PROTECHT

E-BOOK

Risk in motion: A guide to connected, continuous risk management.

How to build a dynamic governance, risk and compliance system program that enables you to stay ahead of risk.

Executive summary

Risk doesn't stand still; neither should your risk management

When not designed or implemented well, risk management tends towards the reactive. Annual reviews, disconnected data, and static reports look backwards at yesterday's picture while tomorrow's threats emerge unseen. That's not good enough any more, especially in a world of accelerating cyber risks, evolving compliance demands, and strategic uncertainty.

Risk in motion changes the game.

This eBook introduces a bold but practical approach to risk: one that's dynamic, integrated, and always moving. It's a blueprint for building a governance, risk, and compliance (GRC) program that connects people, processes, and data in real time, so you can see risk before the incident, not just explain it afterward.

What's inside:

- **A new mindset:** Why risk is a continuous, connected force and how treating it that way boosts visibility, agility, and confidence.
- **A proven model:** Six core processes – RCSAs, metrics, incidents, assurance, actions, and compliance – reflected in a single, intelligent approach.
- **Real-world outcomes:** From fewer audit surprises to better board reporting, discover how dynamic ERM translates into strategic advantage.
- **Dashboards that drive action:** Not just scorecards, but tools that spotlight weak signals, surface insights, and track engagement across the business.
- **Your path forward:** Whether you're starting from spreadsheets or upgrading from legacy tools, risk in motion meets you where you are and grows with you.

This is more than a GRC refresh. It's a shift from compliance-focused box-ticking to a live, operationally embedded risk capability that empowers every part of your business.

You don't need to be perfect. You just need to get started.

Risk appetite in motion.

Risk appetite is the amount and type of risk your organisation is willing to accept in pursuit of its objectives. It's at the heart of the risk in motion concept.

It defines the boundaries for decision-making: balancing opportunity and exposure, ambition and prudence. A clearly articulated risk appetite helps ensure consistency: between strategy and execution, between business units, and across risk types.

But appetite alone isn't enough. It must be actively monitored, clearly communicated, and continuously evaluated as your environment changes. That's where risk in motion adds real power, by turning static statements into dynamic guardrails, embedded in every risk process, from assessments to action tracking.

PROTECHT

Contents

1 The case for change

Enterprise risk management (ERM) should be your strategic radar – scanning for threats, mapping vulnerabilities, and guiding informed decisions. Instead, in too many financial institutions, it functions more like a rearview mirror: static, delayed, and focused on what's already happened.

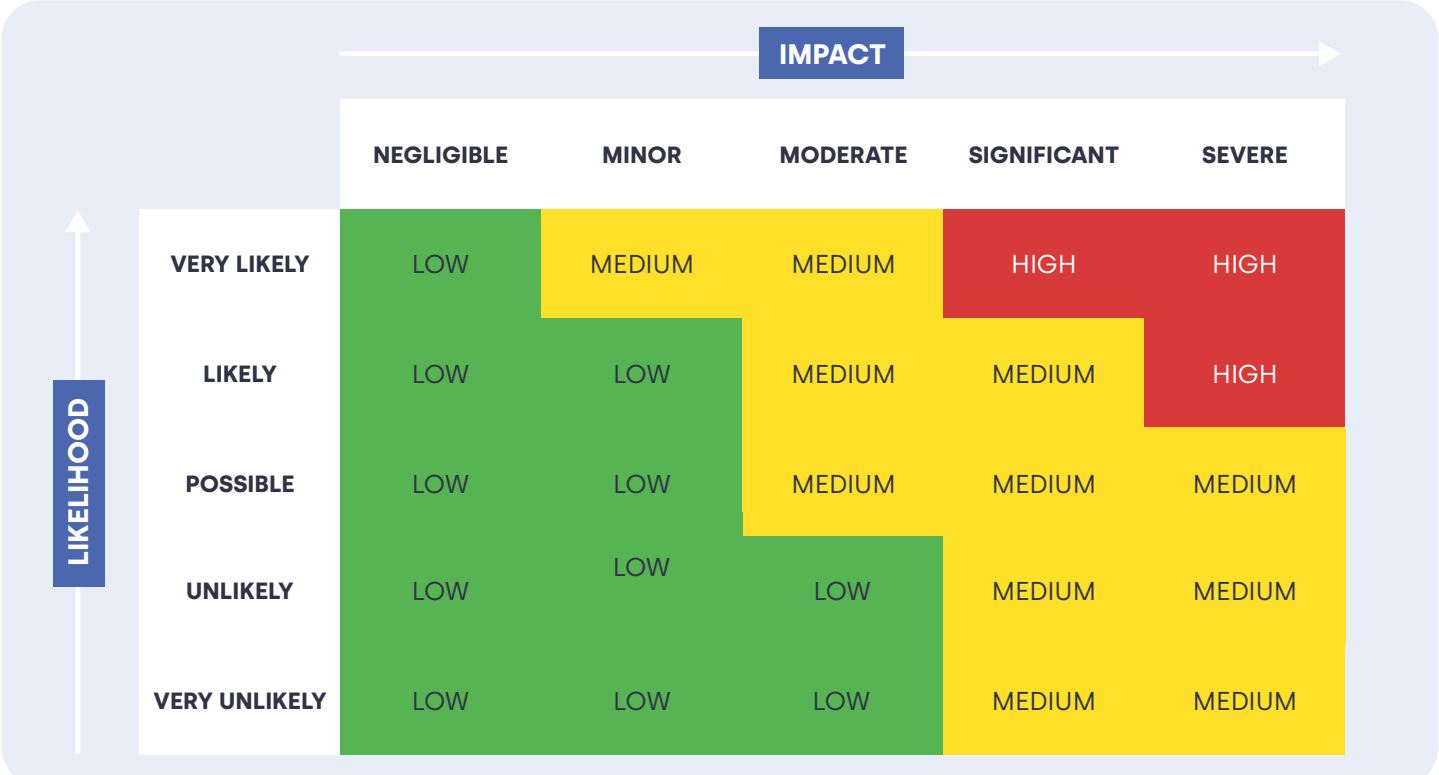
Why are traditional approaches falling short?
Because risk doesn't stand still, and neither should your ERM.

The problem with static risk programs: Heatmaps alone aren't enough

Today, many risk teams still rely on:

- Annual risk and control self-assessments (RCSAs) that can't keep up with evolving threats
- Spreadsheet-based risk registers prone to error, duplication, and oversight
- Siloed systems where cyber, compliance, vendor, and strategic risk are managed separately, each with its own language, controls, and priorities – where the patterns and insights are missed due to program separation and data silos

The result? Risk gets captured but not connected. Tracked but not trusted. And decisions are made based on snapshots of yesterday, not signals from today, like the old static 5x5 risk matrix.



Traditional enterprise risk management (ERM) involves periodic risk assessments based on data gathered over a set period of time and delivered in a matter of days or weeks. It is often presented in a simple grid format, such as the example above.

These legacy risk reporting models have inherent flaws that limit their effectiveness:

Backward-looking

Based on historical risk data and often out-of-date by delivery

Unreliable and inefficient

Managing risk data on spreadsheets or within siloed systems is time-consuming and prone to errors

Disconnected

Only showing one aspect of a given risk and not aligned to standard risk frameworks

The black hole of risk management

You might have a really strong risk culture in your first line, but if the visibility isn't there across lines, that insight disappears into what we call the Black Hole of Risk Management.

This "black hole" is where risk insights go to die. Teams collect data – risk assessments, incidents, audit findings – but they don't talk to each other, and their risk programs fail to provide insights. Each operates in a vacuum.

For example:

- An audit uncovers control failures, but they're not mapped to operational risks
- A compliance obligation is breached, but the root cause doesn't feed into the next RCSA
- A near-miss incident flags a weak control, but it's filed away without action

And when reports are finally generated, they're often incomplete, outdated, or disconnected.

What can go wrong in static risk management

Lack of visibility across lines	Isolated risk domains	Disconnected reporting
Out-of-date information	Incomplete information	Lack of agility

The real cost of siloed risk management

Siloed ERM isn't just inefficient, it's risky. Research shows:

- Organisations with integrated ERM[1] programs see a 14% increase in value compared to those with fragmented approaches
- 61% of companies managing risk in silos[2] experienced a data breach, compared to 30% of those using integrated and automated solutions
- During COVID-19, insurers with strong ERM[3] programs absorbed 32% more of the financial impact on return on equity than those without

Risk management isn't a cost centre. When it's done right, it's a value multiplier.

Scenario: Where the program fails

Imagine a financial institution with a siloed ERM approach:

- RCSAs are done annually, and the last one didn't account for a growing dependency on a cloud provider because vendor products and services were not connected to business functions and processes.
- A vendor failure triggers an outage, but the incident isn't linked to the original risk register entry.
- Compliance raises concerns after the fact, but without integration, there's no audit trail of controls or mitigations.

This isn't a hypothetical. It's the status quo for many risk teams, and exactly what risk in motion is designed to fix.

Why now?

Three key forces are converging to make static ERM untenable:

1. Regulators expect organisations to demonstrate real-time compliance posture and control effectiveness.
2. Boards and executives demand timely, actionable insights that support forward-looking strategic decisions.
3. The risk landscape is shifting faster – cyberattacks, geopolitical threats, AI risks, supply chain disruptions – none of which wait for your next quarterly update.

> *"Risk management that operates in silos is not just inefficient – it actively limits your ability to protect and grow your business."* – ***David Bergmark, CEO, Protecht***

[1] *"The effect of enterprise risk management on firm value"*, Phan, Dang, Nguyen, Ngo, Hoang (2020) – link
[2] *"The Detrimental Impact of Data Silos"*, Hyperproof (2024) – link
[3] *"Does Enterprise Risk Management Enhance Insurers' Resilience?"*, SOA Research Institute (2024) – link

2 From silos to synergy: What risk in motion means

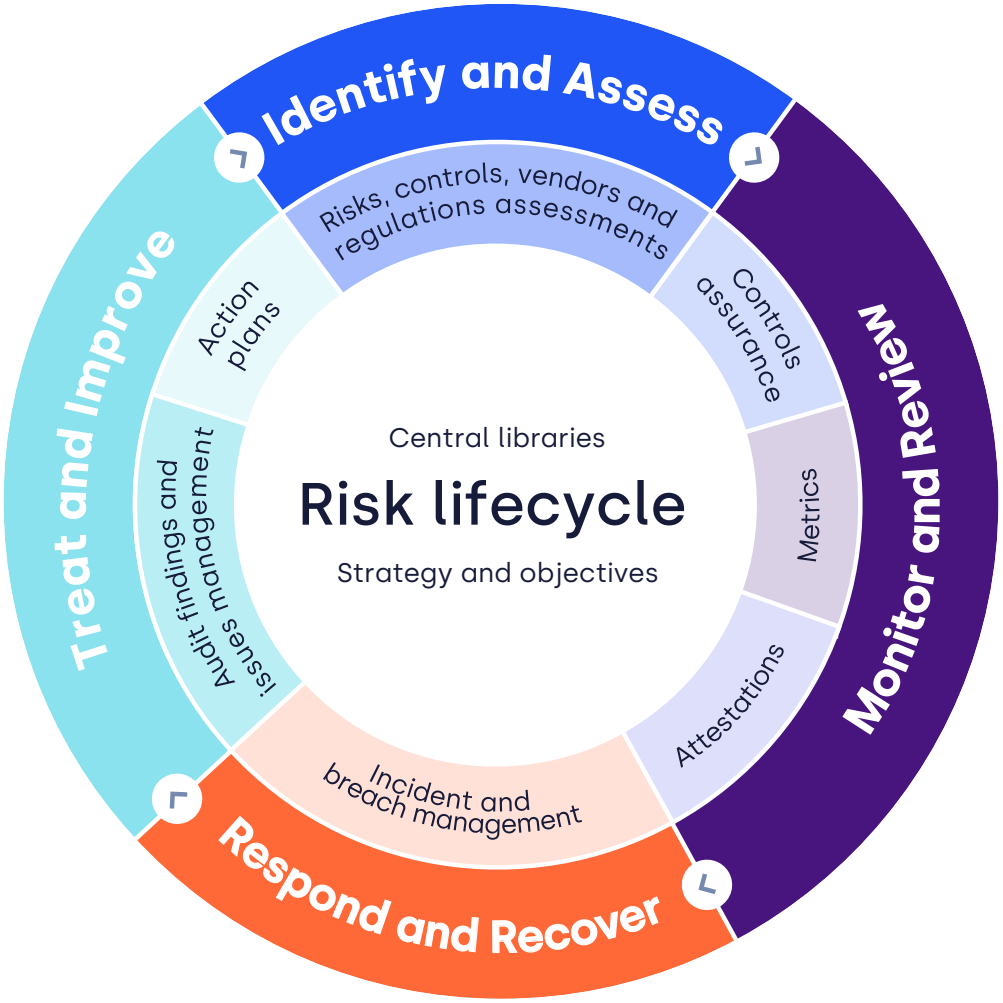
Modern risk isn't static. It's accelerating, overlapping, and shifting across every part of your business. Yet most risk management frameworks still operate as if nothing's changed: isolated systems, periodic check-ins, and blind spots everywhere.

Risk in motion changes that.

It's more than a catchy phrase. It's a fundamental rethinking of what enterprise risk management can – and should – be in today's environment. It's a model that sees risk as a constantly evolving force, and aligns your people, systems, and data to meet it in motion.

The risk in motion lifecycle

At the heart of this approach is a dynamic lifecycle model that connects risk processes across the organisation. Every component – risks, controls, incidents, metrics, obligations, actions – is captured, linked, and updated in real time.



Think of it like a living ecosystem:

- **Identify and assess:** Risks are captured and assessed against strategic and operational objectives
- **Monitor and review:** Key risk indicators (KRIs), metrics, and attestations track early signals of change. controls are tested
- **Respond and recover:** Incidents are flagged, and findings drive action in a resilient progression
- **Treat and improve:** Issues are investigated, plans are created, and lessons learned feed back into the system.

From silos to a single program

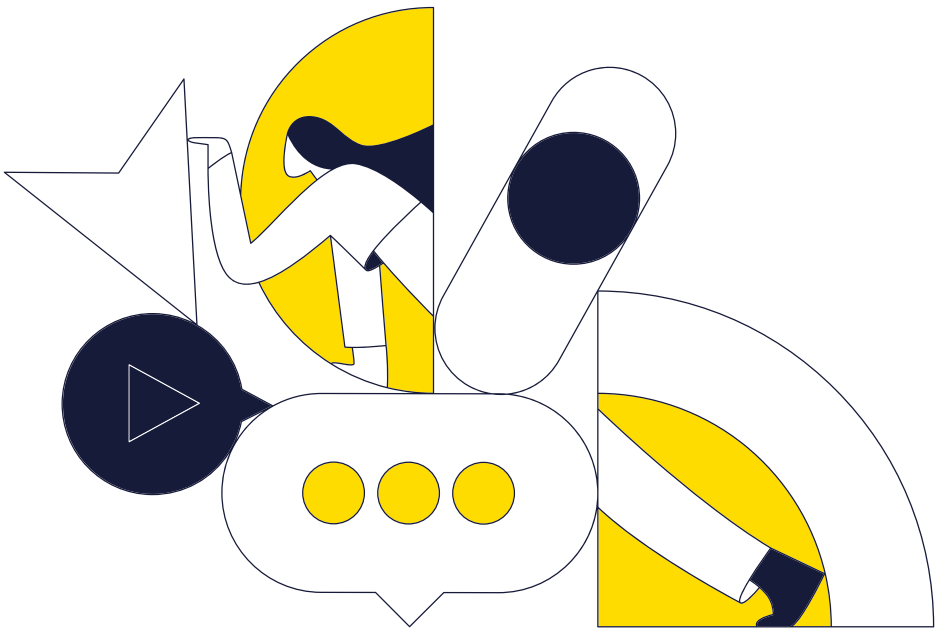
In traditional ERM, every risk domain often runs its own program of disparate and disconnected processes, data, and reporting:

- Cyber risk lives in its own GRC platform.
- Vendor assessments happen in spreadsheets.
- Compliance checklists float in email inboxes.
- Risk owners track actions manually, if at all.

Risk in motion brings them together.

With a consistent set of processes, a common taxonomy, and shared workflows, all risk types – strategic, cyber, operational, third-party, compliance – are managed within the same solution. This doesn't mean one-size-fits-all. It means one foundation, many applications.

"Risk is always in motion. It's just a matter of whether or not it hits you. If you're not seeing it coming, you're already behind."
– Terence Lee, VP North America, Protecht



Why consistency matters

When every department uses the same risk taxonomy and frameworks for assessing, reporting, and acting on risk, three things happen:

1. **You see the full picture**

   Cross-functional linkages expose systemic risks that might otherwise lie in obscurity until they escalate into an incident.

2. **You reduce duplication**

   Actions aren't repeated across business units. Controls are built once, then shared.

3. **You respond faster**

   Alerts and insights flow through connected dashboards – helping you see emerging threats before they escalate.

Specialisation still has a place

Let's be clear: risk in motion doesn't mean flattening every nuance of risk management. Cyber threats require different metrics than regulatory obligations. A breach incident isn't treated the same way as financial underperformance.

But the gears that drive each are the same:

RCSAs. KRIs. Controls. Incidents. Assurance. Actions. Compliance.

With risk in motion, those gears turn in concert, powered by the same system, using the same language, producing insights that leadership can trust.

As one Protecht customer put it, "We used to chase risk around the business. Now we see it coming."

Why this matters to the board:

In 2023, U.S. Bank was fined $15 million by the Office of the Comptroller of the Currency for failures in its internal processes and consumer protections. The underlying issue? Processes were fragmented across departments, leading to inconsistent customer treatment, delayed issue remediation, and a lack of enterprise-wide visibility into critical risks[4].

Protecht's risk in motion approach helps CROs prevent these types of failures before regulators or headlines get involved. By unifying data from risk assessments, incidents, controls, audit findings, and obligations into a single connected view, risk in motion enables earlier action and more credible assurance.

The result? A unified, enterprise-wide risk posture that evolves with your business.

[4] https://www.occ.gov/news-issuances/news-releases/2023/nr-occ-2023-141.html

Enabling strategic agility

Risk in motion isn't just about visibility – it's about movement. It allows your institution to adapt faster, align risk with strategy, and make confident decisions with real-time context.

It enables:

- Risk-based prioritization of resources
- Scenario planning grounded in live data
- Governance reporting that drives action, not just awareness

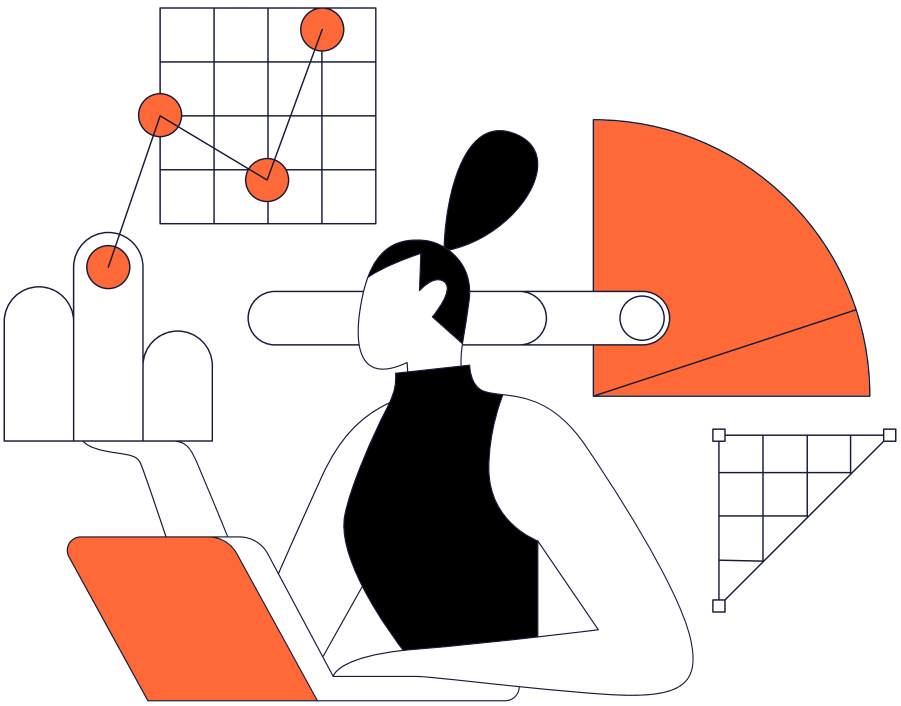
More directly, risk in motion supports the outcomes that boards and regulators care most about:

- **Risk appetite alignment:** Know in real time which risks are operating outside tolerance thresholds, and where intervention is needed
- **Control rationalisation:** Eliminate redundant or ineffective controls by linking assurance outcomes directly to risk appetite and performance
- **Real-time assurance:** Move beyond point-in-time reviews. Show auditors and senior management how your risk profile is changing as it happens

Risk in motion gives CROs and CCOs the tools to demonstrate not just what they know, but how they're acting on it. The result is a more agile, proactive, and strategic risk function, ready for the next exam, the next disruption, and the next decision.

In short, it helps risk professionals move from guardians of compliance to enablers of strategy.

Next, we'll look under the hood of the risk in motion engine: six interlocking processes that transform risk data into clarity, accountability, and resilience.



3 Inside the engine: The six processes of risk in motion

If Chapter 2 was about why risk in motion matters, Chapter 3 is about how it works. At the centre of risk in motion is a tightly connected engine – six core processes that transform risk data into decisions, actions, and outcomes. Each one plays a distinct role. But it's their integration that creates the real power: a system that moves in step with your business.

01. RCSAs	02. Risk metrics and KRIs
03. Incident management	04. Controls assurance
05. Issues and actions	06. Compliance management

Let's break them down.

The six processes

1. RCSAs

The starting point for most risk processes, RCSAs identify your key risks and evaluate the design and performance of the controls in place to manage them. In too many organisations, this is still a spreadsheet exercise completed once a year and left to gather dust.

Risk in motion changes that. RCSAs become continuous and contextual, grounded in business objectives, and updated as those objectives shift. Each risk and control is linked to your central taxonomy. Assessments aren't just stored, they're connected to actions, metrics, controls, and more.

Doing a risk assessment once a year and filing it away is like looking in the rearview mirror while riding a motorbike. Risk in motion gives you a dashboard you can use while riding.

2. Risk metrics and KRIs

Risk metrics are the early warning system of your ERM program. In risk in motion, key risk indicators (KRIs) are collected and monitored frequently, often in real-time. When thresholds are exceeded, the system signals concern and managers can act.

KRIs bring objectivity to risk. They validate (or contradict) what your risk assessments are telling you. Over time, they build trend data. They help highlight false confidence in controls. And because they're linked to your central risk records, they contribute directly to the dynamic risk profile.

3. Incident and near-miss management

If risk is the possibility of something going wrong, incidents are when it actually does. Risk in motion treats incident data as core to the risk lifecycle, not a peripheral function.

Incidents are categorised consistently with your risk taxonomy and tied back to risk events. So are near misses: the events that could have had impact but didn't. These are some of your richest sources of insight, helping you identify patterns, test controls, and prevent recurrence.

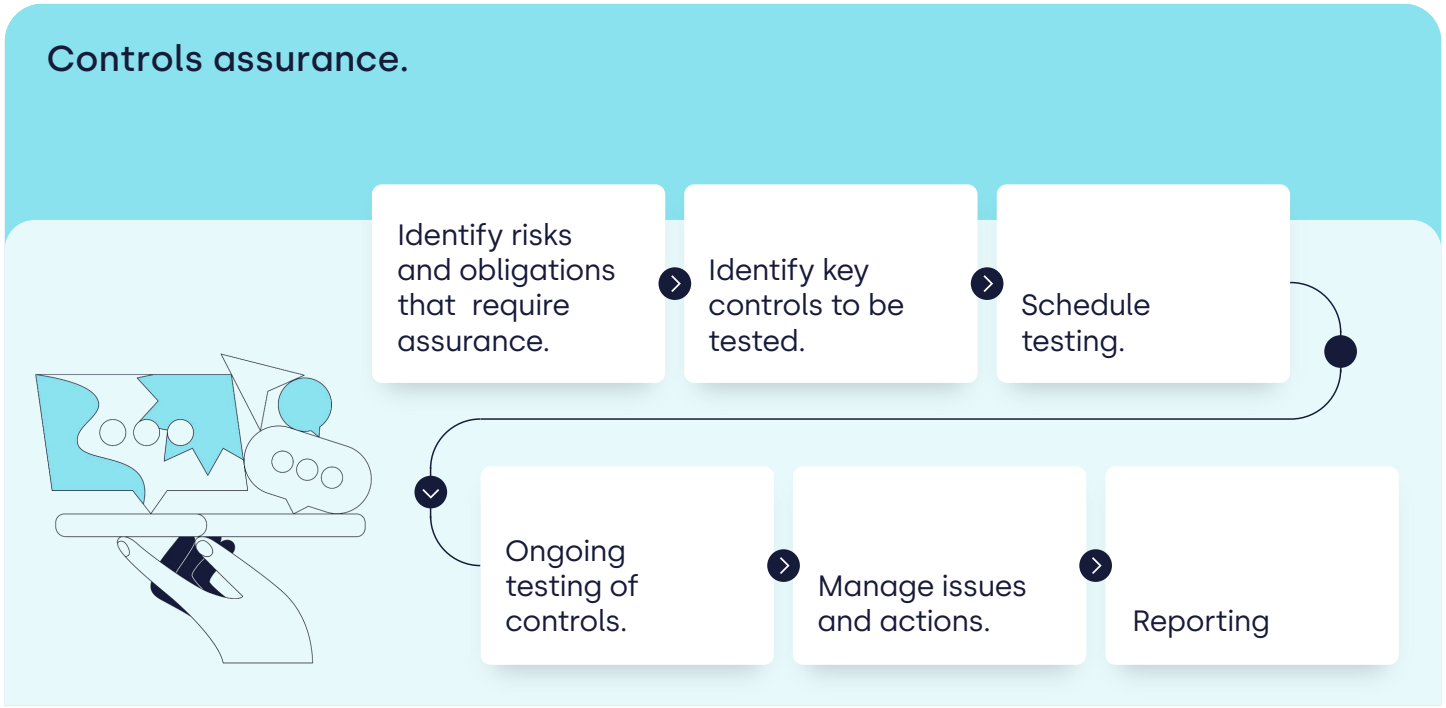
If you're ignoring near misses, you're ignoring the smoke just before the fire.

4. Controls assurance

It's not enough to have controls in place. You need to know if they're working. That's what controls assurance delivers: structured, ongoing testing of your controls' effectiveness.

Risk in motion incorporates formal testing, attestations, and automation to evaluate control performance. Failures trigger issues and actions. Passes build confidence. All results are aggregated to inform your residual risk assessments and reflected in real time on the dashboard.

Good controls don't slow you down. They let the business go faster, with confidence.



5. Issues and actions

When something needs to be fixed, it shouldn't fall through the cracks. Risk in motion helps you to make sure that it doesn't.

Issues can originate from anywhere: failed controls, overdue KRIs, audit findings, incident investigations. Each issue is logged, linked to a risk, and assigned clear actions with deadlines. You can track them across business units and spot duplication, bottlenecks, or systemic gaps.

Effectively, you're organising your risk program like a to-do list with accountability built in.

6. Compliance management and attestations

Compliance is no longer separate from risk. In risk in motion, obligations are mapped directly to risks, controls, and policies. Attestations are used to confirm compliance, validate controls, or test awareness.

When compliance breaches occur, they're captured as incidents. When requirements change, related risks are flagged. This is end-to-end compliance management, built into the daily rhythm of risk.

Reporting

Finally, everything you capture, assess, monitor, and treat needs to be translated into insights.

From board-level risk reports to compliance heatmaps to real-time team dashboards, reporting in risk in motion is designed to inform and activate – not just tick boxes.

Because data means nothing if it doesn't drive better decisions.

Why integration matters

These six processes are common across most risk frameworks. What's different here is how they *talk to each other*.

A failed control automatically links to an issue.

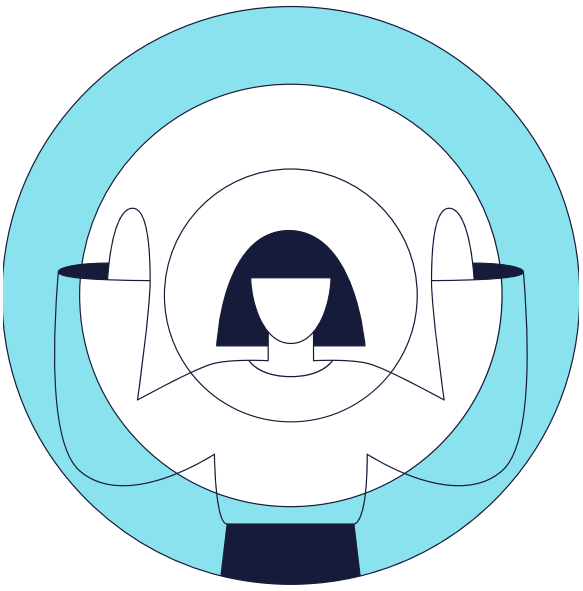
That issue generates actions with owners and deadlines.

The resulting assurance feeds back into the register.

Everything is connected – across teams, domains, and workflows.

This is how risk in motion turns information into momentum.

So how do you bring all this to life in your organisation? Next, we'll explore how to operationalise risk in motion – mapping it to your risk program, aligning stakeholders, and choosing the right tools and workflows to drive adoption. Because the model only works when people use it.



4 Making it real: Operationalising risk in motion

By now, the engine should feel familiar: six interconnected processes that drive continuous, intelligent risk management.

But an engine doesn't run unless it's installed – and fuelled by people, systems, and workflows that keep it in motion.

This chapter is about putting risk in motion to work in your organisation. Turning concept into capability. Framework into function.

Let's break down what that looks like.

Map the model to your environment

Risk in motion isn't a one-size-fits-all formula. It's a flexible blueprint. To make it work, you need to anchor it in your own context.

- **Start with what you have.** Most organisations already have registers, assessments, monitoring activities, and reports in some form. Use them as a foundation.
- **Map existing practices to the six processes.** Where are the gaps? Where is duplication happening? Where are handoffs breaking down?
- **Design for flow.** Think beyond functions: design your processes so that risk moves from identification to action without stalling.

If you don't understand your processes, how can you understand the risks to those processes?

The goal isn't to rip and replace. It's to evolve what you already do into a more connected, more responsive system.

Align the right people

No risk engine runs on tech alone. People are the drivers.

- **Clarify roles.** Who owns risk identification? Who runs control testing? Who responds to issues? Make responsibilities visible and shared.
- **Empower the front line.** Risk in motion depends on real-time data. That means giving the business – not just risk teams – the tools to log, monitor, and respond.
- **Secure leadership buy-in.** Show executives how risk insights feed decision-making. Turn reports into conversations that matter.

When everyone understands their role in the risk ecosystem, motion becomes second nature.

Choose GRC tools that drive momentum

Technology should support risk in motion – not get in the way.

Look for systems that:

- **Connect the dots.** Risk, compliance, audit, cyber, ESG: your tools should unify these, not silo them.
- **Enable automation.** Automated alerts, workflow routing, and data syncs keep things moving without manual effort.
- **Support collaboration.** Risk doesn't sit in a single team. Your system should make it easy for multiple users, across departments, to engage and contribute.

You're not just choosing software. You're choosing the infrastructure for how your organisation experiences risk every day.

Build for adoption, not just compliance

Even the most elegant framework will fail if no one uses it.

- **Design with the user in mind.** Make it simple for someone in HR or IT to log an incident, check a control, or review a risk.
- **Start small, show value.** Begin with a pilot group or a single risk domain. Demonstrate momentum before scaling.
- **Celebrate wins.** Highlight where risks were caught early, where dashboards helped avoid issues, or where assurance flagged a gap before an audit did.

Risk in motion succeeds when it becomes part of the organisational rhythm, not a once-a-year exercise.

Review, refine, repeat

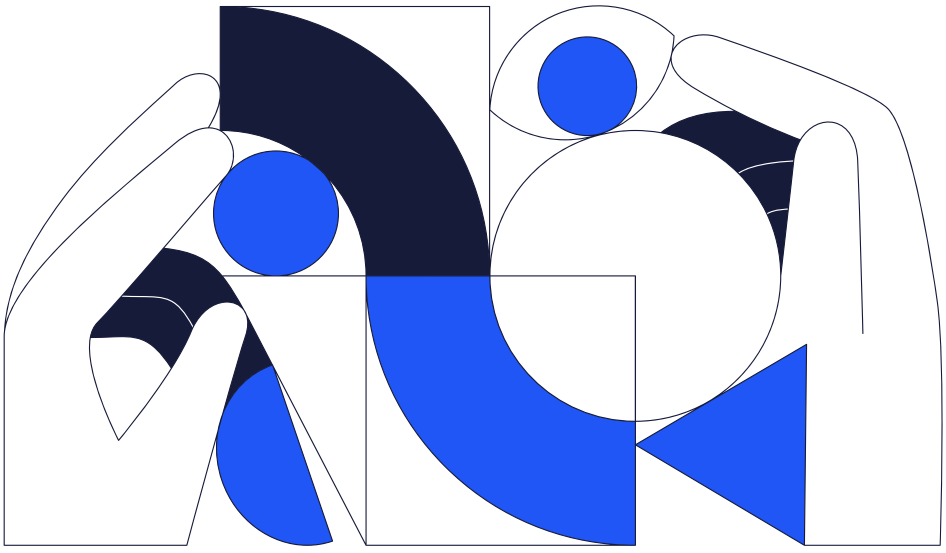
Operationalising risk in motion isn't a project with an end date. It's a capability you mature over time.

- **Hold retrospectives.** What worked? What stalled? Where did teams disengage?
- **Track engagement as well as outcomes.** Are people logging data? Using dashboards? Following up on actions?
- **Continuously improve.** Use feedback loops to refine workflows, update training, and evolve how each process fits your organisation.

In short: treat operationalisation as a living process, just like the risk engine itself.

Operationalising risk in motion brings clarity, connection, and confidence to your risk program. But what happens when you zoom out?

Next, let's explore how risk in motion transforms strategic decision-making. From boardrooms to frontline teams, we'll look at how real-time risk visibility drives agility, resilience, and trust.



5 Seeing risk in advance: Dashboards in action

You've built the engine. You've mapped the processes. Your people and systems are connected and in motion.

Now what? You need visibility.

Because risk in motion isn't just about having the right processes – it's about seeing them work, spotting where they aren't, and acting before issues escalate. That's where dashboards come in.

This chapter explores how risk in motion becomes real-time intelligence through Protecht's dashboards and reports. These aren't just static visuals – they're living systems that show how risk is evolving, how people are engaging, and where attention is needed most.

Let's explore the key tools.

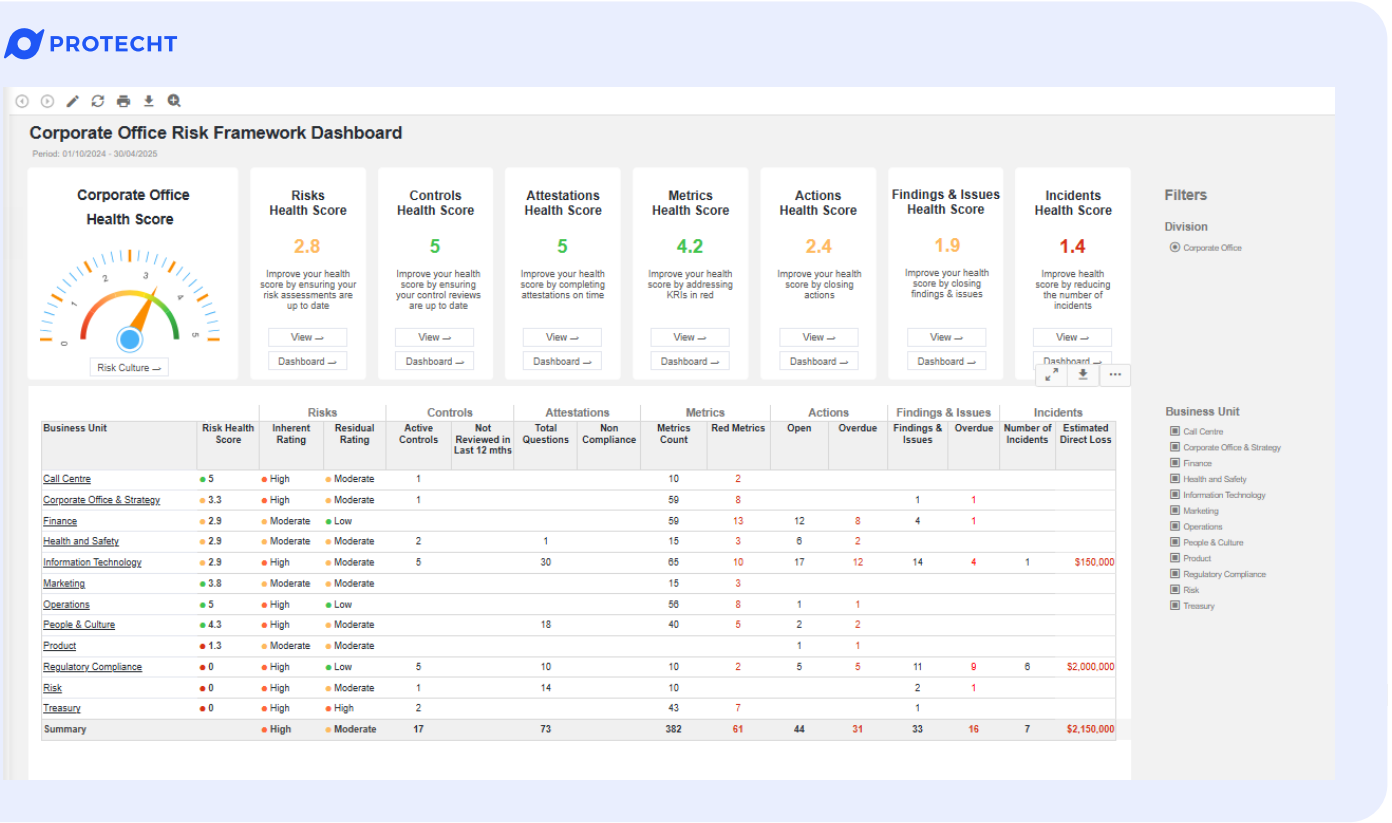
The risk in motion dashboard

If the six gears are the moving parts of your engine, the risk in motion dashboard is the instrument panel, and your risk appetite is the values on the lower and upper portions of your dial.

At a glance, it surfaces the health of your risk program across the lifecycle:

- Risk assessments
- Controls
- Attestations
- Metrics
- Issues and actions
- Incidents

You can see performance by business unit or risk type. Colour-coded tiles highlight what's on track – and what's not. The goal is to shift from passively monitoring risk to actively managing it in real time.



Linked items report: A unified view

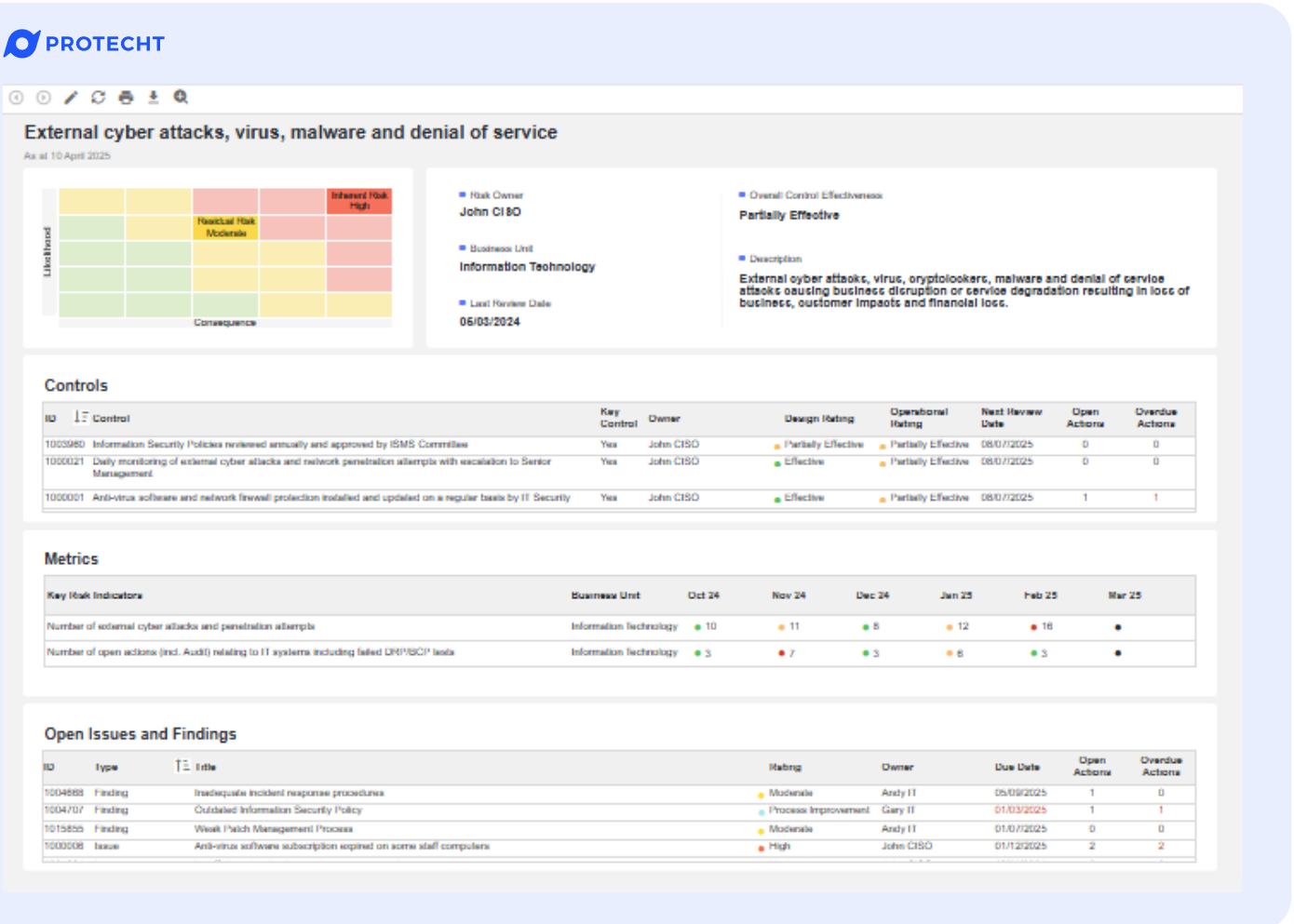
Protecht's linked items report connects the dots.

For any individual risk, you can view everything that matters – controls, incidents, KRIs, compliance obligations, actions, and attestations – in one place. It's not just a list. It's a map of relationships.

Instead of flipping between spreadsheets, documents, and registers, you can trace the story of a risk as it evolves:

- Has control effectiveness changed?
- Are metrics trending in the wrong direction?
- Are open issues being addressed – or escalating?

This unified view enables more than situational awareness. It enables intelligent, predictive decision-making.

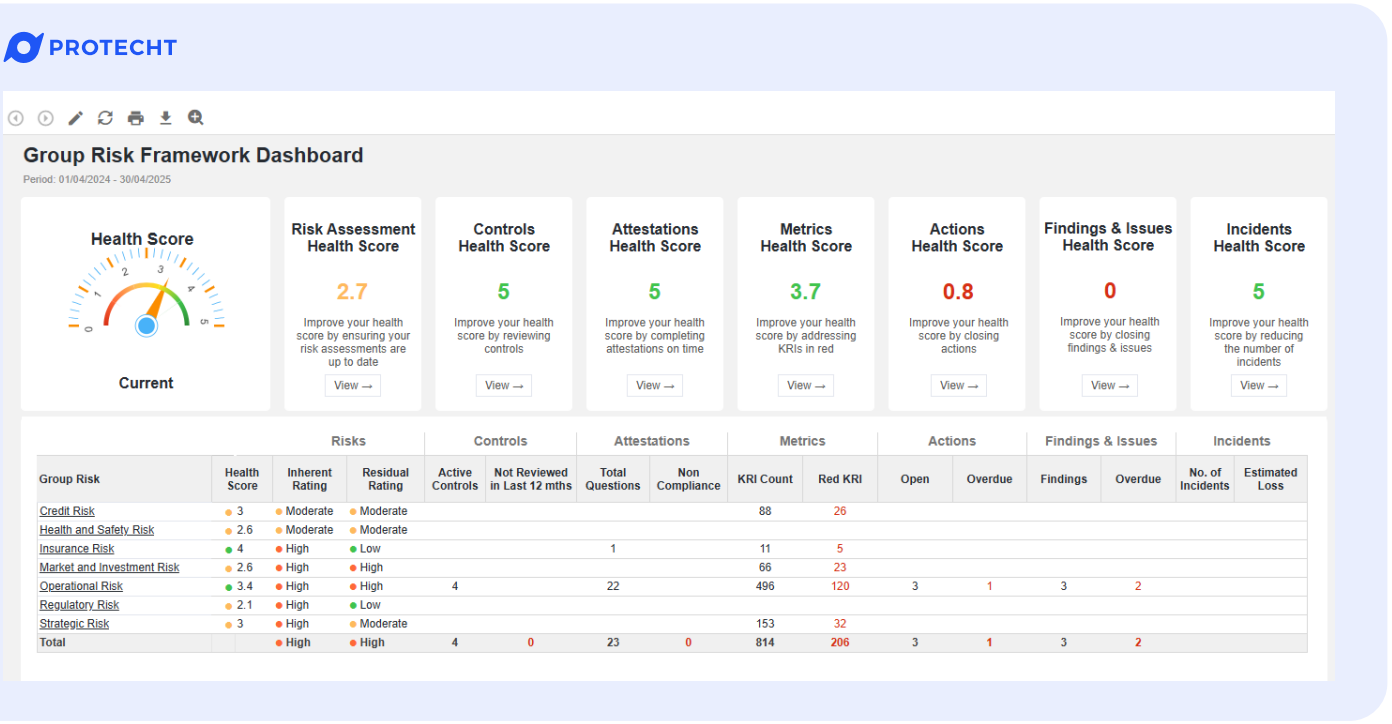


Health scores: Measuring engagement, not just exposure

Traditional ERM tools focus on exposure: what the risk is, how severe it might be. Health scores add a new dimension: How well are people engaging with the risk program?

Calculated using factors like action completion rates, attestation timeliness, and system usage, these scores spotlight areas of low engagement: early warning signs that your processes may not be sticking.

Health scores are gamified, too. Red means trouble. Green means confidence. Yellow means it's time to dig deeper. They're not just performance metrics. They're cultural signals.



				Risks		Controls		Attestations		Metrics		Actions		Findings & Issues		Incidents	
Group Risk	Health Score	Inherent Rating	Residual Rating	Active Controls	Not Reviewed in Last 12 mths	Total Questions	Non Compliance	KRI Count	Red KRI	Open	Overdue	Findings	Overdue	No. of Incidents	Estimated Loss
Credit Risk	3	Moderate	Moderate					88	26						
Health and Safety Risk	2.6	Moderate	Moderate												
Insurance Risk	4	High	Low			1		11	5						
Market and Investment Risk	2.6	High	High					66	23						
Operational Risk	3.4	High	High	4		22		496	120	3	1	3	2		
Regulatory Risk	2.1	High	Low												
Strategic Risk	3	High	Moderate					153	32						
Total		High	High	4	0	23	0	814	206	3	1	3	2		

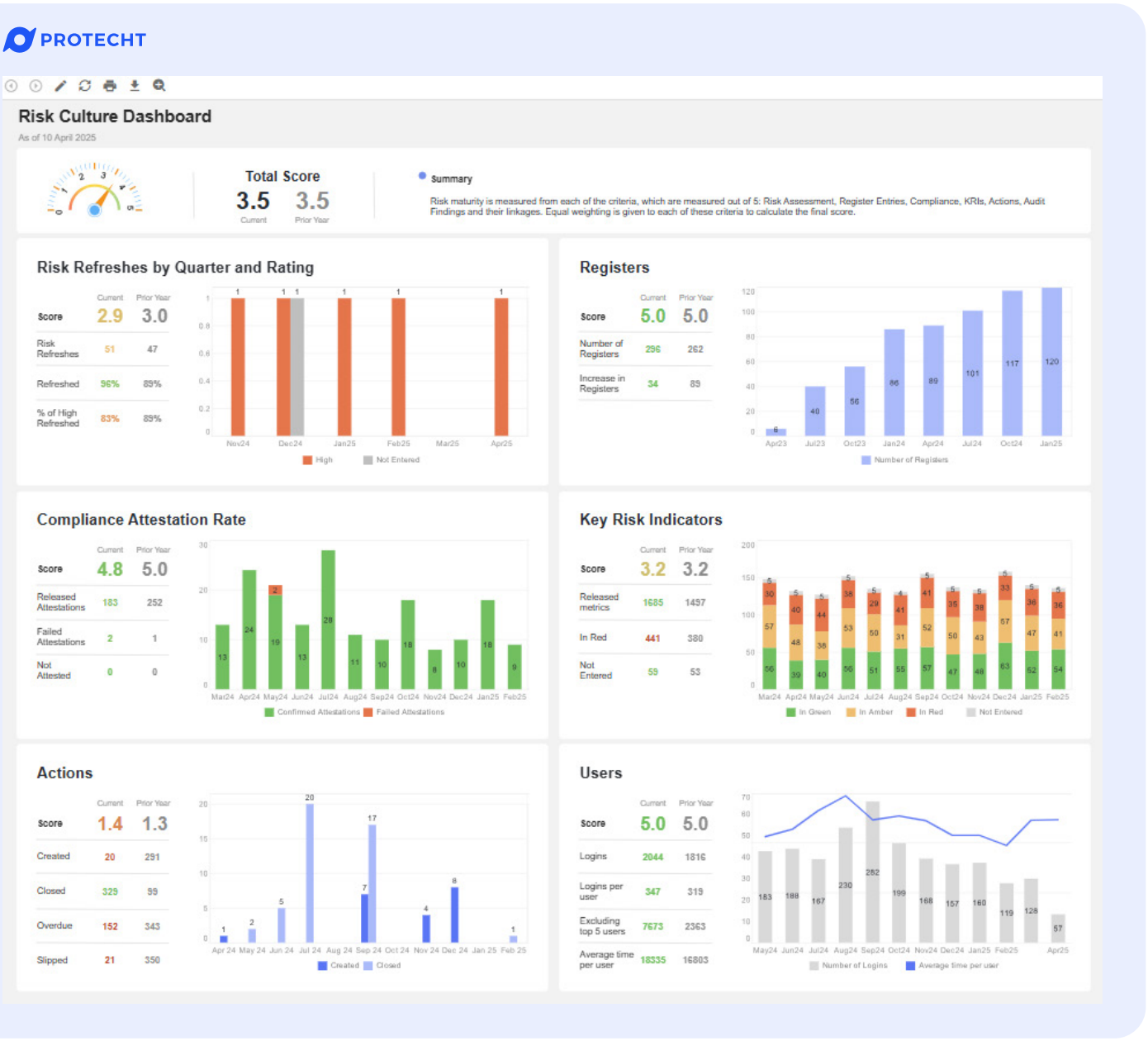
Risk culture dashboards

Dashboards don't just show what risks exist. They show how risk is being managed. The risk culture dashboard tracks system use across your organisation:

- Who's logging in?
- Who's completing attestations on time?
- Which teams are contributing metrics?
- Where are gaps in engagement?

If your people aren't using the system, the system isn't managing risk – it's just holding data.

"Risk management doesn't succeed because you bought the software. It succeeds because your people use it." ***– Terence Lee, VP North America, Protecht***



Conclusion: From visibility to velocity

Risk visibility isn't about looking backward. It's about driving action forward.

Dashboards help you see risk coming. They surface weak signals, like a slow-down in attestations or a spike in overdue actions, before they turn into red flags.

They help you shift from explanation to prevention. From gathering data to making decisions. From static reporting to dynamic governance.

Now, it's time to bring it home. Next, we'll help you take the first (or next) step: assessing your maturity, identifying quick wins, and building your own path to a connected, future-ready ERM program.

Because you don't have to be perfect to get started. You just have to get started.

6 Making risk in motion your reality

You've seen what's possible.

You've explored the gears, examined the dashboards, and understood how risk moves: how it gives off signals before the incident. Now it's time to turn potential into practice.

Because risk in motion isn't a theory. It's a choice. And it starts with a single step.

Know where you stand

No two organisations start from the same place.

Some have mature ERM frameworks but disconnected data. Others rely on manual processes or spreadsheets. Many are somewhere in between.

That's why your first move isn't to overhaul everything. It's to assess where you are today:

- Are your risk processes consistent across departments?
- Can you connect controls, incidents, and actions to specific risks?
- Do you know who's engaging – and who isn't?
- How much time is spent reporting vs. actually managing risk?

A simple maturity scan can help clarify what's working, what's missing, and what quick wins are within reach.

Start small. Connect fast.

Risk in motion isn't all or nothing.

You can start with one gear – say, issue and action management. Map issues to their source. Track resolution. Build momentum.

Then connect another gear: Risk assessments. Or controls assurance. Each addition compounds the value of the others.

The goal is not to implement everything at once. It's to break down silos and build a system that reflects how risk actually operates: connected, dynamic, always in motion.

Use what you already have

Chances are that your organisation already has useful data. It's just trapped in emails, spreadsheets, or separate systems.

Protecht helps you unlock that data and bring it together in a structured, meaningful way.

- Automate control test planning and scheduling with existing control libraries
- Link incidents and obligations to your current risk registers
- Turn monthly metrics into early warning signals
- Use dashboards to show value immediately

You don't have to start from scratch. You just have to make it visible.

READY TO SEE IT IN ACTION?

Risk in motion comes to life in Protecht ERM.

It's more than software. It's an integrated, flexible platform that brings your risk data, processes, and people together – so you can see risk before the incident, act faster, and drive confident decisions.

- **Connect all six gears of risk**
- **Monitor engagement with real-time health scores**
- **Get dashboards tailored to your risks, controls, and objectives**
- **Start anywhere, grow at your own pace**

EXPLORE A PERSONALISED DEMO OF PROTECHT ERM TODAY.

About the authors

Terence Lee
Vice President, North America

Terence Lee is Protecht's Vice President, North America. Terry joined Protecht in 2022 to facilitate our growth in North America, bringing extensive experience in governance, risk, compliance, and incident management. Terry has led sales, product, and marketing teams at risk and compliance software vendors, and is a recognised expert in ERM, vendor risk, business continuity, regulatory change management, and resilience.

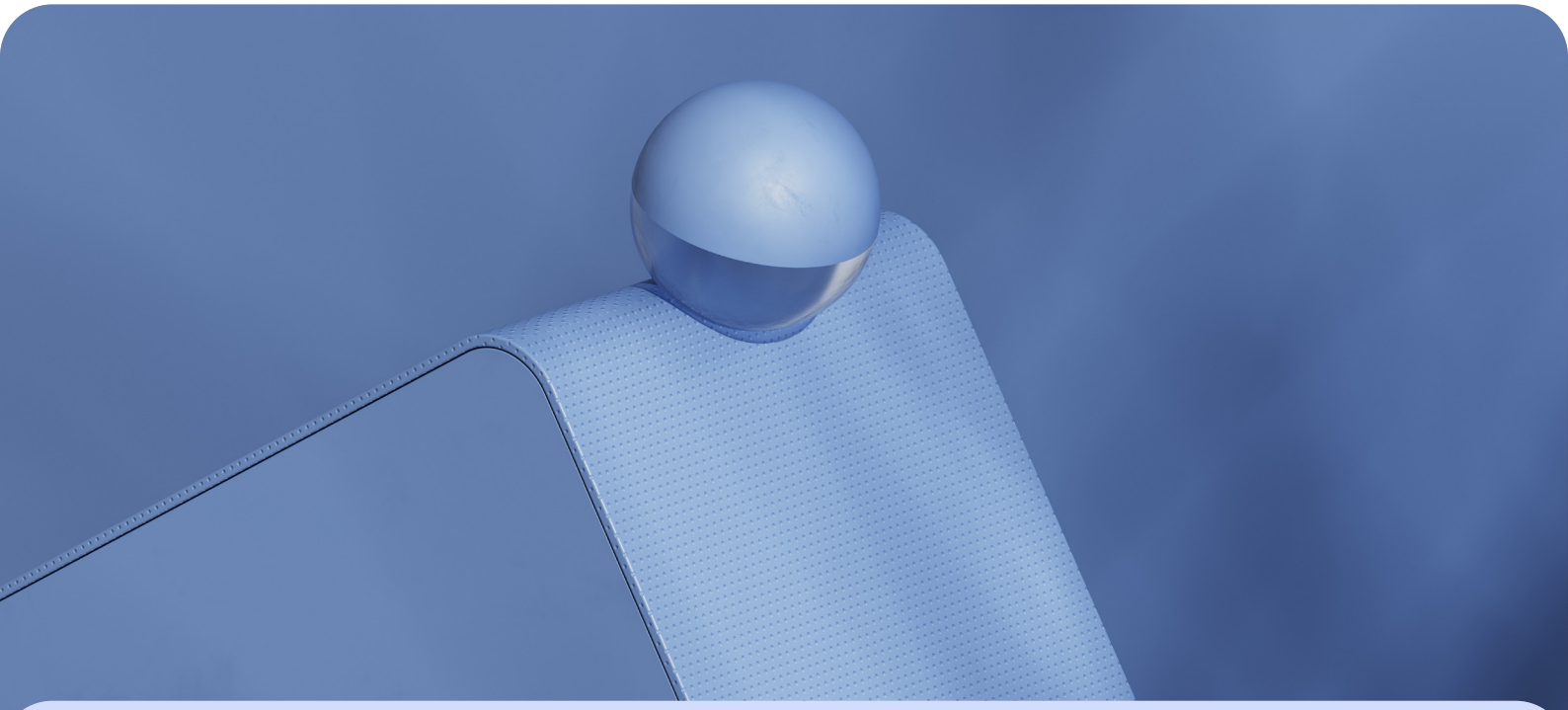
Terry's passion for helping organisations evolve their risk practices and demonstrate resilience is a perfect fit for Protecht. He has spoken at conferences on risk and resilience topics for more than 12 years, and led sales, pre-sales, and inside sales globally for SaaS vendors. His extensive knowledge of the risk and compliance market, competitors, and buyer personas have enabled Protecht to grow its audience and customer success.

Michael Howell
Senior Manager, Research and Content

Michael Howell is Protecht's Senior Manager, Research and Content. He is passionate about the field of risk management and related disciplines, with a focus on helping organisations succeed using a 'decisions eyes wide open' approach.

Michael is a Certified Practicing Risk Manager whose curiosity drives his approach to challenge the status quo and look for innovative solutions. Michael harnesses that curiosity in pursuit of risk knowledge, conducting research and developing content to support and advance risk methodology and product design at Protecht.

Michael's industry experience includes managing risk functions, assurance programs, policy management, corporate insurance, and compliance.



ABOUT PROTECHT

Redefining the way the world thinks about risk.

While others fear risk, we embrace it. For over 20 years, Protecht has redefined the way people think about risk. We enable smarter risk taking by our customers to drive their resilience and sustainable success.

We help you increase performance through better understanding, monitoring and management of risk. We provide a complete solution of risk management, compliance, training, advisory and consulting services to businesses, regulators and governments across the world.

Our Protecht ERM SaaS platform lets you manage your risks in one place: risks, compliance, incidents, KRIs, vendor risk, IT and cyber risk, operational resilience, business continuity management, and more.

We're with you for your full risk journey. Let's transform the way you understand and manage your risk to create exciting opportunities for growth.

AUSTRALIA & ASIA PACIFIC

+61 2 8005 1265
Level 8
299 Elizabeth St.
Sydney NSW 2000
Australia

Visit our website:
protechtgroup.com

EUROPE, THE MIDDLE EAST & AFRICA

+44 (0) 203 978 1360
77 New Cavendish Street
The Harley Building
London W1W 6XB
United Kingdom

Email us:
info@protechtgroup.com

NORTH AMERICA

+1 (833) 328 5471
1110 N Virgil Ave
PMB 95227
Los Angeles
CA 90029
United States

EBOOK-RIM-GL-2025-1.0