The Evolution of Integrated Risk Management

EM360 | ENTERPRISE MANAGEMENT 360

Moving Beyond Silos to Achieve Enterprise Resilience

Sponsored by AuditBoard

Executive Summary

Traditional risk management models are straining under the weight of today's complexity.

Siloed systems, reactive processes, and disconnected data leave organisations exposed. This summary highlights why integrated risk management is gaining traction — and why leaders are rethinking their entire approach to governance, risk, and compliance.

In an era of rapid digitalisation, multiplying cyber threats, and intensifying regulatory demands, traditional siloed approaches to **GRC** are reaching their limits.

GRC
Governance, Risk, and Compliance

Disconnected risk management efforts – where each department runs its own isolated programme – lead to duplicated work, inconsistent data, and dangerous blind spots. Organisations managing risk in silos suffer more frequent security breaches and operational disruptions than those with integrated approaches. The need for a holistic, enterprise-wide strategy has never been clearer.

IRM has emerged as a way forward. Coined by Gartner in 2017, **IRM** encompasses the practices, processes, and cultural mindset required to manage risk across the enterprise in an integrated fashion.

IRM
Integrated Risk Management

Definition

INTEGRATED RISK MANAGEMENT | A unified approach to managing risks across the organisation, aligning them with strategy and embedding them into daily decisions.

It shifts the focus from reactive compliance checklists to proactive risk intelligence and resilience. An effective IRM programme breaks down departmental barriers, unifies risk data and processes on a common platform, and aligns risk management with strategic objectives and performance goals. The payoff is significant: greater agility in decision-making, improved risk visibility, stronger compliance postures, and enhanced enterprise resilience.

The Cost of Siloed Risk Management

Fragmented GRC functions drain resources and obscure the enterprise risk picture.

Surveys show that most organisations cite silos as the biggest barrier to extracting value from data, with over 80% of risk professionals saying silos directly hinder risk management. We outline how these silos form and their real-world impact on risk exposure.

Strategic Drivers for IRM Adoption

Regulatory pressure, stakeholder expectations, and complex third-party ecosystems are pushing organisations toward IRM.

ESG factors are now central to risk discussions. Integrated approaches not only help avoid penalties but enable competitive advantage by embedding resilience into decision-making.

Building a Mature IRM Programme

We break down what a robust IRM programme looks like – from governance structures and unified taxonomies to integrated assessments, coordinated response plans, and enabling technology. Maturity models from leading frameworks help readers benchmark their current state and plan a stepwise journey toward optimisation.

IRM Technology and Vendor Landscape

With the IRM software market expected to grow from **US$10.9 billion in 2023 to almost US$40 billion by 2032**, we analyse the vendor landscape.

Full-suite leaders, cloud-native innovators, and niche specialists are compared with guidance on selecting solutions that enhance integration and visibility.

Emerging Technologies Enhancing IRM

AI, automation, and blockchain are reshaping risk management. From predictive analytics to continuous control monitoring, emerging technologies are enabling a shift from reactive to proactive risk management – provided they're used responsibly with human oversight.

Real-World Insights and Common Pitfalls

Examples from multiple industries show how IRM delivers faster decisions, cost savings, and reputational gains. We also identify common hurdles – from cultural resistance and data quality issues to talent gaps – with practical guidance for overcoming them.

Ultimately, IRM is a journey that needs leadership commitment, cultural change, and the right tools. Organisations that move beyond silos and adopt integrated risk practices position themselves not only to survive complexity but to thrive on uncertainty and unlock new opportunities.

The future of risk isn't guarded perimeters — it's connected defences

Two Approaches to Risk Management

Siloed Risk Management

- Departments guard their own risk data.
- Information stays fragmented and disconnected.
- Blind spots grow between silos, making the organisation more vulnerable.
- Duplication of effort wastes time and resources.

Integrated Risk Management

- Risk data flows across departments in a single framework.
- Teams collaborate to identify, assess, and respond to risks.
- A unified view enables faster, better-informed decisions.
- Resources are focused on prevention and resilience.

From Fragmented GRC to Integrated Risk Management

Most risk programmes weren't built for the speed, scale, or interconnected nature of today's threats. Fragmentation isn't just inefficient — it's dangerous. In this section, we examine how the siloed GRC paradigm emerged, why it no longer works, and what's driving the shift toward integrated risk management.

Modern enterprises face a fast-changing, interconnected risk landscape. A cyber-attack can trigger fines and reputational damage; supply chain disruptions can halt production and create compliance headaches.

Yet, many organisations still manage risk in silos – separate security, compliance, legal, and finance functions each using their own processes and language.

This fragmentation leaves organisations blind to systemic risks.

> *Data silos slow decisions, weaken security and block innovation ~ Wayne Eckerson, President of Eckerson Group and EM360Tech analyst.*

Surveys show 68% of enterprises cite silos as the biggest barrier to using their information effectively, and over 86% of risk professionals say silos hinder risk management.

Companies with siloed programmes are **twice as likely to suffer major breaches** as those with integrated, technology-enabled risk management.

Without shared data and aligned objectives, leadership operates half-blind, risks are duplicated or missed entirely, and enterprise-level reporting becomes nearly impossible.

> *IRM emphasises the "R" – risk – as a unifying thread that must run through governance and compliance activities, as well as strategic and operational processes.*

The roots of this siloed model trace back to early compliance mandates in the 2000s.

Frameworks like COSO and ISO 31000 promoted integration, but many firms adopted them as check-the-box exercises.

As technology and regulation evolved through the **2010s**, quarterly audits and manual risk registers proved inadequate.

Instead, it needed to be **continuous, real-time, cross-functional, and data-driven**.

By **2017**, IRM emerged as a more holistic approach.

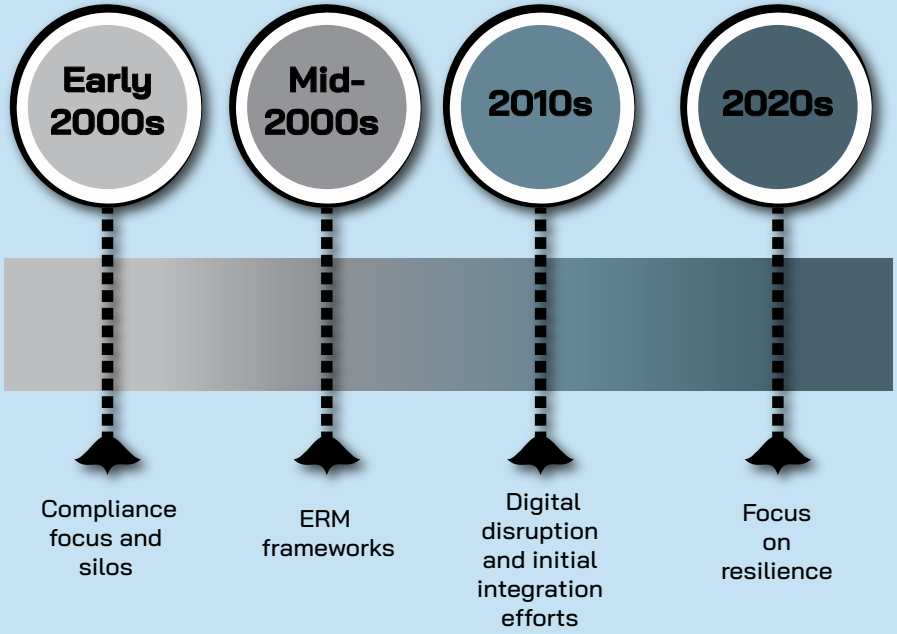
Think of IRM as **breaking the walls between risk silos** and elevating risk management from a back-office function to a strategic, enterprise-wide discipline.

Definition

RISK SILO

A compartmentalised approach to managing risk where each department or function operates independently, using its own processes and data. This isolation prevents a complete enterprise-wide view of risk, leading to inefficiencies, blind spots, and inconsistent decision-making.

Risk Management Evolution



Defining IRM and Its Core Principles

Integrated risk management can be defined as *"a set of practices and processes, supported by a risk-aware culture and enabling technologies, that improves decision-making and performance through an integrated view of how well an organisation manages its unique set of risks."*

In simpler terms, IRM is about viewing and managing risk holistically at the enterprise level, rather than in isolated pockets. The core principles that underpin IRM include:

Holistic Scope

IRM considers all categories of risk – strategic, operational, financial, compliance, cyber, third-party, etc. – in a unified framework. It recognises that risks are interrelated and must be understood in aggregate. This goes beyond traditional ERM by actively breaking down the barriers between risk types and functions.

Strategic Alignment

IRM tightly links risk management to business strategy and objectives. Rather than risk being a purely defensive or box-ticking exercise, it becomes a strategic tool. Decisions at all levels are made with an understanding of risk-reward trade-offs and the organisation's risk appetite.

> Surviving today's chaotic risk environment demands that companies find new ways to get ahead of risk. Business leaders need to be more effective in identifying, understanding, and measuring the risks and risk priorities most relevant to their businesses, enabling them to make better, more risk-informed decisions.
> ~ John A Wheeler.

John A. Wheeler, a former Gartner analyst and founder of Wheelhouse Advisors, argues that surviving today's risk era requires *"connecting people, technology and business"* – in other words, embedding risk considerations into strategy and operations so that companies can take calculated risks and be more agile.

Risk-Informed Decision Making

Turning risk data into actionable intelligence for leadership means moving from static reports to real-time dashboards, forward-looking analytics, and predictive indicators that inform decisions.

> A core goal of IRM is to turn risk data into actionable intelligence for leadership.

Risk management is not just about preventing bad things, but enabling better decisions.

Amanda Cohen, VP of Product at Resolver emphasises shifting from pure risk management to *"risk intelligence"* – using risk insights to uncover opportunities and drive performance improvements. In an IRM culture, project approvals, investments, product launches, and other major decisions all explicitly consider risk information.

Definition

RISK INTELLIGENCE	The ability to gather, analyse, and use risk data to make informed, proactive decisions that protect and create value for the organisation.

Unified Culture and Collabouration

IRM promotes a **risk-aware culture** across the organisation. This involves clear tone-from-the-top that risk is everyone's responsibility, not just the risk departments. It also entails **collabouration across traditionally siloed teams**.

So, IT and Finance might jointly assess technology risks in a digital transformation project, or Compliance and Procurement might together evaluate a vendor's risk profile.

Breaking silos requires overcoming fiefdom mentalities – risk information must be shared, not hoarded.

As one GRC thought leader put it, organisations should replace the old mentality of *"each department protecting its turf"* with a culture where everyone agrees they have a shared mission of safeguarding the enterprise.

Enabling Technology and Data

Practically, IRM is enabled by integrated technology platforms that consolidate risk data and automate workflows.

In contrast to spreadsheets and disparate tools, an IRM system provides **a single source of truth** for risk and compliance data, accessible to stakeholders across lines of business.

Modern IRM solutions leverage capabilities like workflow automation, analytics, and continuous monitoring.

They integrate with other enterprise systems (ERP, IT service management, etc.) to pull relevant data.

The technology underpins everything – without it, attempts at integration often collapse under manual effort. In short, you need the right tools to connect the dots.

> *Integrated platforms provide the robust foundation needed to manage operational resilience and meet regulatory requirements.~ A.G. Lambert, Chief Product Officer at NAVEX*

Finally, IRM embodies a continuous improvement loop. Because the risk landscape is always evolving, IRM programmes must monitor outcomes, learn from incidents (*"lessons learned"* reviews), and adapt processes accordingly.

This echoes quality management philosophies – treat risk management as a living process that regularly updates controls, policies, and training based on what is happening in and around the organisation.

It's a move away from one-off annual risk assessments to continuous risk monitoring and agility.

By adhering to these principles, IRM aims to overcome the limitations of siloed GRC and create a risk management approach suited to the complexity of the modern enterprise.

In practice, many organisations begin their IRM journey by focusing on a few high-impact areas and then expanding.

The next sections delve into exactly why this journey is necessary – examining the pain points of siloed risk management – and how to navigate it successfully.

Lessons Learned Review

A structured evaluation conducted after an incident or project to identify what worked well, what went wrong, and how processes, controls, or responses can be improved to prevent similar issues in the future.

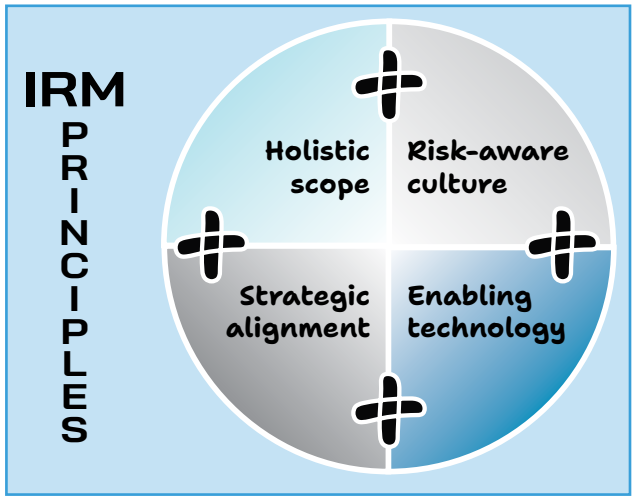
Definition

CONTINUOUS RISK MONITORING

The ongoing process of tracking risk indicators, controls, and emerging threats in real time to quickly detect changes in an organisation's risk profile and enable faster, proactive responses.

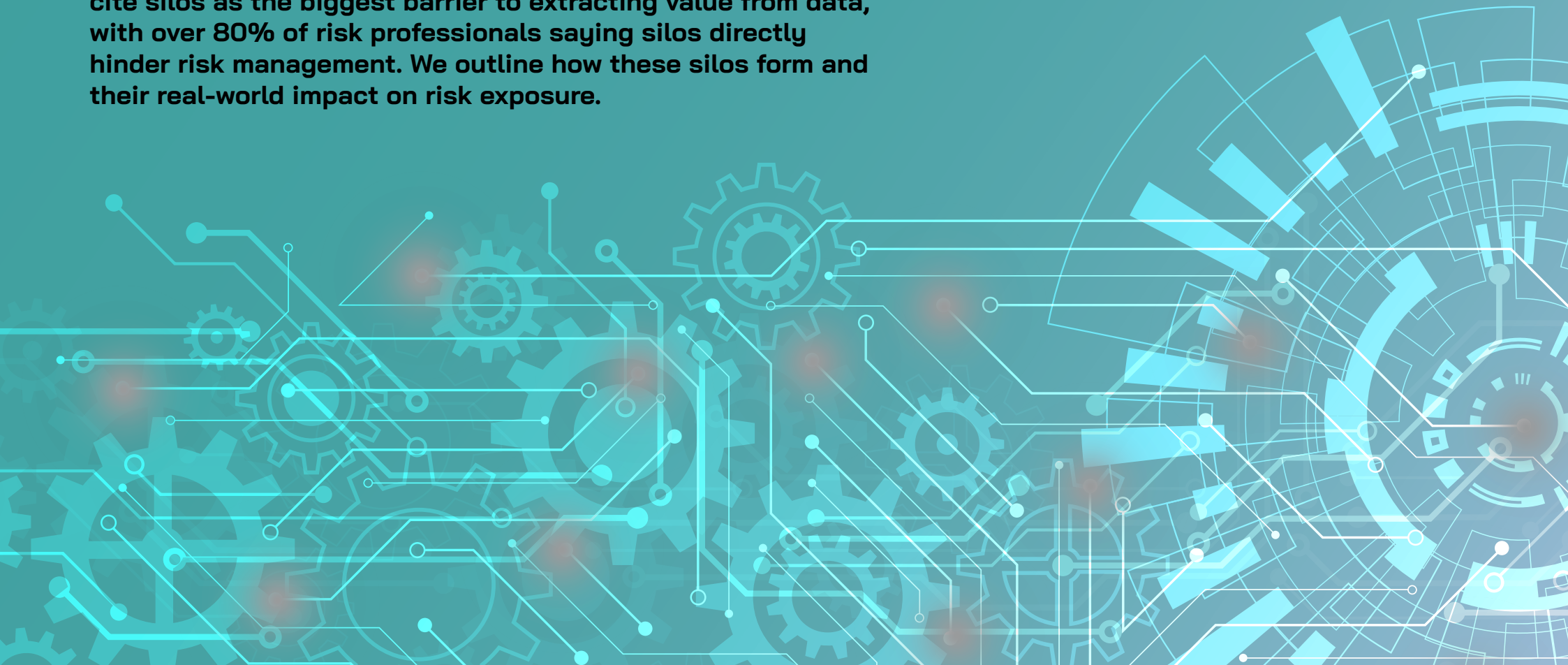
for instance

Start by integrating cyber and operational risk, or by unifying compliance processes across jurisdictions, before moving into advanced analytics and continuous monitoring.



The Cost of Managing Risk and Compliance in Silos

Fragmented GRC functions drain resources and obscure the enterprise risk picture. Surveys show that most organisations cite silos as the biggest barrier to extracting value from data, with over 80% of risk professionals saying silos directly hinder risk management. We outline how these silos form and their real-world impact on risk exposure.



Operating with siloed risk and compliance functions carries significant hidden costs and risks. What may have worked (or at least been tolerated) in simpler times now leaves organisations over-exposed and under-prepared. In this section, we detail the inefficiencies and dangers of the fragmented approach.

1 Redundant Effort and Inefficiency

In siloed environments, different teams often duplicate work without realising it. So the IT risk team, the vendor management team, and the finance audit team might each separately assess the security controls of a key third-party service provider – three duplicate assessments, eating up time and resources. T

here is no central repository or common process, so overlaps abound. This not only wastes effort but can produce slightly different findings (due to inconsistent methods), causing confusion.

A fragmented approach also means multiple disconnected tools and spreadsheets. Staff waste hours reconciling data from different sources and preparing separate reports for each silo. These inefficiencies amount to a *"risk tax"* on the business – consuming resources that could have been spent on growth or innovation.

Definition

RISK TAX

The hidden cost an organisation pays for managing risk inefficiently. It shows up as duplicated work, slow decision-making, missed opportunities, and extra resources spent fixing avoidable issues. Like a silent tax, it drains productivity and resilience without adding value.

2 Poor Visibility and Blind Spots

Perhaps the gravest consequence of silos is the blind spots they create. When risk data is scattered, no one in the organisation has a complete view of risk. The board and C-suite might receive a high-level risk report from each department, but **no aggregate risk** picture.

> *When departments cannot see each other's data, the organisation is effectively flying blind in the spaces between silos.*

Critical interdependencies go unnoticed. A risk deemed minor in one silo could trigger major issues elsewhere, but without an integrated view, this isn't seen until it's too late. Early warning signs of emerging threats (a pattern of minor incidents across silos that add up to a major issue) get missed. It's no surprise that companies with siloed risk data experience more frequent incidents – they're simply not seeing the full picture.

for instance

The operations team might be concerned only with supplier delivery risks, not realising that one of the suppliers is handling customer data in a way that poses a huge privacy compliance risk.

Each silo looks at its own risk in isolation, giving a false sense of security (*"we're green in our area"*) even as red flags mount at the enterprise level.

3 Overwhelming Complexity and Inconsistency

A by-product of siloed evolution is that each risk function develops its own language, metrics, and methodologies. The IT team might use a 5x5 risk matrix and talk about *"vulnerabilities"*, while the operational risk team uses qualitative ratings and talks about *"hazards"*, and compliance uses a traffic-light status for controls. None of these align. When someone tries to aggregate or compare risks across silos, it's apples and oranges. Reporting upward becomes an exercise in translation and simplification, often losing important detail.

Moreover, the over-reliance on manual processes (a hallmark of siloed approaches) makes the overall system fragile and error-prone. People are copying data between spreadsheets, emailing versions back and forth – **so mistakes are inevitable**. Complexity also makes regulatory reporting harder; answering a regulator's enterprise-wide question requires pulling data from five places and reconciling inconsistencies. This erodes confidence in the risk information. Senior executives may not fully trust the risk reports because they know it's cobbled together from disparate sources. Such uncertainty at the top is itself risky – decisions get delayed or made on faulty assumptions.

4 Slow, Reactive Decision-Making

In siloed regimes, risk information tends to flow slowly – often too slowly for today's fast-paced risks. Reports are periodic (maybe monthly or quarterly) and must be manually assembled, so by the time leadership sees a consolidated view (if they do at all), it's looking in the rear-view mirror.

Reactive Risk Posture

An approach to risk management where action is taken only after an incident occurs, focusing on damage control rather than prevention. This posture often results from siloed processes, limited visibility, or inadequate monitoring, leaving organisations more vulnerable to emerging threats.

for instance

If a serious cyber incident happens, an organisation with siloed risk might spend weeks figuring out what went wrong because information is fragmented. In contrast, an integrated approach would have real-time dashboards and possibly have detected precursor signals.

This encourages a reactive posture, akin to playing whack-a-mole with threats after they've materialised. The speed disadvantage of silos can be devastating – consider a sudden supply chain disruption: a siloed organisation might realise only when one factory reports a shortage, whereas an integrated one could have enterprise risk sensors alerting leadership of the issue days or weeks earlier. In an age where risks like ransomware or pandemic impacts unfold rapidly, a slow reaction can significantly increase damage. Siloed processes often handicap the business's agility, meaning companies mired in spreadsheets struggle to pivot when conditions change.

5 Greater Exposure and Vulnerability

Managing risk in silos makes it far more likely that critical risks slip through unnoticed. With no one accountable for enterprise-level oversight, gaps go unmonitored – and that's often where major failures occur. The **2008 financial crisis** showed this clearly: banks had risk managers for credit, market, and liquidity risk, but no holistic view of how falling housing prices would cascade through all three.

White Space Risks

Risks that fall outside traditional departmental boundaries or ownership, often emerging in the gaps between functions or silos. These are overlooked because no one team is accountable for monitoring or managing them.

Modern incidents like data breaches highlight similar problems: IT, process, and human risks intersect, yet siloed programmes handle them separately or not at all. Emerging "*white space*" risks – like AI ethics or combined cyber-physical threats – often don't fit neatly into one department's remit, leaving them unmanaged.

2008 Financial Crisis

A global economic downturn triggered by the collapse of the US housing market and widespread failures in financial risk management. Banks and institutions had siloed approaches to credit, market, and liquidity risks, not seeing how mortgage defaults would cascade through other financial products. The lack of integrated oversight contributed to massive institutional failures, government bailouts, and a prolonged recession worldwide.

This fragmented approach carries tangible costs:

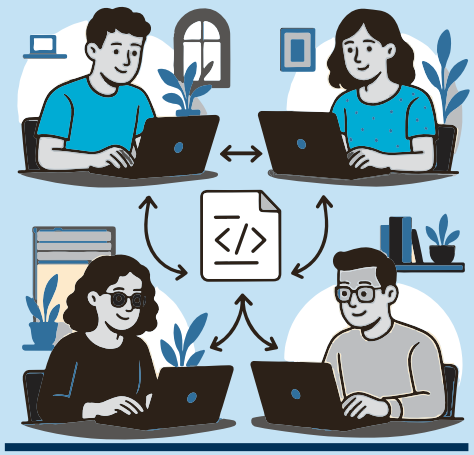
Financial
Duplicated controls and inefficiencies

Strategic
Slower decisions and missed opportunities

Compliance
Higher likelihood of incidents and breaches

It also frustrates staff, who spend more time coordinating between silos than mitigating risks, and damages credibility when departments send inconsistent signals during crises.

Leading organisations recognise these costs and are shifting to Integrated Risk Management – not as a nice-to-have but as a strategic imperative to close these gaps and build true resilience.



79% … of knowledge workers feel that their organisations teams work in silos

68% … said their work is negatively impacted by not having visibility into cross-functional projects

Silos vs IRM: The Difference in Outcomes

Silos – How They Hold You Back

Duplicate work across departments → multiple teams unknowingly assess the same risks or vendors.

Blind spots between functions → no one sees the full picture, leaving hidden vulnerabilities.

Slow response to incidents → delays mount while departments coordinate after the fact.

Conflicting metrics and reports → leadership gets inconsistent information they can't trust.

Higher costs from inefficiency → resources wasted on redundant controls and admin work.

Missed early-warning signals → silo walls prevent weak signals from being spotted in time.

IRM – How It Moves You Forward

Streamlined effort across teams → one framework eliminates duplication and saves time.

Enterprise-wide visibility → risks are viewed in context, across business units and domains.

Rapid, coordinated response → incidents trigger action plans that involve all stakeholders.

Consistent metrics and reporting → leadership gets trusted, comparable information.

Lower costs through efficiency → fewer redundant processes and smarter use of resources.

Proactive detection and foresight → connected data enables predictive risk intelligence.

Takeaway: IRM doesn't just remove the pain of silos — it turns risk management into a driver of resilience and performance.

Strategic Drivers for IRM Adoption

Regulatory pressure, stakeholder expectations, and complex third-party ecosystems are pushing organisations toward IRM. Environmental, social, and governance (ESG) factors are now central to risk discussions. Integrated approaches not only help avoid penalties but enable competitive advantage by embedding resilience into decision-making.

What is motivating organisations to overhaul their risk management approach and invest in integration now?

Several strategic drivers are converging, making IRM not just an option but, in many cases, an essential evolution for enterprises aiming to be resilient and competitive.

Below we outline the primary drivers fuelling IRM adoption:

1 Increasing Risk Complexity and Interdependence

The risk environment has become more complex, with new kinds of risk emerging and traditional risks becoming more interconnected.

Businesses operate in a world of *"unknown unknowns"* where a disruption in one domain can rapidly propagate.

Unknown Unknown

A risk or issue that an organisation is unaware of and has no prior knowledge or experience to anticipate (similar to a zero day exploit in cybersecurity). These are unforeseen events or factors that lie outside existing assumptions, data, or planning, and therefore cannot be directly prepared for until they emerge.

Siloed risk management cannot adequately cope with such interconnected scenarios.

Organisations need integrated approaches to spot correlations – to see that, say, a geopolitical event could affect a supplier and thereby a production line and thereby revenue forecasts.

IRM is driven by this need for **enterprise-wide visibility.** As one IRM framework puts it, companies must *"connect the dots"* between risk events and their enterprise impacts.

Without integration, critical interdependencies are missed, leading to nasty surprises.

The growing complexity of operations (global supply chains, digital ecosystems) simply demands a more unified risk strategy.

2 Regulatory Pressure and Scrutiny

Around the world, regulators have been turning up the heat on risk governance expectations.

New regulations and guidelines increasingly require a holistic view of risk and evidence of well-developed enterprise risk management.

Financial regulators (and not just in banking) now expect board-level oversight of risk and linkage between risk appetite and strategic planning.

In the EU, the Digital Operational Resilience Act **(DORA)** requires financial entities to manage Information and Communication Technology **(ICT)** and cyber risks in an integrated manner across their business.

In the US, recent Securities and Exchange Commission **(SEC)** rules mandate that public companies disclose material cyber incidents and describe their risk management processes enterprise-wide.

Likewise, **ESG** reporting frameworks (like the Task Force on Climate-related

Financial Disclosures – TCFD) compel firms to assess and disclose environmental and social risks alongside financial ones.

DORA
Digital Operational Resilience Act

ICT
Information and Communication Technology

SEC
Securities and Exchange Commission

ESG
Environmental, Social, and Governance

What Does DORA Cover?

ICT risk management

Principles and requirements on ICT risk management framework

ICT third-party risk management

Monitoring third-party risk providers

Digital operational resilience testing

Basic and advanced testing

ICT-related incidents

General requirements Reporting of major ICT-related incidents to competent authorities

Information sharing

Exchange of information and intelligence on cyber threats

Oversight of critical third-party providers

Oversight framework for critical ICT third-party providers

These developments push companies toward IRM because compliance itself becomes an integrated challenge.

As A.G. Lambert of NAVEX noted regarding DORA compliance, an integrated platform provides the foundation to manage operational resilience risks and meet such requirements.

Stakeholders – regulators, investors, even customers – are expecting a joined-up approach and transparency in how risks are managed.

Those expectations act as a strong driver: organisations realise siloed spreadsheets won't satisfy a regulator asking

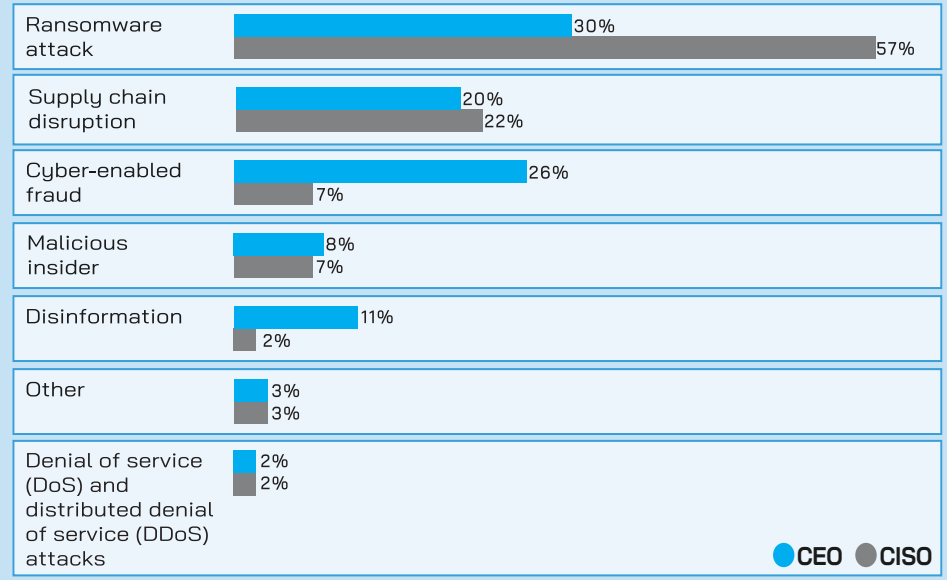
"How do you govern risk across your enterprise?"

3 The Evolving Threat Landscape (Cyber and Beyond)

Cybersecurity deserves special mention as a driver. Cyber threats have escalated in scale and sophistication, and they affect all parts of a business – not just IT. Ransomware is as much an operational risk (disrupting services) and reputational risk as it is an IT issue.

> *Managing cyber risk is a cross-functional effort spanning IT, legal, compliance, finance, HR, and beyond.*

Organisational Cyber Risk – CEO and CISO Views



Definition

MACHINE IDENTITIES

Digital credentials used by non-human entities—such as applications, services, bots, and IoT devices—to authenticate and communicate securely within networks. Managing these identities is critical to prevent unauthorised access and reduce cyber risk.

Organisations have learned that managing cyber risk requires inputs from IT, legal, compliance, finance (for fraud), HR (for training) and more.

This naturally propels integration. Additionally, digitisation means **more assets to protect** and more potential attack vectors. IRM now includes machine identities (bots, service accounts) proliferating across cloud environments, which must be governed.

Integrated risk management brings together cybersecurity with broader enterprise risk processes.

for instance

A critical vulnerability triggers not only an IT response but also a business continuity plan and customer communications, if appropriate.

One can also lump in other fast-evolving risks here – such as data privacy and AI ethics. These tend to cut across silo boundaries. The only effective way to manage them is integrated, involving multi-disciplinary teams.

Leaders increasingly see IRM as a way to be **proactive** rather than reactive. As one Thomson Reuters survey highlighted, 80% of professionals expect AI to have a significant or transformational impact on their work, both as a tool and a source of new risks.

Facing such emerging technologies, an IRM approach allows organisations to evaluate and deploy AI with guardrails (combining compliance, IT, legal, and operational input) rather than in silos that might overlook important considerations.

Transformational impact

Most **(80%)** respondents believe AI will have a high or even transformational impact on their work over the next five years; 38% expect to see those changes in their organisation this year.

Jagged edge of AI adoption

Nearly half **(46%)** of organisations have invested in new AI-powered technology in the last 12 months, and 30% of professionals are now using AI regularly to start or edit their work.

AI strategy is key

Just **22%** of organisations have a visible AI strategy – but those that do are 3.5 times as likely to be seeing a return on investment (ROI) compared to those with no significant plans.

Modern professionals

More than half **(55%)** of professionals have either experienced significant changes in their work in the past year or anticipate major shifts in the coming year.

AI adoption pays

Survey respondents predict that AI will save them five hours weekly or about 240 hours in the next year, for an average annual value of $19,000 per professional.

4 Third-Party and Supply Chain Risks

Modern enterprises rely on vast webs of suppliers, vendors, outsourcing partners, and SaaS providers.

Each third-party relationship introduces risks – cyber, compliance, operational, reputational – that can propagate quickly through the network.

We've seen incidents where a breach at a small vendor led to a major retailer's systems being compromised, or a sub-supplier's factory issue halted a global manufacturer's production line.

Target Third-Party Breach (2013)

Attackers infiltrated Target's network by compromising the credentials of a small HVAC vendor, Fazio Mechanical Services. Once inside, they accessed payment systems and stole data from over 40 million credit and debit cards. The incident highlighted how a single weak link in the supply chain can expose an entire enterprise, underscoring the importance of third-party risk management.

Toyota Aisin Fire (1997)

A fire at a sub-supplier's factory in Japan destroyed production of a small but critical brake component used in nearly all Toyota vehicles. With only hours of inventory on hand under its just-in-time model, Toyota's global production lines were at risk of shutting down. The incident showed how a single-point failure deep in the supply chain can halt operations worldwide, highlighting the need for comprehensive supplier risk management and contingency planning.

In siloed setups, third-party risk is often managed by procurement or vendor management in a limited way, such as with financial due diligence, and not connected to IT's security assessments or compliance's contractual audits. IRM drives a **centralised third-party risk management** approach, standardising due diligence across all departments and continuously monitoring vendor risks.

This has become essential as supply chain disruptions (natural disasters, geopolitical events, pandemics) have shown that third-party risk is business risk.

Companies are now expected – by regulators and their own boards – to have integrated views of vendor exposures.

> *Regulators and corporate boards increasingly expect organisations to maintain a consolidated, enterprise-wide view of all vendor exposures. This means identifying, assessing, and monitoring third-party risks in a centralised way, rather than relying on fragmented assessments within individual departments.*

This driver is very tangible: many firms learned hard lessons in recent years and are adopting IRM to map and mitigate these interconnected supply risks enterprise-wide.

5 ESG and Stakeholder Expectations

ESG factors have moved from peripheral concerns to mainstream risk considerations.

Extreme weather events pose physical risks to operations (floods, wildfires), while the transition to a low-carbon economy poses strategic risks (market shifts, new regulations) and reputational risks.

Social issues – from workforce diversity to human rights in supply chains – can rapidly become legal, financial, and reputational risks. Traditionally, these areas might not have been on the risk register at all or sat in a CSR silo.

> *Investors and regulators now view ESG performance as a core element of enterprise risk management.*
>
> *Organisations are expected to track, manage, and report ESG risks with the same rigour as financial, operational, or cyber risks, ensuring accountability and transparency for stakeholders.*

Now, however, investors and regulators are holding companies accountable for ESG performance, effectively treating it as part of risk management.

Integrated risk management means incorporating ESG risks into the overall framework – connecting them to enterprise strategy and decision-making.

Leading organisations now include key ESG metrics on their risk dashboards, ensuring that, say, a climate risk scenario is weighed alongside financial and cyber risks in planning.

The strategic driver here is twofold:

- **compliance** (keeping up with reporting standards and avoiding greenwashing accusations) and
- **market expectation** (customers and partners want to trust that a company manages ESG responsibly).

By using IRM to tie ESG into the risk programme, companies can demonstrate to stakeholders that these issues are understood and governed like any other critical risk – which increasingly, they are.

6 Competitive Advantage through Resilience and Agility

Beyond defensive motives, many executives see improved risk management as a source of competitive advantage.

If your company can manage risks better, you can afford to take bold opportunities that others might shy away from.

An organisation with integrated risk insights can move faster – launching a new service in a regulated market because it can quickly assess compliance and security risks in one go.

Integrated risk management supports agility. John Wheeler's view aligns with this: connecting risk across people, tech, and process makes an organisation more agile and *"better equipped to take calculated risks and more resilient to shocks."*

In practice, this might mean a company with strong IRM can respond to a sudden market change (like a new regulation or a supply crisis) faster and more confidently, thus gaining an edge over competitors who are bogged down in figuring out their exposure.

Also, a reputation for robust risk management can be a selling point – business customers, insurers, and investors prefer companies that are well-governed and resilient.

Collectively, these drivers make a compelling case for IRM.

for instance

Consider how some telecom companies integrated risk and sustainability: one telco found that by embedding climate risk metrics (energy efficiency, carbon impact) into product development, it not only met compliance goals but also reduced operating costs, giving it a competitive advantage in cost structure.

Such wins show that IRM isn't just about avoiding downsides; it can actively drive upsides like innovation and efficiency.

It's not just risk managers pushing for it – boards and CEOs are increasingly demanding a clearer, consolidated risk picture to navigate the business.

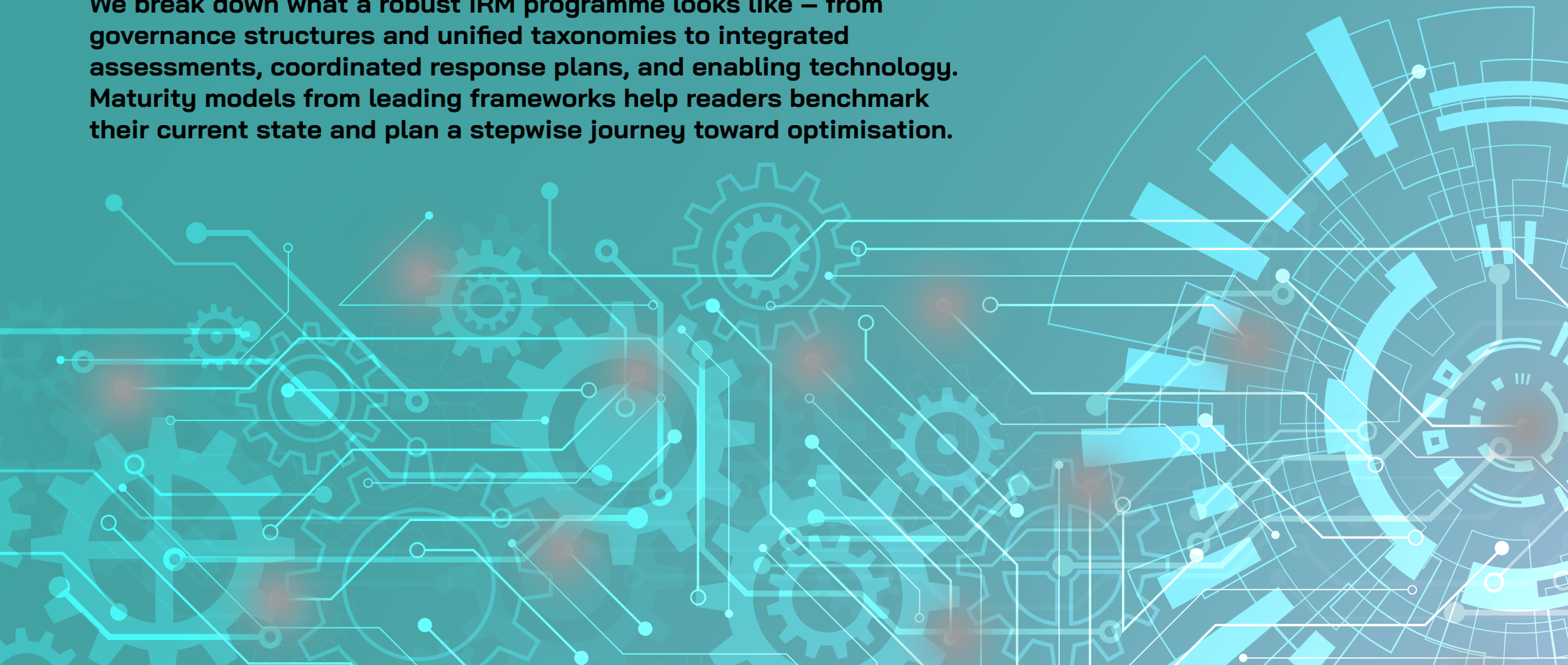
In many jurisdictions, regulators are effectively mandating integrated approaches (especially in finance and critical infrastructure sectors).

And events keep underscoring the need: each major incident or compliance fine that could have been prevented with better cross-functional insight becomes an internal catalyst for change.

> *Siloed risk management leaves organisations less agile and more prone to crises.*

Building a Mature IRM Programme: Components, Maturity Models, and Adoption Roadmaps

We break down what a robust IRM programme looks like — from governance structures and unified taxonomies to integrated assessments, coordinated response plans, and enabling technology. Maturity models from leading frameworks help readers benchmark their current state and plan a stepwise journey toward optimisation.



Moving from concept to reality, what does an effective Integrated Risk Management programme entail? This section breaks down the core components of IRM and provides guidance on developing your organisation's IRM capabilities over time – using maturity models and roadmaps to chart progress. We also highlight practical steps and best practices for adoption, including the human and change management aspects, not just the technical ones.

Core Components of a Mature IRM Programme

Experts and frameworks generally agree on a set of essential elements that a comprehensive IRM programme should have. We can think of these as six interlocking components, each reinforcing the other:

Strategy and Governance

It all starts with governance structure and strategic alignment. An IRM programme needs senior sponsorship and oversight (such as a Risk Committee at the board level or a top-level executive steering group). The organisation must define its risk appetite – ***how much risk are we willing to take in pursuit of objectives?*** – and ensure that this is communicated and understood across all units.

Risk Committee

A cross-functional group, often including senior executives and board members, responsible for overseeing an organisation's risk management strategy. The committee reviews major risks, monitors the effectiveness of controls, ensures alignment with risk appetite, and supports informed decision-making across the enterprise.

Clear policies and standards should establish common risk definitions, criteria, and processes. Essentially, governance sets the rules of the road. A formal risk governance body (like the Enterprise Risk Committee we mentioned before) monitors that the IRM programme is functioning and evolving with the business. Importantly, governance must integrate the three lines of defence model:

- Operational management (1st line) owns and manages risks
- Risk and compliance functions (2nd line) provide frameworks and monitoring,
- Internal audit (3rd line) gives independent assurance

In a mature IRM setup, these lines of defence collaborate rather than work at cross purposes. As Wayne Eckerson would remind us, good governance also requires data governance – standardising and securing data, eliminating silos and defects so that information flows freely and reliably. Without trustworthy, consistent data, even the best governance structure will falter.

Risk Identification and Assessment

This is the process of systematically cataloguing the risks the organisation faces (internal and external) and evaluating them. In an IRM context, risk identification must be enterprise-wide and use a common taxonomy. Instead of each department maintaining its own list, there is a central risk register or library, with risks grouped into **categories that make sense for the business** (strategic, operational, IT, compliance, etc.).

Definition

RISK TAXONOMY	A structured classification system that organises risks into defined categories and subcategories, creating a common language for identifying, assessing, and reporting risks across the organisation.

Many organisations find it useful to start by building such a **risk taxonomy** – essentially a hierarchical map of risks – as it provides a holistic view and common language.

Assessment then involves determining the likelihood and potential impact of each risk, often also considering factors like velocity *(how quickly it could hit)* and persistence.

Mature IRM programmes use both qualitative and quantitative methods: workshops and expert judgement combined with data-driven analysis (scenario analysis, stress tests, statistical models where feasible).

for instance

A risk owner from operations might team up with IT and compliance to jointly assess a cyber-related operational risk.

The goal is to understand not just each risk in isolation, but also aggregate risk (portfolio view) and inter-risk correlations.

Logic Manager's guidance suggests beginning by establishing the taxonomy and relationships, as that creates the foundation for holistic assessment.

Risk Response and Mitigation

Once risks are identified and assessed, the next component is deciding how to address them. Integrated risk management ensures that these decisions are made in line with enterprise priorities, not just departmental preferences. The classic responses – accept the risk, mitigate (through controls or actions), transfer (like insurance or contractual shifting), or avoid – should be applied consistently.

> *Integrated risk management aligns decision-making with enterprise-wide priorities, ensuring that actions are guided by the organisation's strategic objectives rather than isolated departmental interests.*

In a mature IRM programme, risk mitigation efforts are **prioritised at the enterprise level.**

This means, essentially, that if two departments have medium-rated risks but resources allow addressing only one, leadership can compare them and choose based on overall business impact, rather than each department lobbying for its own fix.

Mitigations are tracked centrally: there should be an enterprise risk action plan or register of controls/improvement actions, with clear ownership and deadlines.

Technology greatly helps here – modern IRM platforms provide workflow tools to assign risk owners and track mitigation progress on dashboards.

For third-party risks, mitigation might involve requiring certain controls in contracts, adding redundancy (alternate suppliers), or carrying out additional oversight. A mature programme doesn't just plan mitigations – it **executes and monitors** them, ensuring that risk treatments actually happen and are effective.

Communication and Reporting

Information flow is the lifeblood of IRM. Relevant risk information must reach the right stakeholders at the right time.

KRIs
Key Risk Indicators

This means tailored reporting: the board and CEO might get a high-level heat map and top-five risks summary, while business unit leaders see more detailed dashboards for their areas, and risk owners et granular reports on **KRIs** and control effectiveness.

A mature IRM setup uses **real-time dashboards** and analytics accessible through the risk platform.

> *In a mature IRM programme, risk mitigation plans are not left on paper. Actions are implemented, tracked, and monitored to confirm that treatments are completed and delivering the intended results.*

Visualisations like trend charts, risk matrices, and scenario impact graphs help make the data actionable.

Crucially, IRM fosters open communication: incidents and near-misses are reported and shared as learning opportunities, not swept under the rug. There is a culture of transparency – no *"shooting the messenger"* when someone raises a risk issue.

Regular risk reports are discussed in management meetings, not just filed away. Communication also includes integrating risk disclosures into external reporting (financial filings, sustainability reports, etc.) – ensuring consistency and candour.

In practical terms, a mature IRM programme will often have a **central risk portal** or dashboard where any manager can see the enterprise risk profile and drill into areas of interest, subject to access rights.

This breaks the old pattern where risk information was siloed and shared sparingly. The result is fewer surprises: when a risk is trending negatively, executives find out through the IRM reports, not via a front-page news story or an angry regulator.

Developing Key Risk Indicators

1. **Risk Assessment and Analysis** – Begin by conducting a comprehensive risk assessment to identify and analyze the various risks facing the organisation. This involves identifying threats, assessing vulnerabilities, and evaluating the potential impacts and probabilities of these risks.
2. **Determine Business Objectives –** Understand the organisation's strategic, operational, and financial objectives. KRIs should be directly linked to these objectives to ensure they are relevant.
3. **Consultation with Stakeholders –** Engage with key stakeholders across various departments to gather insights and perspectives on potential risks. This includes management, operational staff, and external advisors. Stakeholder input is crucial for identifying risks that may not be immediately apparent and for ensuring buy-in during the KRI monitoring phase.
4. **Selection of Relevant KRIs –** From the information gathered, select indicators that are most relevant to the identified risks and business objectives. Ensure these KRIs are measurable, actionable, and predictive, as discussed in the characteristics of good KRIs.
5. **Set Thresholds and Limits –** Establish clear thresholds and limits for each KRI. These thresholds will act as triggers for action when breached and should be based on the organisation's risk tolerance and appetite.
6. **Integration into Risk Management Framework –** Integrate the selected KRIs into the existing risk management framework. Ensure that there are clear protocols for monitoring, reporting, and acting on the KRIs.
7. **Review and Refinement** – Regularly review and refine KRIs. As the business environment and internal operations evolve, so too should the KRIs. This ensures that they remain relevant and effective in identifying risks.

Monitoring and Continuous Improvement

IRM is not a one-time project; it's an ongoing discipline.

Continuous monitoring involves tracking both risk indicators and control performance. KRIs – metrics that provide early warning of risk changes – are established for major risks.

> *Continuous monitoring means actively tracking key risk indicators and control performance in near real-time, enabling faster detection of changes or issues that could affect the organisation's risk profile.*

for instance

For a supplier risk, a KRI could be "days of inventory on hand" or that supplier's credit default swap spread, etc.

These are monitored so that emerging problems can be flagged. Likewise, **KCIs** or similar metrics track whether critical controls are functioning (like the percentage of systems patched on time for cyber risk).

KCI
Key Control Indicators

A mature IRM programme will use automation for much of this monitoring – pulling data from systems to update KRIs and KCIs without manual effort. When incidents do occur – and they inevitably will – the organisation conducts post-mortems or lessons-learned reviews.

Definition

POST MORTEM

A structured review held after a project, incident, or failure to determine what happened, why it occurred, and how to prevent similar issues in the future. It examines both what went wrong and what worked well, focusing on root cause analysis, lessons learned, and process improvements rather than assigning blame.

So, after a significant outage or compliance issue, a cross-functional team analyses root causes:

- Did our risk assessment miss something?
- Were controls inadequate or by passed?
- Did communication fail?

The findings from these reviews are used to strengthen the programme – updating risk assessments, improving controls, retraining staff, etc.

This continuous improvement loop is a hallmark of mature IRM.

Over time, it leads to **lower incident frequency and impact**, as the organisation keeps learning and adapting.

It also involves benchmarking against peers and standards – many firms periodically get independent audits or maturity assessments of their risk management, seeking recommendations for improvement. In essence, no IRM programme is ever *"finished"*; it should keep evolving as the business and its environment evolve.

Technology and Infrastructure

Though often listed last, technology underpins every component of IRM. A mature setup typically includes a central risk management platform or GRC system as the system of record.

APIs
Application Programming Interface's

It should integrate with other enterprise tools – ERP, IT security systems, incident management, and regulatory feeds – ideally via **APIs** to automatically pull in relevant data.

Strong *data governance* is essential, ensuring proper access controls, data quality, and audit trails.

> *IRM promotes transparency by treating incidents as learning opportunities.*

Modern platforms increasingly offer embedded analytics, natural language processing, and AI-driven scoring.

But technology maturity isn't about having advanced tools – it's about configuring them to match the organisation's taxonomy, workflows, and reporting needs. A well-tuned platform also supports continuous control monitoring, automatically testing backups, privileged access, and other critical safeguards.

Privileged Access

Elevated system or network permissions granted to specific users, accounts, or processes that allow them to perform critical tasks, such as configuring systems, accessing sensitive data, or managing security settings. Because these rights can bypass standard controls, they require strict management, monitoring, and security to prevent misuse or compromise

Technology makes IRM scalable and sustainable, but it's an enabler, not a silver bullet – people and processes must work in concert with the tools. When all components align, an organisation can claim a mature IRM programme. Most, however, must build capability over time, guided by maturity models and structured roadmaps.

IRM Maturity Models for Self-Assessment

How do you know where your organisation stands on the path to IRM, and what the next level looks like?

This is where maturity models prove useful. A maturity model provides a structured way to gauge the current state of risk management practices and to plan improvements.

Typically, these models outline levels (often five) ranging from rudimentary to optimised.

SANS/GIAC Information Security Maturity Model	• **Focus:** IT and information risk management • **Structure:** Five levels from Initial (ad-hoc) to Optimised • **Differentiator:** Strong emphasis on technical security controls and operational processes • **Best for:** Organisations prioritising cybersecurity maturity as a foundation for broader IRM
Deloitte Risk Intelligence Maturity Model	• **Focus:** Enterprise-wide risk integration • **Structure:** Six domains (governance, strategy alignment, performance, risk assessment, communication, monitoring) with stages from Initial to Optimised • **Differentiator:** Balances governance and culture with quantitative risk performance integration • **Best for:** Large, diversified organisations seeking a holistic view of strategic and operational risk
LogicManager Risk Maturity Model (RMM)	• **Focus:** Practical roadmap to integrated risk management • **Structure:** Eight attributes (including culture, process management, accountability) scored across maturity levels • **Differentiator:** Provides diagnostic scoring and tailored improvement actions • **Best for:** Mid-market and fast-growing companies needing a clear, actionable self-assessment

ISACA Risk IT Maturity Model	● **Focus:** Aligning IT risk with business objectives ● **Structure:** Levels from Non-Existent to Optimised ● **Differentiator:** Strong linkage between IT governance and enterprise risk strategy ● **Best for:** Organisations where technology risk is central to operations or digital transformation initiatives
COSO Enterprise Risk Management Maturity Guidance	● **Focus:** Integrating risk into corporate governance ● **Structure:** Progressive stages of risk capability ● **Differentiator:** Tightly aligned with widely adopted COSO ERM framework, supporting board-level oversight ● **Best for:** Organisations seeking strong regulatory alignment and board engagement in risk management

The Four Stages of IRM Maturity

Stage 0 – Manual & Reactive
- Spreadsheets, emails, ad-hoc processes
- Little visibility, no central accountability
- Risks only addressed after incidents

Stage 1 – Defined & Modernising
- Basic policies documented, some accountability
- Fragmented visibility, manual-heavy processes
- Early steps toward structure

Stage 2 – Integrated & Improving
- Standardised processes across functions
- Central platform with some automation
- Risk data informs planning, silos reduced

Stage 3 – Optimised IRM
- Enterprise-wide integration into strategy
- Continuous monitoring, advanced analytics
- Unified dashboards for real-time visibility
- IRM embedded into culture, enabling resilience

for instance

You might find you're at Level 2 – with repeatable processes but little enterprise integration – and see that moving to Level 3 requires common frameworks, executive sponsorship, and centralised tools.

Maturity models help organisations assess their current state, identify gaps, and plan improvements.

Maturity often varies by component: risk identification may be strong while monitoring is weak.

Many organisations use these models diagnostically, showing leadership where they stand versus peers and what's needed to progress.

> *Maturity models progress from fragmented and reactive to integrated and proactive.*

Ultimately, all models guide the shift from siloed, reactive practices to integrated, proactive, and optimised risk management.

They offer a high-level roadmap, which the next section translates into practical steps for building an IRM programme.

Developing an IRM Adoption Roadmap

Embarking on IRM is a multi-year journey. It requires changes in processes, technology, and mindset.

A structured roadmap can guide this transformation. Here is a high-level approach to developing and executing an IRM roadmap:

Assess the Current State

Begin with a candid evaluation of how risk is managed today. Use the maturity model as a lens. Identify which silos exist and the pain points they cause. Inventory current risk management activities, tools, and reports.

Identify strengths to build on and gaps to close.

This means you might discover that operational risk and IT risk teams already collaborate somewhat (strength), but compliance and audit are completely separate (gap), and there's no central risk view for executives (gap). Also assess data quality and governance – often a big limiting factor. This baseline sets the starting point.

> *Assess your current IRM capabilities to determine where strengths can be leveraged and where weaknesses need addressing, ensuring improvement efforts are targeted and achievable.*

Define the Target State

Clarify what *"good"* looks like for your organisation in, say, 2-3 years. This includes selecting an appropriate target maturity level (you may not aim for Level 5 immediately, but perhaps Level 3+ or 4).

Align this with business objectives: So, if expanding into new markets, maybe strengthening compliance IRM is critical; if digitising, maybe cyber and IT risk integration is key.

The target state should articulate things like *"All key risks will be recorded in a single system with real-time dashboards"* or *"Risk appetite will be defined and linked to KPIs,"* etc.

As John Wheeler suggests, aligning risk initiatives with business goals ensures the roadmap supports the overall strategy.

Prioritise Initiatives

You likely can't do everything at once, so prioritise the initiatives that will yield the highest impact or address the biggest vulnerabilities first.

for instance

if regulatory pressure is a huge concern, prioritise integrating compliance and operational risk reporting.

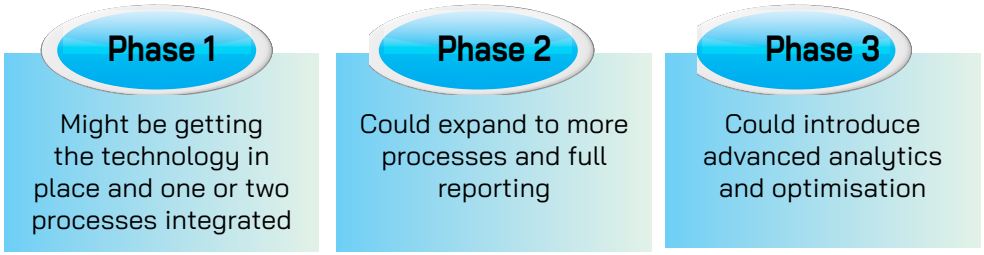
Quick wins are valuable for momentum – such as establishing a common risk taxonomy (which is relatively **low-cost but high impact** in improving consistency), or automating a particularly painful manual report.

It's often wise to tackle foundational tasks early (like data integration, choosing and configuring an IRM platform) because they enable other improvements.

Develop a Phased Implementation Plan

A roadmap should be phased, typically over 1-3 years, with clear milestones. One effective approach is piloting IRM in one part of the business first.

By this we mean something like pilot in a high-risk domain – maybe third-party risk management – using an integrated approach, work out kinks, then roll out to other domains.



Ensure you sequence logically: you wouldn't implement an AI risk analytics tool (advanced) before you have basic risk data consolidated (prerequisite).

Also plan resources – you will need a cross-functional team for this journey, and possibly external expert help at points. Make sure each phase has defined outcomes.

Secure Executive Sponsorship and Governance

IRM roadmaps can falter without strong sponsorship. Ideally, the CEO or at least a C-suite champion (Chief Risk Officer if one exists, or CFO, COO, etc.) is visibly behind it.

Form a cross-functional steering committee with stakeholders from finance, IT, compliance, operations, etc., to guide the roadmap and resolve conflicts. This committee ensures buy-in and helps push through organisational resistance. They also serve as risk 'ambassadors' in their units.

Invest in the Right Technology (but do it smartly)

Selecting an IRM platform or enhancing existing tools is a critical roadmap item. The roadmap should include evaluating vendors or solutions against your needs, doing a pilot or proof-of-concept, and then rolling it out. When selecting, consider not just current requirements but the innovation roadmap of the vendor – you want a solution that will evolve with you (adding AI, etc.).

for instance

- Year 1 deploy core risk register and incident capture modules;
- Year 2 add workflow automation and compliance mapping;
- Year 3 enable advanced analytics.

Also, prioritise integration capability – the tool must talk to your other systems. The roadmap might phase technology deployment. Avoid the trap of trying to implement every module at once – it can overwhelm users. **Configurability is key:** plan time and resources for configuring the software to reflect your processes, otherwise users will reject it. And don't forget training.

Change Management and Culture Building

An IRM roadmap is as much about people as process. Include initiatives for culture change: communications plan to explain why IRM is needed (highlighting pain points of silos, perhaps using incident post-mortems to illustrate), training sessions for different levels (risk 101 for business managers, tool training for end-users, etc.), and perhaps updating performance objectives to include risk management responsibilities.

Organisational resistance is natural – some might fear that integration means loss of control or additional work.

The roadmap should identify likely points of resistance and plan to address them (like involving those teams early in design, finding quick wins to show value, creating incentives for collabouration).

> *Expect some resistance when moving to an integrated approach; team members may worry about losing autonomy or facing more work. Address these concerns early with clear communication on benefits and shared goals.*

Monitor Progress and Adapt

As you execute the roadmap, establish metrics to track progress.

These could include the number of silos eliminated user adoption rates of the new process/ tool, reduction in duplicated audits, improved risk indicator trends, etc.

Regularly review the roadmap in steering committee meetings.

> *Making risk management a team effort and communicating plans clearly is advice that underlines the need for broad engagement. Celebrate early successes: if a new integrated report helped avoid a problem or impressed the board, publicize that internally to build momentum.*
>
> *~ John Wheeler*

for instance

By Q4, implement unified risk register and reporting for Finance and IT risks. By Q2 next year, consolidate 80% of departmental risk registers into enterprise system.

Be prepared to adjust – maybe some things go faster, others slower; maybe a new risk (like a pandemic) forces a reprioritisation to include business continuity planning integration sooner.

A roadmap is not rigid; it's a guide. Also, keep an eye on external benchmarks: are peers moving faster?

Did a new regulation emerge that speeds up your timeline for certain capabilities? Adapt accordingly.

> *An IRM roadmap provides direction but should remain flexible enough to adapt to new risks, technologies, and business priorities as they emerge.*

Executing an IRM roadmap is iterative. It's wise to treat it as a change programme with proper project management discipline. But one must also remain flexible and pragmatic.

for instance

If one business unit is dragging its feet, it might be okay to move ahead with others and let that unit catch up once benefits are proven – rather than stall the whole programme.

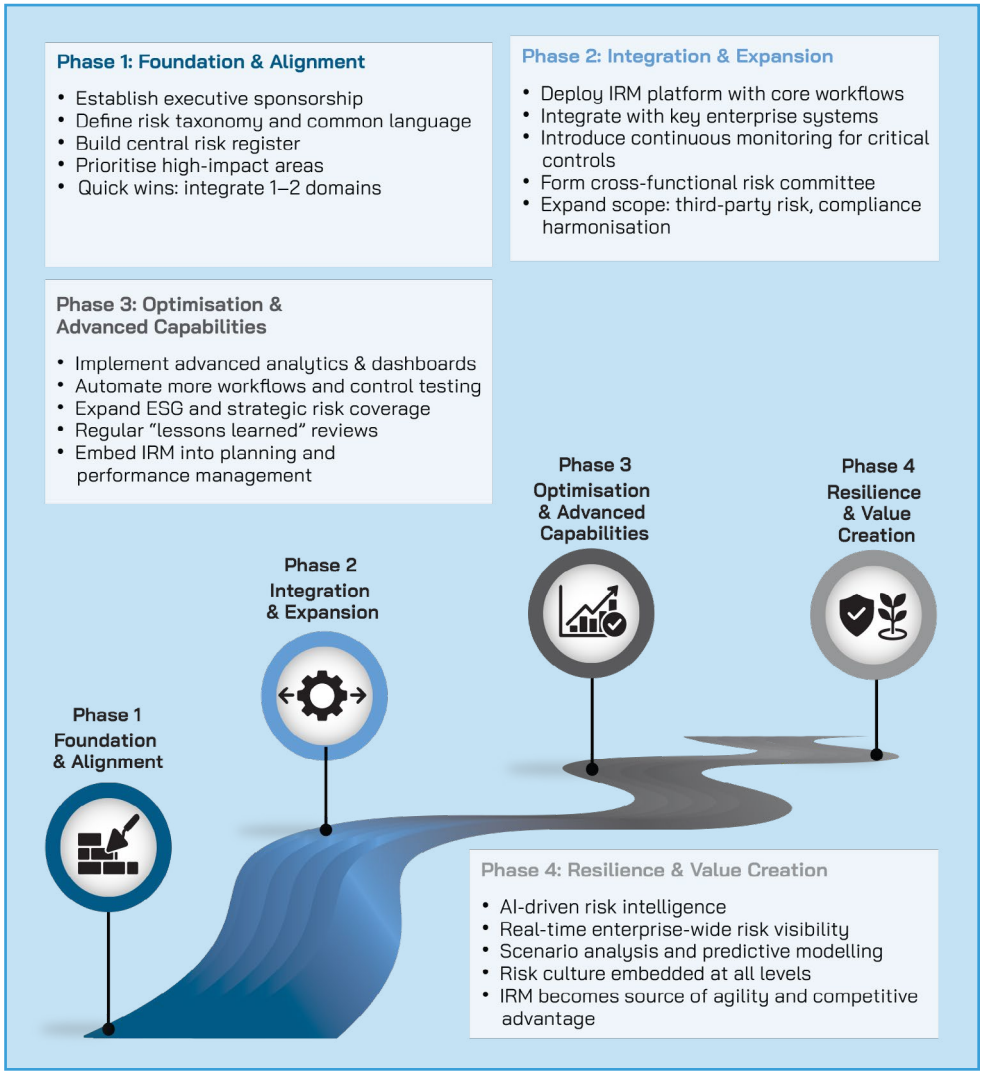
Importantly, maintain a focus on the purpose: improved decision-making, performance, and resilience.

Sometimes risk initiatives can get too inwardly focused (building a perfect risk taxonomy that no one uses). Keep the end-users (management and the board) in mind – are they seeing better information? Are decisions being made faster or with more confidence thanks to IRM?

Periodically revisit the business case – by year 2, you should be able to demonstrate some tangible benefits (even if qualitative) like 'fewer surprise issues' or 'audit prep time reduced by 30%' or 'credit rating improved due to better risk oversight.'

Those help sustain support.

In summary, the IRM roadmap is about **moving systematically from the current fragmented state to the desired integrated state**, in phases that make sense for your organisation's context. It requires balancing quick wins with foundational investments, and managing the human side of change as much as the technical side.



Market and Vendor Landscape

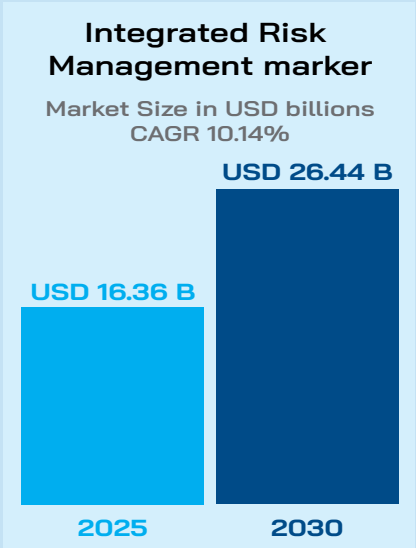
With the IRM software market expected to grow from US$10.9 billion in 2023 to almost US$40 billion by 2032, we analyse the vendor landscape. Full-suite leaders, cloud-native innovators, and niche specialists are compared with guidance on selecting solutions that enhance integration and visibility.

As organisations pursue IRM, they often look to technology solutions to facilitate the integration of risk data and workflows. The vendor landscape for risk and compliance management tools – often labelled GRC (Governance, Risk & Compliance) or IRM software – is broad and evolving. In this section, we provide an overview of the IRM software market, discuss categories of solution providers, and highlight key considerations when evaluating vendors.

Market Overview

The demand for integrated risk solutions has been steadily rising. Industry analysis projects healthy growth for IRM software globally. In fact, Mordor Intelligence estimates **the global IRM market will grow from around US$16.36 billion in 2025 to roughly US$26.44 billion by 2030, a CAGR of about 10%.**

Integrated Risk Management Market Size and Share



Market Overview	
Study Period	2022 - 2030
Market Size 2025)	USD 16.36 Billion
Market Size (2030)	USD 26.44 Billion
Fastest Growing Market	Asia Pacific
Growth Rate (2025 - 2030)	10.14% CAGR
Largest Market	North America
Market Concentration	Medium

This growth is fuelled by the drivers we discussed earlier: regulatory complexity, increasing cyber threats, digital transformation initiatives, expanded third-party ecosystems, and ESG reporting requirements.

In parallel, many vendors in adjacent spaces (like IT service management, security, audit) have been expanding or repositioning their offerings to address integrated risk needs.

We're seeing some consolidation as well – larger players acquiring niche providers to broaden their suites.

Despite some consolidation, the market remains **fragmented**. There isn't a one-size-fits-all IRM solution.

Vendors range from legacy enterprise platforms known for deep functionality (but sometimes higher complexity) to newer cloud-based entrants known for usability and flexibility. Gartner (when it used to cover IRM as a category) and others have identified a *"Magic Quadrant"* of sorts, typically with a handful of Leaders and many Specialists.

Let's categorise vendors in broad groups for clarity:

1 Market Leaders (Full-Suite Providers)

These are the established, comprehensive GRC/IRM platforms often used by large enterprises and heavily regulated industries.

They offer modules covering a wide array of risk domains – operational risk, IT risk, compliance management, internal audit, policy management, third-party risk, etc., usually integrated on one platform.

ARCHER

A pioneer in the space, Archer offers a very comprehensive suite of risk and compliance modules. It's known for high configurability and depth, especially in areas like operational risk and SOX compliance. The flip side is it can be complex to implement and maintain, often requiring significant admin expertise.

metricstream

Another long-time leader, covering enterprise risk, IT/cyber risk, compliance, audits, and case management. MetricStream has strong analytics and is often favoured in financial services and healthcare. They emphasise risk quantification and have rich content libraries (regulations, control standards, etc.).

servicenow

Originally a leading IT Service Management platform, ServiceNow extended into IRM by leveraging its workflow engine. It offers integrated workflows connecting IT issues, incidents, and risk registers. A strength is its wide use within IT – if a company already uses ServiceNow, adding its risk modules can be seamless. It shines in integrating IT risk with IT operations (tying vulnerabilities to risk entries, etc.).

NAVEX

(which now includes Lockpath/Galvanize) – NAVEX is known for ethics/compliance solutions (hotline, policy, training) and after acquisitions, offers a broader risk suite. It provides compliance content (reg libraries) and is strong in things like third-party risk and policy management, with a user-friendly interface.

Diligent

Diligent acquired Galvanize (which had the HighBond platform) and is integrating that with its governance tools (like board reporting software). Diligent's IRM approach focuses on modernising governance reporting and linking risk to ESG and board oversight, with a polished UI.

SAI360

Offers a broad GRC suite and is particularly known for strength in health, safety, and environment (HSE) risk management, in addition to enterprise risk. They often emphasise operational resilience and have capabilities tailored to specific industries (energy, healthcare).

Others in this tier might include IBM OpenPages, SAP GRC solutions, and Oracle's risk modules, although those often come as part of larger ERP/analytics suites rather than standalone IRM offerings.

These full-suite providers typically have strong functionality but can be relatively expensive and require commitment to fully leverage. They often cater to organisations that want an integrated system covering most risk and compliance needs out-of-the-box (with configuration).

2 Fast-Growing Accelerators (Cloud-Native Platforms)

These are newer generation platforms focusing on agility, user experience, and rapid deployment. They appeal to mid-market and also to large enterprises that prioritise flexibility and modern design.

AuditBoard

Starting from audit management, AuditBoard expanded into risk and compliance in an integrated cloud platform. It's praised for ease of use and a modern interface. Many internal audit teams adopt it and then bring risk management into it. It provides automation of testing and integrates controls across frameworks. AuditBoard puts a lot of focus on usability for end users (risk owners can easily log issues, update risks, etc., without much training).

OneTrust

Originating in privacy compliance, OneTrust has grown into what it calls a *"trust platform"* that includes GRC/IRM capabilities. Its strengths are in data governance, privacy, and security risk, leveraging its background in those areas. OneTrust's interface is relatively intuitive and it often finds favour where privacy or vendor risk is a main concern (with integrated templates for those).

LOGICGATE

Offers a no-code "Risk Cloud" that is highly configurable. Users can build custom workflows for different risk processes without coding. It's valued for flexibility – companies can tailor it a lot – and relatively quick to implement for targeted use cases. Often mid-size companies use it to gradually build out risk processes one app at a time.

LogicManager™

Known for excellent customer support, LogicManager provides pre-built content (risk libraries, templates) and a focus on ease for organisations newer to formal risk management. It covers ERM, compliance, incidents, etc., and often markets itself as an affordable, easy-to-adopt solution. They emphasise customer success, guiding clients through implementation with provided best practices.

centraleyes

A newer player focusing on cyber and IT risk with a sleek interface and strong automation/visualisation. They integrate threat intelligence feeds and offer continuous control monitoring, making it useful for real-time cyber risk management in medium enterprises. Their dashboards are a selling point (clear visuals for risk posture).

Resolver.

Provides *"risk intelligence"* software that ties together incidents, continuity, IT risk, and vendor risk to generate insights. Resolver's philosophy (as echoed by Amanda Cohen) is about turning risk data into actionable intelligence for the business. They highlight analytics and the ability to uncover opportunities (not just mitigate negatives) through risk data. The platform is quite integrated and user-friendly, with scenario analysis capabilities.

These cloud-native players tend to have shorter implementation times and focus on configurability and integration. They often allow customers to activate just the modules they need and then expand. Their challenge can be ensuring they scale and meet complex needs as deeply as the full-suite vendors.

However, many are rapidly enhancing functionalities and even surpassing legacy tools in certain areas (like user experience or integrated AI features).

3 Specialists and Niche Providers

Beyond the generalists, there are numerous tools specialising in particular risk domains or industries.

They can be part of an IRM ecosystem by focusing on one slice:

Camms

Camms is a provider from Australia focusing on integrated risk and project management, used in public sector and some industries.

QUANTIVATE

Quantivate offers solutions especially for financial institutions (banks, credit unions) with focus on regulatory compliance management.

MEGA INTERNATIONAL

MEGA International has a GRC offering strong in Europe, often tied with process architecture and BPM (business process management) tools.

Workiva

While known for financial reporting and SOX compliance, Workiva has extended into integrated reporting including ESG. It's used to connect risk data to reporting and is considered an emerging force especially for integrated reporting (financial + non-financial risk data).

riskonnect.

Riskonnect focuses on integrated risk management plus insurance and claims management – useful for industries where insurable risks and claims data are big (they acquired Sword GRC and others).

IHS Markit®

IHS Markit (now part of S&P Global) has tools for third-party and supply chain risk that feed into broader risk programs.

There are also pure cyber risk platforms (like CyberSaint or UpGuard for vendor cyber scores) which some companies use in conjunction with broader IRM software.

And one must mention the mega vendors: **SAP, Oracle, IBM, Microsoft.** Each of these has some offering (SAP has GRC modules; Oracle has risk controls and cloud compliance tools; IBM's OpenPages covers operational risk; Microsoft has compliance manager in its 365 environment, etc.).

These are often chosen if you are heavily invested in that ecosystem.

Increasingly, some younger companies are pushing boundaries – for example, those focusing on AI governance specifically, or combining incident response with risk management in novel ways.

They might be acquisition targets for bigger players in time.

Selecting the Right IRM Vendor

Choosing an IRM solution is a significant decision.

Organisations should consider several factors aligned to their requirements. Some key questions and considerations include:

Scope of Functionality: Decide if you need an all-in-one platform for enterprise, operational, IT, and compliance risk, or a single-domain solution you can expand later. Match vendor strengths to your priorities (such as strong third-party risk management).

Integration: Check how easily the tool connects to existing systems (including ERPs, scanners, incident databases, etc.). Look for native integrations, API support, and partnerships that streamline data feeds.

User Experience and Configurability: Test the interface for different user roles.

Favour intuitive, no-code/low-code platforms that allow easy workflow and form changes without vendor intervention.

Regulatory Content and Frameworks: Ensure the vendor provides templates for frameworks (ISO 27001, COSO, NIST, HIPAA) and updates them as laws change. Built-in content saves setup time.

Analytics and Reporting: Look for rich reporting options (heat maps, dashboards, what-if analysis) and advanced risk quantification. Export capabilities or built-in analytics support deeper analysis.

Vendor Viability and Support: Evaluate vendor stability, roadmap, customer support, training, and community.

Check implementation support and long-term partnership potential.

Cost and Scalability: Balance cost against breadth of functionality.

Understand pricing for different user types, scaling for data volume, and long-term affordability.

Openness and Interoperability: Avoid lock-in with vendors that offer open standards, APIs, and easy data export, ensuring future flexibility.

Use a cross-functional team to define requirements and test top vendors with real scenarios.
Speak to industry references, and invest in proper implementation and change management to fully realise IRM benefits.

Emerging Technologies Enhancing IRM

AI, automation, and blockchain are reshaping risk management. From predictive analytics to continuous control monitoring, emerging technologies are enabling a shift from reactive to proactive risk management – provided they're used responsibly with human oversight.

As Integrated Risk Management practices mature, forward-thinking organisations are exploring how emerging technologies can further enhance risk identification, analysis, and mitigation.

AI
Artificial Intelligence

In particular, **AI** and advanced automation are proving to be game-changers in evolving IRM from a largely manual, retrospective process to a more automated, predictive, and responsive discipline.

This section delves into the ways AI, machine learning, and related technologies are reshaping IRM, as well as other technology trends on the horizon (blockchain, quantum computing considerations, etc.).

We will also stress the importance of using these powerful tools responsibly, with human judgement still in the loop.

AI-Driven Risk Intelligence

Artificial Intelligence and machine learning are already being applied in various risk domains, and their role is set to expand dramatically. As we said before, Thomson Reuters survey found that **80% of audit, risk, and compliance professionals expect AI to have a high or transformational impact on their work within the next five years**. So how exactly can AI contribute to IRM?

The AI Market Growth Projection

Disconnect Between Future Aspiration and Current Pace

80% believe that AI will have a high or even transformational impact on their profession within 5 years, but...

38% expect to see transformational or high levels of change in their organization this year.

53% believe their organization is already experiencing at least one type of benefit from AI adoption, but...

30% believe their organization is moving too slowly in AI adoption.

1 Predictive Analytics

AI algorithms excel at analysing historical data to identify patterns and forecast future events. In risk management, this means using machine learning models to predict the likelihood of certain risks materialising, or to estimate potential losses. To illustrate this; imagine feeding in data on past incidents, near-misses, and external risk factors. An AI could predict an increase in risk levels for, say, supply chain disruptions given emerging news of a region's instability.

Predictive models can also forecast trends like credit default probabilities in financial portfolios or evolving fraud patterns in transactions. This forward-looking ability enables a shift from reactive to *proactive* risk management – catching issues before they escalate.

2 Real-Time Monitoring and Anomaly Detection

Organisations are awash in data streams (IT system logs, transaction data, social media feeds, etc.) that can contain early warnings of risk. AI, particularly techniques like anomaly detection, can continuously monitor these streams to flag unusual patterns that might signify risk events.

> *AI can monitor multiple data streams in real time, detecting unusual patterns or anomalies that may indicate emerging risk events before they escalate.*

for instance

An AI system might watch network traffic and alert on anomalies that suggest a cyber-intrusion attempt (a sort of AI-enabled SOC), or monitor employee expense reports to flag patterns consistent with fraud. Natural Language Processing (NLP) can sift through unstructured data – news articles, regulatory updates, social media – to extract risk-relevant information (like noticing a spike in negative sentiment about a supplier that could indicate reputational or operational trouble).

By analysing multiple sources in real time, AI provides cognitive risk sensing – essentially an always-on radar for emerging risks.

3 Natural Language Processing for Compliances

Compliance risk management often involves parsing large volumes of text – laws, regulations, standards, internal policies – and mapping them to business processes and controls. NLP can assist by reading new regulatory documents and identifying key obligations, or by analysing contractual text to find risk clauses.

So, AI could read a GDPR regulation update and flag which sections of your data handling policy need revision, saving compliance teams a lot of grunt work. It can also help maintain risk taxonomies by clustering and relating concepts across documents.

4 Generative AI for Scenario Simulation

Generative AI, which creates new content or data based on training examples, is finding its way into risk scenario analysis. By training on historical incidents and relevant data, a generative model could simulate **'what-if' scenarios.**

for instance

It might generate a plausible scenario of a cyber-attack on a critical supplier and describe how that could ripple through supply chain and operations. This helps teams test contingency plans. Generative AI can also create synthetic data to test risk models or even draft risk reports and policies (under human review), speeding up documentation.

Definition

SYNTHETIC DATA Artificially generated data that mimics the patterns and structure of real-world data, used for testing, training AI models, or analysis without exposing sensitive or confidential information.

5 Decision Support

AI can serve as an intelligent assistant to risk managers by analysing large datasets and surfacing recommendations. So, it might suggest transferring a particular risk via insurance after recognising a pattern of

high historical losses that were successfully mitigated with policies. In complex environments with thousands of open issues, AI can prioritise which risks most urgently need management attention, enabling teams to focus on what truly matters.

These capabilities are no longer theoretical. Deloitte reports that many financial institutions are already using or testing machine learning to enhance predictive accuracy and efficiency in risk management. One notable example comes from banking: AI models have been used to predict which small business customers are likely to default on loans by analysing their transaction histories, social media sentiment, and macroeconomic factors. These models generated early warning signals months before traditional risk ratings would have, allowing banks to intervene or hedge exposures in time.

On which part of the value chain do you see the Artificial Intelligence use case you have developed having the greatest impact?

Customer service	65%	Back office / operations	78%
Back office / operations	52%	Risk management	56%
Financial advisors	42%	Fraud detection	56%
Fraud detection	31%	Customer service	44%
Risk management	29%	Compliance	22%

The survey also concluded that, overall, the adoption of AI in FS is still in its infancy. Of the firms surveyed, 40% were still learning how AI could be deployed in their organisations, and 11% had not started any activities. Only 32% were actively developing AI solutions.

Cognitive Risk Sensing deserves mention here. This approach combines AI's ability to continuously scan the external environment with human expertise. AI might flag anomalies such as sudden increases in regional illness reports that could disrupt supply chains or early signs of regulatory changes from draft legislation. Human analysts then review these signals to determine which warrant action. This partnership between machine insight and human judgment significantly enhances organisational foresight. However, with great power comes great responsibility – which brings us to oversight and ethical use.

Automation and Orchestration

Beyond AI in analysis, automation technologies are streamlining the execution of risk management tasks:

1 Robotic Process Automation (RPA)

Many risk and compliance tasks are routine and time-consuming – collecting data for audits, checking compliance controls, compiling reports. RPA can perform these by mimicking user actions.

for instance

An RPA bot might scrape data from different systems to fill out a risk report template overnight, saving an analyst many hours.

Or it could automatically send questionnaires to vendors and gather responses, rather than someone emailing each vendor. By automating evidence collection and verification, risk managers free up time to actually analyse and act on risks.

2 Continuous Control Monitoring

Automation can continuously test whether key controls are operating. Instead of a quarterly manual control test, scripts or control-monitoring tools can run daily

for instance

Automatically verifying that all transactions over a threshold had dual approval, or that system configurations remain compliant.

When exceptions are detected, alerts are raised immediately.

This not only cuts labour but catches control failures early (reducing exposure window). Many IRM platforms integrate such scripts or connectors to do these checks against IT systems, financial systems, etc.

> *Automation eases admin work and prevents tasks from being missed.*

3 Workflow Orchestration

IRM involves coordinating activities across different teams – like ensuring an incident triggers notifications, or a risk acceptance goes through approvals.

Modern workflow engines (like in ServiceNow or others) can orchestrate these steps reliably and fast.

for instance

If a risk rating crosses a threshold, the system could automatically route a mitigation plan task to the risk owner and escalate to management.

If a compliance attestation is due, workflows can send reminders, collect approvals, and log the results.

This reduces the administrative burden on risk offices to chase people and track statuses, ensuring nothing falls through cracks.

4 Security Automation (SOAR)

For cyber risks, **SOAR** tools can automatically respond to certain events (like isolate a compromised device when an alert triggers).

When integrated with IRM, these actions become part of the risk mitigation record.

SOAR
Security Orchestration, Automation, and Response

for instance

If a high-risk vulnerability is discovered, a SOAR might apply a patch or block traffic, and the IRM system logs that mitigation was applied immediately. This closes the loop between detection and action within seconds, rather than days if done manually.

In essence, automation ensures risk processes operate at the speed of digital business.

This is vital; threats like cyber-attacks unfold in minutes, and spreadsheets simply can't keep up.

Automation handles volume and speed, while humans handle judgement and complex decisions.

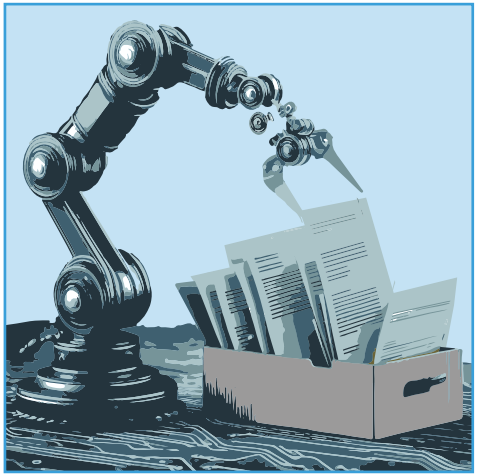
A concrete case: A large tech company integrated RPA to handle compliance checks for user access rights across hundreds of systems nightly.

> *Automation should not be left unchecked; organisations must regularly review automated processes and rules to ensure they remain accurate and effective as conditions evolve.*

The RPA would report any anomalies (like an account that should have been removed).

This replaced an arduous quarterly manual review and caught issues much sooner – significantly reducing insider threat risk.

The caution with automation is to not 'set and forget' – periodic review is needed to ensure automated processes and rules remain valid as business conditions change.



But overall, integrated automation is a force multiplier for IRM teams who are often small relative to the organisation size.

Responsible AI and Ethics in Risk Management

While AI and automation hold immense promise, they also introduce new risks and challenges. Tools that can analyse or decide at scale can also make mistakes at scale, or embed biases, or operate opaquely. It's a classic risk paradox: using AI to reduce some risks can create others. Hence, as organisations embrace AI in IRM, they must also manage the risks of AI itself.

Key considerations include:

1 Bias and Fairness

AI models are only as unbiased as the data and assumptions that shape them. If historical data reflects biases (certain groups being under-served or overly penalised), the AI could perpetuate or even amplify that bias. In risk scoring, this might mean unfairly high risk ratings for certain customer segments or regions simply due to biased past data.

IRM teams should ensure AI models are tested for bias and that their outcomes can be explained and justified. Techniques like AI model explainability and bias audits are crucial. If an AI flags 10 vendors as *"high risk"*, can it explain why in understandable terms? Are those reasons fair and relevant?

2 Transparency and Explainability

Black-box AI is dangerous in risk management. If management is to trust AI-driven insights, they need to understand the rationale.

> *Use AI models that make their decision process transparent.*

Furthermore, regulators (especially in financial services) increasingly demand that AI decisions be explainable. Therefore, when deploying AI in IRM, choose approaches that allow insight into how the model arrived at a result. In other words, use algorithms that provide feature importance (what factors influenced a risk prediction) or use supplementary explanation tools for complex models, and so on.

Black Box AI

An artificial intelligence system whose internal decision-making process is not easily understood or interpretable by humans. While it may produce accurate outputs, the reasoning behind those outputs is opaque, making it harder to verify, explain, or ensure fairness and compliance.

Without this, AI might recommend something inexplicable – and thus be ignored by decision makers. As Richard Marcus, AuditBoard's CISO, has noted, no matter how advanced AI becomes, there will always need

to be a human in the loop for material risk decisions. Transparency enables that human oversight.

3 Data Privacy and Security

Using AI often means aggregating large datasets, potentially including sensitive information.

Risk management AI might pull in HR data, financial data, etc. Strict controls are needed to ensure that in seeking risk insights you don't inadvertently violate privacy laws or create a honeypot for hackers.

Also, if using third-party AI services, assess the vendor carefully (the supply chain risk of AI).

Basically, follow your own risk management process for the AI usage itself.

4 Human Oversight and Governance

One should establish clear governance over AI usage in risk management.

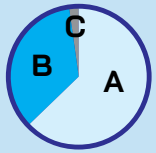
This might involve an AI ethics committee or at least documented policies about where AI is applied, how models are validated, and how often they are reviewed.

Human override mechanisms are essential – AI outputs should inform, not rigidly dictate, especially early on.

As Marcus warned, AI is both an opportunity and a risk – requiring human oversight and adherence to strong governance principles.

> *AI offers powerful opportunities for risk detection and decision support but also introduces new risks. Effective use requires human oversight, ethical safeguards, and strong governance to ensure responsible application.*

Nearly two-thirds of professionals in one survey stressed the need for human oversight in AI-driven decisions. In practice, this means risk managers should review AI findings, especially unexpected ones, and there should be protocols on what decisions can be fully automated vs. which require human sign-off.



Employee Trust Levels In AI

A Two of three people (63%) would trust A to inform - but not make - important decisions at work.

B Over a third (35%) wouldn't trust AI to make important decisions at work, preferring to use human intelligence.

C Just 1% of respondents would trust AI to make important work decisions.

5 Ethical Use

Beyond technical aspects, consider the broader ethics of how AI is deployed. If an AI risk model predicts something sensitive, like the risk of employee fraud or likelihood of a business partner's failure, treat the results with discretion to avoid unfair labelling.

Use AI to augment fairness (such as finding bias) not to secretly monitor in ways that breach trust.

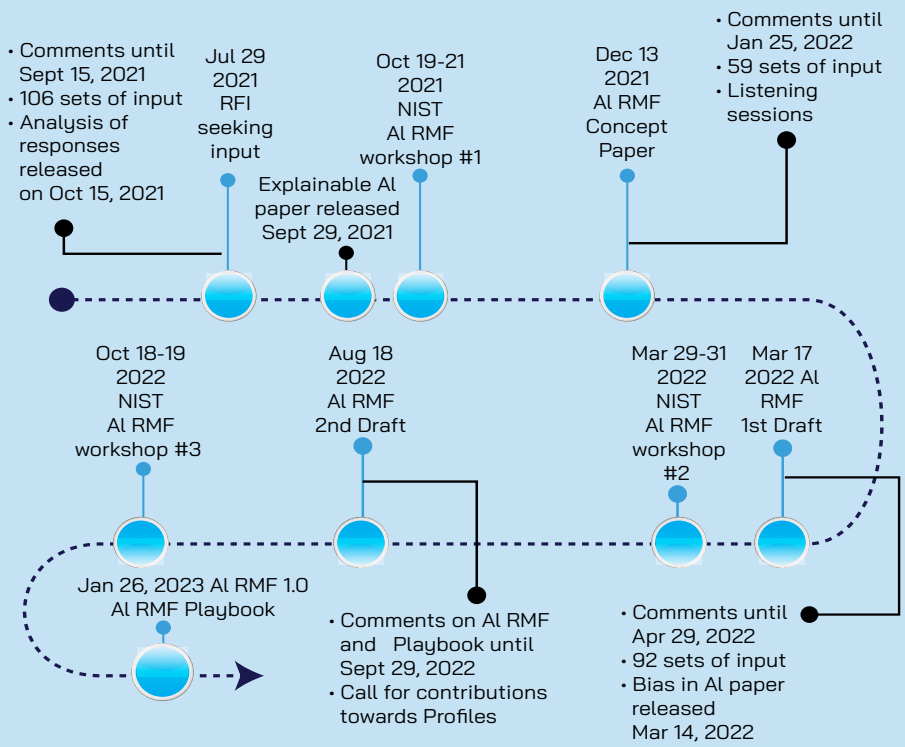
In some cases, being transparent with employees or customers that you use AI in risk processes can build trust – if you can explain it benefits them (like faster response or greater consistency).

Develop guidelines that align with your organisation's values and legal obligations.

Forward-looking risk leaders are already including AI risks in their risk registers.So, listing *"AI Model Risk"* – the risk that AI systems produce erroneous or biased outputs leading to bad decisions or regulatory penalties – and treating it like other operational risks that need controls (model validation procedures, etc.).

Frameworks like the EU's draft AI regulation or NIST's AI Risk Management Framework provide best practices which can be adopted. In summary, embracing AI in IRM should go hand-in-hand with strengthening your governance – essentially IRM for your AI. Those who do this will harness the upside of AI (huge efficiency and insight gains) while mitigating its potential downsides.

AI RFM Timline and Engagements



Other Emerging Technologies and Trends

Beyond AI and automation, several other technological trends are on the horizon of risk management:

1 Non-Human Identities and Identity Sprawl

As businesses automate, machine identities (like service accounts, bots, IoT devices) are exploding in number. These can be harder to track than human users, creating new security and compliance challenges.

Integrated risk management must extend identity governance to these non-human actors to prevent credential leakage or misuse.

So, ensuring a process bot only has access to what it truly needs and its credentials are rotated. Identity sprawl is a risk that lies at the intersection of IT security and operational process – IRM is needed to manage it holistically.

Definition

IDENTITY SPRAWL

The uncontrolled growth and spread of user accounts, credentials, and digital identities across multiple systems, applications, and environments — often without central oversight — increasing security risks and management complexity.

2 ESG Data Management

Emerging tools are using AI to help collect and assure ESG-related data (like carbon emissions, diversity metrics) which feed into risk assessments. However, this also introduces risk if that data is inaccurate or misused.

Risk teams will need to work with sustainability functions to ensure ESG data is integrated, accurate, and given appropriate weight in decisions. Moreover, stakeholders demand assurance on ESG – meaning IRM programs should incorporate ESG risk controls and monitoring (and the tech to do so). It's an evolving area of risk tech: expect more collabouration between IRM platforms and ESG reporting tools.

3 RegTech and Digital Regulation

Regulatory Technology (RegTech) is automating compliance tasks – like automatically updating a compliance control library when laws change, or digital submission of reports to regulators. Some IRM systems now offer regulatory mapping solutions that cross-link requirements to controls and can highlight gaps when regulations update. This reduces the manual burden of keeping up with ever-changing rules and can even provide early warning of regulatory non-compliance risk if, say, a new law is coming into effect and your controls aren't yet aligned. Embracing RegTech can make compliance risk management far more efficient and proactive.

> *Modern IRM platforms often include regulatory mapping tools that link requirements to specific controls, automatically flagging compliance gaps when regulations change.*

4 Blockchain for Transparency and Trust

Distributed ledger technology can provide immutable, transparent records that may be useful in risk management.

for instance

Critical control attestations or third-party audit certifications could be recorded on a blockchain, making them tamper-proof and instantly verifiable.

Critical control attestations or third-party audit certifications could be recorded on a blockchain, making them tamper-proof and instantly verifiable. Supply chain risk is a candidate – tracking provenance of products or compliance of suppliers on blockchain could reduce certain risks.

Smart contracts might automatically enforce compliance requirements (such as not releasing payment if a supplier's risk score falls below a threshold).

While a lot of blockchain hype has cooled, specific use cases like tamper-proof logs of risk assessments or automated insurance contracts (pay-out triggered by defined events) are gaining traction.

> *IRM leaders should monitor blockchain advancements, as the technology is already reshaping trust, transparency, and traceability in sectors like finance and supply chain management.*

IRM leaders should keep an eye on blockchain developments, especially in industries like finance or supply chain, as they could complement risk assurance processes by increasing trust and reducing manual verification.

Smart Contracts

Self-executing digital agreements stored on a blockchain, where the terms are written in code and automatically carried out when predefined conditions are met — without the need for intermediaries.

5 Quantum Computing Risks

Though still a few years out, quantum computing poses a dual risk: it can break current encryption (security risk) but also offers new computational power for risk analysis.

Forward-looking risk programs are inventorying their cryptographic assets and planning for post-quantum cryptography to ensure resilience when quantum attacks become feasible.

Post-Quantum Cryptography

Encryption methods built to withstand attacks from quantum computers, which use quantum mechanics to process information far faster than classical machines. Because quantum computers could break many current encryption systems, post-quantum algorithms are designed to keep data secure in a future where quantum capabilities are widespread.

At the same time, quantum algorithms might eventually allow massively complex risk simulations that today's computers can't handle – potentially a boon for scenario analysis.

Strategic risk management is starting to include quantum readiness – a good example of integrating technology horizon scanning into IRM to ensure long-term viability of controls.

6 Autonomous and Agentic Systems

As AI evolves towards agents that can act autonomously (automated trading bots, autonomous supply chain systems, etc.), they introduce novel risks.

IRM will need to expand to cover governance of AI decisions: ensuring autonomous agents follow policies and ethical guidelines, and having monitoring to catch when they deviate or cause unintended effects.

for instance

An algorithmic trader might pose systemic risk – IRM would call for controls like circuit breakers and oversight of algorithm changes. Integrated risk management will likely partner more with AI governance functions to cover these *"non-human decision-maker"* risks in operations. Transparency, accountability, and emergency intervention paths for AI will be a focus.

7 Cyber-Physical Convergence

Many industries are seeing IT and operational technology (OT) merge – factories, utilities, vehicles now all connected.

This means cyber risks can have physical consequences (and vice versa). Risk management is converging safety management and cybersecurity into a holistic view of operational resilience.

Operational Resilience

An organisation's ability to prepare for, respond to, and recover from disruptions — such as cyberattacks and system failures — while continuing to deliver critical services and protect its core functions.

IRM programs, especially in sectors like manufacturing, energy, transportation, will incorporate safety metrics, incident data, and environmental monitoring alongside traditional IT risk data.

Tools that were separate (like safety incident management vs. cyber incident management) might integrate.

The challenge is bridging cultures – safety engineers vs. CISOs – but IRM can provide a unifying framework to address cyber-physical risks in tandem.

As these trends unfold, it's important to remember that the core principles of IRM remain constant: break down silos, integrate processes and data, align risk with strategy, and nurture a culture that views risk as both challenge and opportunity.

New technology can augment IRM immensely, but it should be adopted with those principles in mind.

Organisations that anticipate these emerging technologies and build flexibility into their IRM programmes will be best positioned to thrive amid the changes to come.

Challenges and Pitfalls to Avoid

Examples from multiple industries show how IRM delivers faster decisions, cost savings, and reputational gains. We also identify common hurdles – from cultural resistance and data quality issues to talent gaps – with practical guidance for overcoming them.

While the benefits of integrated risk management are compelling, implementing IRM is not a trivial endeavour.

Organisations often underestimate the cultural and technical hurdles in breaking down long-standing silos and building unified risk processes.

In this section, we outline common challenges and pitfalls that companies face on the IRM journey, and offer insights on how to address them. Being forewarned of these potential issues can help you plan proactively and avoid derailment.

Organisational Resistance and Siloed Mindsets

People naturally resist change – especially if it threatens established domains or *"fiefdoms."* In siloed environments, risk, compliance, and audit teams may have enjoyed a degree of independence and control.

The move to IRM can trigger fears: "Will my expertise be devalued? Will another department dictate how I manage my risks?" There can also be simple inertia – *"we've always done it this way".*

Different departments might defend their own processes, thinking enterprise integration will slow them down or expose their issues. Overcoming this requires strong tone at the top and change management.

Clear communication is key: leadership should articulate the benefits of IRM not just for the company, but for individuals (less duplication, better support, career development in broader risk skills). Incentives should be realigned to encourage collabouration.

for instance

Shared objectives for risk reduction rather than siloed KPIs

Some organisations use cross-functional teams or rotations to break down the us-vs-them mentality.

> *Show personal benefits and recognise collabouration to build buy-in.*

It's vital to address the *"what's in it for me"* at the individual level, and to recognise and celebrate collabourative behaviour.

Leadership must also model cross-functional cooperation – if department heads remain territorial, their teams will follow suit. Patience is required; culture doesn't change overnight.

But persistence in messaging that integrated risk is a collective mission, plus demonstrating quick wins (like how sharing data prevented a problem), can gradually convert skeptics.

In short, treat cultural change as a project in itself, with executive sponsors actively engaged.

Data Quality and Fragmented Systems

Integrating risk data from disparate sources can reveal inconsistencies, gaps, and errors. Different silos may have different definitions (what one calls *"high risk"* another might call *"medium"*), or simply maintain data at different levels of granularity.

When trying to centralise, poor data quality can undermine trust in the whole IRM system. A common pitfall is rushing to implement a fancy tool without first addressing data governance.

The old adage *"garbage in, garbage out"* holds: if you feed the IRM platform with outdated or misaligned data, reports will be flawed, giving ammunition to naysayers to dismiss the effort. To avoid this, invest early in data cleansing and standardisation.

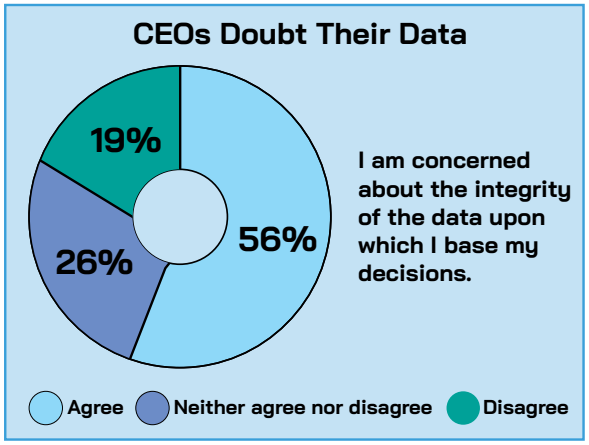
Establish who owns each type of risk data and make them accountable for its accuracy. Create a data dictionary for risk terms and ratings so everyone interprets things the same way.

Definition

DATA CLEANSING

The process of identifying and correcting errors, inconsistencies, or inaccuracies in datasets to improve their quality, reliability, and usability for analysis or decision-making.

You might need to run parallel systems for a short period to cross-validate data until confidence is built in the new single source. It's also wise to start integration with a subset of well-understood data to get quick wins (so start with operational risk events, then add others). Implementing access controls and data quality checks in the IRM system will help maintain integrity (requiring certain fields, using drop-downs to enforce consistent categories, etc.).



Poor data can lead to mistrust in analytics and decisions – one survey found many executives don't fully trust risk reports due to perceived data issues. So, addressing this challenge head-on is crucial. Dedicate part of your IRM project to data governance: define processes to regularly review and reconcile data differences and ensure ongoing quality.

Technology Complexity and Integration Woes

Deploying an IRM platform (or any enterprise system) can be complex. Integrating multiple systems – ERPs, IT ticketing, incident databases – might require more effort than anticipated, especially if you have many legacy systems or a lack of APIs. A pitfall is underestimating the IT resources needed for implementation and integration. If poorly planned, an implementation can disrupt operations or lead to user frustration *("the new risk system is too slow" or "I can't find my data now")*.

> *Before deploying integrations, test them in a staging environment to identify and fix issues without risking disruption to live systems.*

Another issue is over-engineering: trying to configure the tool to cover every exception from day one, which can delay and complicate deployment. To avoid these, **ensure you allocate sufficient technical support** (in-house or external) and adopt an incremental rollout. Perhaps roll out core modules first, then add bells and whistles.

Test integrations in a staging environment to iron out kinks before going live. Also, involve end-users in user acceptance testing to catch usability issues early.

Another approach is to phase by department – onboard one or two departments on the system fully, learn and adjust, then bring others (this manages complexity and shows success to others). If using cloud solutions, ensure your network and security teams are involved to address any connectivity or security reviews needed (often a slow point if not addressed upfront).

And keep training in mind: a common tech pitfall is assuming if you build it, they will use it. If users find the system cumbersome or don't understand it, they'll revert to spreadsheets. Thus invest in a good UX, simplify where possible (do you really need 10-point risk scoring or can 5-point suffice?), and provide training and support during the transition.

In summary, manage the IRM tech project with rigor – project management, stakeholder involvement, clear milestones – to avoid a scenario where a botched implementation becomes an excuse to abandon IRM (sadly it happens).

Smooth tech implementation will accelerate adoption; stumbling will set you back organisationally.

Talent and Skills Gaps

An integrated approach often requires new skills that siloed teams may lack. Data analysis skills become more important when dealing with large integrated datasets and AI tools. Risk teams may need deeper understanding of IT, or IT risk folks may need training in business process analysis. Many organisations find they lack certain expertise.

for instance

Not enough data scientists to support risk analytics, or not enough people who understand both cybersecurity and business continuity to connect those dots.

Additionally, mid-career risk professionals may be set in siloed ways and need upskilling to adopt IRM practices. This challenge can be addressed by a combination of training, hiring, and cross-pollination.

Invest in training your existing staff on new tools and integrated methodologies. Encourage or mandate professional development *(certifications like CRISC, etc., which emphasise integration)*. Consider hiring specialists or consultants for areas like data analytics or specific regulations as a bridge while you upskill internal teams. Another strategy to promote cross-functional understanding is rotating staff or creating joint teams, such as having IT risk members work with operational risk teams to share expertise and perspectives.

> *Use rotations or joint teams to share risk knowledge.*

Partnering with external bodies, like universities or professional associations, can help develop a pipeline of talent – like sponsoring a research project on AI in risk that involves your staff with academic experts. It's also worth noting that integrated risk management itself can be an attractive feature to recruit talent – it signals a modern approach, which especially younger professionals find appealing (they often don't want to work in narrow silos). The key is to recognise talent as a pillar of IRM success; a great system is useless without people who know how to interpret and act on its outputs. So budget and plan for people development as part of your IRM programme.

Regulatory Fragmentation

For multinational organisations, aligning an integrated risk programme with inconsistent regulatory requirements across jurisdictions can be daunting. What's considered an acceptable risk in one country might be forbidden in another due to stricter laws. One pitfall is trying to make one unified system fit all without accommodating local nuances, leading to either compliance gaps or inefficiencies (over-controls in some places). The solution often lies in a core-and-flexible framework: establish a central risk framework mapping to major global standards (like ISO 31000 or COSO) for consistency, but allow local addenda for specific regulatory needs.

for instance

Have a core control set and then country-specific controls where needed. Use the IRM platform's ability to map multiple frameworks – i.e. link one core control to multiple regulatory requirements, and if a country has an extra requirement, add a control mapped only to that.

It's a kind of mapping layer approach. Also, maintain a dialogue between central risk function and local compliance officers to update each other – perhaps include local reps in the design of the programme so they buy in and see that local needs are respected. In some cases, technology can help by filtering dashboards so each locale sees the view relevant to them while feeding data to the central repository.

> *Harmonise processes but keep sub-programmes where needed for compliance.*

Overall, harmonisation is the aim but not at the expense of compliance; pragmatically,

you might be running sub-programmes within an overall IRM to satisfy outliers. The pitfall to avoid is either extreme: total fragmentation (separate programmes per country, defeating IRM) or rigid uniformity (ignoring key differences, risking violations). Aim for a hybrid – a core integrated approach with 'bolt-ons' for local specifics.

Vendor Lock-in and Technology Over-Reliance

On the technology front, one risk is becoming too dependent on a single vendor or system, especially if it's not easily interoperable. If you choose an IRM platform that doesn't allow easy data export or integration, you might find yourself stuck if the vendor's direction doesn't align with your needs or costs escalate.

To mitigate this, evaluate openness *(as noted in the vendor section)* and maintain backups of critical data outside the system periodically.

Also, watch out for over-reliance on technology as a panacea – IRM is not solved by software alone.

If people start trusting the system outputs blindly without critical thinking, or conversely blame the system for issues rather than addressing process root causes, the true risk management culture might suffer.

Ensure that the introduction of automation doesn't lead to a false sense of security or set and forget mentality.

> *Continually test and validate automated risk indicators and models to ensure they remain accurate, relevant, and aligned with current business conditions.*

Regularly test and validate that the automated risk indicators and models are working as intended. As with autopilot in aviation, human oversight remains crucial.

This is more of a subtle pitfall – the idea that because you have a flashy risk dashboard, you think you're fully managing risk. It's important to continuously engage risk owners and not let the system 'run on autopilot' without active management.

Addressing these challenges requires planning, resources, and often a change in mindset. Planning and patience are particularly important – IRM is a multi-year journey, not a one-quarter project. Stakeholder engagement is continuous; you must keep demonstrating wins and listening to concerns. Organisations that succeed with IRM focus on culture as much as technology. They put effort into creating a sense of shared purpose (*"we are all risk managers in our areas"*), invest in people via training and clear roles, and recognise that integration is an evolving journey, requiring continuous learning and adaptation, rather than a one-off rollout.

Those who neglect these human and organisational aspects often find that after initial fanfare, teams slip back into old siloed habits (especially if a big incident occurs and blame games ensue). One more note: sometimes failure can come from trying to do too much too fast – leading to initiative fatigue. It's often better to get a few things integrated well (and celebrate that) than to attempt full integration and end up with disillusionment.

Case studies of IRM failures often cite lack of change management and leadership support as root causes – example, a company tried to implement an enterprise risk system without aligning it to decision-making processes, so it became a checkbox exercise and was eventually abandoned, leaving them effectively back in silos.

> *Overloading teams with rapid, large-scale changes can lead to initiative fatigue and undermine adoption; so pace implementation to maintain engagement and momentum.*

Avoiding pitfalls thus also means ensuring IRM is embedded into core management routines (strategy planning, budgeting, etc.), not treated as a parallel compliance task. In closing off this section, being forewarned of these challenges means you can craft your IRM roadmap and execution plan to mitigate them. Every challenge has solutions as discussed – they require intention and effort, but none are insurmountable. Many organisations have navigated them successfully by learning from others and being proactive.

Final Thoughts: Integrated Risk Management Equals Enterprise Resilience

We bring together the key insights from this report, highlighting the shift from siloed GRC to integrated risk management, the drivers behind adoption, and the practical steps organisations can take to build resilience. And close it all off with expert perspectives and a forward-looking view of IRM as a strategic capability.

In today's dynamic and uncertain environment, one thing is increasingly clear: organisations cannot achieve true resilience by operating in silos. The traditional fragmented approach to risk – each department looking out for its own narrow slice – leaves companies flat-footed in the face of complex, cross-cutting threats.

Whether it's a cyber-attack with business-wide implications, a pandemic disrupting every facet of operations, or a rapid regulatory shift altering the market landscape, the challenges of the modern world do not confine themselves neatly to departmental boundaries.

Therefore, the only sustainable way forward is to integrate risk management into the very fabric of how the business operates.

Integrated Risk Management builds upon the foundations of GRC but takes them further, extending across silos and embedding risk awareness into decision-making at all levels. It connects risk data, processes, and culture so that enterprises can anticipate threats, respond swiftly, and even seize opportunities that a less risk-aware organisation might miss. When done well, IRM turns risk management from a reactive cost-centre activity into a proactive capability that underpins strategic success and innovation.

Key Statistics

77%
of companies faced unexpected operational hallenges in the last 5 years

75%
of executives anticipate major shifts in their organization's business continuity planning and crisis management strategies

$32.06 billion
is the projected size of the global risk management market by 2033

A well-designed IRM programme – supported by the right technology, guided by a clear roadmap, informed by expert insights, and fuelled by a risk-aware culture – equips leaders to navigate uncertainty with confidence and clarity.

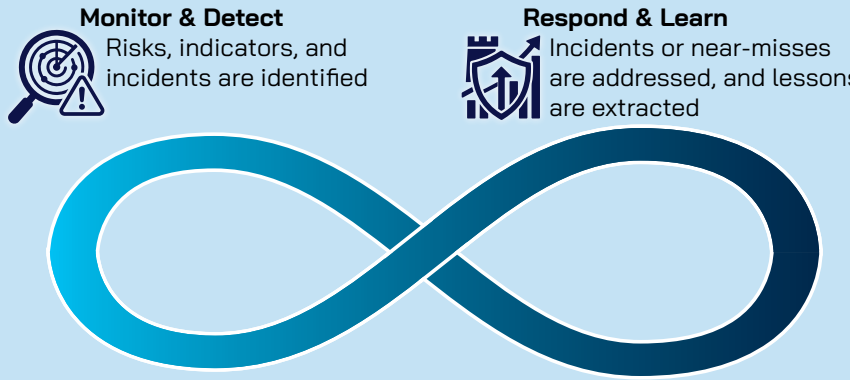
It provides that unified view from the cockpit, as opposed to siloed portholes. It means fewer surprises, and more agility when the unexpected occurs.

By moving beyond fragmented risk management and embracing integration, organisations position themselves not just to survive in an increasingly complex world, but to thrive in it.

> *IRM is a journey, not a destination.*

We have seen throughout this paper that those who have adopted IRM report faster decision cycles, better resource prioritisation, improved compliance posture, and often a competitive edge in responsiveness and stakeholder trust. In contrast, those clinging to siloed approaches often learn their lesson through costly failures or near-misses.

An Ongoing Journey of Resilience and Learning



It's worth emphasising that IRM is a journey, not a destination. Enterprise resilience is not a one-time achievement but an ongoing state to be maintained.

Risks will continue to evolve – new technologies, new business models, and new uncertainties will arise. An integrated risk approach gives you the flexibility to adapt your risk governance to whatever comes next.

It institutionalises a learning mindset: each incident, each *"close call"*, becomes a source of improvement for the whole organisation, not just one silo.

Finally, while we've focused on process and technology, remember that success in IRM comes down to people and mindset.

Encouraging a culture where information is shared, not hoarded; where risk is seen as everyone's business rather than *"someone else's problem"*; and where transparency and trust are the norm – that cultural foundation will carry your risk management through any storm. It enables IRM to flourish beyond the pages of policy into daily decisions.

In closing, Integrated Risk Management is more than a framework or system – it's a philosophy of running a resilient, principled business.

It aligns with the idea of principled performance: achieving objectives while upholding strong governance and preparedness for both threats and opportunities. In a world that shows us repeatedly that the only constant is change, IRM is essentially about building nervous system for the organisation – sensing, communicating, and responding to stimuli effectively.

As you move forward with strengthening your IRM capabilities, keep the end goal in sight: to create an organisation that not only protects value in the face of risks, but also creates value by being able to take risks confidently. Integrated risk management is a means to that end – a more intelligent, cohesive way of steering the enterprise.

With the insights, strategies, and examples discussed, we hope you are well-equipped to advance your IRM journey and, in doing so, secure a resilient future for your enterprise.

AuditBoard's Take:

IRM in 2025 at a Glance

As enterprises push beyond siloed GRC, AuditBoard points to five realities shaping the path forward. These insights echo the challenges and opportunities we've explored in this report, while sharpening the focus on what matters most for leaders in 2025:

What's being prioritised

Organisations are racing to connect the risk dots into a single picture while preparing for emerging risks like AI, data sovereignty, and geopolitical volatility.

Where firms still struggle

The three lines of defence remain fragmented, and many boards hesitate to fund IRM capabilities until after an incident — leaving gaps in accountability and sponsorship.

How technology helps

Automation and connected platforms reduce manual effort, centralise risk data, and tie insights directly to strategic objectives. They also enable forward-looking modelling and *"what if"* planning.

Underserved domains

Most domains — from third-party and ESG to IT and compliance — are under-managed when risks stay siloed. IRM closes these gaps by treating risk as an interconnected whole.

Winning buy-in

Demonstrating ROI — efficiency gains, avoided costs, and stronger decisions — is the most effective way to secure executive support and embed IRM as a driver of resilience.