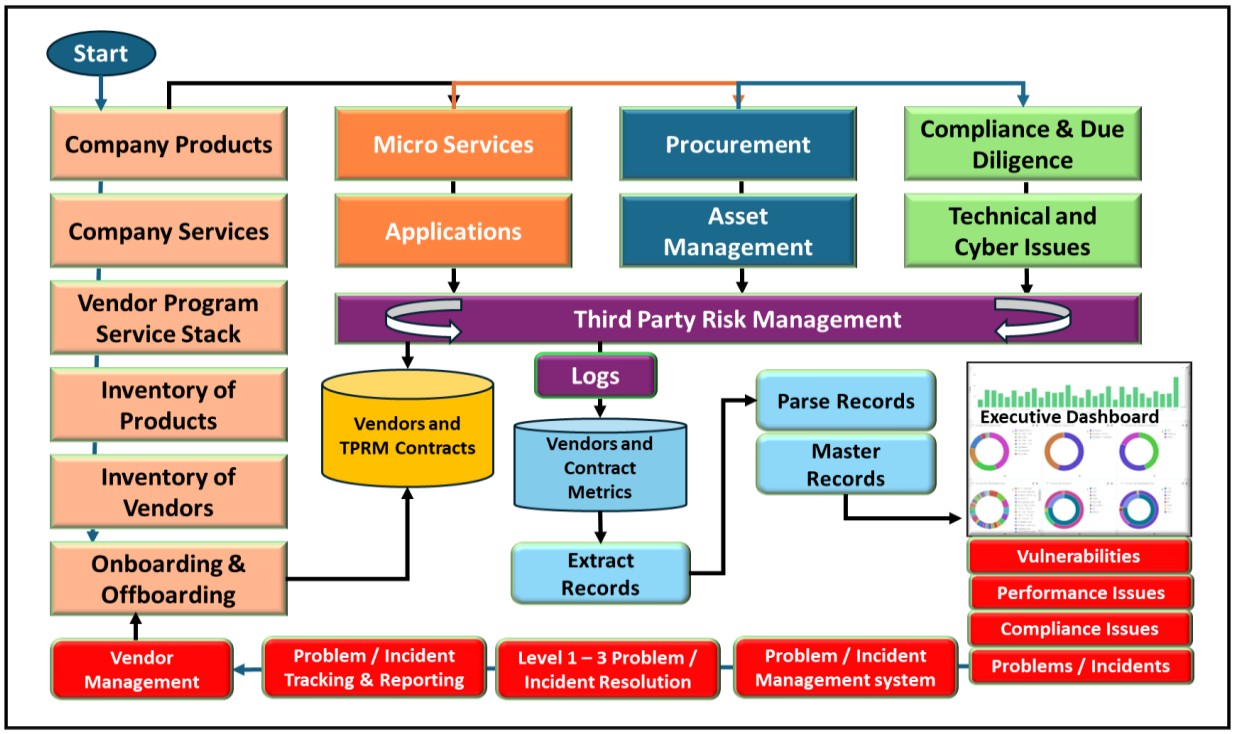
Third-Party Risk Management

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

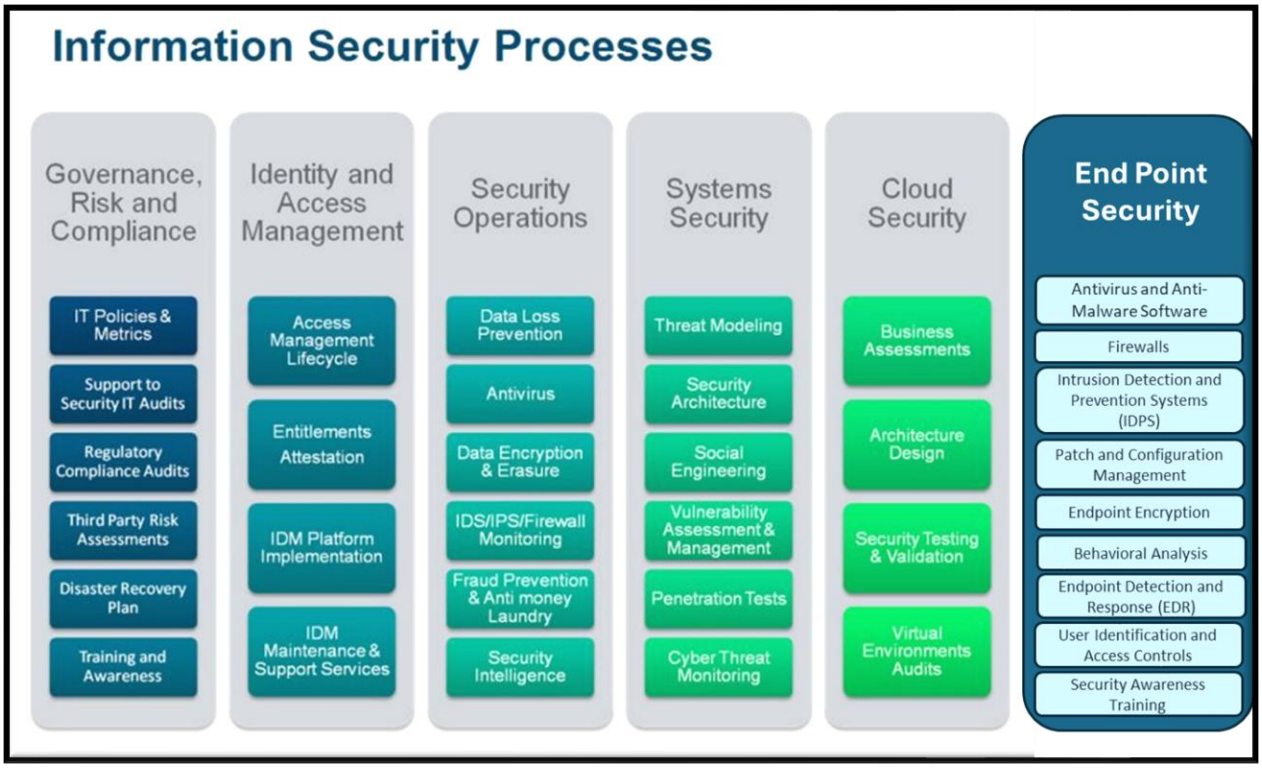
Sample Vendor Riks Management Executive Dashboard



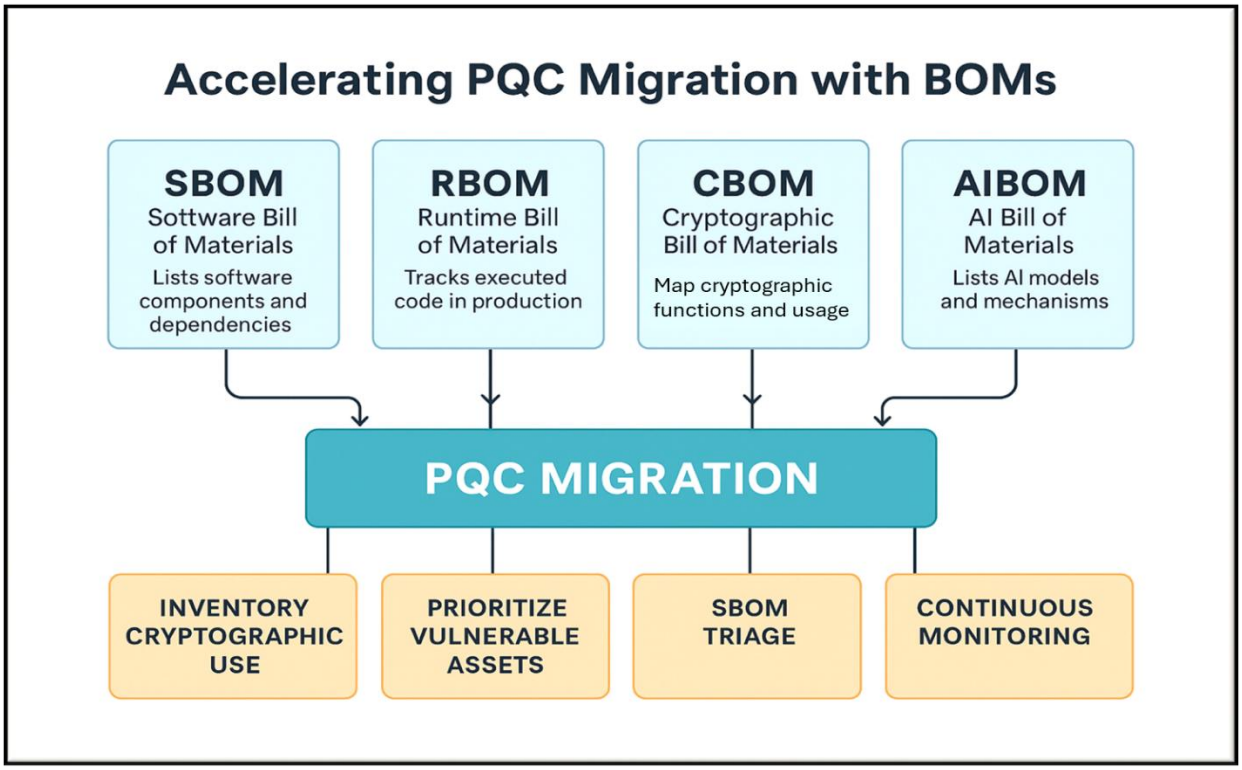
Third-Part Risk Management Project Overview



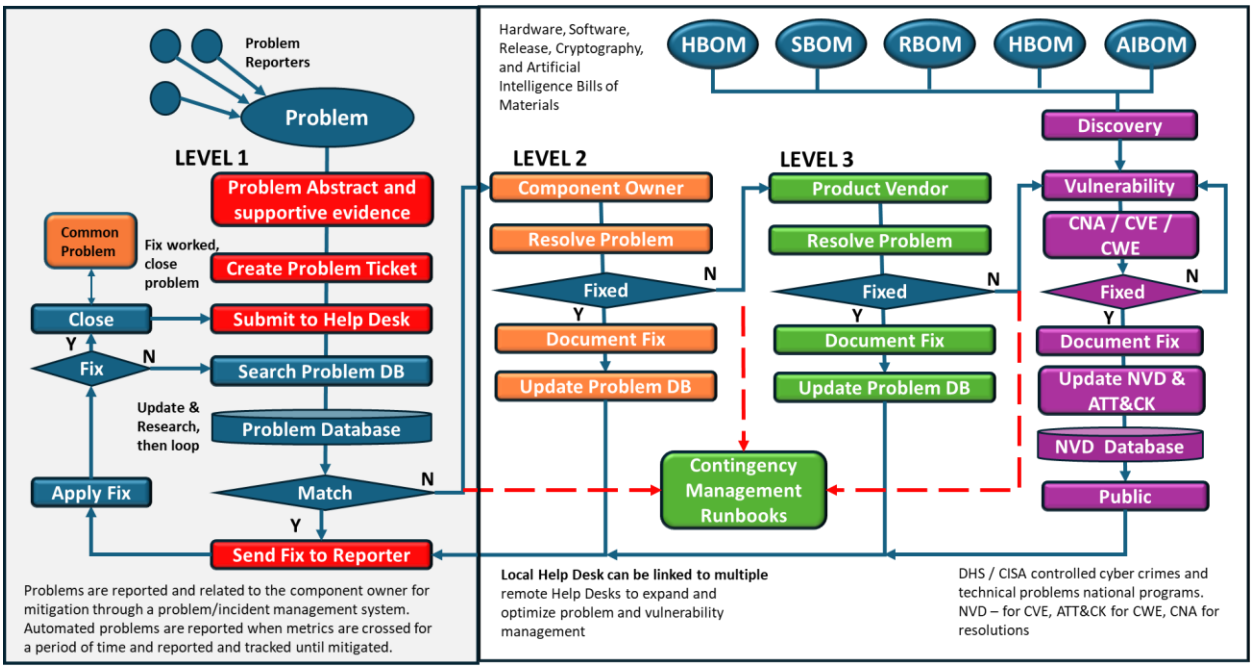
Information Security



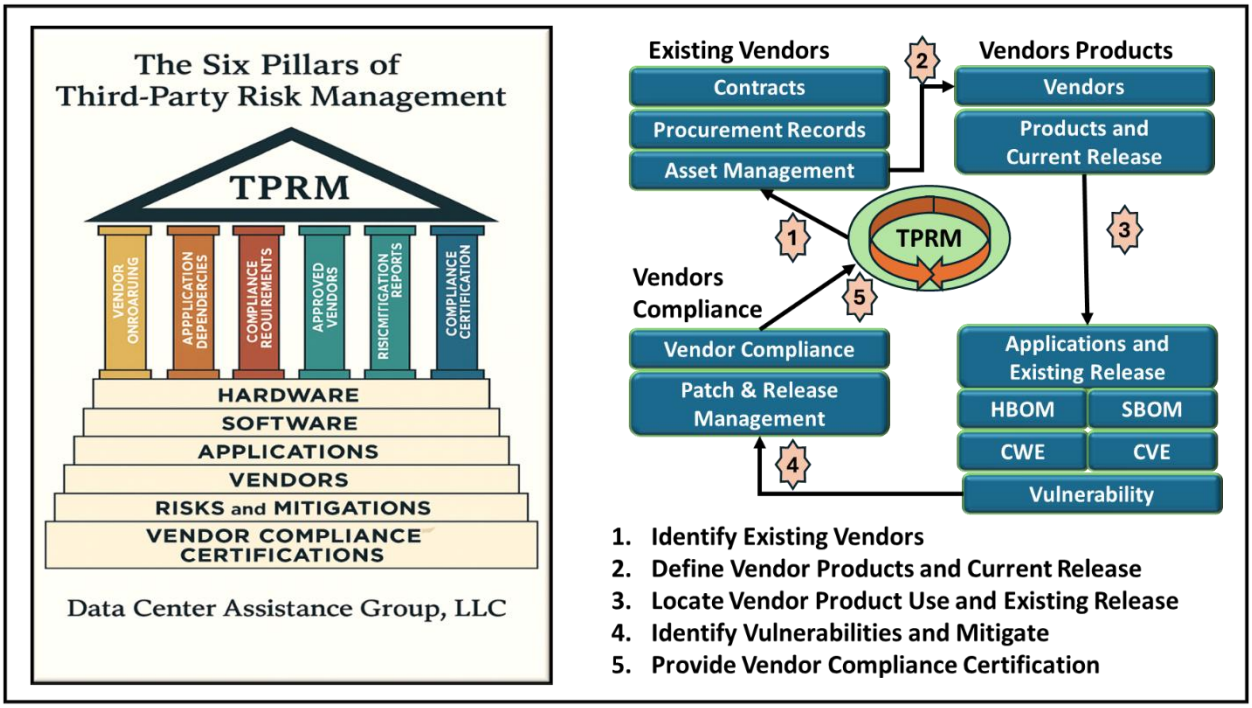
Accelerating PQC Migration and the use og BOMs



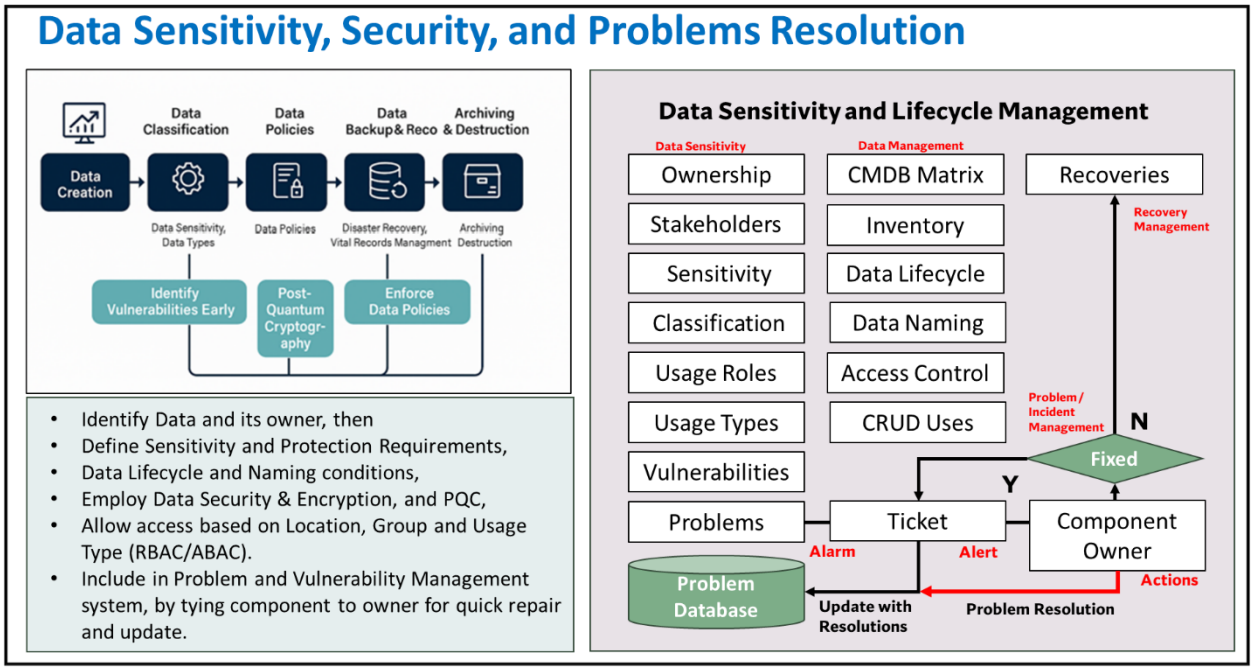
Problem / Incident Management with the use of BOMs



Third-Party Risk Management overview



Data Sensitivity, Security, and Problem Management



Application Security Testing - DevSecOps