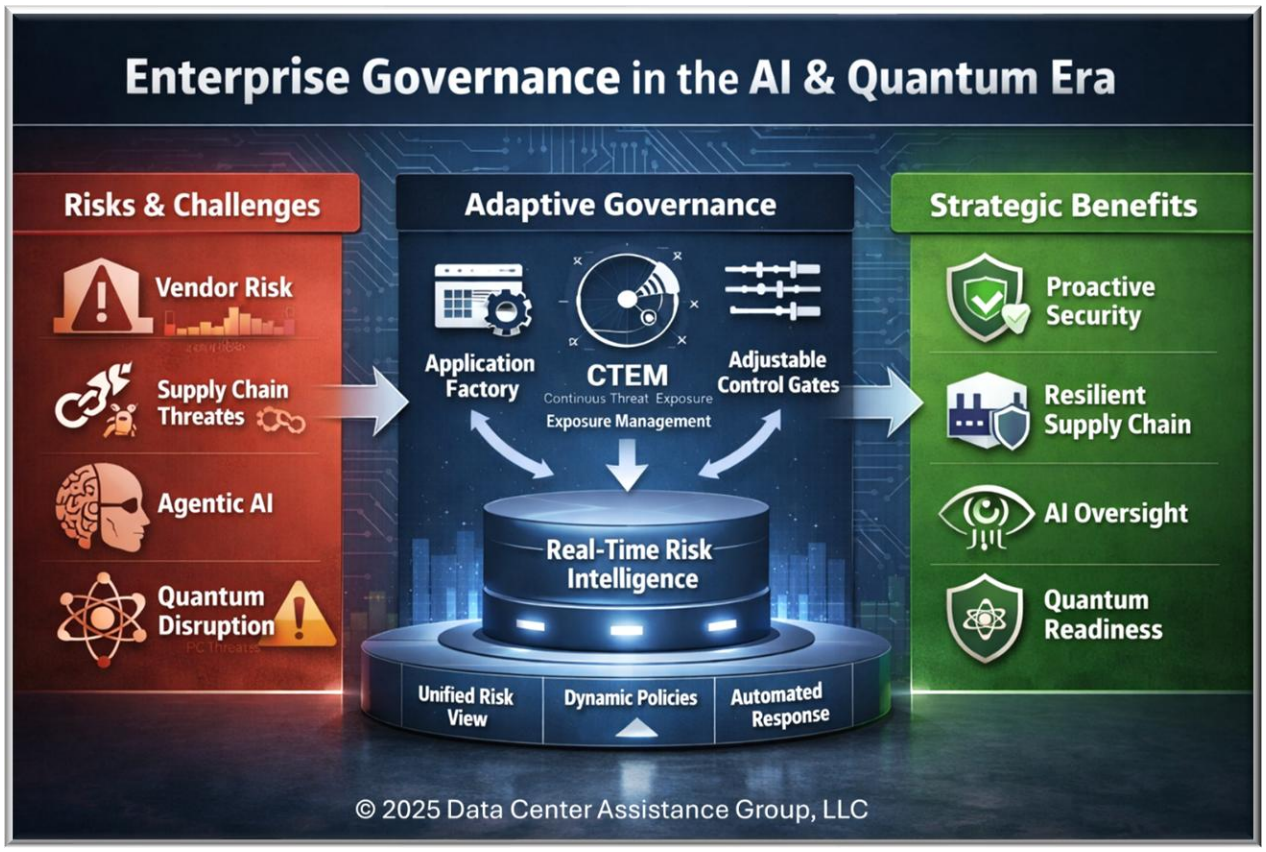

Governing the Un-Governable

Why Vendor Risk Management, Application Factories, and CTEM Must Evolve in the Era of AI and Quantum Computing

By Thomas Bronack
Executive Product Strategist | Enterprise Resilience Advisor
Data Center Assistance Group, LLC

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

Contents

Deliverable 1:

Executive Context: Control Is No Longer a Static State

Most enterprises still treat **control** as something you *achieve*.

- A vendor is onboarded.
- An application is approved.
- A system passes security review.

Then the organization moves on.

That model worked—when systems were slow, vendors were stable, and change was human-paced.

That world no longer exists.

Today's enterprises—especially those operating critical infrastructure—are governed by **continuous change engines**:

- Machine learning models retrain themselves.
- Agentic AI systems act autonomously.
- Software supply chains shift daily.
- Cryptographic assumptions are on a countdown clock.

Yet most governance, risk, and continuity structures remain **event-driven**, not **state-aware**.

This is not a tooling problem.

It is a **control philosophy problem**.

Vendor Risk and TPRM: Designed for Contracts, Not Collapse

Traditional Vendor Risk Management (VRM) and Third-Party Risk Management (TPRM) programs were built for a simpler question:

"Is this vendor acceptable at the time of onboarding?"

But modern failures do not originate during onboarding. They emerge **later**, when:

- A vendor updates a component.
- A SaaS provider changes an API.
- An AI model behaves unexpectedly.
- A downstream supplier quietly fails compliance.

In critical infrastructure environments, this delay is dangerous.

Risk now propagates faster than review cycles.

This is why VRM and TPRM must evolve from:

1. Questionnaire-driven processes
   to
2. **Operationally integrated control systems**

Risk must be observed, reported, acted on, and mitigated - not inferred.

The Supply Chain Is Now an Execution Layer

We often talk about "the supply chain" as if it were external.

Today's supply chain:

- Executes code inside your environment.
- Influences operational decisions through AI.
- Determines recovery feasibility during incidents.

This makes the supply chain part of your **runtime environment**, not just your procurement function.

Which raises a critical executive question:

If your supply chain can execute inside your enterprise, why isn't it governed like your enterprise?

The Application Factory as a Governance Instrument (Not a Dev Tool)

An **Application Factory** is often misunderstood as a productivity accelerator.

The Application Factory's most significant role is **governance enforcement on a scale**.

When designed correctly, an Application Factory becomes:

- A control plane
- An adjustable policy enforcement mechanism
- A risk gating system

The key is adjustable control gates.

Not every application, vendor integration, or AI workflow deserves the same scrutiny.
But *every one of them* must pass through adjustable control logic.

Adjustable gates allow:

- TPRM requirements will vary by criticality.
- Security controls to align with exposure.
- Resilience requirements reflect recovery expectations.
- AI usage to be constrained by trust and impact.

This is how governance becomes adaptive instead of obstructive.

CTEM: From Security Practice to Executive Nervous System

Continuous Threat Exposure Management (CTEM) is often positioned as a cybersecurity capability.

That undersells it.

CTEM is best understood as an **enterprise nervous system**:

- Sensing changes in exposure,
- Correlating risks across vendors, applications, and infrastructure, and
- Signaling when assumptions are no longer valid.

For executives, CTEM answers questions such as:

- *Which dependencies are becoming unsafe right now?*
- *Where does technical risk threaten operational continuity?*
- *What must be acted on before it becomes a business event?*
- *How can "Left of Boom" implement a proactive environment for better protection.*

CTEM does not replace governance.

It feeds it with reality.

Why AI and Agentic Systems Break Legacy Control Models

AI introduces a fundamental governance shift:

Behavior is no longer fully deterministic.

Agentic AI systems:

- Make decisions.
- Trigger actions.
- Interact with systems and vendors autonomously.

This means:

- Risk is no longer only human-initiated.
- Controls must operate **continuously.**
- Oversight must be embedded, not episodic.

In this context, governance must answer a new question:

"What is allowed to act, under what conditions, and how do we revoke trust in real time?"

Legacy approval models cannot keep up.

Quantum Computing: The Silent Deadline Executives Are Underestimating

Quantum computing introduces a different kind of risk:

- Not operational instability,
- But **delayed catastrophe.**

Data encrypted today may be compromised tomorrow.

Executives must recognize:

- Cryptographic trust is a **time-bound asset.**
- **Harvest Now, Decrypt Later (HNDL)** allows hackers to copy encrypted files containing your most sensitive data, put it on the shelf until Quantum Computing becomes available, decrypt it and then hold you at ransom, or sell off your secrets. If you do not protect yourself now and your sensitive data is stolen, there is nothing you can do to overcome the theft.
- **Post Quantum Cryptography (PQC)** must be implemented before 2030 to best protect data.
- Vendor and application dependencies inherit cryptographic risk.
- Future compromise invalidates past assumptions.

Quantum risk reinforces the need for:

- Visibility into components
- Control over dependencies
- Governance that spans **time**, not just systems

Deliverable 2:

The Collaboration Pivot

From Thought Leadership to Action

This is where most articles stop.

This one does not.

Because recognition without execution is exposure.

The Real Question for Executive Leadership

How do we translate governance intent into operational control—without slowing the business?

The answer is **not another policy**.

It is a **governed execution model**.

The Emerging Requirements Pattern (Executive View)

Organizations ready to move forward typically converge on a shared need:

1. A unified view of vendor, application, and supply-chain risk,
2. Control gates embedded directly into workflows,

3. Continuous exposure awareness via CTEM,
4. Adaptive governance for AI and autonomous systems, and
5. Futureproofing against cryptographic disruption.

These are not technology requirements.

They are **operating model requirements**.

A Call for Structured Collaboration

Rather than prescribing a one-size-fits-all solution, the next step is **co-creation**:

- Define enterprise-specific **governance objectives (Audit Universe).**
- Translate them into **adjustable control gates (Automated Compliance).**
- Align CTEM signals with executive decision thresholds (Incident / Problem Management).
- Build a phased roadmap that respects:
  - Operational reality
  - Regulatory expectations
  - Business speed

This is where a **requirements document and project plan** become strategic assets—not paperwork.

Closing Perspective: Governance Is Becoming a Living System

In the AI and Quantum era, control is no longer something you install.

It is something you **operate continuously**.

Enterprises that recognize this early will:

1. Move faster with confidence.
2. Absorb disruption without collapse.
3. Govern AI and autonomy instead of fearing it.

Those that do not will discover—too late—that compliance without control is just documentation.

About the Author

Thomas Bronack is an executive advisor specializing in enterprise resilience, vendor risk, application governance, and emerging technology risk. Through **Data Center Assistance Group, LLC**, he works with executive leadership to design governance models that function under real-world conditions—before disruption forces the issue.

