PROTECHT | UNSW SYDNEY

CASE STUDY

# How UNSW transformed cyber risk visibility and reporting

Automated assurance, simplified dashboards, and end-user access in a complex IT environment.

protechtgroup.com

## Summary

UNSW's cyber risk team needed a better way to manage the growing complexity of IT risks, assurance activities, and regulatory compliance across a distributed university environment. Manual processes, rigid systems, and limited reporting capabilities created inefficiencies and hindered oversight.

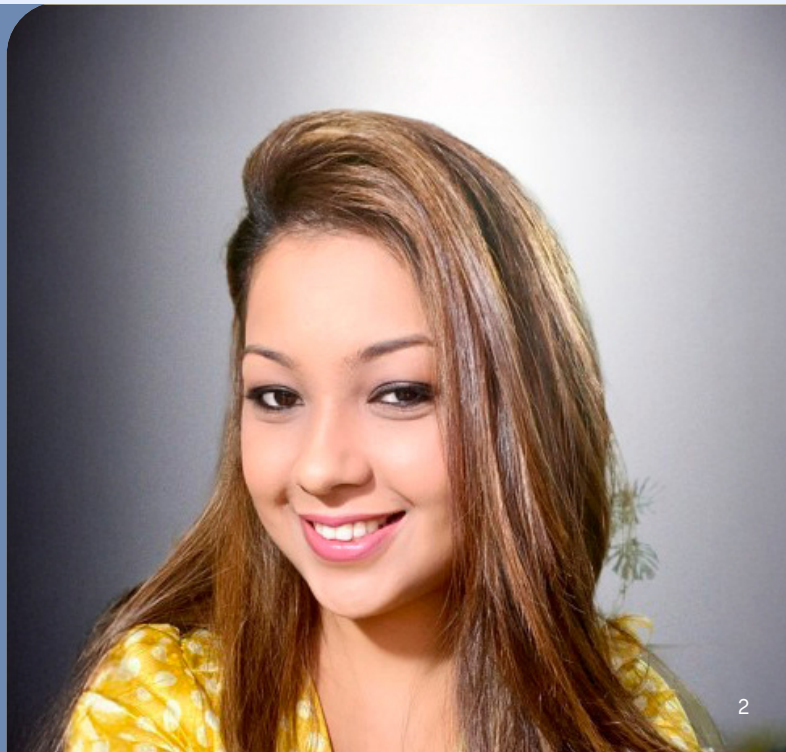
By implementing Protecht ERM, UNSW established a dynamic, user-friendly platform for managing ISO 27001 compliance, tracking assurance activities, and maintaining asset-level visibility. The solution enabled real-time dashboards, automated reporting, and structured workflows that engage users across the university – saving time, reducing risk, and laying the foundation for AI-driven innovation.

## About UNSW

As one of Australia's leading universities, UNSW manages a complex and evolving cyber risk landscape. The cyber risk function has responsibility for managing distributed risks across hundreds of systems and services. To support its internal risk management framework and ISO 27001 obligations, the team needed a scalable, adaptable platform to centralise risk information, support assurance activities, and drive user engagement across business units.

"Every day there are new applications onboarded into the environment. You need a platform that can handle that ongoing risk management."

**Nivi Newar**
Deputy CISO, UNSW



## The challenge

UNSW operates in a highly decentralised and complex IT environment. With a very large number of applications in active use across the organisation, maintaining an accurate, up-to-date view of cyber risk was a significant challenge. Many of these systems are managed across different departments, often with varying levels of maturity in risk and compliance practices.

Previously, cybersecurity risk assessments were closely tied to the university's project management office (PMO) approval gates. While this structure provided a degree of control, it created rigidity in the process and generated frustration among project stakeholders. Many initiatives struggled to progress due to inflexible timelines and delays in risk sign-off.

In addition, the university's existing tools were not designed for continuous risk monitoring or engagement. Risk information was scattered across spreadsheets, static registers, and disparate systems. Reporting was manual and time-consuming, with teams often relying on cut-and-paste methods to compile dashboards and audit responses.

Some processes – such as tracking team KPIs – relied on systems like the HR MyCareer platform, which were static, point-in-time solutions lacking any real workflow or dynamic functionality. This hindered efforts to embed risk awareness and performance management into day-to-day operations.

The cyber risk team needed a new approach – a platform that could not only streamline and automate their existing processes but also support meaningful engagement with risk owners across the university, deliver actionable insights, and scale with the institution's growing needs.

## Why UNSW chose Protecht

UNSW selected Protecht ERM after the careful evaluation of several options. For the university's cyber risk team, it was essential to find a platform that could not only meet today's compliance and assurance demands but also grow with the institution's evolving needs.

Ultimately, the decision was made based on Protecht ERM's flexibility, configurability, and ability to support distributed use:

- The team wanted a solution that could be rolled out beyond the cyber team, allowing business units and risk owners to view, attest to, and manage their own risk data
- Protecht's structured registers, low-code configurability, and JSON-based workflows made it possible to design custom risk and compliance processes without relying on consultants
- The ability to share templates and configurations with other universities further reinforced its value

"This is a strategic platform for us. We've made it accessible to staff across the university, not just within the cyber team."

**Nivi Newar,**
Deputy CISO, UNSW

# How Protecht helped

With Protecht ERM, UNSW was able to transform its cyber risk management approach from fragmented and reactive to structured, proactive, and data-driven. The platform provided not only the necessary technical capabilities, but also the flexibility to support an evolving strategy.

"Everyone in the team is trained to build reports and schedule them. It's just part of how we work now."

**Nivi Newar,**
Deputy CISO, UNSW

## Protecht's key value-adds included:

### End-to-end ISMS management

UNSW uses Protecht to manage its ISO 27001-aligned Information Security Management System (ISMS) from end to end. Registers support:

- Control effectiveness and design testing
- Statement of Applicability (SoA) tracking
- Asset-level risk assessments and compliance attestation
- Remediation workflows for findings and assurance gaps

### Dashboards and audit-ready reporting

Dashboards play a central role in how UNSW monitors, manages and communicates cyber risk across the university. Designed for both technical users and executive audiences, the dashboards provide a real-time overview of the institution's risk posture, assurance activity status, and compliance gaps. Reports are not only visual, but also actionable and aligned with internal governance cycles.

- Custom dashboards provide real-time oversight for senior stakeholders and working groups.
- Reports for ISO 27001 audit readiness are automatically generated and distributed weekly.
- Power BI integration supports visualisation and ongoing analysis using enterprise-standard tools.

### Asset compliance and attestation

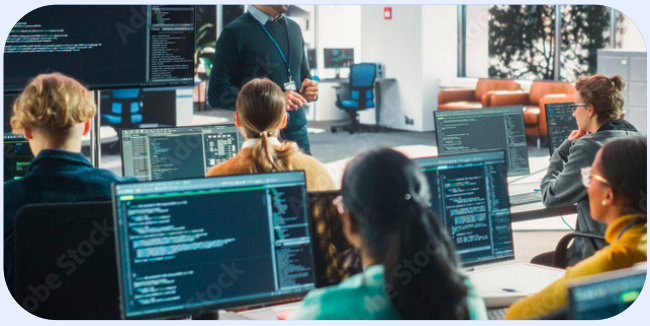
Managing the compliance of so many active systems and applications requires a scalable and accessible register. Protecht's centralised asset register became the foundation for compliance monitoring, enabling the cyber team to maintain up-to-date records and ensure accountability at the business unit level. Crucially, staff can attest compliance directly or trigger remediation workflows when needed.

- A centralised asset register tracks the compliance status of all active systems.
- Staff can self-attest compliance or flag exceptions, with required evidence for "fully compliant" responses.
- Bulk operations allow the team to apply updates efficiently across large datasets.

### Automation and workflow flexibility

Protecht allowed UNSW to move from static processes to dynamic workflows, significantly improving team productivity and responsiveness. Custom rules and branching logic support scenarios like project manager handovers, access delegation, and status-driven routing. Notification templates include embedded instructions, while tutorial videos guide users through more complex actions.

- Delegation workflows, notifications, and escalation rules support day-to-day management.
- Instructional content is embedded in the platform, including AI-generated tutorial videos.
- Custom registers for team KPIs and productivity replace static HR systems.



## Results and impact

The implementation of Protecht ERM has delivered tangible improvements across multiple dimensions of cyber risk management at UNSW. By consolidating risk data, automating manual tasks, and improving stakeholder engagement, the platform has enabled the team to operate more efficiently, with greater confidence in their compliance and assurance processes.

- **Time savings: Bulk** operations and automated workflows have drastically cut down the manual effort required to update records, onboard new assets, and generate reports. Previously time-consuming tasks like tracking control compliance or refreshing dashboards now happen with a few clicks. For example, the team saves days simply by being able to bulk update compliance fields for all assets in AWS.
- **Improved audit readiness:** Audit cycles, especially ISO 27001 preparations, have become smoother and less stressful. Risk and control information is readily accessible in structured registers, and dashboards are designed to surface nonconformities and remediation progress in real time.
- **Increased user engagement:** By exposing the system to end users and enabling intuitive workflows, the cyber team has built a stronger culture of ownership and accountability. Staff now actively update compliance statuses, respond to notifications, and interact with embedded support materials.
- **Scalability: The platform's** use of configurable registers, reusable templates, and JSON-based design allows UNSW to continuously evolve its system. As risk and compliance needs change, new registers or processes can be added with minimal friction.

## Looking ahead

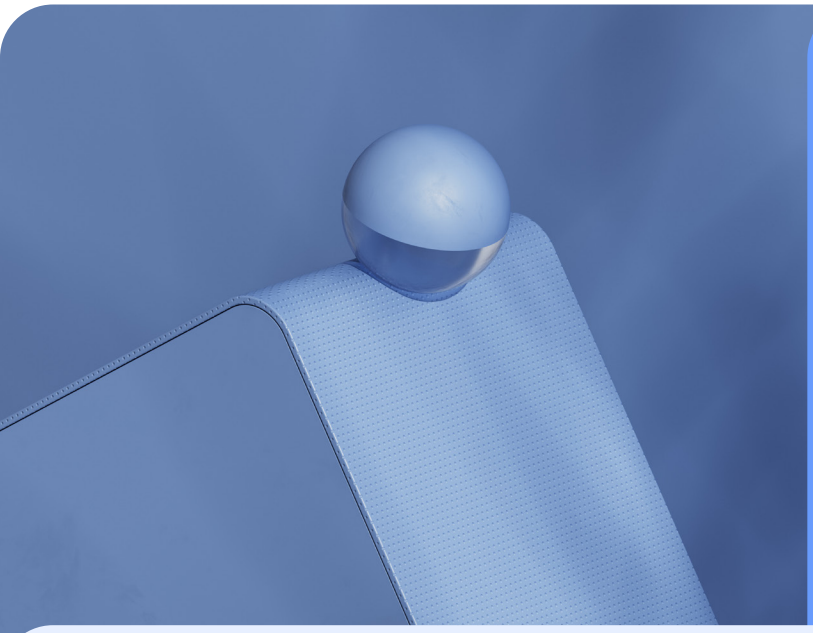
UNSW's experience with Protecht has positioned the cyber risk team to take even bolder steps in modernising their risk and assurance capabilities. Looking forward, the team is exploring several enhancements to deepen automation, improve scalability, and support broader collaboration across the higher education sector.

Key priorities include embedding more AI-driven features into workflows, particularly to support staff who are less familiar with technical policy language. AI tools are being tested to assist with natural-language queries and policy interpretation, reducing friction for end users and supporting self-service.

UNSW is also working on pilots to automate elements of risk formulation and assessment, using input tokens and structured logic to prepopulate risk records and enable faster decision-making. These initiatives are aimed at further streamlining processes while maintaining the human oversight necessary for contextual accuracy.

Finally, as early adopters of Protecht in the cyber space, the UNSW team is committed to helping other institutions benefit from their success. They continue to share templates, JSON files, and practical insights with peer universities, lowering the barrier for adoption and demonstrating the power of community-driven learning in risk management.

> "We've moved away from Excel and encourage using Protecht registers instead."
>
> **Nivi Newar,**
> Deputy CISO, UNSW



"We're designing solutions that extend beyond UNSW and can be adopted and enhanced by other institutions."

**Nivi Newar,**
Deputy CISO, UNSW

## Why Protecht?

UNSW's experience shows how Protecht helps organisations move from reactive, fragmented cyber risk processes to proactive, data-driven management that scales. Key advantages include:

- **Implement IT controls frameworks consistently:** Build trust with customers by establishing a systematic approach to IT control standards and frameworks
- **Provide visibility to information security risk owners:** Help risk owners in the business know what they need to do and how they can achieve it
- **Streamline reporting to boards, executives and regulators:** Provide appropriate insights to boards, executives, regulators and other stakeholders overseeing information security risk management
- **Demonstrate compliance with standards:** Streamline the demonstration of IT standards compliance to achieve certification and give comfort that you are protecting yourself and customers from security risks

## Ready to see it in action?

Book a demo and explore how Protecht can transform your cyber and IT risk management:

Request a demo

**Website**
protechtgroup.com

**Email us**
sales@protechtgroup.com

**Call us**
+61 (2) 8005 1265 (APAC)

+44 (20) 3978 1360 (EMEA)

+1 (833) 328 5471
(US and Canada)

CS-UNSW-GL-2025-10