Deloitte.

Reimagining modern integrated risk management

The next frontier will leverage advanced AI to drive efficiency, insight, and proactive risk management for IRM programs globally.

Artificial intelligence (AI) is rapidly transforming integrated risk management (IRM), creating new efficiencies such as earlier threat detection, more proactive and precise risk assessments, and streamlined processes. Notably, 44% of organizations now have teams dedicated to drafting AI policies and mitigating risks[1], and 44% of Generative AI (GenAI) applications in cybersecurity are delivering return on investment (ROI) above or significantly above expectations[2].

But AI also introduces complex new risks for organizations to navigate. Governance models should be redefined to address ethical and regulatory considerations, leveraging AI to forecast potential areas for improvement and generate tailored metrics and reporting. The significant shift in technology architecture necessitates vendors to reshape their solutions and build new AI capabilities to efficiently identify, assess, respond to, and remediate these new risks proactively.

The future of IRM: Embracing AI

A blueprint for an AI-powered future: This model presents a strategic, AI-driven approach to IRM that aligns people, technology, and workflows by offering a roadmap to help organizations modernize cybersecurity, integrate AI-powered IRM services, and strengthen defenses against emerging digital threats. The blueprint deconstructs and compartmentalizes the processes that run the IRM function, provides a foundation to map the current tech capability, and enables a mapping of AI to reimagine IRM. The legend below identifies the new and evolved AI-enhanced services.

Governance
- Oversight and decisions
- Operating model
- Business objectives
- Strategy and roadmap
- Investment planning and tool rationalization
- Policies and standards

Risk
- Risk governance and ownership
- Risk library/risk register creation
- Risk identification
- Data-driven risk assessment
- Risk tolerance/appetite
- Risk response and monitoring
- Risk events and historical analysis

Cyber metrics, analytics, and reporting (CMAG)
- Board/executive/management reporting
- Decision intelligence insights
- Quantitative risk and advanced analytics

Policy
- Policy life cycle
- Policy exceptions
- Regulatory mapping
- Stakeholder policy acknowledgement

Compliance
- Control ownership
- Control library
- Control attestations and testing
- Continuous control monitoring
- Compliance case management
- Regulatory mapping

Audit
- Risk assessment
- Plan development
- Engagement planning
- Fieldwork execution
- Evidence request
- Audit support

Core solutions for IRM
- **Policy management**
- **Compliance management**
- **Risk management**
- **Audit management**
- **Regulatory change management**
- **Issue management**
- **Third-party risk management**
- **Business continuity management**

Issues
- Issue identification
- Triage and analysis
- Validation and closure
- Issue acceptance

Integrated assets
- Asset inventory (CMDB)
- Risk/control mapping
- Risk/compliance data modelling for assets
- Information technology asset management (ITAM) life cycle

Business continuity
- Process and dependency mapping
- Business impact analysis (BIA)/Business continuity plans (BCPs)
- Exercise planning and testing
- Crisis management

Risk culture
- Workforce training and upskilling
- Awareness, outreach, communications
- Organizational change management

IRM operations
First line support
- Asset owners, risk owners, control owners, etc.
- Assess risks and controls
- Manage issues

Second line support
- Establish risk and control structures/libraries
- Oversight to IRM functions
- Approvers

Third line support
- Internal audit
- Provide independent and objective assurance

Third party
- Vendor inventory
- Risk domains
- Vendor business performance
- Vendor to asset/service mapping

Core data
- User inventory
- Locations
- Enterprise architecture

IRM platform/solution deployment and administration
- Design and architecture for IRM
- Platform/solution build (DevOps)
- Integrated third-party tools
- Testing and solution deployment
- Access control
- Platform administration and maintenance
- Model training and validation

LEGEND

- **AI-led (significant AI uplift)**
- **AI-assisted (partial AI uplift)**
- **AI-native**
- **Manual process**

1. ServiceNow Enterprise AI Maturity Index 2025 - ServiceNow
2. Deloitte's State of Generative AI in the Enterprise Quarter 4 Report – Deloitte

Connect to accelerate

Contact our leaders to dive deeper into the blueprint and reimagine what's possible for your IRM organization.

Mark Nicholson
Principal
Cyber AI GTM Leader
Deloitte & Touche LLP
manicholson@deloitte.com

Naresh Persaud
Principal
AI Transformation Leader
Deloitte & Touche LLP
napersaud@deloitte.com

Raj Mehta
Partner
IRM Leader
Deloitte & Touche LLP
rmehta@deloitte.com

Steve Ruzzini
Senior Manager
Cyber AI GTM
Activation Lead
Deloitte & Touche LLP
sruzzini@deloitte.com

AI for IRM: Functional uplifts to achieve greater efficiency

Explore how harnessing AI and smarter solutions can reduce manual effort and accelerate results across specific functions.

IRM process/function	AI solution description	Potential resulting impact
Control attestations* and testing	Automated review of control attestation evidence with a recommended compliance status, confidence score, and justification	• Time saved via automated evidence review • Increased quality of evidence reviews • Increased reporting advantages
Data-driven risk assessment	Automated scoring of inherent impact and inherent likelihood with provided justifications	• Time saved via automated evidence review • Increased quality of evidence reviews • Increased reporting advantages
Risk response and mitigation	Automated mitigation actions based on the risk, asset, and mapped mitigating controls	• Time saved via automated plan generation • Data-driven insights and summarization • Adaptive strategies: GenAI can adjust plans dynamically
Quantitative risk and advanced analytics	Transformation of complex, unstructured cyber information into concise, actionable summaries	• Reduced effort via automated data transformation • Saved time in generating actionable insights from complex unstructured data
Regulatory taxonomy management	Automated PDF importing of authority documents, parsed into citations and mapped with references	• Time saved via automatic importing • Minimized human error in importing spreadsheets • Reusable and lightweight tool to import regulations or frameworks
Issue triage and root cause analysis	Automatic summary of issue contents during analysis; analysis of summaries across Issues to identify trends	• Time saved from analyzing dozens of fields particular to a single-issue record

AI, GenAI, and agentic AI risk management framework

A strong AI risk-management framework aligns with core principles and contemplates the AI life cycle stages, regulatory jurisdictions, adjacent programs and control frameworks, and governance needed to manage AI risk for both internal and external stakeholders.

AI operating model | **AI risk governance** | **Tech enablement**

Trustworthy AI capabilities

Change management

Roles and responsibilities	Life cycle management	AI policies, standards, and guidelines	Regulatory and functional alignment	AI development solutions	AI guardrails
Distributed, clear ownership and inventory of AI use across the organization *Training and awareness to enable proper testing, development, and monitoring*	Defined accountability and risk reviews across the AI lifecycle, from intake through monitoring *Integrated, operational risk management procedures for guidance and checks*	Authoritative documents to set expectations and guidelines on AI use and development *Trustworthy AI requirements and enforcement across technology and operations*	Risk and regulatory stakeholder coordination to manage multifaceted AI risks and controls *AI risk domain controls (e.g., privacy, security, third party, model risk management)*	Tech-enabled risk identification and measurement within MLOps/AI development *Model validation, bias testing, threat analysis/red teaming within development*	Administrative safeguards and technical guardrails to defend against emerging AI risks *Human-in-the-loop, input/output guardrails, model monitoring, etc.*

*As used herein, attestation refers to control activities performed to understand and evaluate data and does not mean a financial statement audit.