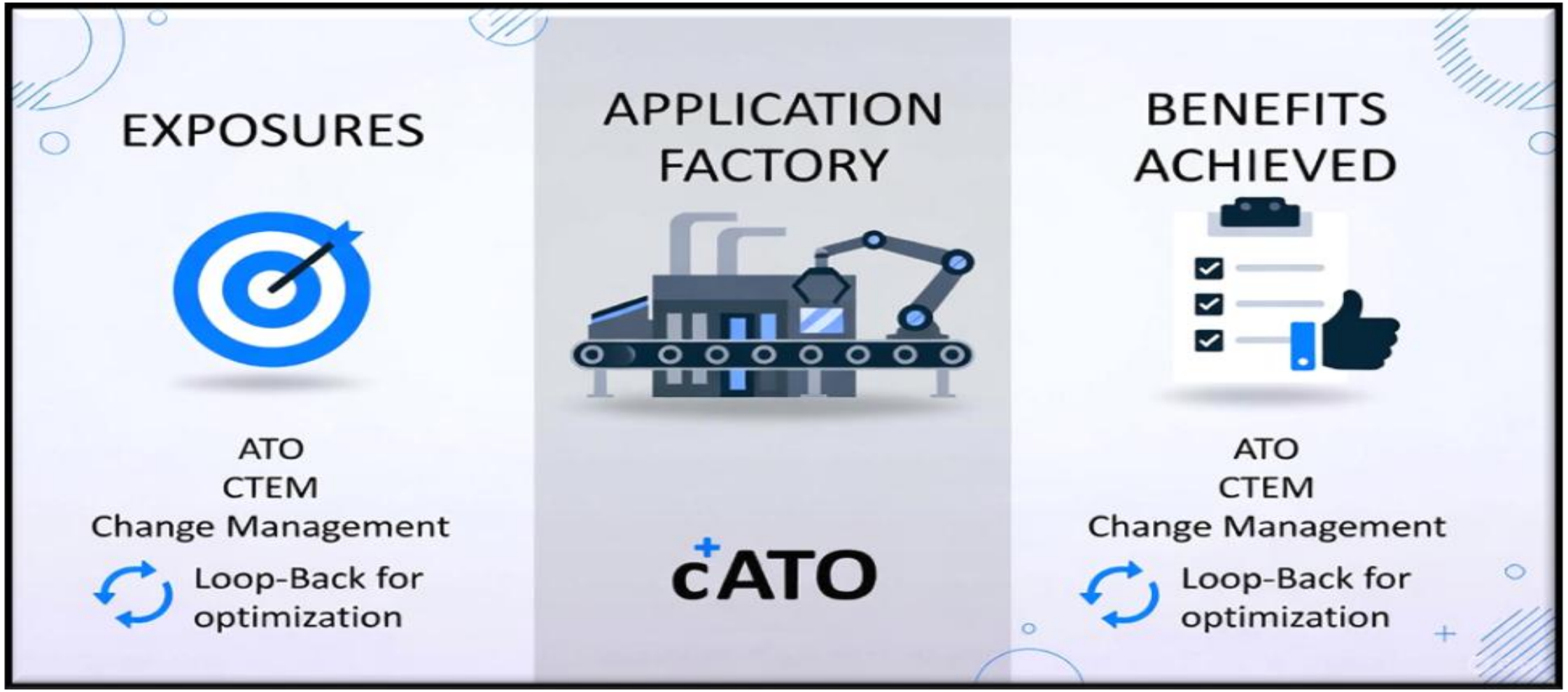


Application Factory

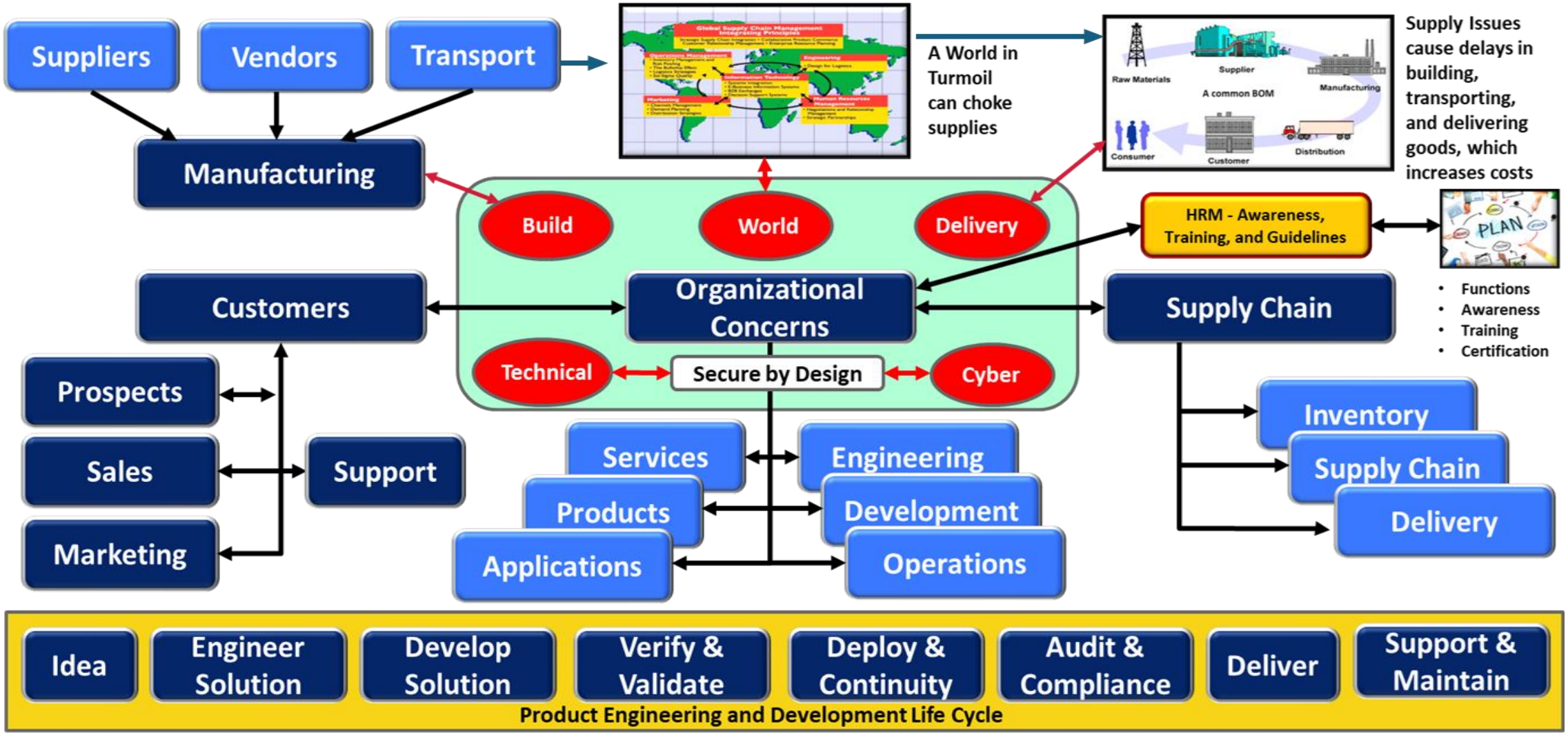
With adjustable quality control gates

Utilizing “Secure by Design” guidelines from DHS/CISA

Agenda

01	Executive Mandates
02	Why do we need an Application Factory
03	Delivering Quality Applications
04	Ideas, New Products / Services, Enhancements
05	Adherence to Due Diligence
06	Achieving ATO and cATO

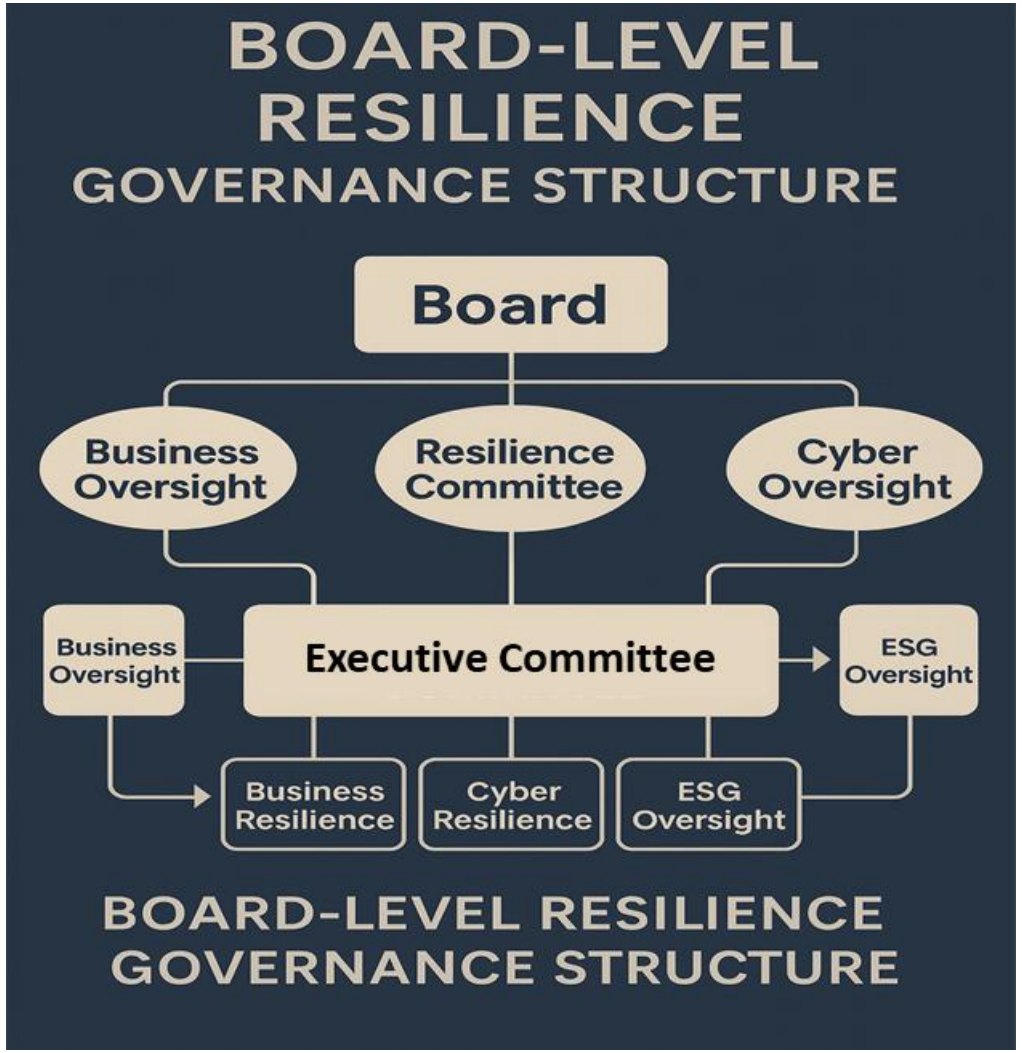
The Problem – a world in Turmoil



EXECUTIVE IMPERATIVES
The Mandate for Resilience & Governance

1. Lead with AI Governance & Safety	2. Secure the Foundational Core	3. Achieve Operational Autonomy	4. Enforce Continuous Resilience & Compliance
• Approve AI autonomy levels and guardrails (Tier 1/2). • Mandate Application Factory with Control Gates (secure-by-design). • Require AI-aligned roadmap and continuous model validation.	• Drive PQC migration across critical data stores. • Enforce Zero Trust identity modernization (password-less, machine identity). • Fund EROS deployment as the enterprise control plane.	• Implement Autonomous Operations (AIOps/SRE). • Establish Time-to-Autonomous-Containment (TTAC) targets. • Build Digital Twins for resilience simulation.	• Mandate CTEM for exploitability-driven prioritization. • Establish regulatory readiness score and evidence fabric. • * Prioritize multi-cloud resilience and supply chain integrity (CBOM).

Executive Mandates

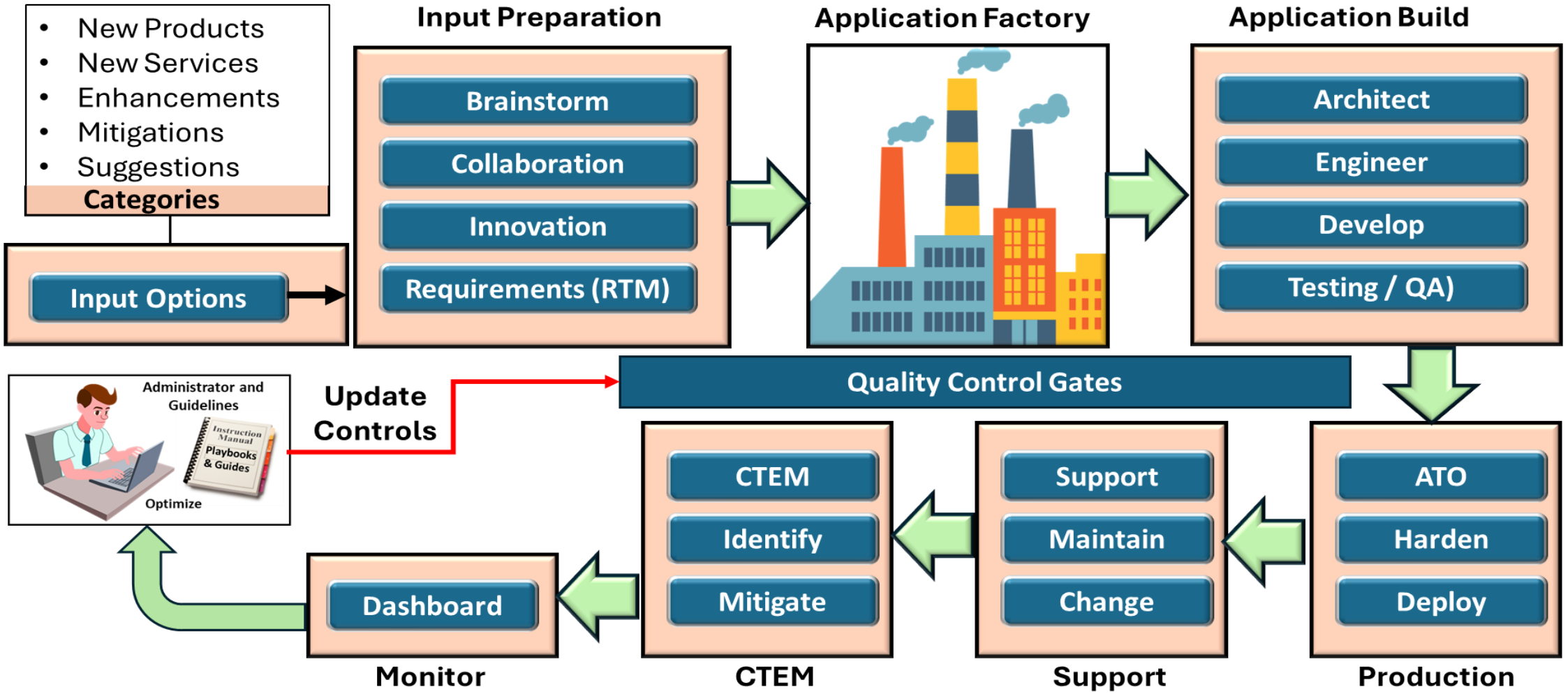


- Board & Governance Layer (Strategy, Oversight, Fiduciary Duty)
- Enterprise Risk & Compliance Layer (NST CSF 2.0, Security-by-Design, ESG)
- PQC & Crypto-Agility Layer (CBOM, ML-KEM, ML-DSA, Hybrid Cryptography)
- CTEM & Threat Management Layer (Exposure Validation, Continuous Controls Testing)
- AI Governance & Control Gates Layer (Drift, Safety, Bias, Runtime Oversight)
- Digital Twin & Predictive Ops Layer (Failure Forecasting, Scenario Simulation)
- Active-Active Infrastructure Layer (Zero RPO, Autonomous Failover, High Availability)

Why do we need an Application Factory

- Adhere to “**Secure by Design**” guidelines from DHS/CISA.
- **One System** combines all Products / Services / Enhancements / Improvements / Suggestions into a unified applications Development, Support, and Maintenance process for best control.
- **Adjustable quality control gates** to verify quality, security, compliance, and recovery.
- **Ensure** all pertinent Artefacts and Runbooks are included in turnover package.
- **Provide** Awareness and Training sessions to all required personnel.
- **Unified process** based on DevSecOps with Vendor Packages, In-House Tools, and Agentic AI Agents whenever possible.
- Provided **executive dashboard** to ensure Due Diligence and Fiduciary responsibility.
- **Administration** to provide improvements until optimized.

Application Factory – Controlled Phases



(EAF) Enterprise Application Factory

Optimize

Start

Idea, Fix, or new Product

Create Work Order & PO Trace

OK

Pass

Fail

All Phases

Stakeholder approval

Brainstorm

OK

Pass

Fail

Executive approval

Collaborate

OK

Pass

Fail

Innovator approval

Innovate

OK

Pass

Fail

END

Vendor Product

Requirements Definition & RFP

Analysis of Alternatives (AoA)

Select Vendor

Select Product

ONBOARDING

VRM, TPRM, C-SCRM

Documentation Repository

Create and Record a Project, then maintain all project related information

Build In-House

Requirements Transparency Matrix (RTM)

POA&M

Architecture Process

CATO — Update

CTEM — Support

ATO — Deploy

Acceptance — Accept

SDLC — Develop

SELC — Engineer

1. Product Inception through Go/No-Go.
2. Adjustable Control Gates at every phase.
3. Build in-house or select Vendor Product.
4. RTM, POA&M to Build / Implement product.
5. ATO to Production, with CTEM and CATO after production for continued protection.
6. Integrate automation as needed.

Overview of Application Factory

Enterprise Application Factory with adjustable Quality Control Gates

New Product, New Service, Enhancements, Mitigation, or Idea.

Ideation → Brainstorming → Collaboration → Innovation → RTM – Requirements → Architect → Engineering → Development – CI/CD → Testing → Quality Assurance → Acceptance → ATO - Deployment → Production → CTEM - Support → Identification & Mitigation -Risk Score → Maintenance - cATO

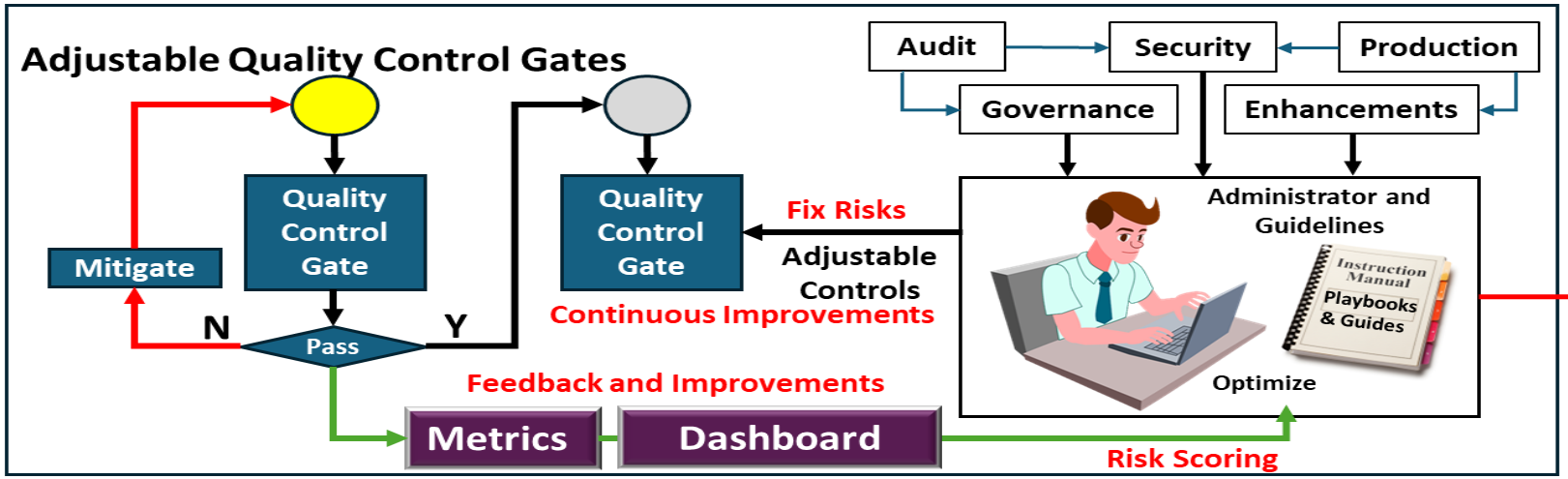
Feedback Loop to implement Improvements

Improve / Correct

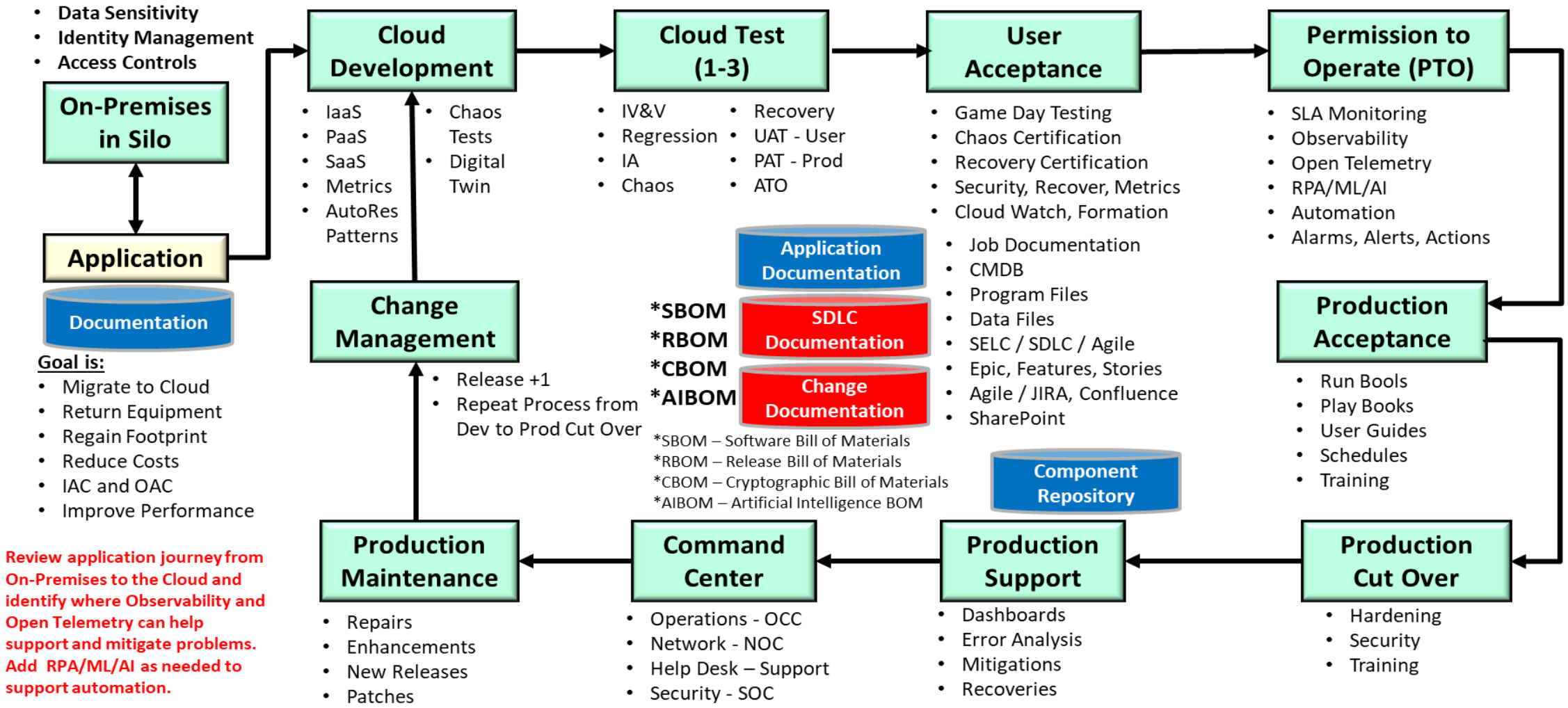
From Idea to Full Concept	Agile: Epic Features Stories POA&M	SELC	SDLC	Pre-Production (ATO)	Post-Production (cATO)
Rapid maturity from idea to defined concept ready to be developed and deployed with Oversight		Engineering Tools	Application Development Tools	Authorization to Operate (ATO), Hardening, Production Operations	Continuous Problem/Incident Monitoring and Reporting via CTEM to achieve cATO
		Assets, VRM, TPRM, Supply Chain, BCM			

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



Application Detailed Phases and Actions



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, POA&M 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, reduce weaknesses, and achieve optimization

Administrator Adjustments

Executive Dashboard

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.

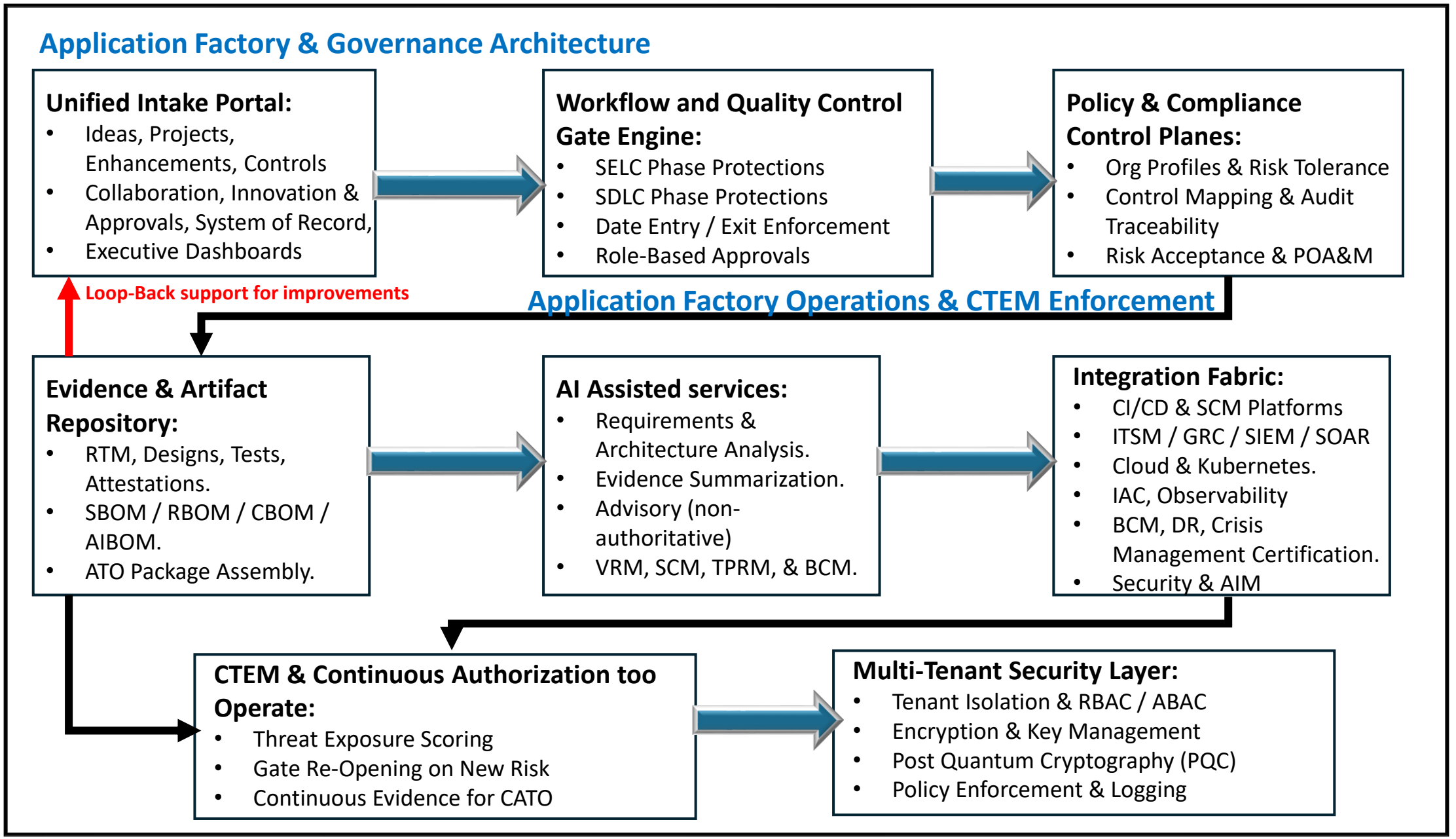
Setup

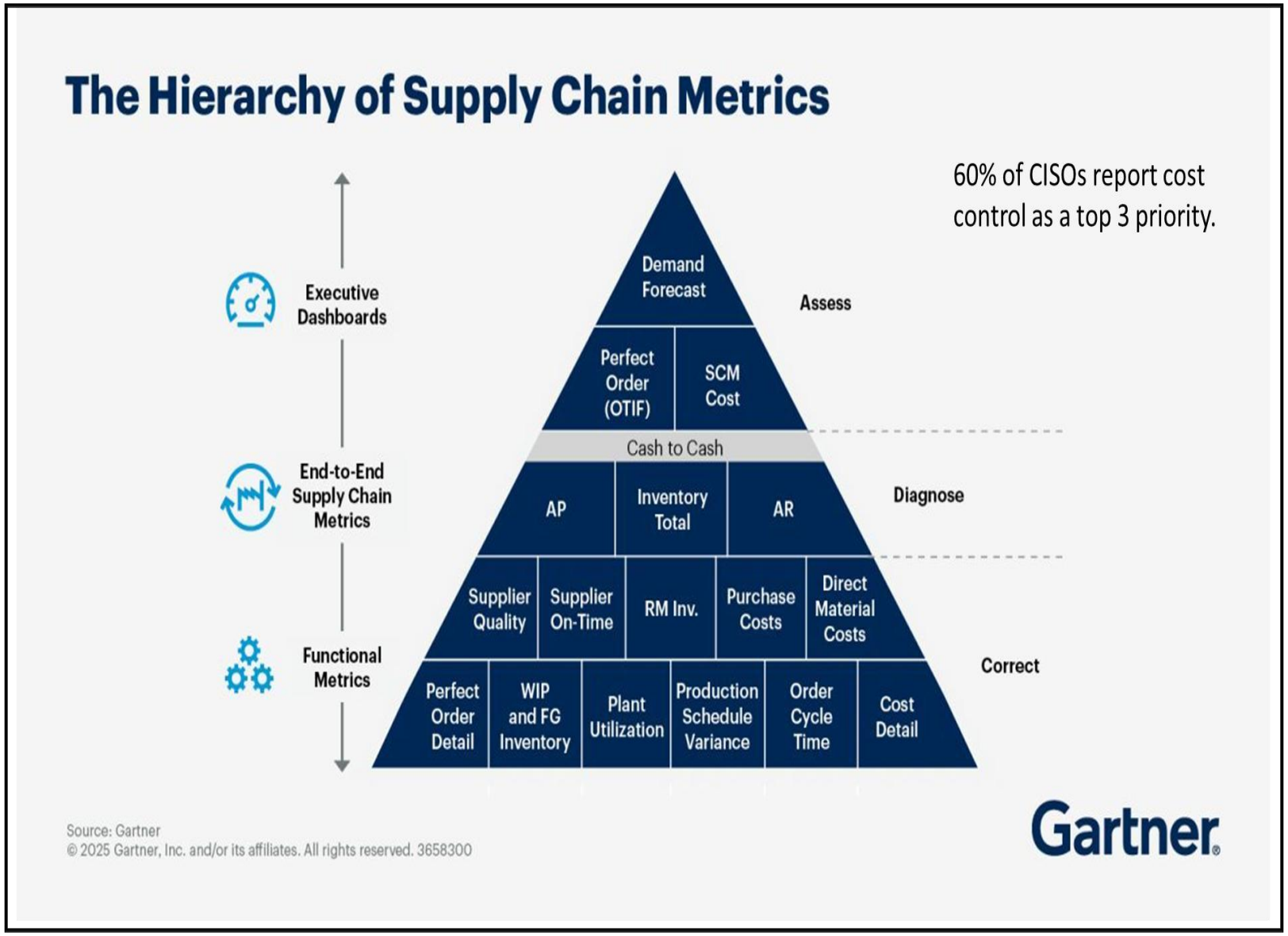
Feedback

Administrator

Optimize

Application Factory & Governance Architecture



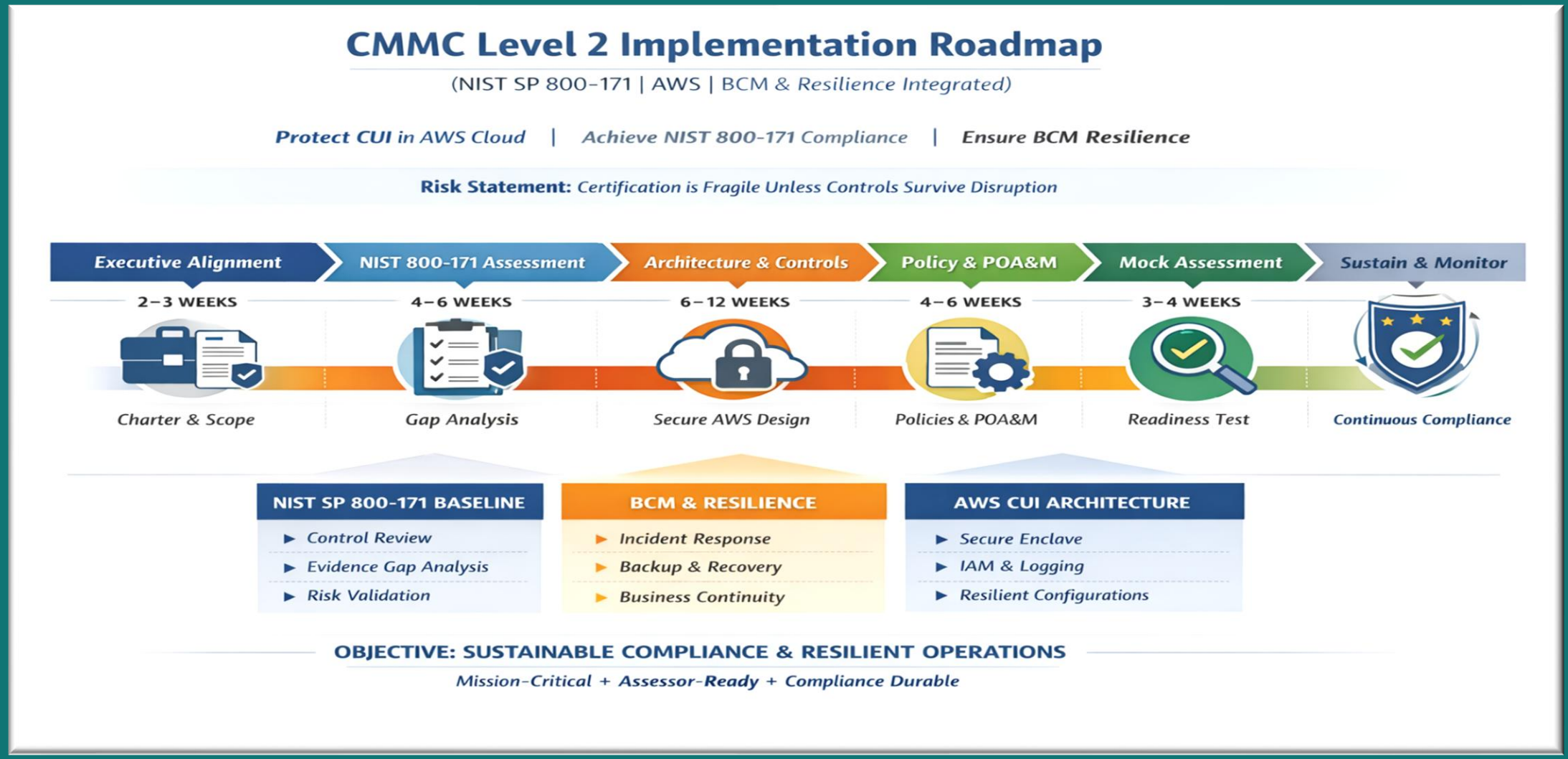


Vendor Management Requirements

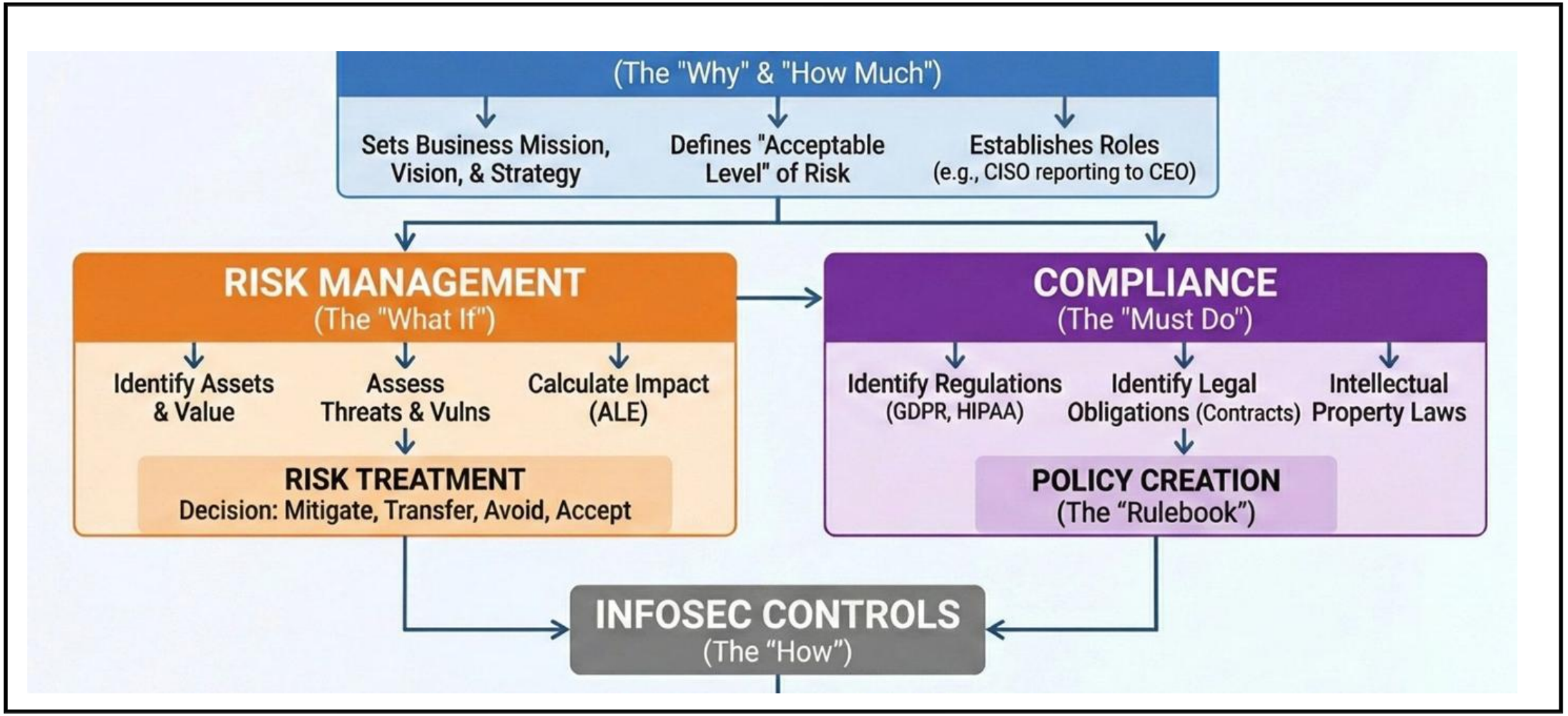
- Link to Supply Chain Data from Gartner
- **Define future needs and controls.**
- **eDiscovery of vendors and analysis of end-to-end supply chain weaknesses.**
- **Ensure Vendors meet compliance and cost requirements.**
- **Ensure vendors can meet supply demands and have alternative delivery methods.**
- **Vendor contracts with SLA.**
- **Vendor Onboarding.**
- **Vendor monitoring and management.**
- **Correct Vendor weaknesses or offboarding of vendors.**
- **Provide Executive Dashboard for clarity.**

Vendor Risk Management (VRM) – Problems & Benefits

CMMC Roadmap

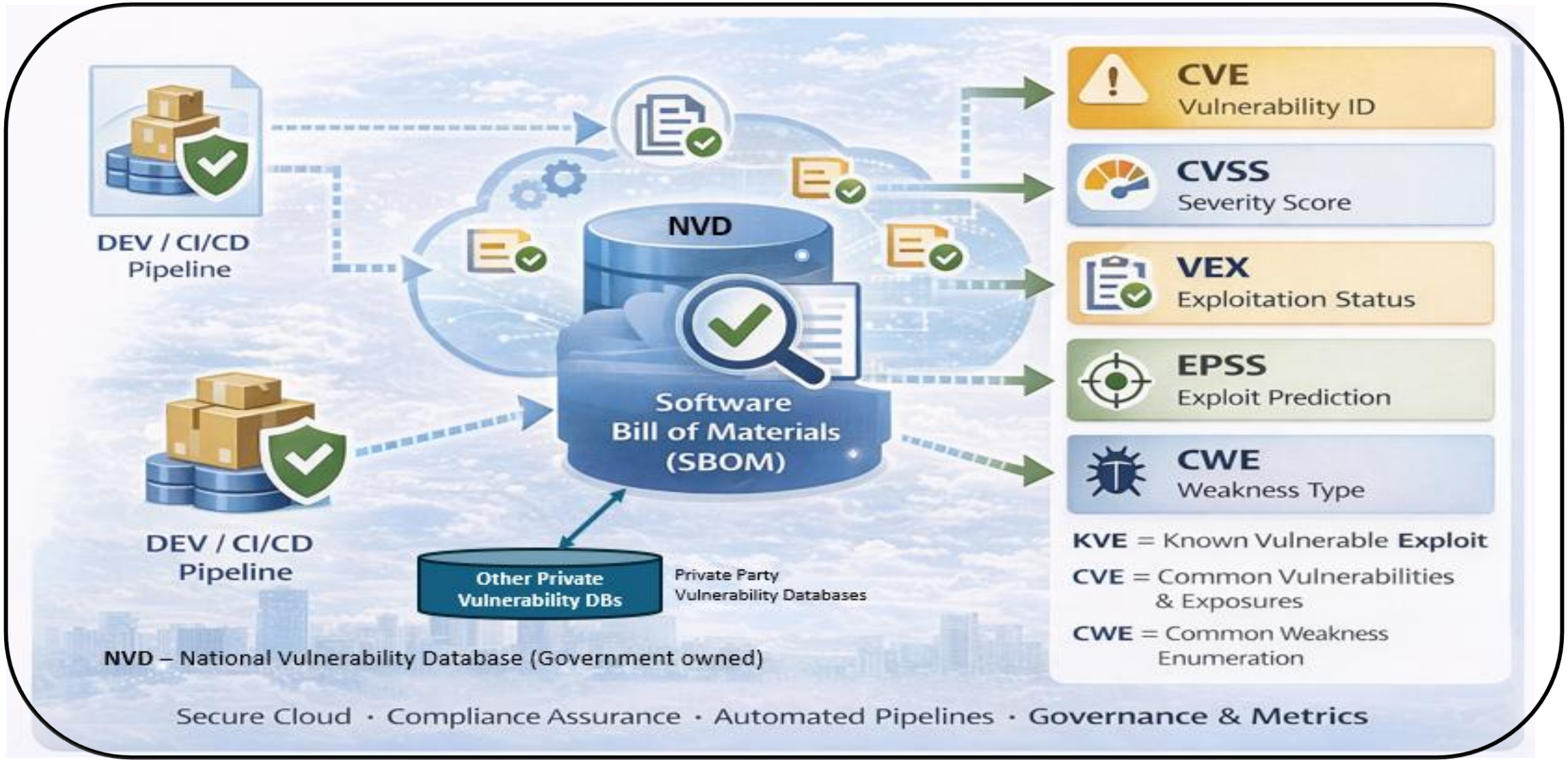


Information Security Controls



SBOM in operation

Hardware Vulnerabilities to be aware of:
UEFI – Unified Extensible Firmware Interface exploitation
Secure Boot – Validates System Boot prior to UEFI
Tee – Trusted Execution Environment



Control of C-SCRM, VRM, TPRM, SCM & BCM

The Quantum Threat to Data Security

- **Quantum computers** will break current encryption standards
- **Data encrypted today** can be stolen and stored for decryption later ("harvest now, decrypt later") by Hackers
- **Only Post Quantum Cryptography** (PQC) can protect your data, but only if you convert to PQC before data is stolen.
- **Protect** your critical infrastructure, financial systems, supply chains, and sensitive data at risk
- **Timeline:** Quantum computers capable of breaking RSA encryption within 5-10 years

Quantum Computing Threat

Current encryption methods like RSA and ECC will be vulnerable to quantum algorithms.

Developing a Quantum-Readiness Roadmap

Shor's Algorithm can factor large numbers exponentially faster than classical computers, breaking encryption that secures your data today. Grover's Algorithm can rapidly crunch numbers

CISA Post Quantum Readiness Report

Business Case for PQC Implementation

- **Risk mitigation:** Protect against future quantum attacks
- **Competitive advantage:** Early adoption demonstrates security leadership
- **Compliance:** Meet emerging regulatory requirements
- **Customer trust:** Ensure long-term data protection
- **Protect Against Harvest Now, Decrypt Later (HNDL):** Protect your most important encrypted data from being copied now and decrypted later by Hackers. Once they have your data, there is nothing you can do to protect yourself.

ROI Considerations

Implementation costs: $250K-$500K for mid-sized enterprise

Cost of breach: Average $4.45M per incident (IBM 2023)

Risk reduction: Early implementation reduces exposure by 65%

Market advantage: 73% of customers value future-proof security

Next Steps

- **Executive sponsorship** and resource allocation
- Establish **PQC implementation team**
- **Discover** where encryption is presently being used and prioritize components and data usage
- Develop detailed **technical project plan** with migration waves
- Begin **cryptographic inventory assessment**
- **Complete conversion** in priority order by due date.

Timeline

Month 1-2: Assessment and team formation

Month 3-4: Risk analysis and solution selection

Month 5-8: Testing and pilot implementation

Month 9-18: Phased full deployment

Project Personnel Requirements & Skills
Plus, cost estimates for services

Role	Number Needed	Key Skills
Project Manager	1	Project coordination, stakeholder communication, risk management
Cryptography Expert	1–2	Deep understanding of PQC algorithms, cryptographic systems
Security Analyst	2–3	Risk assessment, vulnerability analysis, compliance knowledge
Systems Engineer	2–3	System integration, network architecture, performance tuning
DevSecOps Specialist	1–2	CI/CD pipelines, security automation, infrastructure as code
Training Coordinator	1	Developing training materials, conducting sessions, feedback collection

Phase	Duration	Consulting Hours	Cost (@$150/hr)
Assessment & Planning	4–6 weeks	240–360	$36,000–$54,000
Design & Pilot Implementation	6–8 weeks	360–480	$54,000–$72,000
Full-Scale Deployment	12–16 weeks	720–960	$108,000–$144,000
Monitoring & Maintenance	Ongoing	Varies	Varies
Total	22–30 weeks	1,320–1,800	$198,000–$270,000

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

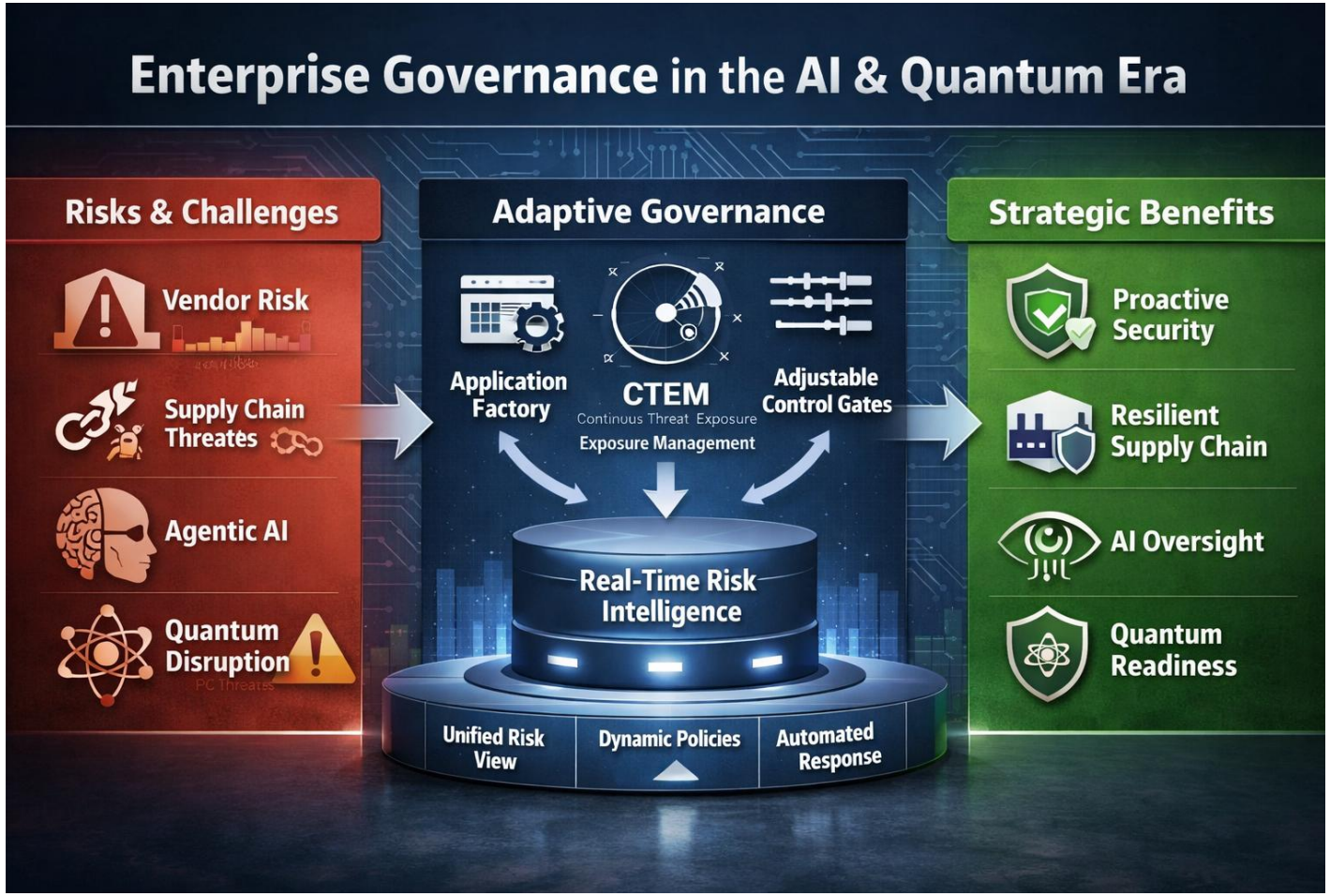
1. eDiscovery – Inventory & Configuration
2. Risk Assessment and Vendor Identification.
3. Prioritize and sequence mitigation.
4. Define Vendor onboarding requirements.
5. Define Vendor Contract and SLA.
6. Onboard or reject vendors.
7. Monitor & Maintain Vendor approvals.

Roll System Out in Waves

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

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 .

Fully implemented Enterprise Governance in AI and Quantum Era with Application Factory



- **Continuously Achieve Due Diligence and Fiduciary Responsibilities (Dashboard).**
- **Implement Application Factory with Adjustable Quality Control Gates and CTEM to fully automate security & compliance.**
- **Provide Real-Time Risk Monitoring and Controls (Vendor, Vulnerability, PQC, etc.).**
- **Automated Security protection.**
- **Automate Dynamic Policies.**
- **Automated Responses for continuous optimization.**
- **Quantum Readiness and use of ML/AI automation.**

Your Goal - The Ideal Environment

Board KPI's Reported

Compliance:

- Control effectiveness > 95%
- Audit findings closed < 30 days

Resilience:

- BCM exercises passed
- RTO/RPO achieved

Efficiency:

- Cycle time reduction
- Automation optimized
- Adherence to "Secure by Design"
- Error-Free environment

KPI = Key Performance Indicators