WHITE PAPER

Integrated Assurance Maturity Model (IAMM)

The Blueprint for Unifying Resilience

An executive guide to measuring and advancing assurance across the enterprise.

Resilience does not come from having more frameworks. It comes from connecting governance, architecture, operations, risk, measurement, and culture so the organization can see whether assurance actually works.

Patrick M. Hayes

Integrated Assurance®

Executive white paper • September 2026

EXECUTIVE SUMMARY

From fragmented assurance to enterprise resilience

Organizations operate inside increasingly interconnected environments shaped by cloud platforms, third parties, regulation, artificial intelligence, supply chains, and rapid business change. Traditional frameworks provide valuable foundations, but enterprises often implement them in separate functions. The result can be strong compliance activity without a unified view of whether the business can withstand disruption.

The Integrated Assurance Maturity Model (IAMM) addresses that gap by embedding assurance across six domains: Governance, Architecture & Engineering, IT & Operations, Risk, Compliance & Audit, Metrics & Reporting, and Culture & Collaboration. It gives organizations a structured way to understand current maturity, expose gaps between functions, and determine where improvement will have the greatest impact.

IAMM defines five progressive levels of maturity. Organizations move from fragmented practices, through defined and aligned ways of working, toward assurance that is embedded in normal operations and ultimately institutionalized as an enterprise capability.

IAMM is designed to help leaders answer three questions:

- **Where are we fragmented?** Identify where assurance exists only inside functions, projects, tools, or compliance activities.
- **Where is assurance actually operational?** Determine whether controls, responsibilities, evidence, and recovery practices work in normal business workflows.
- **What maturity is appropriate?** Advance the domains that matter to the organization's risk, industry, obligations, and strategy rather than pursuing Level 5 everywhere.

> **IAMM is not another compliance framework. It is a maturity model for turning assurance into an integrated, measurable, and sustainable enterprise capability.**

The problem is fragmentation, not a shortage of frameworks

NIST, ISO, COBIT, CMMI, SABSA, COSO and other established approaches have shaped governance, security, architecture, process maturity, and risk management for years. Their value is not the issue. The difficulty is that organizations often apply them through separate teams with separate language, evidence, metrics, and priorities.

That fragmentation can create an enterprise that appears well governed on paper while remaining difficult to operate under stress. A completed audit does not prove that recovery objectives will be met. A green dashboard does not prove that controls will survive change. A security architecture does not prove that engineering teams are consistently implementing it.

IAMM closes the gap between principles and execution

- **Operational integration.** Maturity is demonstrated through working practices, automation, enforcement, recovery, and evidence, not documentation alone.
- **Cultural adoption.** Assurance becomes sustainable when roles, leadership sponsorship, incentives, and accountability reinforce it.
- **Real-time measurement.** Continuous telemetry and business-relevant metrics replace reliance on periodic snapshots as the primary view of assurance.

> **Integrated Assurance is not a single initiative. It is a discipline that connects strategy, operations, technology, risk, and behavior. IAMM provides the roadmap for building that discipline.**

Assurance has to work across the enterprise

Governance

Defines decision rights, ownership, forums, accountability, exception handling, and the connection between assurance and enterprise strategy.

Architecture & Engineering

Translates assurance into secure and resilient design, reusable patterns, threat modeling, policy-as-code, infrastructure-as-code, and automated validation.

IT & Operations

Embeds assurance into change, incident, recovery, service management, telemetry, hardened baselines, drift detection, and daily operational work.

Risk, Compliance & Audit

Connects business risk, harmonized controls, evidence, continuous validation, audit, and regulatory obligations instead of managing them as separate exercises.

Metrics & Reporting

Measures outcomes and business impact, provides useful views for different audiences, and turns assurance data into decisions and accountability.

Culture & Collaboration

Builds shared responsibility across business, IT, security, compliance, risk, and leadership so assurance becomes part of how work is performed.

> **The domains are deliberately interdependent. Strong governance cannot compensate indefinitely for weak operations. Strong engineering cannot overcome a culture that routinely bypasses controls. IAMM makes those relationships visible.**

A progression from fragmented practice to institutionalized capability

Level 1 - Fragmented

Practices are absent, inconsistent, or dependent on individual teams and people. Controls and decisions are applied unevenly, with little shared visibility.

Level 2 - Defined

Policies and processes exist, but they remain siloed. Functions may be improving independently without consistent integration or enforcement.

Level 3 - Aligned

Cross-functional coordination begins. Shared forums, telemetry, language, design practices, and responsibilities start to connect assurance across the enterprise.

Level 4 - Embedded

Assurance is operationalized in normal workflows. Controls are automated where appropriate, policies are enforced through processes and pipelines, and resilience is regularly validated.

Level 5 - Institutionalized

Assurance becomes a strategic enterprise capability. It influences investment, transformation, board decisions, customer trust, and continuous improvement.

> **The maturity levels are not a race to Level 5. Their purpose is to make the current state visible and help leaders decide what level of maturity is appropriate for each domain.**

Maturity becomes visible in how work is actually done

DOMAIN	LOWER MATURITY	HIGHER MATURITY
Governance	Siloed decisions and weak ownership	Cross-functional decisions, clear accountability, assurance integrated into strategy
Architecture & Engineering	Controls added late and inconsistently	Secure patterns, threat modeling, policy-as-code, continuous validation
IT & Operations	Uptime dominates; assurance is separate	Shared telemetry, automated controls, tested recovery, assurance KPIs
Risk, Compliance & Audit	Static registers and periodic audit	Harmonized controls, continuous evidence, active risk ownership
Metrics & Reporting	Activity counts and disconnected dashboards	Outcome measures tied to business impact and decision-making
Culture & Collaboration	Assurance belongs to specialists	Shared responsibility reinforced by leadership, incentives, and daily behavior

IAMM measures more than whether a control exists. It asks whether assurance has authority, is integrated into workflows, can be demonstrated with evidence, and influences business decisions.

05 | BALANCED MATURITY

Level 5 everywhere is not the objective

A common question is whether every organization should pursue Level 5 maturity across all six domains. IAMM treats Level 5 as aspirational rather than mandatory. The appropriate target depends on business risk, regulatory obligations, operating complexity, industry expectations, and the consequences of failure.

Highly regulated sectors may require stronger maturity in Governance and Risk, Compliance & Audit to demonstrate defensibility. Technology organizations may place greater emphasis on Architecture & Engineering and IT & Operations because rapid delivery makes design consistency and automated assurance especially important. Other organizations may achieve the resilience they need with Level 3 or Level 4 maturity across most domains.

Balance matters more than isolated excellence

- A Level 5 capability in one domain does not eliminate fragmentation elsewhere.
- Consistent Level 3 or Level 4 maturity across the six domains can be more defensible than one exceptional function surrounded by weak dependencies.
- Culture & Collaboration may not need the same target as Governance or Risk, Compliance & Audit, but it must be mature enough to sustain shared accountability.
- Targets should reflect the business and the consequence, not a theoretical maximum.

IAMM is a model for convergence and balance. The question is not 'How do we get everything to Level 5?' It is 'What level of assurance does this organization need, and where are the gaps that prevent us from trusting it?'

06 | PRACTICAL ADOPTION

Build momentum through evidence, not a massive transformation program

IAMM adoption is not a one-time project. The source model recommends a deliberate transformation that connects leadership, operations, architecture, risk, measurement, and culture. Progress is easier to sustain when organizations start with visible problems and demonstrate value before expanding.

Begin with high-impact pilots

Choose areas such as software delivery, sensitive identity governance, or high-risk third parties where outcomes can be measured and business relevance is clear.

Operationalize compensating controls

Treat temporary safeguards as governed, time-bound measures with ownership, monitoring, reassessment, and a path toward remediation.

Build feedback loops into workflows

Put assurance criteria into change, incident, project, and review processes so teams learn continuously rather than waiting for an audit.

Shift security from gatekeeper to accelerator

Use pre-approved patterns, guardrails, automation, and embedded expertise so assurance helps delivery move with confidence.

Align incentives and recognition

Make assurance part of performance, leadership expectations, and recognition so it is valued rather than treated as extra work.

Establish a common risk vocabulary

Create shared language across security, operations, compliance, risk, and business leadership so decisions are made from the same understanding.

Integrate assurance into strategy and continuity

Include assurance in budgets, transformation decisions, investment priorities, and crisis planning.

Use metrics to drive accountability

Tie KPIs and KRIs to ownership, corrective action, funding, and decision-making rather than reporting activity alone.

Evidence is what turns maturity into something leaders can trust

IAMM repeatedly shifts the emphasis from activity to outcomes. A pilot is valuable because it produces evidence. A control is valuable because its performance can be observed. A dashboard is valuable because it changes a decision. Measurement therefore has to show whether assurance is reducing exposure, improving recovery, increasing consistency, or strengthening collaboration.

Examples of useful assurance evidence

- Time to remediate material vulnerabilities or control failures.
- Rate of configuration or control drift across critical systems.
- Recovery performance compared with stated objectives.
- Percentage of controls validated continuously rather than only during audits.
- Use and adoption of approved secure architecture and engineering patterns.
- Frequency and age of exceptions and compensating controls.
- Cross-functional incident resolution and root-cause follow-through.
- Trends in risk convergence, resilience, and business impact.

Metrics should be role-based. Engineers need operational detail. Executives need consequence, trend, ownership, and decisions. Boards need enough evidence to understand whether resilience is becoming more or less defensible.

Use IAMM as the connective layer, not a replacement

IAMM was designed to complement established approaches. Organizations can continue using the frameworks that fit their regulatory, technical, governance, and architectural needs while using IAMM to understand whether those expectations have become integrated enterprise capabilities.

FRAMEWORK	STRENGTH	IAMM CONNECTION
NIST CSF	Cybersecurity governance and risk outcomes	IAMM connects those outcomes to maturity, operations, evidence, and cross-functional execution.
ISO/IEC 27001	Information security management and control structure	IAMM helps show whether management-system requirements are embedded and operationalized.
COBIT	Governance and management of enterprise technology	IAMM extends governance into observable assurance across architecture, operations, metrics, and culture.
COSO ERM	Enterprise risk linked to strategy and performance	IAMM connects risk decisions to technical and operational assurance.
SABSA / TOGAF	Business-aligned security and enterprise architecture	IAMM makes resilient design part of a broader maturity journey across the enterprise.
CMMI / ITIL	Process and service-management maturity	IAMM connects process maturity and service execution to resilience and assurance outcomes.

The distinctive value of IAMM is operationalization. It turns framework principles into maturity states that can be observed, tested, measured, and improved.

Can your organization demonstrate assurance, or only describe it?

IAMM becomes useful when it changes the questions leaders ask. Instead of focusing only on whether policies, committees, controls, or frameworks exist, leadership can examine whether those mechanisms influence real decisions and remain effective during change and disruption.

Questions worth asking across the enterprise

- Where are assurance decisions still being made inside functional silos?
- Can we trace policy and risk expectations into architecture, engineering, and operational controls?
- Are recovery and resilience practices continuously validated or simply documented?
- Do risk, compliance, and audit share evidence and control mappings, or are we repeatedly proving the same thing?
- Do our dashboards measure activity, or do they show business consequence and control effectiveness?
- Are assurance responsibilities visible in performance expectations and leadership behavior?
- Where are compensating controls becoming permanent workarounds?
- Which domain is materially weaker than the others, and what dependency does that create?
- What maturity level is actually appropriate for our industry, risk, and strategic priorities?

The purpose of maturity assessment is not to produce a score for its own sake. It is to reveal where confidence is supported by evidence and where the enterprise is still relying on assumptions.

Assurance becomes an enabler when it is part of how the enterprise operates

At higher maturity, assurance influences more than compliance. Governance shapes transformation and investment. Architecture makes resilience a design constraint. Operations validate recovery and control performance continuously. Risk and audit provide current evidence. Metrics influence decisions. Culture reinforces shared accountability.

This matters during modernization, cloud migration, acquisition, AI adoption, vendor selection, and other forms of change. Organizations do not have to choose between speed and assurance if the necessary guardrails are built into the way work is designed and executed.

The strategic outcome is defensible trust. Regulators and auditors can see evidence. Customers and partners can see resilience in practice. Boards can make decisions with better risk visibility. Teams can move faster because assurance is integrated rather than added late.

> **IAMM shifts the conversation from compliance to resilience and from risk avoidance to defensible growth.**

CONCLUSION

The blueprint is integration

Organizations rarely suffer from a complete absence of frameworks, controls, policies, or expertise. The more persistent problem is that those capabilities remain disconnected. Governance does not always reach operations. Architecture does not always shape engineering. Compliance evidence does not always reflect operational reality. Metrics do not always tell leaders whether the organization can withstand disruption.

IAMM was developed to address that gap. Its six domains create a common view of assurance across the enterprise. Its five maturity levels provide a way to understand how fragmented practices become aligned, embedded, and institutionalized. Its adoption guidance emphasizes evidence, feedback, accountability, and practical integration rather than another layer of documentation.

The objective is not perfection. It is an enterprise in which assurance is visible enough to guide decisions, operational enough to survive disruption, measurable enough to defend, and embedded enough to endure organizational change.

> **Trust and resilience should not be left to chance. IAMM provides a way to make them part of how the organization operates.**

About the source work

This white paper is a condensed executive treatment of Patrick M. Hayes's Integrated Assurance Maturity Model (IAMM) work, including the six maturity domains, five maturity levels, practical adoption recommendations, guidance on appropriate maturity, and alignment with established governance, security, architecture, risk, and service-management frameworks.

About Patrick M. Hayes

Patrick M. Hayes is an author, strategist, executive advisor, and keynote speaker whose work focuses on Business Survivability, Integrated Assurance, cybersecurity, AI, governance, and organizational risk. His work examines how organizations make assurance operational so leaders can make better decisions under conditions of disruption and change.

patrickmhayes.com | info@integratedassurance.co