QRMC RISK, SAFETY AND BUSINESS ADVISORY CONSULTANCY

insight
QRMC NEWSLETTER

Issue 155 May 2025

Insight aims to provide useful information, links and tips in the areas of Risk Management, Work Health and Safety, Business Continuity Management, and other areas relating to management systems and corporate governance.

What's the Difference between an Enterprise Risk Register and a WHS-Specific Strategic Risk Register?

In risk management, both the enterprise risk register and the Work Health and Safety (WHS) specific risk register are crucial tools used to identify, assess, and manage risks within an organisation. However, they each serve distinct purposes, focus on different types of risks, and require unique methodologies and legislative considerations.

There are some obvious differences in **Purpose and Scope**, with the Enterprise Risk Register (ERR) capturing all the business's risks (ranging from strategic, financial, operational, to reputational risks that have the ability to impact on the business objectives), versus the WHS-Specific **Risk Register** focuses solely on health and safety risks that have the capacity to affect workers, contractors, and visitors within the workplace.

From a **legislative perspective**, while it makes good business sense to implement an ERR, there is no specific legislative requirement that mandates one. Organisations are encouraged to follow guidelines like those provided by ISO 31000 (Risk Management). This standard offers a framework for identifying, assessing, and managing a wide array of risks at the enterprise level. However, specific sectors (e.g., finance, healthcare) may have regulatory requirements to manage certain types of risks. Conversely, a WHS risk register, whilst not directly required under WHS legislation, is generally accepted as the best way to provide evidence of the identification, prioritisation and management of WHS risks (which is required under the WHS legislation).

In relation to **Risk Identification and Assessment,** ERR risks are typically identified through strategic workshops, and audits; and then assessed, based on their potential impact on the organisation's goals. On the other hand, WHS-risks require workplace-level identification processes that consider the environment and work processes that could cause

workers harm. This process is underpinned by legislative requirements.

The **Risk Management Methodology** also varies between the two. The ERR follows a more strategic framework, whereby organisations may choose from various mitigation strategies such as transferring, avoiding, accepting, or reducing the risks. The risk management process also includes setting risk tolerance thresholds or risk appetites. In relation to the approach for managing WHS risks, the methodology is more prescriptive, with the legislation mandating that risks are to be eliminated, or "*if it is not reasonably practicable to eliminate risks to health and safety, to minimise those risks so far as is reasonably practicable*" (as per Sec 17 of the WHS Act). To achieve this, it is prescribed that the hierarchy of controls (WHS Regulation s.36) are applied.

Between the two, the response to the **Residual Risk Score** also varies, with the 'high' or 'extreme' risks on an ERR able to be considered 'acceptable' within business operations depending on the risk appetite of the organisation, whereas for WHS, risks at this level are certainly not acceptable. 'Extreme or High' WHS risks typically warrant a 'shutting down' of the work, and raising of the issue with Senior Management, and then the development of control measures that will lower the risks to a level that is as low as reasonably practicable.

In general, distinctions between the 2 registers all stem from their context: an ERR focuses on a broader organisational perspective, supporting strategic decision-making; while a WHS-specific register requires consideration of the risks that have the potential to harm workers and others on the workplace.

Please contact QRMC for more information.

Preparing for Queensland's New Privacy Laws: What organisations need to know

The *Information Privacy and Other Legislation Amendment Act* 2023 (IPOLA Act) introduces significant reforms to Queensland's privacy laws, impacting government agencies (state Ministers, state departments, local governments, and public authorities) and their contracted service providers. Most changes are set to commence on 1 July 2025, with some provisions for local governments delayed until 1 July 2026.

Key changes affecting businesses engaged with government agencies

1. **Unified Privacy Principles**: The IPOLA Act replaces the existing Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) with a single set of Queensland Privacy Principles (QPPs), aligning more closely with the Australian Privacy Principles under the Commonwealth Privacy Act 1988.
2. **Mandatory Data Breach Notification**: Agencies and their service providers must notify the Information Commissioner and affected individuals of eligible data breaches—those likely to result in serious harm—within 30 days of becoming aware of the breach.
3. **Privacy Complaint Handling**: Agencies are required to respond to privacy complaints within 45 business days. If unresolved, complainants may escalate the matter to the Information Commissioner.

Action steps for businesses engaged with government agencies

- **Review and Update Privacy Policies**: Ensure your privacy policies and collection notices comply with the new QPPs.
- **Develop Data Breach Response Plans**: Implement procedures to detect, assess, and respond to data breaches promptly.
- **Train Staff**: Educate employees on new privacy obligations and data handling practices.
- **Audit Information Handling Practices**: Assess current practices for collecting, storing, and disclosing personal information to identify areas needing improvement.

Businesses engaged with government agencies should obtain legal advice for their specific circumstances and take proactive steps to ensure compliance. For more information refer to the Office of the Information Commissioner Queensland's resources here.

Please contact QRMC for more information.