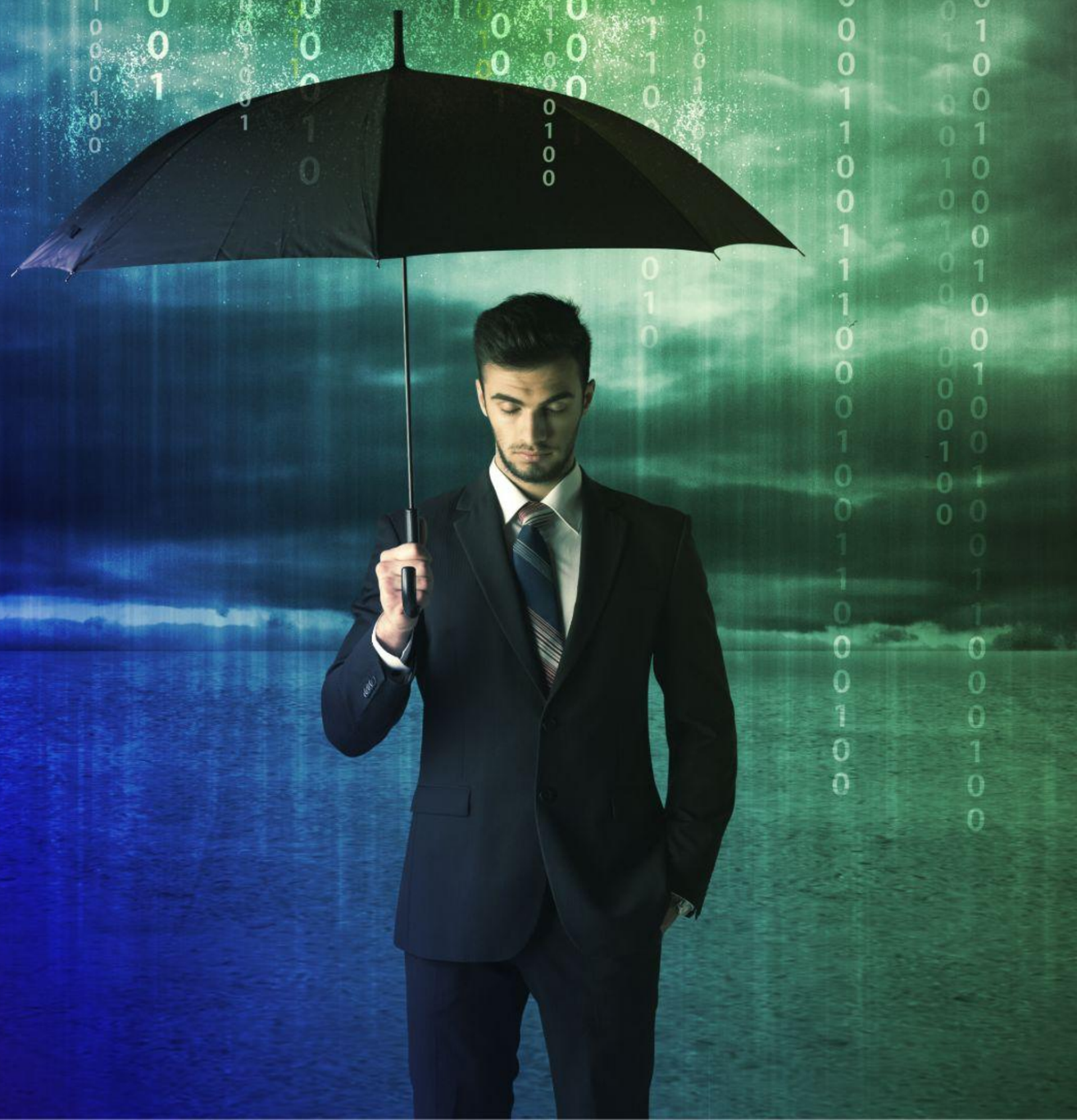
IBRS

Webinar

by Andrew Fox

Beyond The Breach



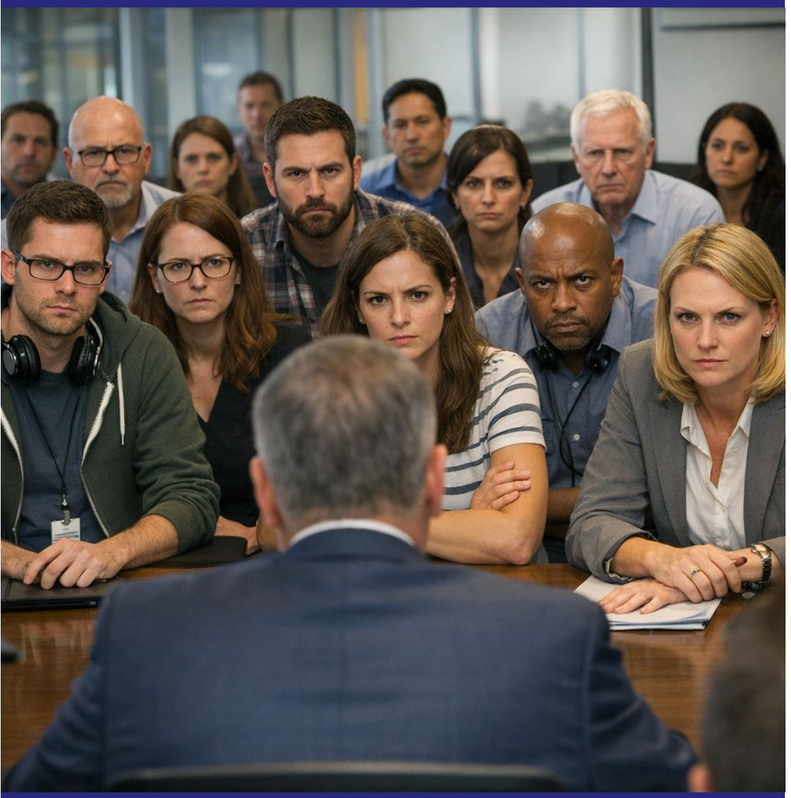
Scope of This Webinar

- Discuss the critical role of the CIO in influencing key stakeholders to effect material improvement in the organisation's cyber security posture.
- Identify the critical internal stakeholders that CIOs must influence to foster a culture of accountability, action and a shared cyber security responsibility.
- Discuss how to leverage tools such as cyber security frameworks and specific controls in these frameworks such as cyber security awareness programs (CSAP), and the organisation’s enterprise risk management (ERM) as communication tools to influence and inform.
- Demonstrate the how to integrate these tools with a stakeholder based approach to gain traction in addressing perennial cyber security bugbears such as legacy technical debt and supply chain risks such as shadow IT.

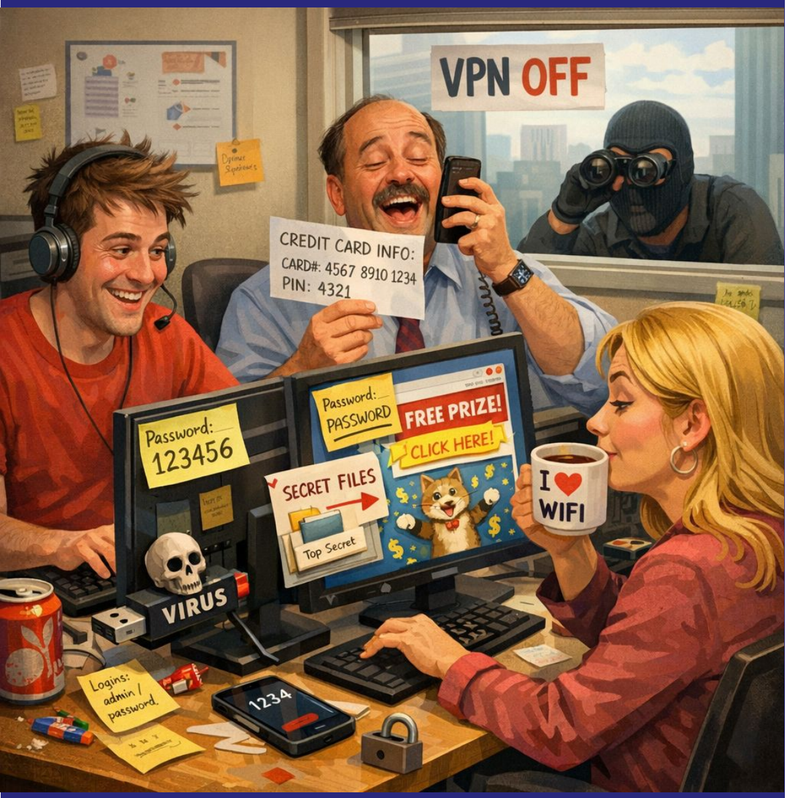
Driving Resilience Through Influential Leadership

In order to build effective cyber resilience a CIO should actively leverage cyber security frameworks in combination with their organisations ERM as strategic communication tools to influence the following critical outcomes:

- Transcending the ‘IT silo mentality to create a culture of shared responsibility
- Converting the organisations employees from being our weakest link into a human firewall
- Converting random acts of security into a structured and efficient program of work
- Encouraging accountability among business systems owners (BSOs)
- Bridging the linguistic barrier with the board
- Securing funding for cyber resilience



Our Stakeholders



The Employee: The Front-Line Threat Vector

"I'm too busy to watch everything I do, I have to get my work done."

The Challenge: Human error (e.g., phishing) remains the single biggest threat vector. How do we change employee behaviour and organisational culture to create a human firewall?

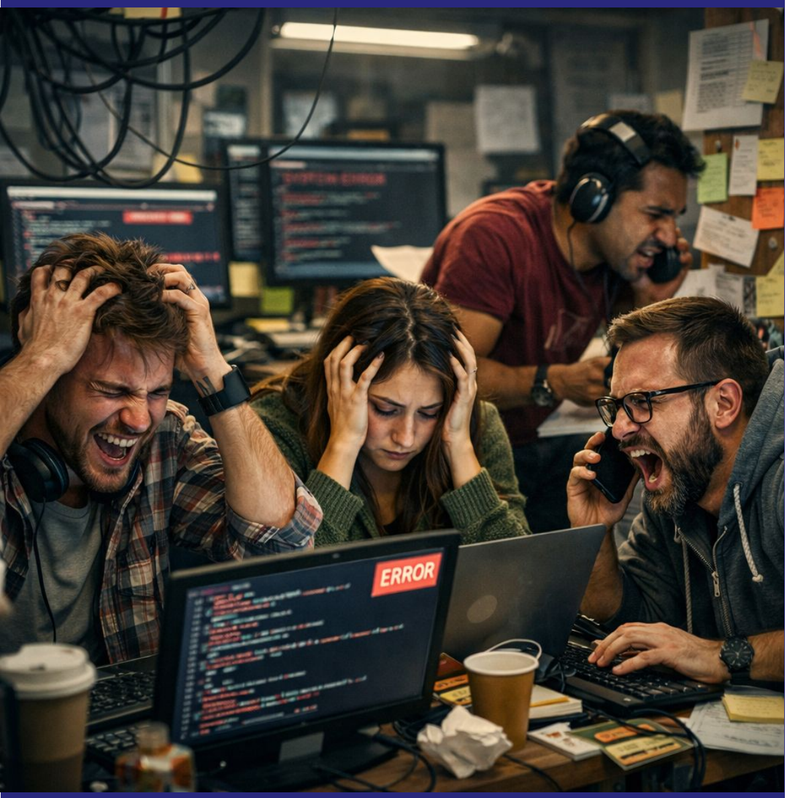
The 2025 Verizon Data Breach Investigations Report (DBIR) found that 60% of all breaches globally involve the human element.

The Approach: Engage employees, change behaviours and influence culture through an effective CSAP that aligns and matures with the controls established in your cyber security framework.

The Benefit: This converts your 'weakest links' into cyber aware individuals and teams who don't click on dangerous links, report suspicious activity, adhere to security protocols and demonstrate support and understanding for the challenges facing their colleagues in IT.

IBRS

May 2026



The IT Worker: Managing the Task Overload

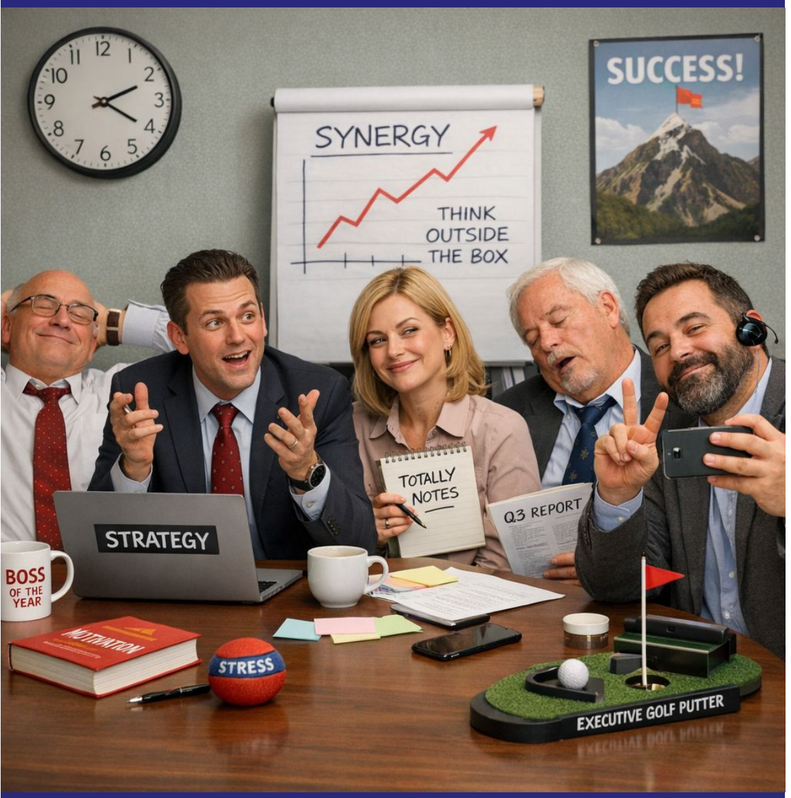
"There are too many tasks for me to execute with too little time and resources."

The Challenge: Overwhelmed by technical debt, infinite patching and requests to implement and integrate new and unfamiliar systems, how do you manage their capacity and capabilities to secure the business?

Sophos' Report, "The Human Cost of Vigilance: Addressing Cybersecurity Burnout in 2025," which surveyed 5,000 IT and cyber security professionals across 17 countries found that 76% of respondents were experienced cyber fatigue or burnout.

The Solution: Drive efficiency and reduce fatigue through cyber security frameworks that provide clear task alignment with prioritisation informed by the organisation's ERM framework.

The Benefit: This moves IT workers from executing 'random acts of security' to executing clearly focused tasks that apply measurable, prioritised and efficient controls informed by the organisation's risk appetite.



The Manager: The Business Systems Owners

"It is IT's job to protect my systems and data."

The Challenge: Managers own the 'crown jewels' (business data and systems) but all too often their abdicate security responsibilities. They are also the primary drivers of poorly or unmanaged 'shadow IT'.

The IBM Cost of a Data Breach Report 2024, revealed that 35% of breaches involved shadow IT.

According to Datacom's 2026 Cybersecurity Index, only 32% of Australian organisations report having a formal business continuity response plan.

The Solution: Drive shared accountability by leveraging your cyber security framework to map control vulnerabilities, while noting system owners, to critical systems and data to inform risk through the ERM framework.

The Benefit: This fosters a culture of responsibility, through clear ownership and informed decision-making, among managers, ensuring that those who own the critical business data and systems are directly informed of risks and their potential impact on business outcomes.

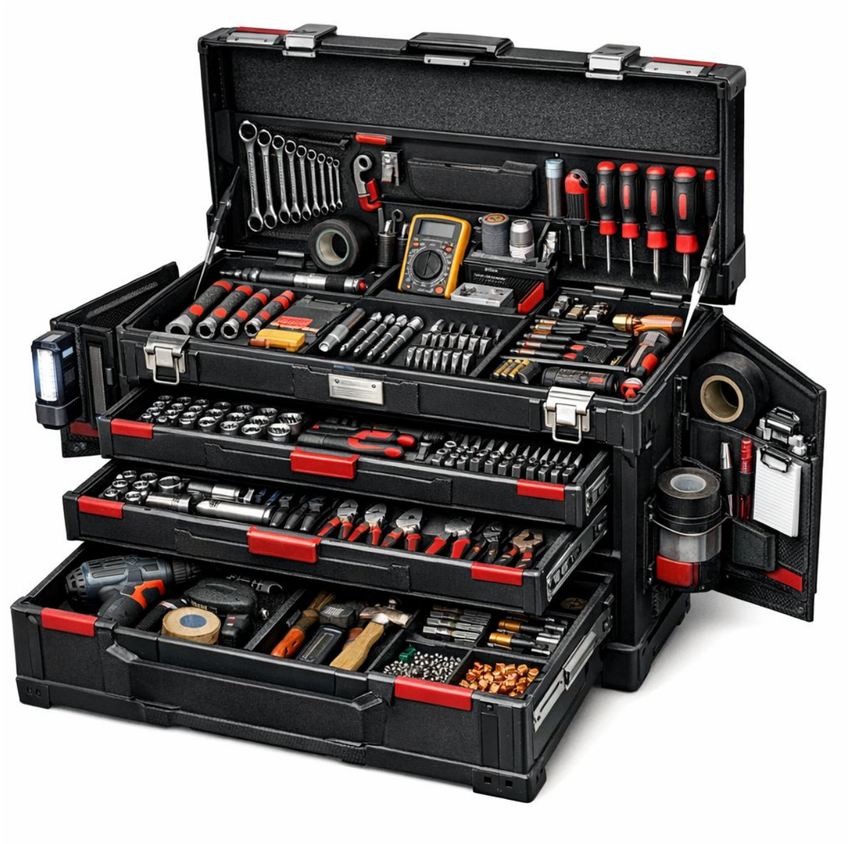
The Board:
The Accountable Authority

"I need to know that we aren't going to get hacked."

The Challenge: The new Cyber Security Priorities for Boards of Directors 2025–26 jointly published by AICD and ASD calls for boards to treat cyber risk as a core business issue, not a technical one, yet directors and CIO's often face a linguistic barrier that divides them. Technical metrics don't effectively inform fiduciary decisions.

The Solution: Speak the board's language by recognising that the organisation's ERM is the primary mechanism for boards to demonstrate they are fulfilling their fiduciary duties in an increasingly litigious and regulated environment.

The Benefit: Leveraging the organisations ERM allows CIOs to translate technical vulnerabilities into business impacts, allowing directors to make informed decisions that allow them to satisfy their fiduciary obligations.



The Tool Box

Cyber Security Frameworks

IBRS

May 2026

Beyond the Breach

Cyber Security Frameworks

- **ACSC Essential Eight (E8):** Mandatory for non-corporate Commonwealth entities (NCCEs) – limited focus on eight technical mitigation strategies (e.g., multi-factor authentication, patching applications, restricting admin privileges).
- **ASD Information Security Manual (ISM):** The ‘big book of rules’ for government agencies and their contractors – a massive list of hundreds of controls tailored to the Australian context.
- **NIST Cybersecurity Framework (CSF) 2.0:** The universal language for talking to boards and international partners – another massive list of structured controls with a focus on building a continuous risk management culture.
- **ISO/IEC 27001:2022:** The "I have a certificate to prove it" framework. It’s an information security management system (ISMS) rather than just a technical list. It focuses on processes, documentation, and continuous improvement.
- **CIS Critical Security Controls:** The ‘quick start’ guide for technical teams – with a focus that is highly prioritised, telling you exactly which 18 controls to do first to stop the most common attacks.
- **Industry-Specific Frameworks:** Such as the AESCSF (Australian Energy Sector Cyber Security Framework)

Poll 1:
Which cyber security frameworks are you using?

- ◯ Essential 8
- ◯ ASD ISM
- ◯ NIST
- ◯ CIS18
- ◯ ISO/IEC 27001
- ◯ An industry specific framework
- ◯ A framework bespoke to your organisation
- ◯ More than one framework

Framework Benefits – *The Employee*

Cyber security framework controls provide the CIOs with concrete tools to influence employee behavior:

- Mandatory awareness and training (CSAPs)
- Creation of a ‘human firewall’ through real cultural and behavioural change
- Provision of clear and enforceable operational guidelines
- Technological behavioral shaping

Framework controls also provide *visible* technical mitigations that serve to reinforce behaviour while providing a safety net when employees inevitably lose focus:

- Restricting privileges
- Multi-factor authentication (MFA)
- Email and web browser protections

Framework Benefits – *The IT Worker*

Cyber security framework controls provide the CIOs with a critical tool to support their IT workers by clarifying responsibilities, standardising operations, clarifying and automating repetitive tasks, to reduce manual toil to prevent burnout and drive efficiency:

- Automation of repetitive configuration
- Structured change management
- Centralised monitoring efficiency
- Automated patching
- Reduction of decision fatigue
- Clarity in asset ownership

Framework Benefits – *The Manager*

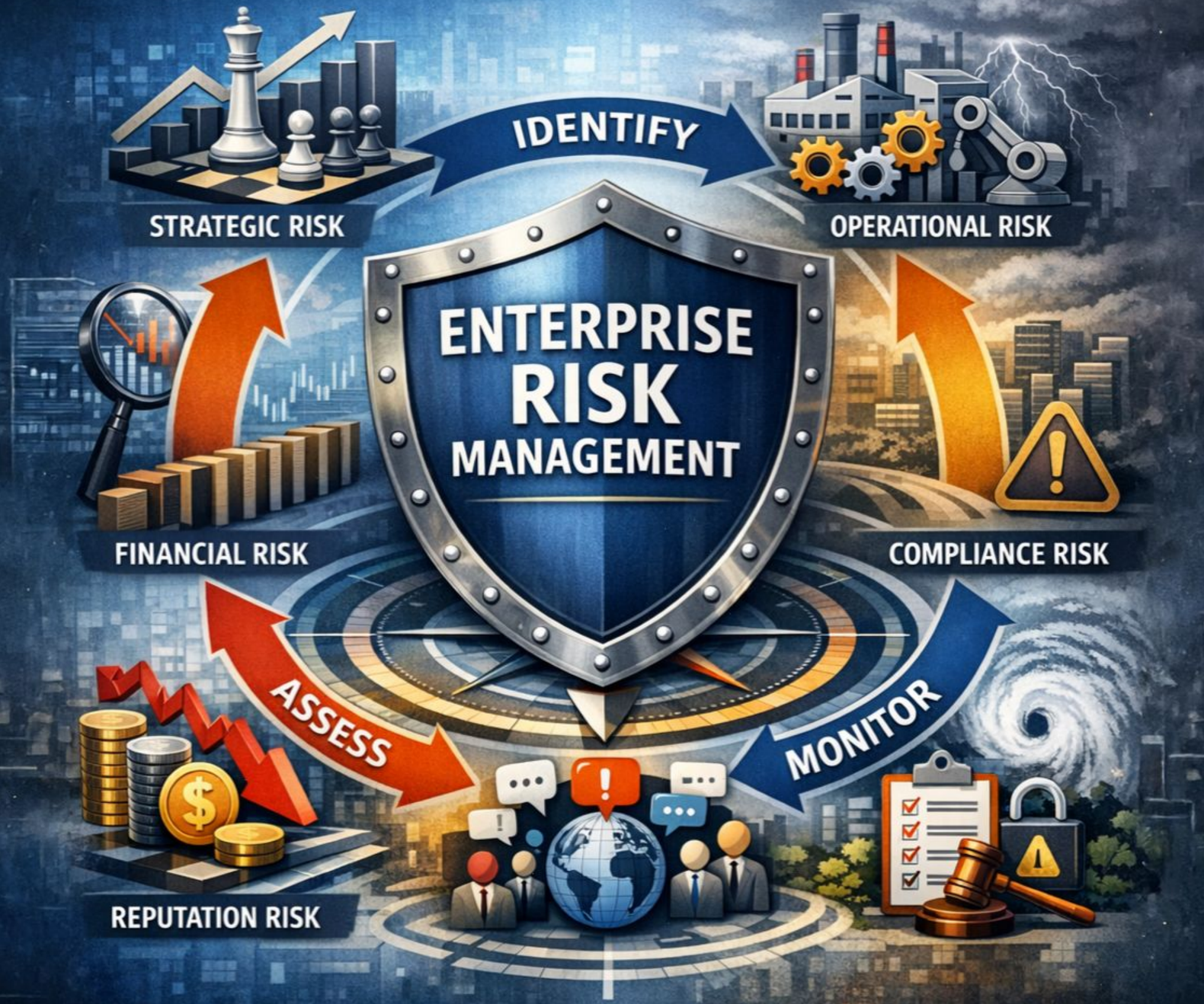
Cyber security frameworks provide a powerful tool to drive accountability for BSOs by defining ownership and ensuring managers are both responsible for their data and systems and are fully aware of the threats against them:

- Designated system ownership
- Direct risk dissemination
- Explicit data ownership
- Acceptance of technical debt
- Asset responsibility and inventory
- Security in design accountability

Framework Benefits – *The Board*

Cyber security frameworks provide CIOs with a toolset to bridge the linguistic barrier with the board by translating technical control gaps into business risk and strategic alignment. Specific controls and control families can help with providing

- Risk framing
- Penetration testing
- Maturity level reporting
- Governance accountability
- Management review
- Measures of performance


IDENTIFY
STRATEGIC RISK
OPERATIONAL RISK
ENTERPRISE RISK MANAGEMENT
FINANCIAL RISK
COMPLIANCE RISK
ASSESS
MONITOR
REPUTATION RISK

Enterprise Risk Management (ERM)

The list of risk frameworks used by Australian organisations to ensure that technical risks such as cyber are managed within the broader context of business objectives is a short one.

- ISO 31000:2018 Risk Management Guidelines.
- COSO Enterprise Risk Management (ERM) Framework.
- NIST Risk Management Framework.
- COBIT (Control Objectives for Information and Related Technologies)
- Industry-Specific Frameworks such as the APRA Prudential Standards

Poll 2: How is cyber security framed within your organisations ERM?

- ◯ Cyber security is a top 5 risk on the enterprise risk register
- ◯ Cyber security is a top 10 risk on the enterprise risk register
- ◯ Cyber security is on the enterprise risk register but is not in the top 10
- ◯ Cyber security is not considered in the enterprise risk register
- ◯ We have no enterprise risk management process

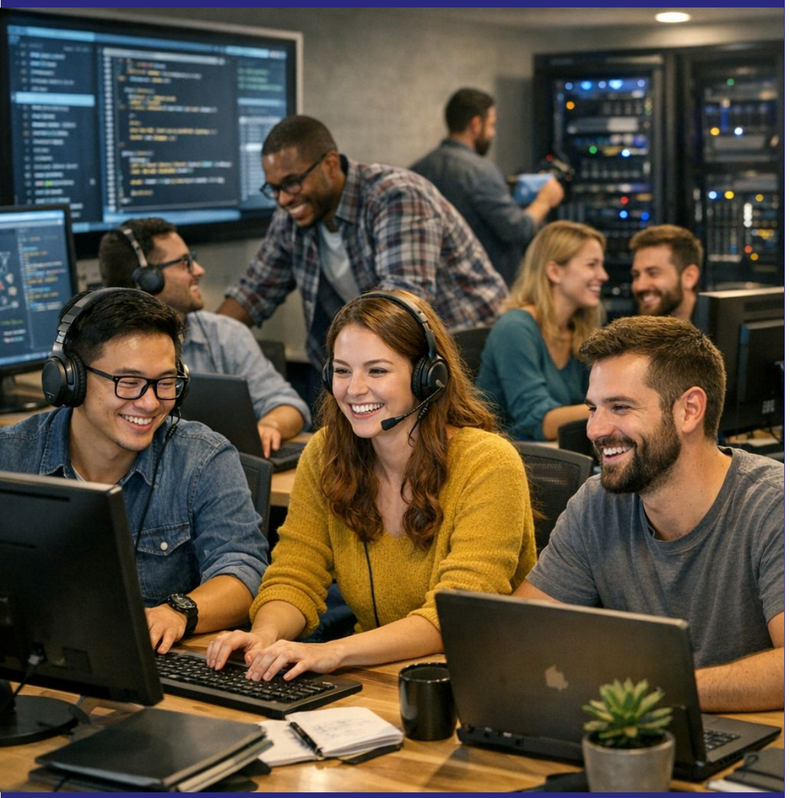
IBRS

May 2026

The Employee: Humanising Risk

Integrating cyber security into the ERM framework helps employees understand how their personal actions impact the organisation’s overall resilience and mission, transforming security into a shared responsibility.

- Connects individual cyber hygiene to business impacts and job security.
- Shifts the narrative from ‘IT compliance’ to protecting shared organisational value.
- Uses ERM risk categories (financial, reputational) to explain the 'why' behind security controls.
- Incentivises risk-aware behavior by linking security metrics to performance and resilience.
- Reduces the prevalence of unmanaged shadow data by clarifying its impact.
- Fosters a culture of psychological safety where employees can report errors as risk events without fear.
- Simplifies cyber awareness by focusing exclusively on the most critical enterprise-level risks.



The IT Worker: Efficiency Through Prioritisation

Aligning technical tasks with the ERM enables IT workers to move away from firefighting to focus their capacity and expertise on the most critical threats that jeopardise the organisation's strategic goals.

- Supports the eradication of random acts of security by aligning daily tasks with the enterprise risk.
- Provides a data-driven basis for prioritising technical debt retirement.
- Reduces burnout by establishing a ‘risk-based triage’ for high-priority tasks.
- Clarifies the organisation’s risk appetite, allowing teams to stop over-securing low-risk assets.
- Justifies budget and headcount requirements by articulating gaps in risk mitigation capabilities.
- Aligns tactical security operations with board-approved risk tolerance and strategic goals.
- Facilitates cross-functional collaboration using a shared language of risk between the business and technical teams.

The Manager: Enforcing Ownership

By aligning technical risks with business outcomes in the ERM, managers gain clarity about their ownership of risk and gain a view of security investments as critical to operational continuity.

- Maps technical vulnerabilities directly to specific business systems and revenue streams.
- Translates shadow IT into unmanaged business risks that managers must acknowledge and own.
- Encourages ‘security in design’ by integrating ERM checkpoints into the procurement lifecycle.
- Justifies cyber expenditure as a critical operational investment
- Links security maturity directly to departmental business continuity and disaster recovery plans.
- Formalises the legal and operational acceptance of residual risk.
- Provides managers with visibility on how their choices affect the organisation's overall risk posture.

The Board: Fiduciary Oversight

Leveraging the ERM allows the CIO to provide the board with a transparent, unified view of cyber risk, enabling governance that aligns investments with the board's fiduciary goals and risk appetite.

- Translates complex technical jargon into the board's own language.
- Demonstrates proactive governance and compliance.
- Aligns the cyber security investment roadmap with the board's explicitly defined risk appetite.
- Frames cyber resilience as a core capital investment in business sustainability.
- Delivers a clear 'risk scorecard' benchmarking posture against enterprise-wide standards.
- Facilitates informed strategic trade-offs between business growth and tolerable risk levels.
- Streamlines regulatory reporting (e.g., SOCI Act) using ERM as the single source of truth.

Integrating the Tool Box

Case Study: The RMF Lifecycle for a CRM

The example below demonstrates how leveraging your cyber security and risk management frameworks together to implement a new CRM application bakes security into the system lifecycle.

RMF Phase	*Key Activity*	*CRM Application Example*	*Involved Personas*
Governance	Risk Framing	Strategic determination that a breach of customer personally identifiable information (PII) is a 'high' risk.	**Board**
Preparation	HVA Identification	The CRM is registered as a high value asset (HVA) and inherits common identity controls.	**BSO, IT Worker**
Categorisation	Security Impact	High impact for confidentiality; moderate impact for integrity and availability.	**BSO, IT Worker**
Selection	Control Selection	Mandatory MFA and encryption-at-rest are selected to protect PII.	**BSO, IT Worker**
Implementation	Configurations	Engineers configure database encryption and corporate MFA integration.	**IT Worker, BSO**
Assessment	Verification	Assessors run penetration tests to confirm data is inaccessible without MFA.	**IT Worker**
Authorisation	Risk Decision	Authorising official reviews the package and issues an authorisation to operate (ATO).	**Board, BSO**
Monitoring	Vigilance	Teams monitor for unauthorised access; end users act as sensors for suspicious activity.	**IT Worker, BSO, End User**

Governance: Persona Process Flow

Strategic

The board sets risk appetite, signaling to business owners which assets (like the CRM) require the most protection.

Technical

IT workers translate business needs into technical specifications and implement the necessary safeguards.

Accountable

The business owner remains accountable for security, while the board formally accepts the risk to the enterprise.

Vigilant

IT workers monitor logs while end users act as sensors by reporting anomalous or suspicious system activity.

This process flow *ensures that risk management is a cohesive organisational effort rather than a siloed IT task.*

Governing Technical Debt

Ensure that technical debt isn't perceived as IT issue, but as an unmanaged business liability.

Risk Framing	Move from 'outdated server' to 'foreseeable operational harm' in the enterprise risk register.	■ Recognise technical debt as a fiduciary risk to business continuity. ■ Quantify the 'Cost of Failure' vs. the 'Cost of Upgrade'.
Ownership Enforcement	Map legacy systems to the BSOs who derive value from them.	■ The BSO formally acknowledges that their system is a 'high value asset' with 'critical' vulnerabilities. ■ Technical debt is now a departmental risk, not an IT overhead.
Execution Efficiency	Utilise the data on the IT worker's manual toil to prioritise retirement roadmaps.	■ Demonstrate how legacy maintenance drains capacity from strategic growth.
Formal Acceptance	Require the authorisation to operate (ATO) decision for every legacy system.	■ If the BSO/board refuses to fund the upgrade, they must formally sign the risk acceptance for a breach.

Governing Shadow IT

Prevent the unvetted entry of shadow IT into the organisation's supply chain.

Governance & Risk Framing	Redefine the supply chain perimeter at the board level to include any SaaS or 3rd-party service handling company data.	■ Establish that unauthorised vendor onboarding is a breach of the risk tolerance. ■ Frame BSO-driven shadow IT as a high-risk operational liability rather than innovation.
Asset Categorisation	Mandate that BSOs register all departmental tools in the enterprise HVA list.	■ The BSO must determine the impact if the shadow vendor's PII is breached (e.g. confidentiality: High). ■ If a BSO fails to register a tool, they are bypassing the enterprise control framework.
Technical Vetting & Implementation	IT workers utilise discovery tools to unmask shadow IT and map it against the organisation's supply chain standards.	■ Evaluate the vendor's security posture (e.g. SOC2, MFA integration) before the contract is finalised.
Authorisation Gate	Require a formal authorisation to operate (ATO) for any system accessing enterprise data or identity services.	■ If a BSO insists on a high-risk shadow vendor, they must formally accept the financial/legal liability for a breach.


Questions?
IBRS

IBRS | ANALYSIS INSIGHT JUDGEMENT

IBRS is a boutique Australian ICT Advisory Company.

We help our clients mitigate risk and validate their strategic decisions by providing independent and pragmatic advice while taking the time to understand their specific business issues.

https://ibrs.com.au info@ibrs.com.au 02 4758 9111 PO Box 519, Hazelbrook NSW 2779, Australia