



### Reimagining modern integrated risk management

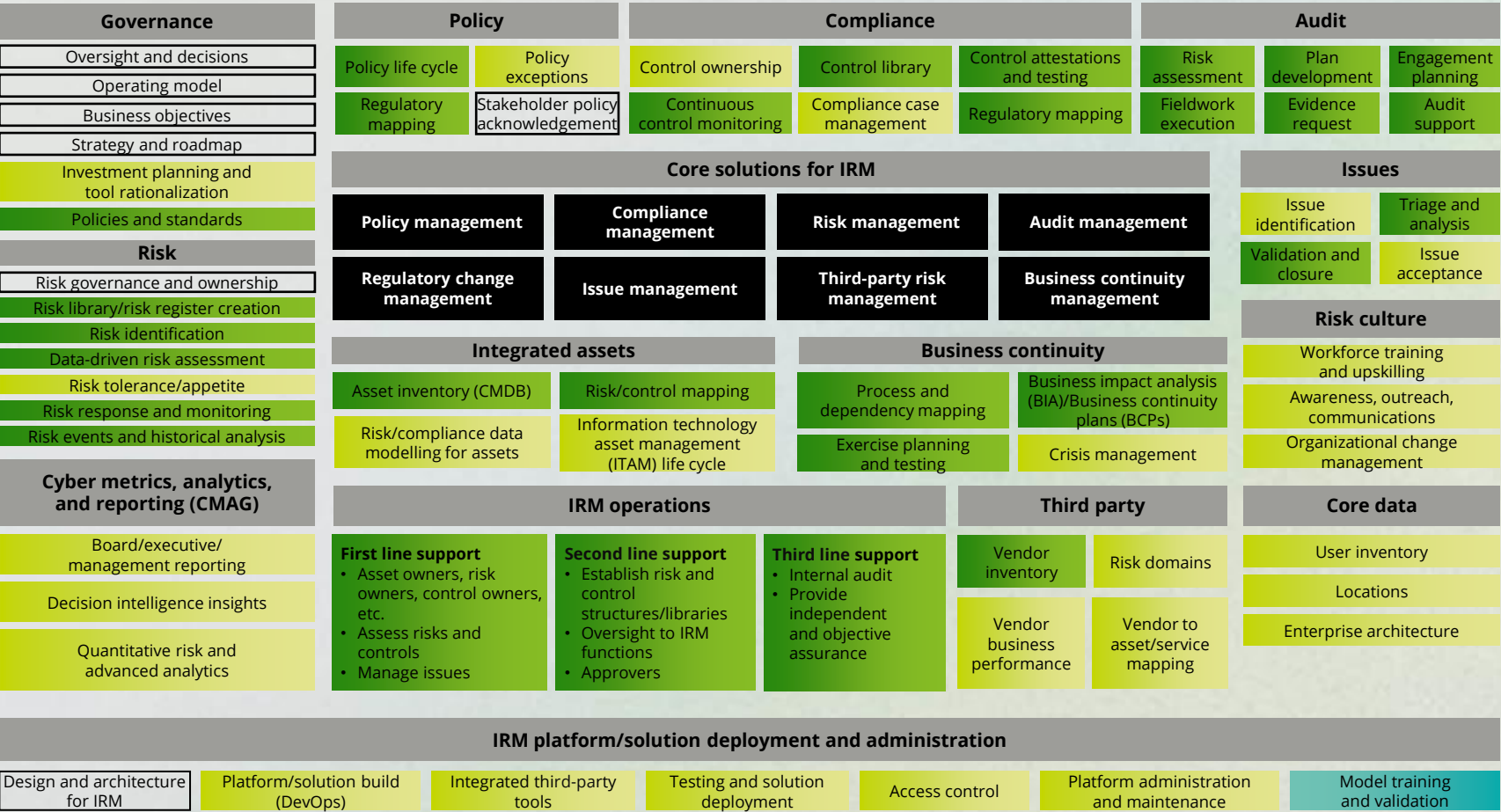
The next frontier will leverage advanced AI to drive efficiency, insight, and proactive risk management for IRM programs globally.

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<sup>1</sup>, and 44% of Generative AI (GenAI) applications in cybersecurity are delivering return on investment (ROI) above or significantly above expectations<sup>2</sup>.

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.



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

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for adetailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting. Copyright © 2025 Deloitte Development LLC. All rights reserved.

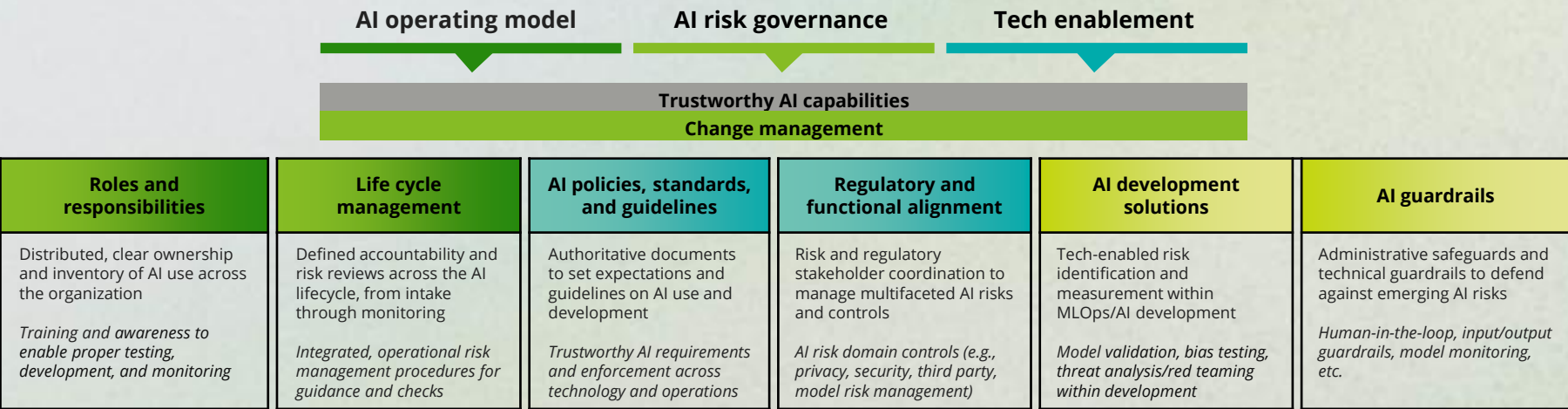
AI for IRM: Functional uplifts to achieve greater efficiency

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	<ul style="list-style-type: none"><li>Time saved via automated evidence review</li><li>Increased quality of evidence reviews</li><li>Increased reporting advantages</li></ul>
Data-driven risk assessment	Automated scoring of inherent impact and inherent likelihood with provided justifications	<ul style="list-style-type: none"><li>Time saved via automated evidence review</li><li>Increased quality of evidence reviews</li><li>Increased reporting advantages</li></ul>
Risk response and mitigation	Automated mitigation actions based on the risk, asset, and mapped mitigating controls	<ul style="list-style-type: none"><li>Time saved via automated plan generation</li><li>Data-driven insights and summarization</li><li>Adaptive strategies: GenAI can adjust plans dynamically</li></ul>
Quantitative risk and advanced analytics	Transformation of complex, unstructured cyber information into concise, actionable summaries	<ul style="list-style-type: none"><li>Reduced effort via automated data transformation</li><li>Saved time in generating actionable insights from complex unstructured data</li></ul>
Regulatory taxonomy management	Automated PDF importing of authority documents, parsed into citations and mapped with references	<ul style="list-style-type: none"><li>Time saved via automatic importing</li><li>Minimized human error in importing spreadsheets</li><li>Reusable and lightweight tool to import regulations or frameworks</li></ul>
Issue triage and root cause analysis	Automatic summary of issue contents during analysis; analysis of summaries across Issues to identify trends	<ul style="list-style-type: none"><li>Time saved from analyzing dozens of fields particular to a single-issue record</li></ul>

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.



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