QRMC RISK, SAFETY AND BUSINESS ADVISORY CONSULTANCY

insight
QRMC NEWSLETTER

Issue 141 November 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.

Developing and Implementing an Information Security Management System (ISMS)

Following on from our previous article on Simplifying Information Security Management, this month we will look at how to go about developing an ISMS.

Given the current spate of cyber security-related attacks and data breaches across Australia, having an effective Information Security Management System is becoming essential to protect your data, demonstrate good governance and instil customer confidence.

The most important concept to keep in mind is that an ISMS does not need to be overly complex. A good starting point is to look at the requirements of the international standard AS/NZS ISO/IEC 27001:2023 *Information security, cybersecurity and privacy protection – Information security management system–Requirements*, that provides the framework for developing and implementing an ISMS. The new standard was published in 2022 and in many respects, simplifies what is required of an ISMS.

Like all current management system standards, ISO 27001 applies the Annex SL that provides the overarching structure for the standard within the 10 regular headings:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organisation
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

However, ISO27001 is more granular than most standards and goes on to specify an *Annex A Information Security Controls*. This includes 93 Controls that are grouped into 4 themes:

- People (8 Controls)
- Organisational (37 controls)
- Technological (34 controls)
- Physical (14 controls)

These controls are directly derived from and aligned with those listed in ISO/IEC 27002:2022 *Information Security Controls* that now allocates five 'attributes' to make them easier to categorise:

1. Control type – when and how the control modifies the risk (preventive, detective, corrective)
2. Information security properties – which characteristic of information the control is targeted at (confidentiality, integrity, availability)
3. Cyber security concepts – the association of the controls to cybersecurity concepts within ISO/IEC TS 27110 (identify, protect, detect, respond, recover)
4. Operational capabilities – from the practitioner's perspective of information security capabilities (governance, asset management, information protection, Human Resource Security etc.)
5. Security domains – one of four information security domains (governance and ecosystem, protection, defence, resilience)

In most cases not all 93 controls apply to all organisations: a business must formally consider and substantiate any exclusions in a Statement of Applicability.

The task of developing an Information Security Management System from scratch can appear overwhelming due to the detailed and extensive requirements of the standard. However, in practice, most businesses probably already have both formal and informal processes in place, which can serve as a strong foundation for establishing their Information Security Management System.

A starting point would be to acquire the AS ISO/IEC 27001:2022 Standard and then conduct a Gap Analysis, identifying what requirements are currently in place and where there are gaps.

Please contact QRMC for more information.

It's beginning to look a lot like Christmas …

As we approach the Festive Season and the end of the year, it's important to be particularly aware of the 'seasonal' trends in mental health impacts. While Christmas is a portrayed as a time for families to reconnect and relax, there is an established pattern of mental health concerns that come to the fore at this time of year.

It is more than likely that your organisation will have its fair share of workers going through a rough period at this time, as the Christmas period is renowned for bringing home mixed feelings for those without family, with difficult personal relationships, or who have lost loved ones. And if we overlay this with the heightened workload demands – with that usual end-of-year push to get projects finalised before the break (which is either forced upon us from Management or self-imposed by our own professionalism) – it makes for a 'perfect storm'. (And if you give credit to the theory that the lunar cycle affects our mental health there may be an influx of concerns with the full moon due on Dec 27th.)

So, it is timely to look at how to focus on supporting our workers through this period.

The introduction of the Managing the Risk of *Psychosocial Hazards at Work Code of Practice* this year highlighted that PCBUs have a responsibility to manage the psychosocial (mental) health of their workers. It made us realise that, as an industry, we have become used to the mechanisms of managing the adverse mental health impacts (e.g. via the use of EAP providers and our on-site Mental Health First Aiders), but how good are we at identifying and managing the preventative side of the risk?

Does your organisation have programs or processes in place that are truly proactive and preventative in nature, and do not rely on a 'breakdown' event?

On the positive side of things, yes, there has been an emergence of mental health awareness and resilience training and a marked increase in the uptake on EAP usage, and there is much more open and normalised discussion about the mental health challenges we are facing, and the impacts – both psychological and physical – that these are having on us. This is a really positive starting point, but it also serves as a further reminder that we need to do more, get more focussed on this risk area, and get proactive.

Comcare recently reported that unsafe job demands are the most common psychosocial hazard in Australian workplaces, calling for improvements in the design of work like scheduling work to avoid intense or sustained workloads, planning shifts to allow adequate rest and recovery, planning work to avoid large fluctuations in demand, and reconsidering resourcing

requirements. This indicates that there is a need for engagement and regular conversations with staff about work expectations, workloads and deadlines, client or customer demands, and all the other stuff that is going on in the background, as well as implementing processes for the early escalation of concerns before they become bigger problems.

Perhaps we could also use the Festive Season as a reminder to stop, take a breath and make a conscious effort to be a little kinder to everyone as we approach this holiday season.

Holiday Wishes

This edition of *Insight* is the final for 2023. The first edition in the New Year will be issued in February 2024.

QRMC Risk Management Pty Ltd will be closing over the Christmas period, from close of business Friday 15 December, reopening Monday 8 January 2024.

QRMC wishes all our clients, supporters and readers a relaxing, happy and safe holiday season. We look forward to your company in the New Year!