QRMC RISK, SAFETY AND BUSINESS ADVISORY CONSULTANCY

insight

QRMC NEWSLETTER

Issue 143 March 2024

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.

Chain of Responsibility

The Victorian sentencing of a trucking scheduler, following an incident which tragically resulted in the death of four Police Officers, highlights the responsibilities under the Heavy Vehicle National Law on those performing supervisory and scheduling roles.

The prosecution provided evidence that the scheduler / supervisor was warned that the driver was not in the right mental or physical state to drive a truck, but this warning was not heeded, with tragic results. This is a timely reminder that everyone working in the supply chain for the transporting of goods via Heavy Vehicles (for vehicles with GVM greater than 4.5 Tonnes) has a responsibility under the *Heavy Vehicle National Law (HVNL)* and its supporting state-based legislation.

The *Heavy Vehicle National Law (HVNL)* came into play throughout most of Australia around 10 years ago, imposing a framework of duties/responsibilities on all parties within the supply chain from the raw producer of goods through to the end user. The responsibilities are structured around which role(s) you fulfill in the supply chain, and recognise that a single person may fulfil a range of roles including consignor, packer, loader, driver / operator, unloader, and scheduler. Each of the roles has an ability to influence the Supply Chain, and some overlap with the common goal of ensuring the safe use of the road when transporting goods.

The primary duty of the HVNL mirrors the approach from the WHS laws, with the requirement for each role to manage the risks associated with their transportation activities. In other words, it is no longer just the driver carrying the responsibility for the safe transporting of goods via heavy vehicles.

There is still work to be done to address these requirements, as reflected within the Australian Government's annual Road Trauma Involving Heavy Vehicles Report. The 2023 Report details that there are still high numbers of accidents involving heavy vehicles on Australian roads – representing 17% of all road fatalities (equating to 764 hospitalisations). These statistics have remained fairly consistent since the introduction of the HVNL, so there is still much to do to implement a supporting and robust risk management program around organisations' heavy vehicle and transportation activities, regardless of where you sit within the Chain of Responsibility.

Please contact QRMC for more information or assistance.

The Growing Importance of Information Security

In our previous articles on Information Security Management, we have discussed Information Security Management Systems (ISMS) and the need to keep them simple.

The international standard AS/NZS ISO/IEC 27001:2023 *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*, is a risk-based standard that requires organisations to consider their risks relating to information security, and then implement the required controls to manage these risks.

For many businesses, the thought of implementing yet another management system may seem overwhelming and unnecessary. It must be recognised, however, that a management system is simply a structured manner to document an organisation's approach to a risk: in this case, information security.

At its core, any Management System should satisfy 3 simple steps:

1. "***Say what you do***" – The necessary policies, procedures, guides, instructions etc.
2. "**Do what you say**" – The implementation of these documents throughout the organisation, with implementation referring to the complete spectrum from strategic to operational.
3. "**Prove it**" – The ability of an organisation to be able to verify that the system is current, implemented in all relevant areas, evaluated and reviewed for effectiveness, and is achieving its objectives.

This approach provides a simple mantra: 'Say it,' Do it,' 'Prove it.'

These 3 steps must be considered when developing an ISMS, even for smaller organisations. While certification to ISO 27001 is not currently a universal requirement, larger organisations and many government agencies are moving towards the implementation of an ISMS being mandatory.

For example, the Queensland Government's Information security policy (IS18:2018) mandates that Departments must implement and operate an ISMS based on the current version of ISO 27001.

A starting point for any organisation in wanting to develop an ISMS is to review the context of the organisations information security risks using the ISO 27001 standard controls. These are contained within the standard's *Annex A Information Security Controls* and include 93 Controls grouped into 4 themes:

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

Very seldom will all 93 controls apply within an organisation, hence it is important to review what is applicable to the organisation (noting that of the 93, only 34 are actually Technological or IT related, with the rest being People, Organisational and Physical controls).

Mapping these controls within the context of the organisation is the first step towards demonstrating an awareness of your information security risks, and can assist you towards the development of a simple and effective ISMS.

Should your organisation require assistance, please contact QRMC for more information.

The material contained in this publication is in the nature of general comment only and neither purports, nor is intended, to be advice on any particular matter. No reader should act on the basis of any matter contained in this publication without considering and, if necessary, taking appropriate professional advice regarding their own particular circumstances.