PROTECHT

E-BOOK

Sustaining risk, compliance and trust in healthcare.

How you can integrate governance, risk and compliance management in Australian healthcare organisations to protect your patients and staff and maintain trust.

Executive summary.

Healthcare is the highest-stakes environment there is. Lives, public trust, and scarce resources are all on the line. Governance, risk, and compliance (GRC) failures here don't just cost money: **they endanger patients, damage reputations, and jeopardise funding.**

⚠ The pressures on hospitals and health services:

- Expanding regulation across safety, privacy, cyber, and critical infrastructure
- Complex third-party ecosystems from locum agencies to medical device suppliers
- Rising expectations for transparency, safety, and accountability
- A stretched workforce with little margin for error

💡 Why integration matters

Risk can't live in spreadsheets, binders, or siloed departments. To protect patients and sustain trust, GRC must be:

- Live: embedded into daily practice
- Connected: linking incidents, obligations, controls, and third parties
- Actionable: delivering real-time insights to frontline staff, managers, and boards

What this eBook covers

- The governance and cultural foundations for effective risk management
- Practical processes for managing compliance, controls, incidents, and change
- How to integrate risk and compliance into one connected framework

How Protecht helps

Protecht unifies governance, risk, and compliance in a single platform built for healthcare. With real-time dashboards, automated workflows, help from our AI assistant Cognita and pre-configured templates from our Marketplace, providers can:

- **Identify risks early**
- **Respond to incidents with confidence**
- **Manage compliance consistently**
- **Strengthen resilience against disruption**

See Protecht in action

Request a demo with a healthcare specialist

Find out more about our solution

PROTECHT

Contents

1 Why governance matters in healthcare.

⚠ The challenge

Hospitals don't just balance budgets: they balance lives, public trust, and scarce resources. Governance failures are never abstract: they can mean harm to patients, reputational damage, or even loss of funding.

Governance in healthcare is about more than ticking accreditation boxes. It's about ensuring that risks are managed in real time, incidents are responded to, and a culture of continuous improvement is embedded.

Risks exist at every level, across networks, hospitals, and every patient interaction. They can be strategic (expanding services), operational (managing rosters, cyber resilience), or clinical (patient safety).

Good governance means:

- Integrated risk registers across clinical, cyber, vendor, and operational domains.
- Linkages between incidents, obligations, risks, and controls.
- Board visibility through dashboards and assurance reports

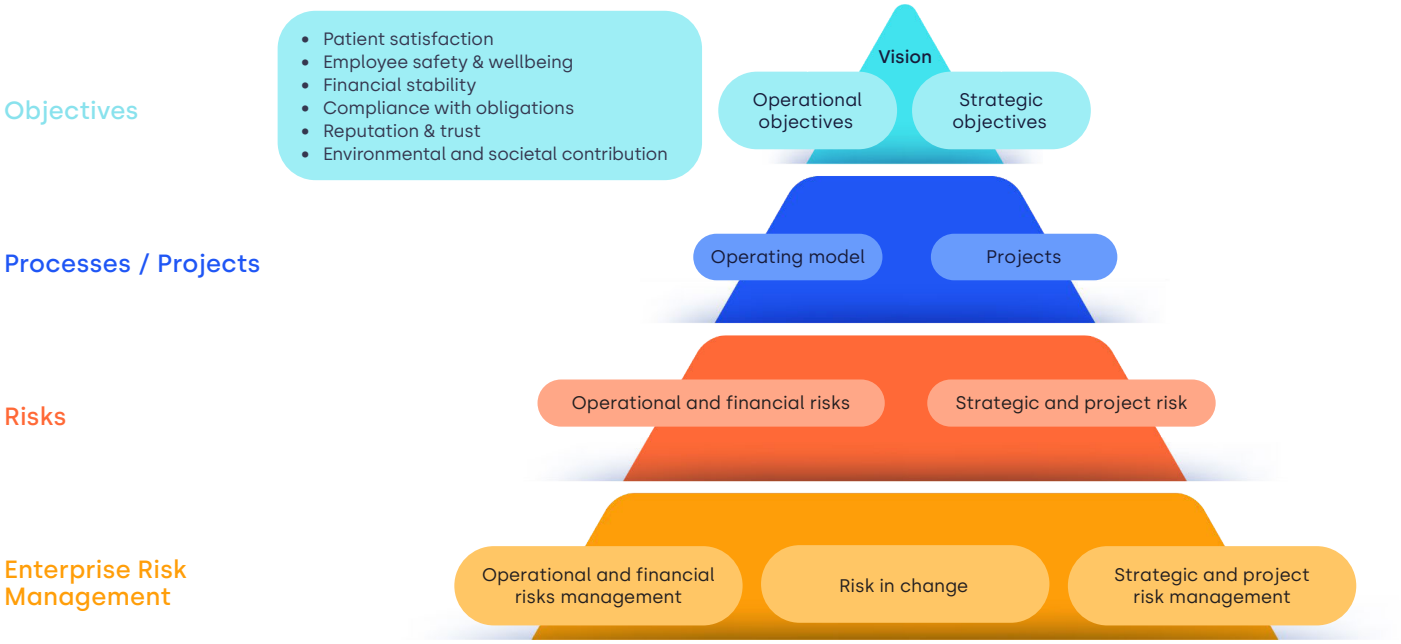
It also requires deliberate tone at the top that influences risk perception and responses across these dimensions.

Applying a risk/reward lens

While patient safety is the north star, it is one of many objectives that healthcare organisations strive to meet. These objectives are typically broken down into strategic objectives (those aimed at changing the organisation) and operational objectives (those related to running the organisation). While they may vary in importance, most healthcare organisations share common operational objectives.

Pursuit of objectives also brings risk. Below is Protecht's risk/reward framework, which visualises the relationship between risk management and objectives.

Risk and reward framework



- **Objectives layer:** Every organisation has a vision or mission (whether explicit or implicit) that supports objectives. The left side of the pyramid includes operational objectives (such as patient safety) while the right represents strategic objectives (e.g. expand the range of services offered).
- **Processes/projects layer:** This includes the business operating model required to deliver on the operational objectives. This layer also includes the strategic projects being introduced to deliver on strategic objectives.
- **Risks layer:** No activity is without some level of risk. Operational and financial risks arise out of the chosen operating model. Strategic risks include making poor strategic decisions, and risks that result in project blowouts – an unfortunately common occurrence in healthcare.
- **Enterprise risk management:** This layer includes the processes, systems and tools to identify and manage risks. If management of specific risk types are handled independently or in silos that don't integrate into your ERM framework, you may not have a complete view of risk, inefficient use of resources, or risks not being addressed.

💡 Tip: Risk management done well is outcome management

This highlights the benefit of an effective ERM framework, encompassing clinical, operational, corporate and strategic risk. Risk management becomes outcome management. This approach keeps those objectives sharply in focus.

How Protecht helps

Protecht provides a unified framework that aligns governance, risk, and compliance across both clinical and corporate operations:

- **Board-level dashboards give directors confidence that risks are being managed.**
- **Role-based access ensures frontline staff see their responsibilities clearly.**
- **Integrated workflows connect risks, incidents, and compliance activities in real time.**

Outcome: governance structures don't just sit on paper, they translate into daily action, supported by one system.

2 Managing risk in healthcare.

⚠ The challenge

Risk in healthcare isn't abstract, it's immediate.

- A clinical error can harm a patient.
- A cyber breach can shut down hospital systems.
- A missed rostering control can delay life-saving treatment.

From the patient's perspective, there's no difference between a cancelled procedure due to a cyber attack or one that fails because of a governance lapse. Both represent broken trust.

Obligations set the floor; risk management protects patients and enables strategy. Hospitals must have in place frameworks and processes to manage the broad set of risks that can undermine achievement of strategic objectives and performance, from clinical to corruption to continuity.

The ISO 31000 risk management guidelines set out a set of key steps that can be adapted to any risk type or context.

1: Risk identification

While patient safety is paramount, healthcare organisations will need to manage risks that affect all of the organisation's objectives. A typical set of risks that may need to be reported to the board or governing body include:

1. **Strategic risks** – are we making the right decisions and are we executing on them effectively?
2. **Financial risks** – Funding, liquidity & cashflow, and profitability
3. **Operational risks including:**
    a. Safety and wellbeing
    b. Clinical
    c. Cyber and information security
    d. Technology
    e. Infrastructure
    f. People & Culture
    g. Fraud and corruption
    h. Business disruption
    i. Third party risks

The specific risks and their effects will differ depending on the context of each hospital or healthcare network, and the specific services they provide.

2: Risk analysis

The aim of risk analysis is to gain a better understanding of the risk. Techniques such as bow tie analysis help map causes, impacts and controls of identified risks. This enables understanding the size of risk, while helping to identify potential control gaps.

These assessments may be supported by contextual calibration, such as the frequency per-patient day, detectability, patients or staff exposed.

3: Risk evaluation

Risk evaluation compares the level of risk with risk appetite – the level of risk the hospital is willing to accept for particular types of risk. Some risk types, such as those that impact on consumer safety, are likely to be very low.

4: Risk treatment

Risk treatment is the set of steps taken to address a risk if it is outside of the hospital's risk appetite. Common risk treatments include:

- Process re-engineering to change exposure to the risk
- Implementing or improving controls
- Transferring some of the impact, such as insurance
- Formal risk acceptance for a defined period
- Avoid the risk by stopping the activity that gives rise to the risk
- Reducing excessive controls

These treatments often require investment, not only in financial terms, but also an investment in people. Actions and accountability for implementation must be clear.

5: Monitoring & review

Documenting risks is not a set and forget exercise. Structures and processes must be in place to monitor those risks to assess how they are evolving, whether chosen treatments are being implemented as expected, that controls are having the intended effect, and risks are not escalating beyond defined thresholds.

Tip: From checklists to insights

Paper checklists can catch issues in the moment, but they don't show patterns. Moving to automated workflows and dashboards reveals trends across wards, shifts, or hospitals, reducing duplication and audit fatigue.

6: Risk Reporting

Boards, governing bodies and their sub-committees are accountable for the oversight of the organisation, executives must develop and implement strategy, and managers must make informed day-to-day decisions.

Risk reporting supports these stakeholders by providing them with timely information to support their key accountabilities and responsibilities. Effective risk reporting should support at least one of these four main objectives:

- **Assurance:** Provide assurance to stakeholders that risks are being managed, and that compliance obligations are being met
- **Red flags:** Highlight issues that may warrant further attention
- **Support decision making:** All decisions must balance risk and reward
- **Compliance:** While it should be secondary to the objectives above, reporting to regulators or external stakeholders may need to meet specific criteria

How Protecht helps

Protecht supports the full ISO 31000 risk cycle: identification, analysis, evaluation, treatment, monitoring, and reporting. Built-in risk bow ties, centralised libraries, and automated reporting allow hospitals to manage both clinical and operational risks with consistency. Integrated workflows link assessments with controls and incidents, so risks are monitored and acted on in one place.

Dealing with risk on the front line

Risk is dynamic, and nowhere is this more evident than in healthcare. Some risk management activities may be required daily in a clinic, at every shift handover, or any time a change occurs. This can include ensuring equipment is ready and accounted for, regular site audits, or drug counts.

Paper checklists may be quick and simple to implement, but information can be lost, and accountability harder to trace. They might tell you in the moment if there is something to escalate or pay attention to, but are impractical to identify trends, either over time, or where the same approach is applied in multiple wards, locations or hospitals.

A well-designed spreadsheet offers some improvements, but they lack automation, scale, and auditing.

Better tools to manage this process include:

- Automated scheduling and assignment of templated checklists for completion
- Ability to issue ad hoc checklists outside of defined schedules
- Permission based issuing and access to checklists. For example, enabling individual wards to view their own checklists, while a Director of Nursing has visibility over the whole hospital or network
- Automated workflows and escalation for non-completion, or based on specific answers that require further attention
- Trend analysis of answers, enabling benchmarking of different areas of the hospital or healthcare network

These tools can also result in reduced duplication, alleviating stretched rosters and removing audit fatigue. All of these activities are designed to monitor risk on a more dynamic basis, and enable action to be taken on the front line.

How Protecht helps

- **Template once, use everywhere.** Schedule mobile-ready checklists for ward rounds, equipment readiness, drug counts, site audits, plus issue ad-hoc forms when something changes.
- **Right visibility, right level.** Role-based access lets wards see their own activity while NUMs/Directors view hospital-wide performance and executives see network roll-ups.
- **Never miss a red flag.** Workflow and escalation trigger on non-completion or risk-based answers, creating actions with owners and due dates.
- **Single source of truth.** Link checklists to related incidents, risks, controls, and audits so frontline signals flow into enterprise risk.
- **Spot trends early.** Built-in analytics and benchmarking surface patterns across wards and facilities, highlighting hotspots and improvement opportunities.
- **Prove compliance.** Automatic time-stamped audit trails, evidence capture, and register reporting support NSQHS and internal assurance.
- **Cut duplication & fatigue.** Replace paper and spreadsheets with governed forms, reusable templates, and automated reminders to free up stretched rosters.
- **Ready to grow.** Integrates with existing IT/HR/clinical systems; scales from a single facility to multi-entity networks.
- **My Task.** Improve cultural adoption as every user has a single 'My Task' page containing everything they are required to complete.
- **Higher-quality data.** AI-guided prompts help staff capture complete, consistent records for stronger root-cause analysis.

OUTCOME: Dynamic, frontline risk monitoring that accelerates action, reduces rework, and strengthens patient safety and organisational assurance.

3 Navigating the compliance landscape.

⚠ The challenge

Healthcare providers face an evolving and fragmented compliance landscape. From the NSQHS Standards to jurisdictional reporting requirements, accreditation programs, privacy laws, and new mandates such as device incident reporting, obligations are constantly shifting. The challenge is twofold:

- Ensuring every obligation is captured, understood, and linked to the right part of the organisation.
- Demonstrating ongoing compliance across audits, regulators, and boards without burning out frontline staff or compliance teams.

While the Minister for Health and Aged Care is a national role that declares facilities as hospitals under the Private Health Insurance Act (which enables funding), hospitals and health networks are established, licenced and managed at the state and territory level. This means that in addition to national standards, they also need to comply with a patchwork of local regulatory requirements. Some providers may operate across borders; this not only adds more regulation, but a requirement to understand how they inter-operate.

However, compliance is more expansive than just regulation.

💡 What is compliance?

Compliance – Meeting all of the requirements that the organisation mandatorily has to comply with as well as those that an organisation voluntarily complies with.

As defined by ISO 37301 – Compliance management system

From individual patients and employees up to third parties and government agencies, trust is the cornerstone of healthcare. This trust isn't built by only meeting mandatory requirements and ticking boxes. It's forged by going above and beyond, and demonstrating compliance with voluntary obligations. This may include:

- ISO 9001 Quality Management Standard
- ISO 27001 Information Security Management System
- ISO 14001 Environmental Management
- Optional accreditations offered by Australian Council on Healthcare Standards or other providers

Healthcare organisations must have comprehensive practices to monitor and manage this broad set of obligations.

Cyber and privacy compliance

Hospitals and healthcare organisations must collect, hold, process and share sensitive personal information in order to carry out their services safely. That comes with a duty to protect that information – both morally, and legally under multiple regulatory frameworks.

Despite this, the health sector does not have the greatest record – results released by the Office of the Australian Information Commissioner (OAIC) in May 2025 mark healthcare as the highest reporting sector for data breaches at 20% of total notifications. For example, in 2024, a ransomware attack on MediSecure, a prescription delivery service, exposed the personal and health information of approximately 12.9 million individuals.

Technology and data flows across health organisations can be complex. From corporate infrastructure, bedside medical devices, digitised health records, and third-party integrations that enable data sharing, attack surfaces can be large. Hospitals require a consistent, repeatable and defensible approach to managing cyber risk, with controls mapped to trusted frameworks.

Data breaches typically occur at the intersection of privacy and cyber risk, but hospitals also need to consider them as distinct concepts. Consider these incidents:

- Healthcare provider repurposing identifiable records for IT testing and troubleshooting which were shared with vendors outside of Australia[1]
- Improper access of patient records without clinical need and data shared with third parties for marketing purposes without sufficient consent[2]
- Ransomware attacks that shut down services without an accompanying breach of personal information[3,4]

This reinforces the need to have a strong framework in place to both understand these requirements, and ensure they are being met.

Defining a compliance management process

To meet this complex web of requirements, hospitals or health networks should adopt a single model for compliance management across the entity or group. That process typically consists of the following steps:

Step	Description	How Protecht helps
1. Document obligations	This documents the specific requirements. You need to know what you must meet.	**Obligations register** – centralised repository of all obligations across regulatory standards, contracts, and internal requirements.
2. Risk-rate the requirements	While you need to meet all requirements, some may have higher consequences for the hospital or patients if they are not met.	**Risk-rated obligations** – assign consequence and likelihood ratings, helping leaders prioritise monitoring and assurance activities.
3. Define activities to achieve compliance	Document policies, procedures, or controls that need to be performed in order to comply.	**Policy register** – maintain structured policies, procedures, and controls linked directly to obligations.
4. Ongoing compliance activities	These ensure ongoing compliance, e.g. attestations, compliance deep dives, QA checks, or formal control testing.	**Automated attestations, QA registers, and control testing** – streamline evidence capture, testing, and assurance activities through workflows.

[1] ABC News
[2] ACCC
[3] ABC News
[4] Australian Computer Society

5. Report on compliance	Key stakeholders should receive assurance that compliance activities and monitoring are being conducted adequately and provide evidence the hospital is meeting obligations.	**On-demand dashboards and scheduled reports** – configurable reporting for boards, executives, and frontline managers.
6. Monitor change	Regulations and standards evolve alongside community expectations (e.g. from March 2026, reporting medical device-related incidents to the TGA). Requires updating obligations, reassessing processes, and maintaining ongoing assurance.	**Regulatory newsfeeds** – continuous updates from trusted sources, feeding directly into the obligations register to keep compliance current.

Tip: Treat compliance management as a connected process.

Break down obligations into plain language, map them to risks and controls, and assign ownership at the right level of the organisation. Build in proactive monitoring and reporting, so compliance activities aren't just about passing audits, but also about improving patient safety and organisational resilience.

How Protecht helps

- Obligations register: **Capture all obligations in one place, mapped to risks, controls, and activities for a single source of truth.**
- Plain-language interpretation: **Convert complex regulatory language into practical obligations that staff can act on.**
- Automated compliance scheduling: **Schedule attestations, QA reviews, and control testing with workflows and escalation.**
- Dashboards & reporting: **Provide real-time assurance to executives, boards, and regulators through configurable reports.**
- Preconfigured accelerators: **Deploy off-the-shelf solutions from Marketplace.**
- AI-enabled guidance with Cognita: **Support staff with contextual prompts, categorisation, and up-to-date regulatory intelligence so no requirement slips through the cracks.**

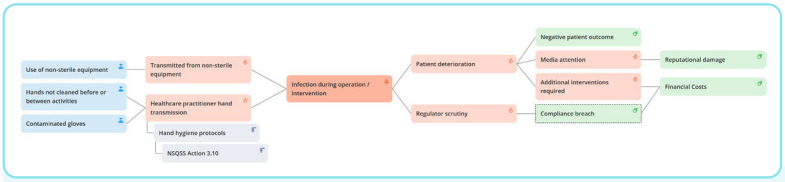
OUTCOME: **Compliance shifts from being a reactive, resource-heavy exercise to an integrated, proactive system that keeps pace with regulatory change while embedding accountability across the organisation.**

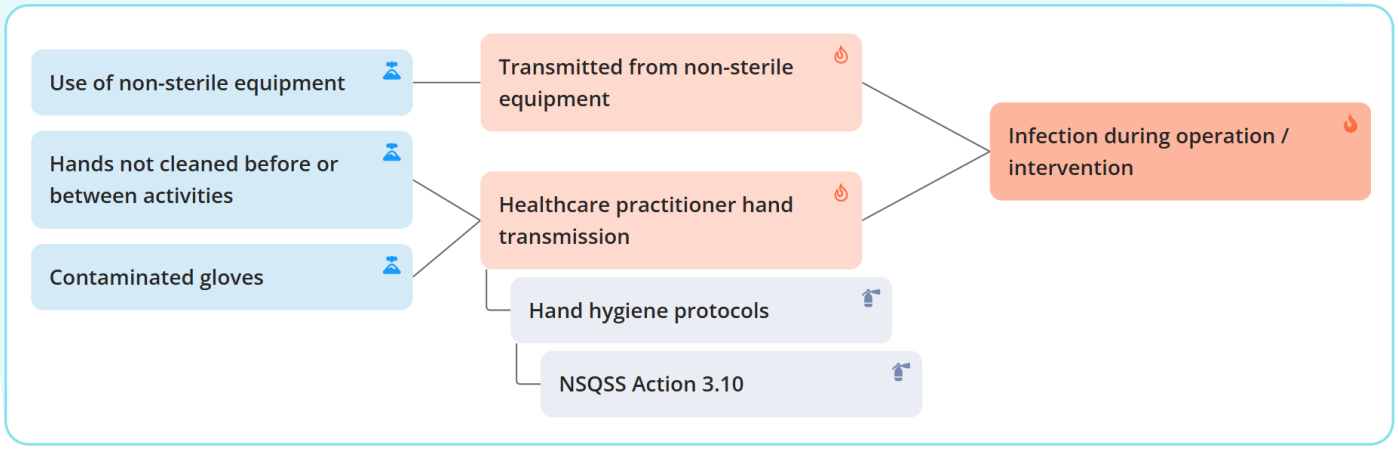
4 Controls: Where compliance and risk overlap.

⚠ The challenge

Hospitals and health services rely on thousands of controls, from infection prevention protocols and medication management to cyber safeguards and financial checks. Yet controls are often tracked in silos (spread across policies, audits, spreadsheets, and local registers). This leads to duplication, missed assurance activities, and limited visibility for boards and executives.

The bridge is controls. A single control can meet one or more obligations while also reducing risk. Let's bring that to life with a risk bow tie example:





In this example, there is an obligation to implement effective hand hygiene, aligned with NSQHS Standards Action 3.10. Hand hygiene controls can be mapped to meeting that specific obligation, but those protocols exist to manage infections, and all of its potential negative outcomes.

At Protecht we use an extended definition of controls:

"A measure or action that reduces the likelihood of a risk occurring, the impact if it were to occur, and / or to meet a compliance requirement."

Controls that are mapped to obligations should also be mapped to their relevant risks.

Tip: Don't think of controls as static checklists.

Controls should be seen as living mechanisms that need to be tested, monitored, and linked back to risks and obligations.

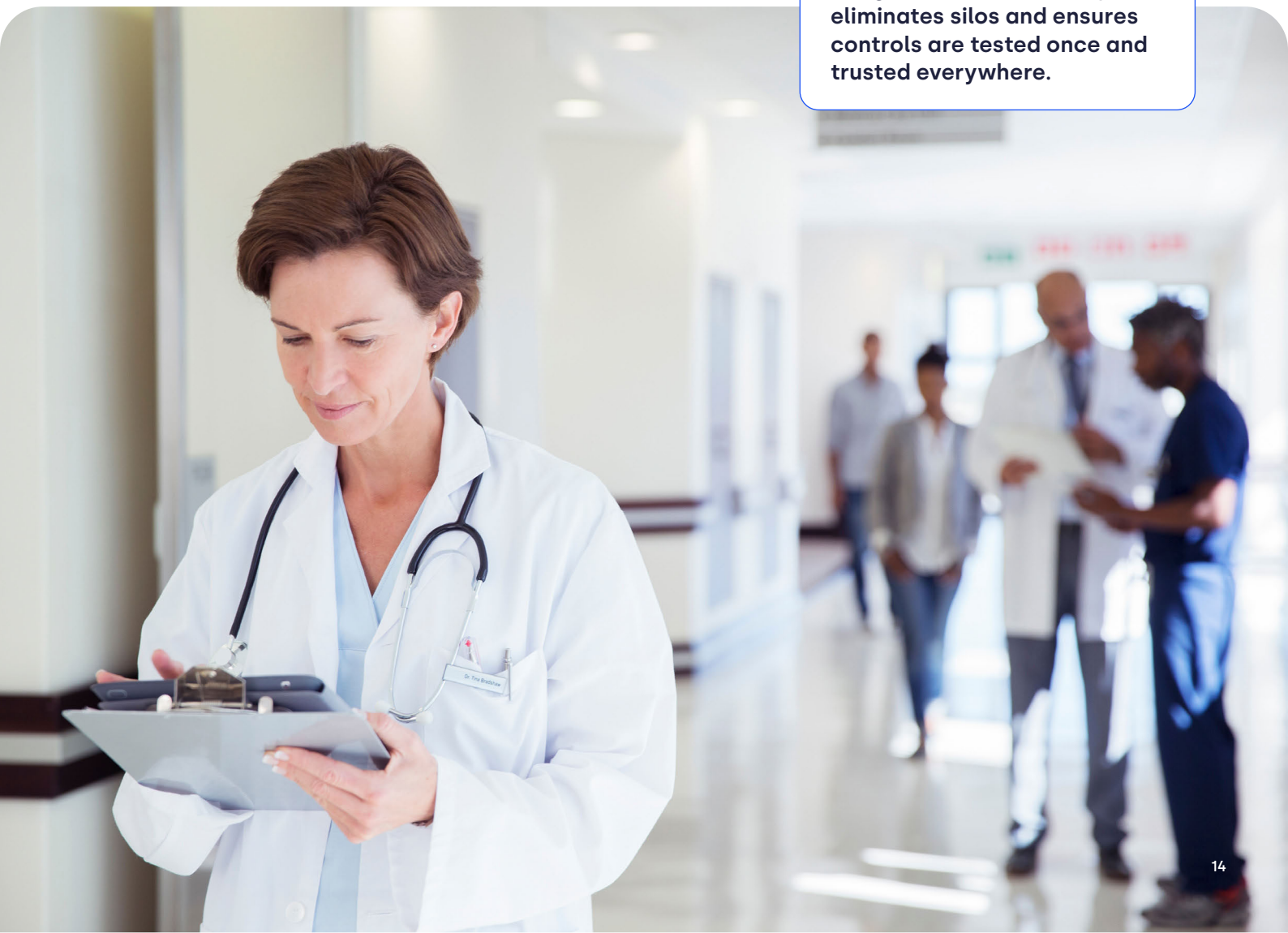
Effective controls management means:

- Maintaining a single source of truth for all controls.
- Establishing clear ownership and accountability.
- Streamlining testing and assurance to reduce manual effort.
- Analysing results to spot weaknesses, overlaps, or gaps.

Without centralisation, silos and duplication occur. A well-designed control library ensures one test provides assurance across compliance, risk, and quality.

How Protecht helps

Protecht centralises controls management, linking each control to both risks and compliance obligations. With standardised templates, consistent testing, and dashboards that highlight assurance status, providers can be confident their controls meet NSQHS and other standards. One integrated control library eliminates silos and ensures controls are tested once and trusted everywhere.



5 Incident management.

⚠ The challenge

Incidents in healthcare extend well beyond clinical safety. They can include cyber breaches, fraud attempts, continuity failures, and corporate governance issues, all of which may have significant consequences for patients, staff, and the wider community.

The NSQHS Clinical Governance Standard requires systematic management of clinical incidents, but every type of incident needs to be captured, analysed, and acted upon. Fragmented reporting systems or paper-based processes often mean:

- Near misses aren't logged consistently.
- Lessons learnt and quality improvement activities arising from incidents are not properly actioned and implemented.
- Root causes aren't identified, so the same problems reoccur.
- Complaints and incidents are managed separately, making it harder to see systemic patterns.
- Lack of AI support to identify duplication and incident trends whether they be causal factors, types, locations or other points in common.
- Boards and regulators lack confidence in incident assurance.

Complaint reporting

Complaints don't always map one-to-one with incidents, but both should be connected to risks and controls for systemic insights.

The NSQHS Standards require health service organisations to have an organisation-wide complaints management process.

Understanding the relationship between complaints, incidents and risks requires a deliberately designed set of interrelated processes with effective data management.

💡 Tip: Treat incident management as a learning opportunity.

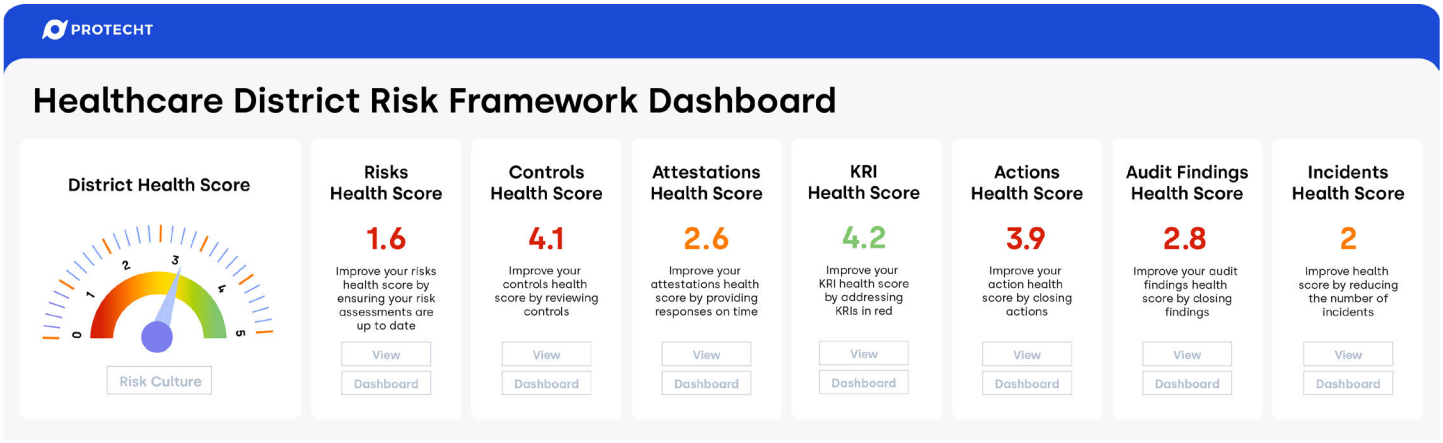
Encourage a culture where reporting is simple and supported, near misses are valued, and analysis goes beyond surface causes to uncover systemic issues. Integrate complaints with incident records where appropriate, and link incidents directly to risks and controls so that learnings drive preventative action.

How Protecht helps

Protecht provides a centralised, AI-powered system for capturing, analysing, and resolving incidents and complaints:

- **Centralised reporting:** Capture all incidents, near misses, and complaints in one governed system with structured workflows for triage, escalation, and resolution.
- **AI-enabled capture with Cognita:** Step-by-step guidance, AI-assisted prefill, and smart categorisation ensure reports are complete, accurate, and accessible for non-risk experts.
- **Root cause analysis:** Use Protecht's comprehensive bow tie method and cause taxonomy (grouped under people, process, systems, external events) to uncover real drivers of incidents.
- **Near miss integration:** Record and analyse near misses alongside incidents to surface control weaknesses before harm occurs.
- **Complaints linkage:** Understand the interplay between incidents, complaints, and risks, identifying systemic issues that impact patient safety or service quality.
- **Dashboards & audit trails:** Provide executives, boards, and regulators with real-time assurance supported by complete, time-stamped records.
- **Preconfigured accelerators:** Deploy incident and complaints management templates from Marketplace for rapid implementation aligned to NSQHS and jurisdictional requirements.

OUTCOME: Incidents become more than compliance obligations: they provide a foundation for continuous learning, stronger governance, and safer healthcare outcomes.

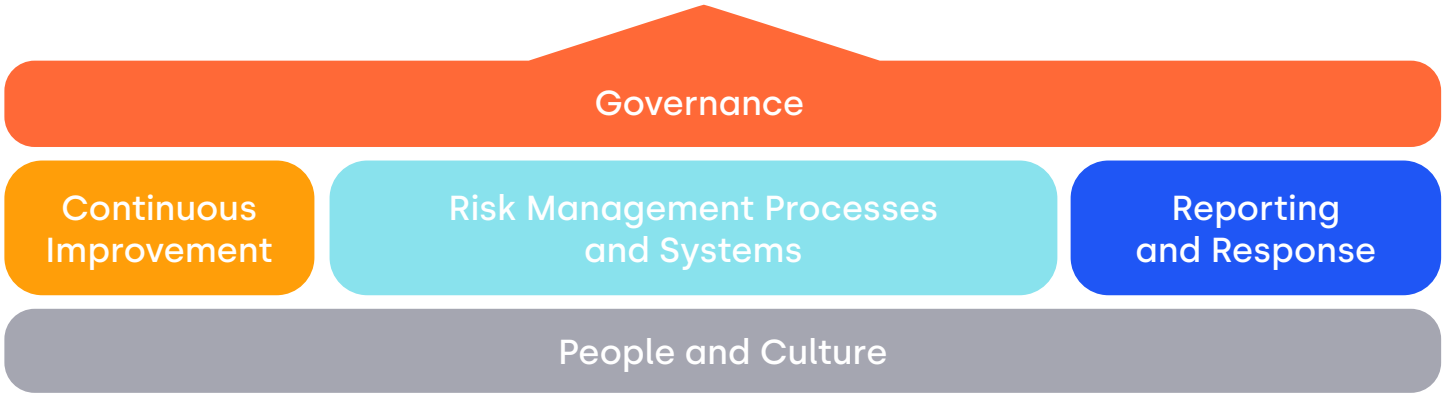


6 Bringing it all together.

⚠ The challenge

Healthcare organisations don't just face isolated risks: obligations, controls, incidents, vendors, and complaints all overlap. When these are managed in silos, assurance breaks down, duplication increases, and executives lose confidence in the data they're relying on.

Strategic risk, operational and clinical should be integrated as part of a broader enterprise risk management framework (ERMF). At Protecht we use the analogy of the "ERMF House".

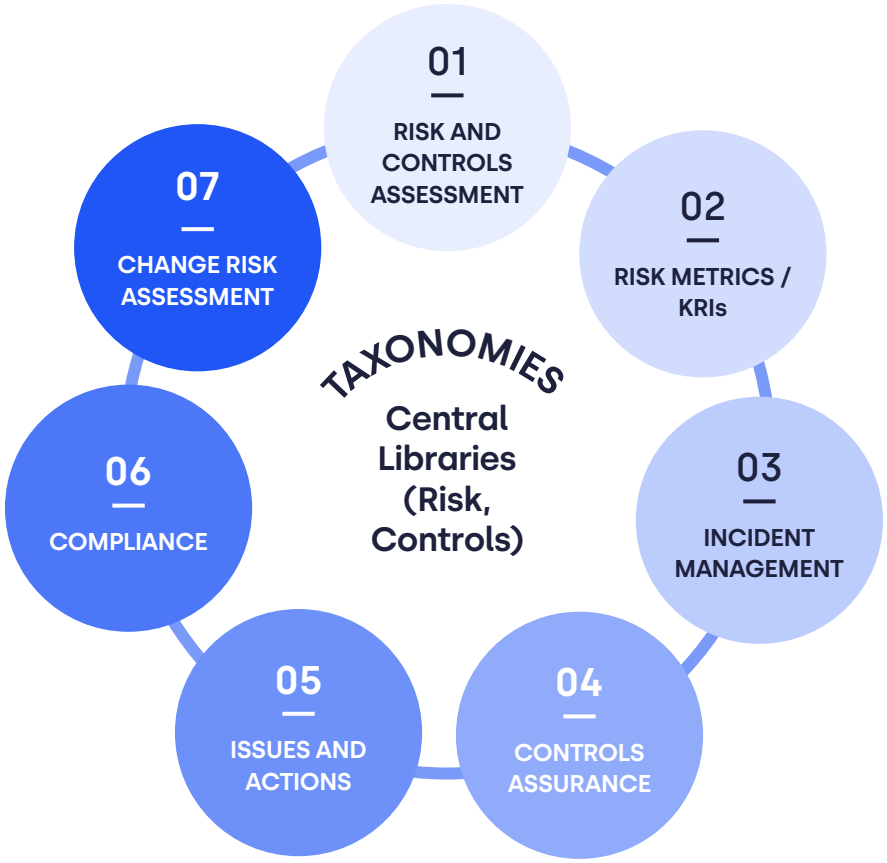


The enterprise risk management framework house.

- **Governance:** The roof of the ERMF house is governance. It defines accountability and decision rights across the board, committees (risk, audit, compliance, clinical governance), executives, managers, and frontline staff. Governance also sets risk appetite and policies that align with organisational strategy.
- **People and culture:** The foundation is culture. A clear risk culture sets expected behaviours for managing and responding to risk, from executives to casual night-shift staff and contractors. Embedding this across the workforce ensures consistent practice at every level.
- **Risk management processes:** At the centre is the engine: the day-to-day activities that bring the ERM framework to life. These processes must be outcome-focused, repeatable, and supported by tools that provide efficiency and visibility.
- **Reporting and escalation:** Good processes produce actionable insights. Reporting should ensure the right people receive the right information at the right time, with data collected once and repurposed for multiple audiences to reduce duplication.
- **Continuous improvement:** The framework itself should be regularly reviewed. Boards and executives need assurance that reporting supports strategic objectives, while frontline staff need tools designed for ease of use.

The engine room

Protecht has a common set of interconnected risk processes that support effective risk management across any domain. Let's consider them in the context of healthcare.



Protecht's risk processes diagram.

1. **Risk and control self-assessment (RCSA):** Identify, analyse, and respond to risks at enterprise, departmental, ward, project, or clinical procedure level, using common taxonomies and tools like bow tie analysis for consistency.

2. **Risk metrics:** Use early warning indicators, such as patient flow, triage times, or response rates, alongside performance measures to drive timely action.

3. **Incident management:** Capture and manage all incidents, including clinical, cyber, and operational, in a single enterprise workflow with shared taxonomies to uncover systemic causes.

4. **Controls assurance:** Regularly test controls to ensure they are designed and operating effectively, providing confidence for inherently risky activities.

5. **Issues and actions:** Track issues from risk processes or audits in a central register, with actions allocated and monitored through to completion.

6. **Compliance management:** Link obligations directly to risks and controls for a single source of truth and streamlined assurance.

7. **Change risk assessment:** Forecast how initiatives such as new technology, medical devices, or process changes will alter the risk profile, and implement controls to minimise delays or surprises.

How Protecht helps

Protecht connects all the core risk processes in one system.

- **Risk and control assessments: Pre-configured healthcare libraries and bow tie analysis tools give a consistent, repeatable approach.**
- **Risk metrics: Dashboards and alerts track key indicators in real time, helping teams respond before issues escalate.**
- **Incident management: Integrated taxonomies ensure clinical, cyber, and operational incidents feed into the same workflows.**
- **Controls assurance: Testing and monitoring can be centralised, with results shared across stakeholders.**
- **Issues and actions: Track corrective actions and improvement plans through to closure.**
- **Compliance management: Link obligations directly to risks, incidents, and controls for a single source of truth.**

Resilience and business continuity

Managing disruption must form part of a healthcare provider's enterprise risk management framework. Depending on the services provided, they may need to prepare for both external emergencies (acute patient surge of critically injured patients) and internal emergencies (failure of equipment required for critical services).

Simple desktop exercises or testing recovery of single assets only provide limited information on capacity to recover end-to-end services, and not whether your people will know what to do when a crisis hits. Instead, exercising a set of severe but plausible scenarios enables health service organisations to understand their complete capability. Those scenarios might stress not only a range of assets, but also the hospitals' ability to respond. Plans are full of assumptions that must be vetted. Could a variation of a given scenario mean:

- You can't actually make a required phone call or reach a critical contact
- Specimens or lab results won't be available or lack integrity
- Patient transfer sites are either unavailable or can't be reached

Many of these scenarios may be extreme versions of known and documented risks, a combination of multiple risks with a common cause, or a set of interrelated and cascading risks.

How Protecht helps

Protecht's operational resilience and business continuity management capability enables healthcare providers to:

- **Map critical services and supporting resources across people, data, facilities, and equipment.**
- **Define recovery time and recovery point objectives that reflect patient safety and care continuity.**
- **Develop and exercise severe-but-plausible scenarios to test readiness.**
- **Link continuity planning to risk, controls, and third parties, so resilience becomes part of the wider risk framework.**

PROTECHT

Integrating third party risk management

Hospitals and healthcare networks operate in a complex ecosystem of third-party providers, sometimes invisible to the patient. Outsourced medical imaging or services may be conducted by third parties, even if they are on the same site. Medical staff may be provided by agencies who verify and vouch for credentials. Suppliers of medical equipment and consumables may need to meet industry standards. Healthcare networks may have hundreds, even thousands of third parties.

Those third parties bring risk that may be obscured, as the hospital does not have direct oversight:

- How confident are we that medical staff are credentialed appropriately?
- How do we know this equipment is safe to use on our patients?
- How confident are we that this medical device is secure?

It's important not only to assess third parties upfront, but also to manage them throughout the entire lifecycle.

Upfront tiering and due diligence sets the tone for the ongoing relationship:

- Does the third party support critical operations? If they fail, will it affect business continuity?
- Will they have access to patient data or sensitive internal information?
- Are they integrating directly with any of our systems?

Ongoing monitoring closely mirrors the common risk processes. Risk assessments still need to be conducted, metrics may be monitored or provided by the third party, and incident management protocols need to be established.

How Protecht helps

Protecht provides a single platform for managing third-party vendor risk across the full lifecycle, from onboarding and due diligence to ongoing monitoring and incident response.

- **Centralised oversight: All third-party vendor data, assessments, and risk records are captured in one governed system, giving consistent visibility across wards, hospitals, and multi-entity networks.**
- **Tiering made simple: Apply upfront tiering and due diligence templates to prioritise high-impact providers and streamline lower-risk engagements.**
- **Consistent assessments: Use pre-built or customisable questionnaires, including Shared Assessments SIG, to ensure every third party is assessed to the same standard.**
- **Continuous monitoring: Automate reminders, track metrics, and integrate incident reporting so risks are managed throughout the relationship, not just at onboarding.**
- **Linked to enterprise risk: Third-party vendor risks are connected to controls, obligations, and incidents, ensuring they are managed in the same framework as internal risks.**

OUTCOME: Hospitals and health services can manage a complex web of suppliers and providers with confidence, consistency, and complete oversight, reducing duplication while improving assurance.

7 Next steps for your healthcare organisation.

⚠ The challenge

Hospitals and health services face an enormous task in overhauling governance, risk, and compliance. With risks spanning everything from clinical safety and cyber resilience to regulatory compliance and third-party oversight, the complexity can be paralysing. How do you drive transformation without overwhelming staff, losing focus, or stalling progress by trying to tackle everything at once?

You don't need to roll out every capability at once. By focusing on the areas that deliver the greatest immediate impact, you create early wins, reduce strain on staff, and lay the groundwork for continuous improvement.

Over time, each step strengthens your governance and resilience. And because every process is connected through one integrated platform, you can expand at your own pace while ensuring consistency and visibility across the entire organisation.

💡 Tip: Start with the most urgent challenge.

The challenge might be clinical incident reporting, compliance with NSQHS standards, or giving your board visibility of enterprise risk. Early wins create confidence, reduce burden on frontline teams, and build the foundation for broader transformation. Expand step by step, knowing each new process connects into the same framework.

PROTECHT

How Protecht helps

Protecht allows health service providers to:

- **Start where it matters most.** Begin with priority areas such as incidents, compliance, or controls, then expand when ready.
- **Stay coordinated.** Configure workflows and dashboards to match immediate organisational needs and evolve with your services.
- **Scale with confidence.** Grow seamlessly from a single hospital department to a multi-site health network, all on the same platform.
- **Build on one foundation.** Maintain a single, integrated system so each new module connects, reducing duplication and silos.
- **Enable your team with Cognita:** Cognita is your intelligent AI assistant for risk and compliance. Get step-by-step guidance on risks, incidents and system usage to help upskill non-risk experts and ensure good quality data is recorded.
- **Accelerate with Marketplace.** Deploy preconfigured registers, dashboards, and workflows from our Marketplace, giving you a turnkey launch with best-practice templates for healthcare, IT, vendor risk, compliance, and more. Marketplace content is continually updated, so you stay aligned with changing regulations and emerging risks.

You don't have to do everything at once, but with Protecht, Cognita and Marketplace you can move faster, expand smarter, and always stay connected as your risk and compliance needs grow.

Protecht for healthcare

Start where it matters. Scale without friction.

Move beyond spreadsheets and disconnected tools. Protecht gives your hospital or health service a single, integrated foundation for incidents, obligations, controls, and risk so you can deliver early wins, reduce burden on frontline teams, and expand at your own pace.

See Protecht in action

Request a demo with a healthcare specialist

Find out more about our solution

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 Protecht ERM SaaS platform you can dynamically manage all your risks in a single place: risks, compliance, incidents, KRIs, vendor risk, cyber and IT risk, internal audit, operational resilience, business continuity, 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

EBOOK-HEALTH-APAC-2025-1.1