QRMC RISK, SAFETY AND BUSINESS ADVISORY CONSULTANCY

insight
QRMC NEWSLETTER

Issue 140 October 2023

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.

Simplifying Information Security Management

In our increasingly digital world, the term "Information Security Management System" (ISMS) might sound complex and intimidating, but at its core, it's just a structured and organised approach to keeping an organisation's information safe.

What is an ISMS?

An Information Security Management System (ISMS) is a set of rules, processes, and practices that an organisation develops and follows to protect its information from theft, damage, or unauthorised access. This includes both digital and hardcopy information. Think of it as a comprehensive plan for keeping your valuable data safe, like the locks on your doors and windows at home. An ISMS should typically incorporate employee conduct and procedures, in addition to data and technology.

Why is it Important?

1. Data Protection: An organisation's digital information is like a treasure trove. It can be customer data, financial records, trade secrets, or personal information. An ISMS outlines the systems and processes that keeps your information safe from potential intruders.

2. Legal Compliance: Laws and regulations around data protection are getting stricter. An ISMS helps your organisation follow these rules, avoiding breaches, legal non-compliance and fines.

3. Customer Trust: People want to know that their data is safe with you. When you have a robust ISMS in place, it sends a clear message to your customers that you take their privacy seriously.

4. Business Continuity: Unexpected disasters can disrupt your operations. An ISMS includes plans to ensure you can keep running smoothly even in challenging situations.

How Does It Work?

An ISMS does not have to be overly complex and should be developed to suit your organisation using the following few basic principles:

1. Risk Assessment: Imagine you're protecting a castle. First, you identify weak points in the castle's defences, such as a broken wall or a loose gate. In the digital world, this means finding vulnerabilities and risk exposures in your systems that hackers could exploit.

2. Security Measures: Once you've spotted the weak points, you put up controls or defences, like fixing the broken wall or reinforcing the gate. In the digital world, this means installing security software, setting up firewalls, and creating strong passwords.

3. Regular Monitoring: A good castle doesn't just protect against one attack and then stop. You need to keep watch to make sure everything stays secure. In the digital realm, this means ongoing monitoring, software updates, and regular checks for security issues.

4. Incident Response: Sometimes, even with all the precautions, a castle might face an attack. You need a plan for how to respond - whether to call for reinforcements, evacuate, or negotiate. In the digital world, this is your response to a data breach or cyberattack.

Who Needs It?

All organisations that manage data should have some form of ISMS, from small businesses to big corporations, government agencies, healthcare providers, and financial institutions. If you collect, store, or use data, you need to protect it.

In simple terms, an ISMS is your information security strategy. It's your way of making sure your digital treasure remains safe, your customers trust you, and you're prepared for any potential threats. Understanding and implementing an ISMS is becoming crucial and expected in our digital age.

ISO 27001 is the international standard for information security. Its framework requires organisations to identify information security risks and then develop appropriate controls to manage these risks. The full name of the standard in Australia is AS/NZS ISO/IEC 27001:2023 *Information security, cybersecurity and privacy protection - Information security management systems – Requirements*. We will explore how to go about implementing an ISMS using ISO 27001 in a follow up article.

Please contact QRMC for more information.

The Current Challenges with WHS Resourcing

One of the key duties placed upon the WHS Officer(s) of an organisation is to "*ensure that the person conducting the business or undertaking has available for use, and uses, appropriate resources and processes to eliminate or minimise risks to health and safety*". Typically, these resources come in the form of *financial* resources (allocated budgets, monies and equipment) and *human* resources (both quality and quantity of personnel to complete the activities of the WHS function, as well provision of related training).

Getting suitably qualified and experienced WHS people to fill these roles, however, is proving difficult for a lot of organisations in the current employment market. And if you are in a rural or remote area, this can be extremely challenging with some WHS roles currently remaining vacant for months on end.

There are many reasons why this is the case at the moment, including:

- The July 2023 update from the Australian Bureau of Statistics currently has Australia's unemployment rate at 3.5 %. While not a historic low, the unemployment rate coming out of COVID has been trending downwards and is comparably low. A quick glance at SEEK reveals there are currently over 5,500 job opportunities for WHS-related jobs around Australia. This number continues to grow as organisations recognise their duties for WHS and compliance with legislative requirements.
- Although the employment demographics tell many stories, one that is universal across all industries is that younger people are changing jobs more often and staying long-term with one employer less often.
- There are not many full-time WHS roles based in rural and regional Australia, so many qualified and experienced professionals seek employment in the major cities, leaving voids in local job markets.
- Furthermore, there is no doubt that the remuneration for qualified and experienced WHS professionals is higher in the cities than it is in the regions, and this is contributing to longer-term vacancies in regional locations.

Muddying the water somewhat is that, to be employed in a WHS-related role, it is not essential to have a WHS-related qualification. So where does this leave the need for organisations to both "ensure" and make "appropriate" resources available?

Potential solutions here could include:

- Flexible employment arrangements such as job-sharing, which allows for the WHS function to be shared with another organisation or within another department or individual internally.
- Greater use of Health and Safety Representatives (HSRs) to perform routine safety tasks such as WHS inspections, risk assessments and lower-level incident investigations.
- Looking longer-term to train up HSRs or other interested internal resources (e.g. Training or HR) to have then 'grow into the role'.
- Re-engaging with recent retiree WHS Advisers to provide flexible and short-term support.
- Use of self-help technology solutions to complete routine safety activities such as worker/contractor inductions, logging of WHS incidents, and generation of WHS statistics and reports.

One important consideration for organisations is that when managing high and extreme WHS risks particularly, expert advice should be sought. Relying on advice for these critical risks by WHS personnel just learning their safety skills may not be enough to meet the "ensure" and "appropriate" definition tests.

Leadership and commitment to WHS at the highest level within an organisation is another essential part of ensuring appropriate resourcing is maintained. It is a challenging job market at the moment, so organisations need to be innovative, flexible and committed to making their WHS resourcing a priority.

Please contact QRMC for more information.