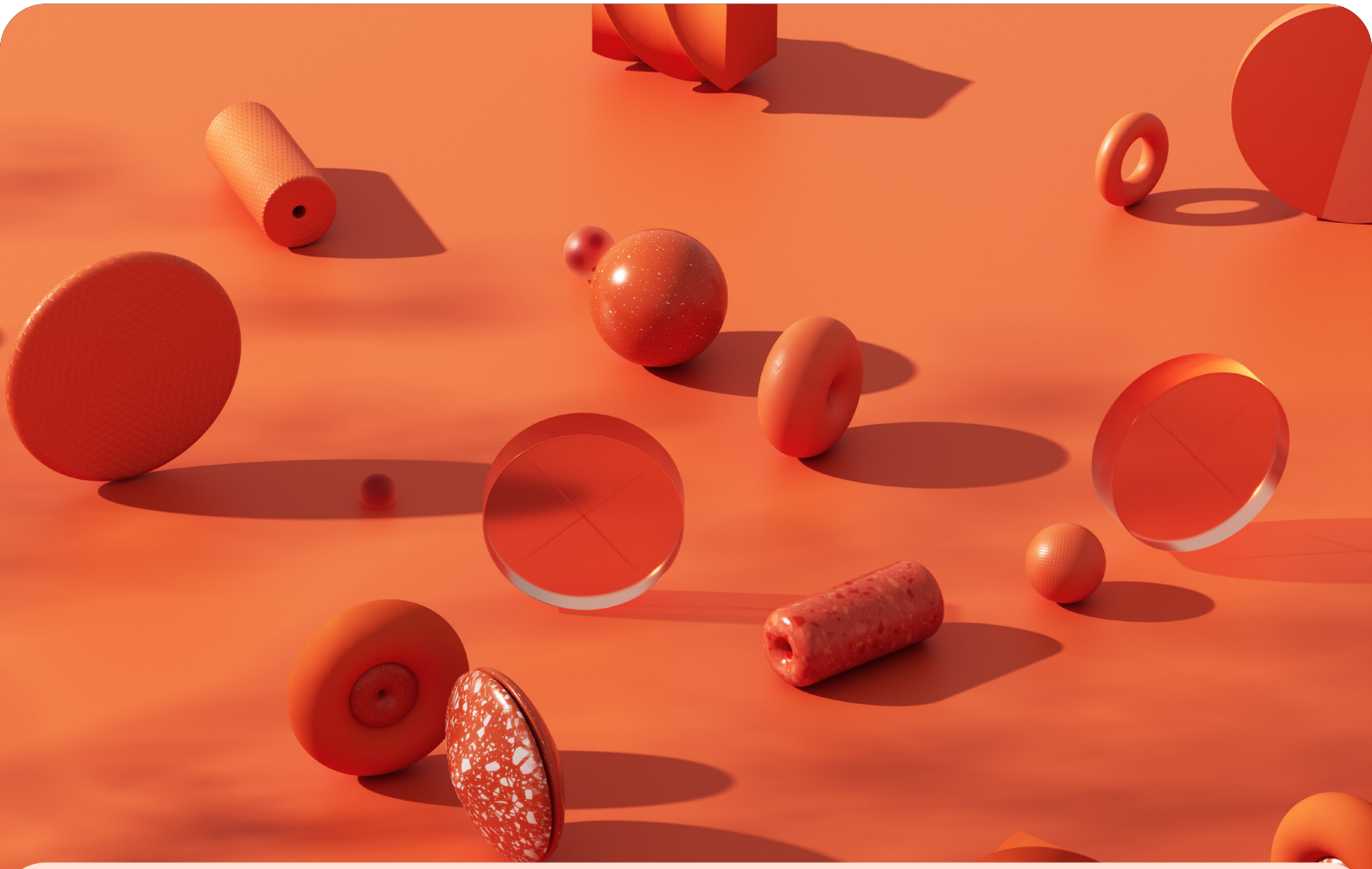
PROTECHT



E-BOOK

Risky business: What to do when your GRC tools become the problem.

Your GRC tools once promised clarity, but fragmented systems and manual reconciliation are quietly eroding confidence in governance. As visibility declines, so does your ability to act with speed, certainty, and control.

PROTECHT

Executive summary.

For many organisations, GRC tools built to reduce risk are now increasing operational friction, slowing decision-making, and eroding confidence in the numbers. Here's how:

85%

of risk and compliance professionals say compliance complexity has accelerated during the past three years

(PwC)

63%

say disaggregated data is making compliance more difficult

(PwC)

65%

say streamlining or automating processes would reduce complexity and costs

(Thomson Reuters)

Repeated delays in delivering insight start to erode confidence in the system.

AI is cranking up the pressure on GRC platforms and adding new risks to the mix.

GRC tools deployed to simplify risk management have become another layer of complexity.

Shadow ecosystems solve individual problems but create a fragmented risk landscape.

Risk information now lives in multiple places and board packs take weeks to pull together.

The average enterprise wastes US$370 million a year on technical debt and outdated systems. *(Pega/Savanta)*

Risk-averse leadership teams are often still reluctant to switch to an improved platform due to previous experiences.

>> This eBook explores how we got to this point and provides a route from complexity to clarity.

Contents.

1 Introduction.

You always knew that every day would bring a complex set of challenges as a chief risk officer or head of operational risk, but it's increasingly likely that your teams are working harder just to stand still if you're managing governance, risk and compliance (GRC) through legacy tools.

At any given time, your teams might be running control testing cycles to ensure that internal controls are operating effectively and preventing compliance issues.

They're mapping overlaps and aligning controls across multiple frameworks and regulatory standards.

Maybe the RCSA cycle has just closed, while another round of attestations is already beginning.

Risk owners are updating registers, and the next committee pack is due in a matter of weeks.

Then there's the daily grind of managing the issue remediation backlog, reprioritising the gaps and bugs that need to be fixed as new ones are identified and logged.

And you've always got one eye on how regulatory changes will impact the business model and compliance obligations.

Data integrity is constantly under threat from human error, system failure, migration issues and security breaches, creating the risk of inaccuracies, inconsistencies and duplication. Broken reporting definitions between committees are reducing the effectiveness of oversight, delaying necessary action, and leaving the business at risk of failing to meet its statutory obligations.

At some point, the shift stops being subtle.

The problem is no longer just the complexity of your risk environment.

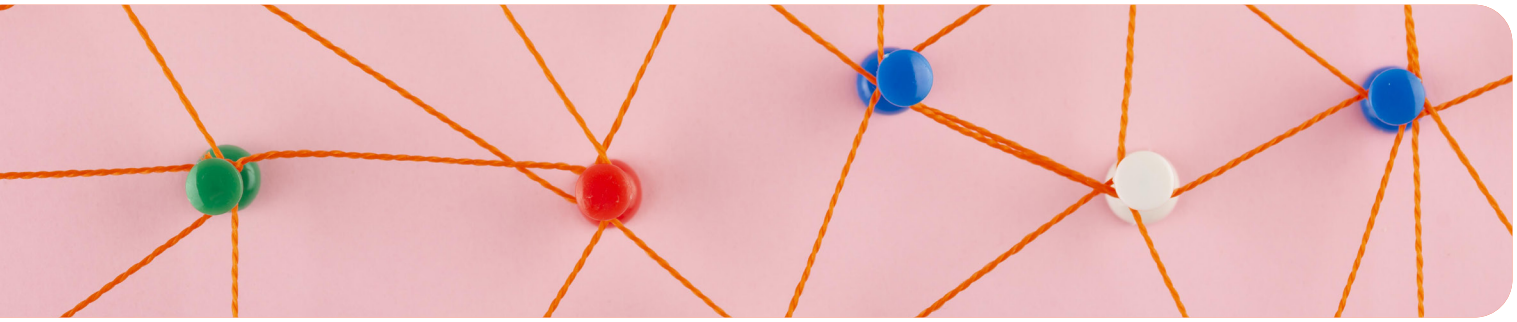
It's that the system designed to manage it is now making it harder to do your job.

Your legacy tools are slowing analysis, fragmenting information, and forcing teams back into spreadsheets and manual workarounds.

When the solution becomes the problem

This is the moment most replacement journeys begin. Not because of a board mandate or regulatory pressure, but because risk teams realize the system is no longer fit for purpose. Work arounds become permanent. Confidence in the data drops and the cost of doing nothing starts to outweigh the cost of change.

In most cases, the decision to replace a legacy GRC tool doesn't begin with the board or regulators. It begins



inside the risk function. Teams realize that the system intended to simplify risk management is now making their work harder. Processes take longer, evidence can't easily be reused, and reporting requires increasing levels of manual effort.

There are user adoption challenges to be managed, burnout and disengagement can lead to risk and control self-assessment fatigue, while system configuration restraints sometimes make it feel like you're fighting with one arm tied behind your back.

The rise of shadow systems

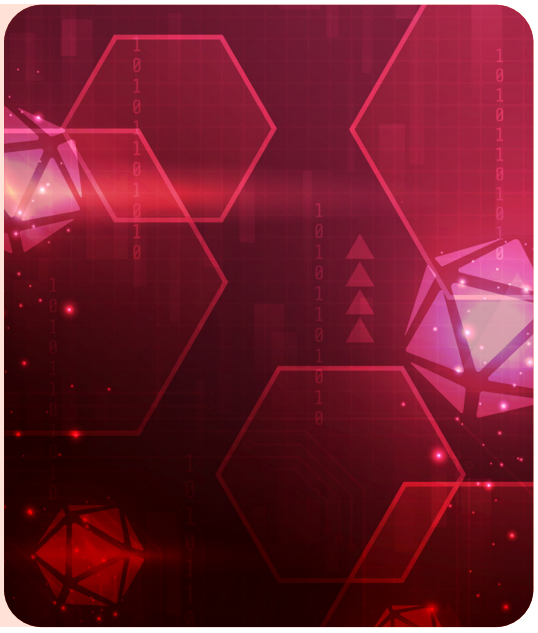
To compensate, organisations often build a shadow ecosystem around the GRC platform, with spreadsheets tracking remediation actions, SharePoint lists capturing attestations, and local trackers used for vendor assessments. Each of these solves a problem, but together they create a fragmented landscape where risk information lives in multiple places and confidence in the system begins to erode. The GRC platform becomes the system of record, but not the system of work.

How disengagement cuts across the three lines

>> For the first line, risk processes start to feel like administrative exercises disconnected from real risk rather than meaningful risk management. Managers are asked to complete repeated attestations or provide the same evidence for multiple frameworks. Minor system changes turn into projects and evidence can't be reused with confidence.

>> For the second line, risk management increasingly turns into reconciliation work. Teams spend time chasing updates, reconciling control libraries and stitching together reports rather than analysing operational risks.

>> For internal audit, assurance becomes harder to demonstrate when evidence is spread across modules, spreadsheets and shared drives rather than linked within a single traceable system.



>> This eBook explores why legacy GRC tools have reached this point, what effective and usable governance looks like in practice, and how organisations are beginning to move from complexity to clarity.

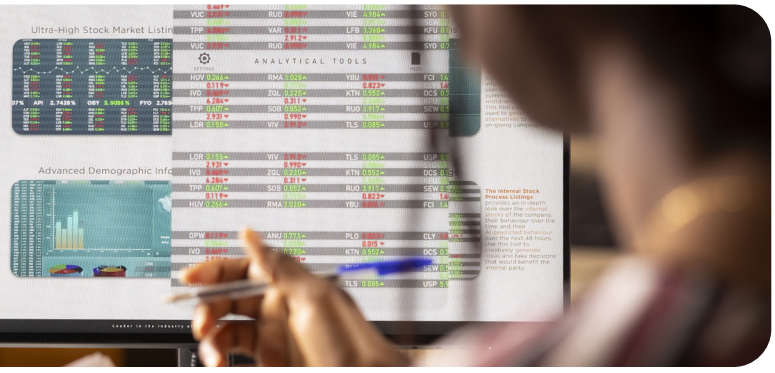
2 The problems with legacy tools.

Your GRC platform should be an important asset in helping internal teams to navigate the daily complexity of managing risk within your operating environment, but the reality is often very different.

You likely adopted your current GRC platform to move away from spreadsheets and manual tracking. And for a time, it worked. But as regulatory demands grew and frameworks expanded, the systems designed to simplify risk management became more complex and disconnected from how the business operates. Evidence got duplicated across frameworks, stored in different systems, and difficult to trace back to the controls or obligations it was meant to support.

Your team already knows something is wrong because simple tasks are taking too long. One of the clearest and most common indicators is when your team is unable to provide a quick and clear answer to a simple question posed by a board member. This is a growing issue for many organisations, with 85% of respondents telling PwC's Global Compliance Survey 2025 that compliance complexity has accelerated during the past three years.[1]

Despite this, your board and executive leadership need your team to move quickly in line with the pace of business. Delayed insights will see them start to question your ability to support the decision-making process. Confidence will be completely lost if these delays happen repeatedly.



Example scenario:
Board packs built on reconciliation, not reality

A mid-sized insurer has a legacy GRC tool for risks and controls, but key risk indicators live in business intelligence dashboards, incidents sit in a service desk tool, and audit findings are tracked in spreadsheets. When the board asks a simple question: "Are our top operational risks trending up or down?", the risk team spends two weeks reconciling extracts, reformatting charts, and negotiating which numbers carry the most weight. The board gets a polished pack, but confidence is low because everyone knows it's a snapshot stitched together after the fact.

Regulation and AI turn up the pressure

The regulatory environment has also seen significant change, with regulators now expecting demonstrable operational resilience rather than static compliance. Your focus needs to be on delivering fast and accurate responses in a continually shifting environment, so annual box-ticking just isn't going to cut it anymore.

To make matters worse, artificial intelligence has cranked up the pressure on your existing GRC platform. It's adding new risks to the mix as business units experiment with generative tools, developers embed AI capability into products, and regulators issue guidelines for using AI.

1. PwC, Global Compliance Survey.

Data disaggregation disunifies the picture

Disaggregated data is another major contributor to the complexity that your GRC teams are wading through every day, with 63% telling PwC that it makes compliance more difficult. Fragmented tools fail to deliver a unified picture, leaving risk information unclear and out of date. More rules and system sprawl create more places for multiple stories to emerge.

This data issue results in conflicting truths, unclear ownership and inconsistent evidence that makes compliance more difficult. These contradictions are killing your governance efforts, forcing committees into debating the quality of data instead of using it to support a risk appetite position. Fingers are pointed as people look for someone else to blame, but the problem is usually structural.

Example scenario:
Controls testing done three times for three frameworks

A bank runs multiple frameworks across different teams for internal controls, information security, and regulatory obligations, each with their own testing calendar and evidence repository. Standard controls including privileged access reviews are tested in different ways, at different times, with different evidence requirements. When the audit team asks for traceability from an obligation to the control and its latest evidence, GRC teams scramble across folders and emails. Everyone is busy, but the organisation can't confidently say that testing is aligned and that the evidence stands everywhere it should.

Framework duplication is a related issue to disaggregation, and can easily become embedded within your organisation when you're running multiple regulatory regimes, internal standards and assurance cycles without a connected control model. Overlap is inevitable, but duplication is not. The biggest issue is not the number of frameworks, but rather the absence of structural mapping between them.

Manual inputs lead to disengagement

The final major issue with legacy GRC tools is that they require manual input. Usually lots of it. This problem is amplified by the growing need for faster insights in an increasingly complex operating environment.

These outdated platforms can't keep up with the needs of your business and have long since become systems of record. Progress stalls time and again because changes require IT support or input from external consultants and, as a result, upgrades often feel too hard. Over time, this creates a dependency trap: The system can't evolve without external help but the business keeps changing. Teams in every department are using unauthorized tools to do their real work, adding to the disaggregated data issue and creating unnecessary risk.

This is a world of shadow ecosystems where frustrated teams have taken matters into their own hands because of system rigidity and change request backlogs. The feeling that they can't change anything without going through the IT department or a consultant makes going back to spreadsheets an increasingly attractive proposition.

Example scenario:
We can't change anything without a consultant

A government department has a heavily customized legacy GRC tool that only a small number of external specialists understand. When new regulatory reporting requirements arrive, the risk team needs to adjust fields, workflows, and reporting views. Instead of making the change internally, they log a ticket, wait for scoping, negotiate costs, and delay implementation. Over time, the organisation ends up with a clunky system of record undermined by a shadow ecosystem that everyone relies on.

What these problems have in common

Legacy GRC tools were designed around separate modules rather than connected data models. This means risks, controls, obligations, incidents and issues are captured in different parts of the system. Links between them are partial.

This leads to a series of workarounds and fixes with spreadsheets introduced to reconcile information, additional testing cycles created to satisfy overlapping frameworks and external consultants brought in to customize workflows the platform can't easily support.

Over time, this creates a fragmented governance architecture where risk information is difficult to trace and confidence in the system begins to erode.

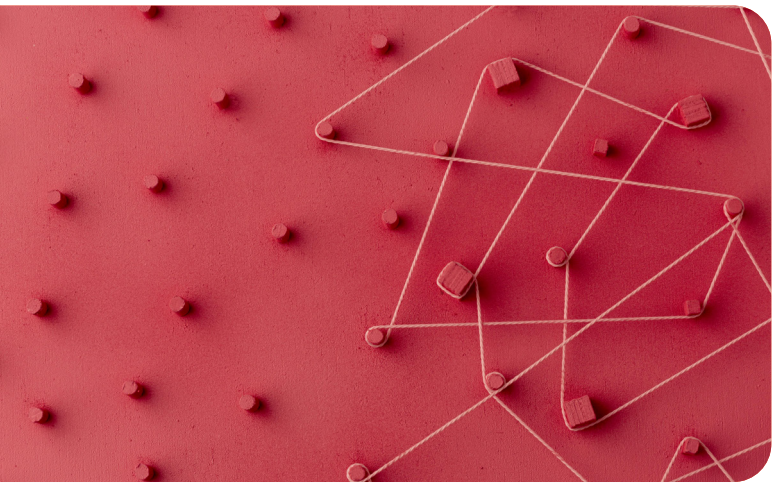
3 Detailing the cost of inaction.

We've already covered the reputational damage that the slow and contested insights delivered by legacy tools inflict on governance, risk and compliance teams, but there are also more tangible financial costs as every workaround creates friction, every exception to a rule is thrown on the admin pile, and every change request becomes a new project.

Research conducted by workflow automation platform Pega and research consultancy Savanta shows that the average global enterprise wastes more than US$370 million a year on inefficiencies that come from technical debt and outdated systems.[2]

The business case for fixing this problem is not about introducing better software, it's about reducing a measurable drag on effective governance. So, given the very real reputational and financial costs, why do organisations delay switching?

Despite knowing that the system is failing them, they often hesitate to do anything about it because switching feels risky, especially if they've had bad implementation experiences in the past. This sometimes makes leadership teams more risk averse and reluctant to implement major change. Inaction feels safer but it quietly compounds operational risk.



Example scenario:
We're scared to switch after a failed implementation

A university spends 18 months implementing a legacy GRC tool but never manages to drive adoption beyond the risk team. Frontline stakeholders complain that it's too complex and express frustration that every change requires IT support. Leadership views the platform as a sunk cost and is reluctant to make changes even though critical registers are being managed in spreadsheets. When a new chief risk officer raises the prospect of switching platforms, leadership balks at the idea because the previous failure is still fresh in the memory.

Just 9% of organisations surveyed by Pega reported that transformation initiatives have fully retired or replaced all legacy applications, fuelling anxieties around upgrading outdated systems.

At the same time, it's important to remember that inaction is a choice that comes with its own cost and control risks. Replacement of an outdated GRC platform should be viewed as a risk reduction play. So, what does success look like?

2. Pega/Savanta, Average global enterprise wastes more than $370 million every year through technical debt, says research.

4 Traceability is the foundation of confident governance.

When a risk shifts or a control fails, leaders must be able to move quickly. This requires a connected operating model in which obligations, risks, controls and evidence are structurally linked, accountability is explicit, and testing is reusable.

At its core, modern GRC is about enabling leaders to make decisions with confidence. Traceability matters because it provides the evidence chain that allows organisations to trust the risk information those decisions rely on.

Consider whether you can trace from a board-issued key risk indicator or regulatory obligation to the underlying control and its latest evidence without reconciliation. Is every critical control clearly owned by a named individual, not a committee? Are you able to test controls once and reuse evidence across frameworks?

Let's say a regulator asks how a new reporting requirement affects operational risk exposure. In a traceable model, you can:

- Identify the obligation.
- See mapped controls.
- Review test results.
- Confirm ownership and remediation status.

In a reconciled model, the answer requires extracts from multiple modules, spreadsheet cross-checks, and interpretation meetings.

When it comes to helping leaders trust the numbers, it's important to understand the difference between producing reports and instilling confidence. Effective reporting is much easier when it's based on solid, traceable work. If the board and executive team don't trust your definitions and lineage, the report feels more like a sales pitch than a clear analysis of the facts.

> **Governance, risk and compliance teams understand the benefits of streamlining or automating manual processes, with 65% of respondents telling Thomson Reuters that this would reduce complexity and associated costs.[3]**

AI becomes powerful when risks, controls, obligations and evidence are structurally linked. This is because it can draw from a single, consistent data model and reference evidence stored within controls. It can quickly turn raw data into valuable insights and clearly explain how conclusions were reached.

Building trust is about constantly increasing consistency, auditability and traceability. This use of AI shortens reporting cycles and gives risk teams the freedom to focus on making judgements rather than managing reconciliations.

How AI adds value in GRC

When risk data is structured and traceable, AI can begin to surface insights that would otherwise remain hidden. For example, it can identify patterns in control testing failures across business units, highlight emerging risk concentrations, or flag inconsistencies between risk assessments and incident data. Instead of manually searching across spreadsheets and reports, risk teams can focus on interpreting insights and acting on them.

3. Thomson Reuters, Risk and compliance report.

5 Taking the next step.

Most organisations don't lack tools. They lack confidence in the ones they have. Replacing a legacy GRC tool is rarely a simple technology decision. It's a shift in how risk information is structured, shared and treated across the organisation.

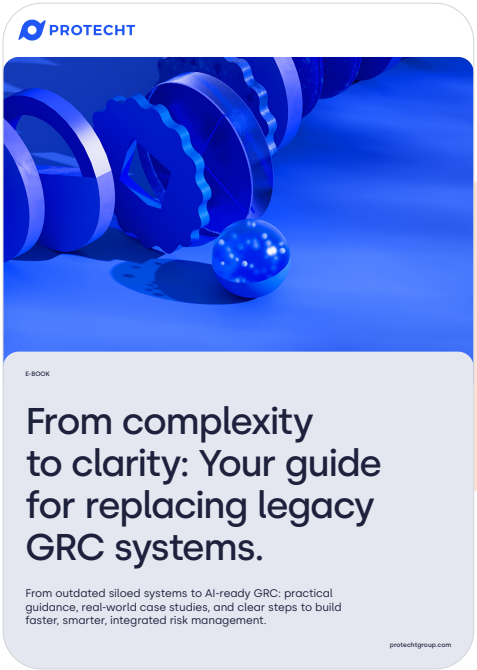
Before beginning a formal evaluation, many risk teams find it useful to step back and clarify what their organisation needs from a GRC system. This means asking practical questions like:

- Can we trace a regulatory obligation to the controls that mitigate it?
- Can control testing evidence be reused across frame-works?
- Can frontline users complete risk tasks without heavy training?
- Can leadership access reliable risk insights without weeks of report preparation?

These questions form the foundation of any successful GRC transformation.

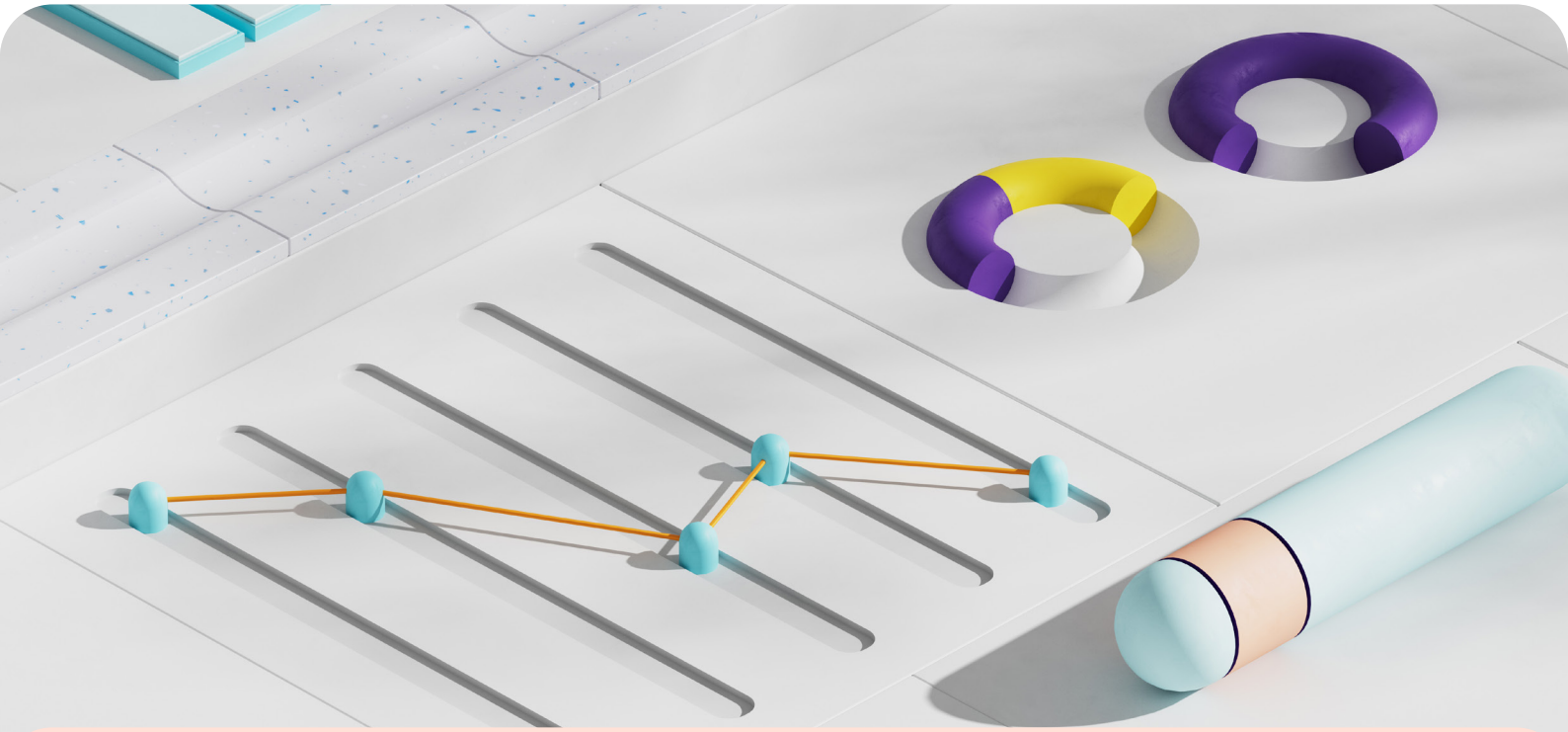
The organisations moving beyond legacy GRC are not simply replacing software. They are redesigning how risk information flows through the business.

For organisations exploring these issues in more detail, our guide for replacing legacy GRC systems provides a practical framework for evaluating vendors, defining requirements and building a business case for change.



If you're ready to take the next step, you can find the guide here.

Download now



ABOUT PROTECHT

Redefining the way the world thinks about risk.

While others fear risk, we embrace it. For over 25 years, Protecht has redefined the way people think about risk management. Through our people, we enable smarter risk taking by our customers to drive their resilience and sustainable success.

We help our customers increase performance and achieve strategic objectives through better understanding, monitoring and management of risk. We provide a complete solution of AI-enabled governance, compliance and risk management software supported by training and advisory services to businesses, regulators and governments across the world.

With our flagship SaaS GRC platform you can dynamically manage all your risks in a single place: enterprise risk, cyber and IT risk, incidents, vendor risk, operational resilience, business continuity, compliance, internal audit, workplace safety, 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.

Visit our website:
protechtgroup.com

Email us:
info@protechtgroup.com