Enhancing Cyber Security and Asset Management Standards in the Australian Mining and Minerals Sector

WHITE PAPER

June 2023

RMIT UNIVERSITY
Centre for Cyber Security Research and Innovation

JASANZ

Australian Government
Department of Industry, Science, Energy and Resources

Acknowledgement of Country

RMIT University acknowledges the people of the Woiwurrung and Boon wurrung language groups of the eastern Kulin Nations on whose unceded lands we conduct the business of the University. RMIT University respectfully acknowledges their Ancestors and Elders, past and present.

RMIT also acknowledges the Traditional Custodians and their Ancestors of the lands and waters across Australia where we conduct our business.

Artwork: *Luwaytini* by Mark Cleaver, a proud Palawa person and RMIT Master of Human Resource Management student.

Acknowledgements

This White Paper is a result of the collaboration between the RMIT Centre for Cyber Security Research and Innovation (CCSRI) and the Joint Accreditation System of Australia and New Zealand (JASANZ). JASANZ's involvement in the study has been facilitated through support from the Australian Government, Department of Science, Industry and Resources. Special thanks to RMIT Staff involved: Dr Arezoo Ghazanfari, Dr Banya Barua, Dr Konrad Peszynski, Dr Abebe Diro, Lee-ann Phillips, Amal Varghese, Professor Matthew Warren and Laki Kondylas.

The RMIT University Centre for Cyber Security Research and Innovation

The RMIT University Centre for Cyber Security Research and Innovation (CCSRI) is a multi- disciplinary research centre that draws researchers from across RMIT's schools and colleges to bring a truly multidisciplinary approach to the organisational, human, and technical aspects of cyber security.

The Joint Accreditation System of Australia and New Zealand (JASANZ)

The Joint Accreditation System of Australia and New Zealand (JASANZ) helps markets work better by providing internationally recognised accreditation services that create economic benefit. JASANZ accredit the bodies that certify or inspect organisations' management systems, products, services or people. It specifies the assessment criteria that certifiers and inspectors must meet to become accredited within industry sectors.

Contents

Terminology

The following terms are used in this White Paper:

ACSC refers to the Australian Cyber Security Centre, the organisation that leads the Australian Government's efforts to improve cyber security. The ACSC monitors and investigates cyber threats and provides advice and information about online protection. The ACSC is part of the Australian Signals Directorate.

Asset refers to an item, thing or entity that has potential or actual value to an organisation (ISO 55000, 2014 (3.2.1)).

Asset management refers to the coordinated activity of an organisation to realize value from assets (ISO 55000, 2014 (3.3.1)).

A **critical infrastructure asset** is an asset defined by the Security of Critical Infrastructure Act 2018 (SOCI Act). A single critical infrastructure asset may be comprised of multiple component parts such as premises, computers, and data, which function together as a system or network (Cyber and Infrastructure Security Centre, 2022).

Critical minerals are those minerals that are essential for the energy, transport, aerospace, defence, medical, automotive and telecommunications sectors (Department of Industry, Science, Energy and Resources, 2022).

Cyber security refers to the measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them (ACSCb). Information security and information technology security, including cyber security, encompass the security of any piece of information and any technology that is used to store information.

Essential Eight refers to the eight essential mitigation strategies from the ACSC's Strategies to Mitigate Cyber Security Incidents that it is recommended organisations implement as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise an organisation's systems (ACSCa).

Information Security Manual (ISM) produced by the Australian Cyber Security Centre (ACSC), the manual outlines a cyber security framework an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats (ACSCc).

ISA/IEC 62443 refers to the International Electrotechnical Commission series of standards around Security for Industrial Automation and Control Systems, which specifies the process requirements for the secure development of products used by industrial automation and control systems (International Society of Automation, 2020).

IoT (Internet of Things) refers to the devices or instruments with sensing capability and contextual awareness that are interconnected using the Internet. They collect data, without human intervention, and may provide enormous economic benefits through improved efficiencies for the users and organisations that collect data.

ISO refers to the International Organization for Standardization, an international standard development organisation composed of representatives from the national standards organisations of member countries. The ISO prescribes standards and practices that are aimed at ensuring consumers can have confidence that products and services are safe, reliable and of good quality.

NIST refers to the National Institute of Standards and Technology, the U.S. government body responsible for developing cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public.

Operational Technologies (OT) refers to operational technology (OT) encompasses a broad range of programmable systems or devices that interact with the physical environment or manage devices that interact with the physical environment (NIST).

SCADA (Supervisory Control And Data Acquisition) is a computer-based system for gathering and analysing real-time data to monitor and control equipment that deals with critical and time-sensitive materials or events. SCADA is used in power plants as well as in oil and gas refining, telecommunications, transportation, and water and waste control.

Introduction

The Joint Accreditation System of Australia and New Zealand (JASANZ) commissioned the RMIT University Centre for Cyber Security Research and Innovation (CCSRI) to conduct a study into whether the mining and minerals industry utilises three international standards (AS ISO/IEC 27001 - Information Technology; AS ISO 55001 - Asset Management; and AS ISO 22301 – Business Continuity) and any potential barriers to their implementation.

This White Paper builds on the findings from the CCSRI report *An Overview of Cyber Security and Asset Management Standards in the Australian Mining and Minerals Sector* (The Key Findings Report). The report outlines in detail the current landscape regarding the adoption of the three ISO and ISO-IEC Standards in Australian mining and minerals companies, as well as the key barriers to their wide use in the industry.

The objective of this report is to demonstrate the key problems, as to the relative strengths of the ISO and ISO-IEC Standards compared to similar frameworks being used in the mining and minerals industry and how all three standards can better be promoted and used in Australian mining and minerals companies to ensure they are cyber secure and resilient and their assets are protected.

The Key Findings Report outlined the key challenges for the mining sector:

- Uptake of the ISO and ISO-IEC Standards is relatively low when compared against alternative frameworks, particularly in small and medium-sized organisations; organisations do not necessarily see the benefits in implementing ISO and ISO-IEC Standards due to the perceived complexity of the standards, the costs of the standards and implementation process, and the availability of other standards and frameworks.
- Organisations have poor visibility and understanding of cyber security risks; it is not considered a priority in a mining context and funding is a key challenge.
- Standards by themselves do not address all the cyber security, asset management and business continuity requirements of organisations, and organisations themselves may not have control of their own technologies due to outsourcing arrangements.

The study found that the three ISO and ISO-IEC Standards had significant benefits, namely:

ISO/IEC 27001 – Information Technology:

- Creating a proactive security posture for the organisation;
- Reducing cyber security vulnerabilities, threats;
- Determining roles and responsibilities regarding cyber security within the organisation;
- Building confidence for customers, partners, and stakeholders that the organisation is committed to information security;
- Maintaining the organisation's security reputation.

AS ISO 55001 – Asset Management:

- High level of physical asset reliability;
- Improvement performance by providing systematic processes for asset-based decision-making;
- Improving safety by having more reliable assets;
- Improving the quality of products.

AS ISO 22301 – Business Continuity Management:

- Improving organisational security;
- Minimising cyber security incidents;
- Reducing unplanned interruptions;
- Ensuring continued critical operations;
- Financial savings.

This White Paper outlines how these identified challenges can be overcome, and how the strengths of the three ISO and ISO-IEC Standards (AS ISO/IEC 27001, AS ISO 55001 and AS ISO 22301) can be harnessed to protect the industry from cyber incidents and ensure their assets are protected; and their businesses are resilient. This will require concerted action from governments, industry peak bodies, and mining and minerals companies.

Key Points

Mining and minerals companies posture regarding cyber security and asset management falls short in many ways and a significant improvement is needed to ensure this vital national industry remains vibrant and safe.

A summary of the findings of the study and ways to strengthen practices with regard to cyber security, asset management and business continuity in the mining and minerals sector are outlined below:

- There is no overarching legal, regulatory or policy framework around cyber security and asset management in the mining industry.
    - **A uniform legal, regulatory, code and/or framework around cyber security and asset management is needed to ensure the sector is prepared, can adequately respond to, and recover swiftly from cyber incidents.**
- Boards and senior management need to be more accountable for cyber vulnerabilities and asset management risks within their business, especially in OT (Operational Technologies) equipment and their arrangements with third parties.
    - **Making boards and senior management accountable for cyber breaches and risks from poor asset management practices, may incentivise them to prioritise these risks.**
- Approaches to cyber security are changing rapidly, given the recent data breaches at major ASX companies. Large mining companies recognise the potential damage of a cyber incident to their brand and reputation.
    - **A strong legislative framework around data breaches and cyber incidents may help organisations more effectively manage cyber incidents.**
- The workforce maturity and capability around managing cyber security risks and asset management vulnerabilities is relatively low. In short, these are not priority areas for the industry in terms of knowledge, awareness, or training.
    - **Greater funding needed for cyber security training programs.**
- ISO and ISO-IEC Standards are deemed to be static and not fit-for-purpose when it comes to meeting the dynamic threats posed by cyber security attacks.
    - **Regular updates to the ISO and ISO-IEC Standards, like software updates, may be beneficial for businesses that want to "stay ahead" of developing cyber security threats.**
- Larger mining and minerals companies had greater awareness of the three ISO and ISO-IEC Standards AS ISO 55001, AS ISO/IEC 27001 and AS ISO 22301 and ISO standards more generally, when compared with smaller and medium-sized companies.
    - **Government(s) could better promote the ISO and ISO-IEC Standards through national roadshows where they distribute copies of the ISO and ISO-IEC Standards, at no cost to mining and minerals companies.**
    - **Government and industry could collaborate to create an industry network of ISO Champions to advocate for and promote the ISO and ISO-IEC Standards within the mining and minerals industry.**

- There is no standardised vetting mechanism mining and minerals companies use when they review third party contractors, with respect to cyber security and asset management practices.
    - **The use of ISO and ISO-IEC Standards should be heavily encouraged amongst larger mining companies to ensure third parties are not just ISO certified but also that they are sophisticated, in terms of their operational practices.**
- The cost of ISO and ISO-IEC Standards is a major deterrent in their use in mining and minerals companies, of all sizes, particularly compared to other frameworks such as NIST, ISM and Essential Eight which are freely available online.
    - **The cost of ISO-IEC Standards should be subsidised by the Government so that these security standards are freely available to companies.**

Study Recommendations

The study found ten key problems (barriers) facing the widespread use of ISO and ISO-IEC Standards in the mining and minerals industry, and more broadly, why the sector does not have a well-coordinated, proactive cyber security, asset management and business continuity posture.

The RMIT CCSRI proposes 16 recommendations to help improve cyber security in terms of enhancing the mining sector's cyber security, asset management and business continuity posture.

Problem 1: Lack of Regulatory Framework

The mining and minerals sector is a major contributor to the national economy. The Minerals Council of Australia estimates that Australian resources contributed $2.1 trillion in export revenue between 2011-12 to 2020-21, and it has contributed $132 billion in company taxes between 2010-11 to 2019-20. Following the COVID-19 pandemic, the sector is reliant on automated and connected operational technologies (OT) to support remote workforces and control operations without being on-site. This means a significant part of the national economy is vulnerable to cyber-attacks.

Recommendation 1: Government should consider a legislative, policy and/or regulatory framework for mining and mineral companies to comply with to ensure the sector is prepared and can adequately respond to, and recover swiftly from, cyber incidents. This may include mandating the use of ISO and ISO-IEC Standards when large companies onboard and manage third-party vendors.

Recommendation 2: JASANZ should map what obligations mining and minerals companies, and their supply chain, will be required to undertake if the sector is classified, and included, as a possible future critical sector, in the *Security of Critical Infrastructure Act 2018* (SOCI Act).

Problem 2: Boards and Company Officers Visibility

The Key Findings Report found that Australian mining and minerals companies' boards and senior management had little understanding and visibility of operational technology vulnerabilities in their field operations and risks that may exist within their (usually extensive) supply chain arrangements. Under the *Corporations Act 2001* boards have a risk of incurring liability if a personal breach of duty by them results in personal injury or damage or if they authorised and directed the actions which caused the event giving rise to liability.

Recommendation 3: Boards and senior company officers should be encouraged to undertake training around cyber security and asset management risks, with a focus on the risks and vulnerabilities of operational technologies; and supply chain risk management.

Recommendation 4: The Government should consider holding boards accountable for cyber breaches and incidents from poor asset management practices, where those result in serious harm to the community. The Government could consider amending the *Corporations Act 2001* and through more targeted legislation focused on the obligations of boards and company officers more broadly within the mining and minerals industry.

Recommendation 5: Mining and minerals companies Chief Information Security Officers' (CISOs) should be required to report on the cyber security and asset management status of the company through annual reports to ensure the company is adequately managing cyber security risks.

Problem 3: Awareness of ISO and ISO-IEC Standards Compared to Alternatives

Awareness of ISO and ISO-IEC Standards is relatively low amongst small to medium-sized mining companies when compared with alternative frameworks such as the NIST *Cyber Security Framework*, the ACSC's *Essential Eight* and the Informational Security Manual (ISM). This is despite the fact that ISO and ISO-IEC Standards were deemed to add value to organisations' business goals and operations by helping them maintain an international level of quality in operations and providing guidance to middle management.

Awareness of standards was particularly low for smaller companies which is likely due to the fact that they have fewer dedicated resources to plan for, and respond to, cyber security and asset management risks. In short, they do not have time or money to spend on investigating these issues.

Recommendation 6:	a) Government(s) could better promote all relevant security standards including the ISO and ISO-IEC Standards through national roadshows where, as an incentive, they distribute copies of the ISO and ISO-IEC Standards, at no cost to mining and minerals companies. b) JASANZ should consider subsidising the cost of ISO and ISO-IEC Standards so that they are freely available for small and medium-sized mining organisations, alongside existing standards such as the NIST Cyber Security Framework and the ACSC Essential Eight, which are freely available.
Recommendation 7:	JASANZ should develop case studies and develop strategies for adoption, targeted at small and medium-sized enterprises to illustrate how using ISO and ISO-IEC Standards will have a positive impact on their business.
Recommendation 8:	JASANZ should further investigate how small organisations work with larger mining companies, and why larger companies do not use the ISO and ISO-IEC Standards.
Recommendation 9:	Industry bodies such as the Minerals Council of Australia and chambers of commerce across Australia should run cyber security and asset management awareness, training, and skills programs at minimal or no cost, to ensure the mining and minerals sector is upskilled and ready to meet the challenges of operating in a highly evolving digital environment.
Recommendation 10:	JASANZ should create an industry network of ISO Champions to help promote the ISO and ISO-IEC Standards within the mining and minerals industry.

Problem 4: The three ISO and ISO-IEC Standards are not complementary

The three ISO and ISO-IEC Standards (AS ISO/IEC 27001 - Information Technology; AS ISO 55001 - Asset Management; and AS ISO 22301 – Business Continuity) are not complementary to each other.

Recommendation 11:	JASANZ should develop a scheme to better integrate the three Standards and ensure that the standards are updated to ensure they are complementary to each other and also develop a mapping tool to show how the standards are complementary.

Problem 5: ISO and ISO-IEC Standards are Difficult to Understand

There is the perception that the ISO and ISO-IEC Standards are difficult to understand and too technical in nature. Most users of ISO and ISO-IEC Standards in mining and minerals companies are non-technical managers and executives.

Recommendation 12: JASANZ should collaborate with Standards Australia to influence simplification of future ISO and ISO-IEC Standards to ensure they are more easily understood by a non-technical audience. Testing should be undertaken with prospective users, especially with non-technical users, to ensure they are appropriate. This will ensure it is used as a tool of choice by users, to protect their businesses against cyber incidents and protect their assets.

Problem 6: ISO and ISO-IEC Standards are Not Suitable to Sector's Unique Environment

Many larger mining and minerals companies have developed, and use, in-house standards and frameworks because they found the ISO and ISO-IEC Standards to be too generic and they do not fulfil their requirements.

Recommendation 13: JASANZ should engage with the mining and minerals industry to explore ways to ensure the Standards are suitable to all mining and minerals companies' context. This could entail developing case studies of how specific ISO and ISO-IEC Standards would add business value to mining and minerals companies' business risks.

Problem 7: ISO and ISO-IEC Standards are Not Suitable for Evolving Threats

The ISO and ISO-IEC Standards were found to be static and not flexible enough to meet the evolving cyber security threat environment that mining and minerals companies face. The ISO and ISO-IEC Standards are not regularly updated and therefore are not useful for dealing with emerging, and fast-changing threats. Given the ever-changing threat vector around cyber security and asset management, there is a view that ISO and ISO-IEC Standards are outdated and do not deal with contemporary threats in a timely manner.

Recommendation 14: JASANZ and Standards Australia should seek to influence more regular updating of ISO and ISO-IEC Standards to ensure that they are able to address emerging security concerns.

Problem 8: ISO and ISO-IEC Standards are Not Used Widely in Procurement

Larger companies have extensive arrangements with third-party vendors, including data storage services (of highly sensitive commercial data). Mining and minerals companies' do not use a standardised vetting mechanism when reviewing third-party vendors, with respect to cyber security and asset management risks.

Recommendation 15: To improve the cyber and asset management resilience of supply chains, mining and minerals companies should require third-party suppliers to be ISO Certified by a certification body holding appropriate IAF Member Body accreditation where possible.

Problem 9: Cyber Security is a Major Challenge

Following recent data breaches at major ASX companies, many mining and minerals companies are finding that they are facing major challenges when it comes to cyber security.

Recommendation 16: Mining and minerals companies should consider applying ISO and ISO-IEC Standards within their companies, as a way to develop an ongoing security culture in their organisation and to build trust with the wider community. Companies will be perceived to have strong governance frameworks around cyber security and asset management.

Problem 10: Mining and Minerals Companies Use of Legacy Systems

Mining and minerals companies use legacy systems, particularly operational technologies (e.g. SCADA systems) in the field. These are easily compromised and highly vulnerable to sophisticated attacks due to the age of the systems and lack of security features. Implementing security into these systems is not feasible from a technical perspective, or the original supplier of the system may not be in business.

Recommendation 17: Mining and minerals companies should invest in newer systems, including newer Operational Technology systems. If this is not feasible, they should review the legacy systems and should consider compensating controls that could be implemented.

Summary of Recommendations

The recommendations presented are provided for consideration by government, industry bodies and mining and minerals companies. The table below provides a summary of recommendations for each of these groups.

Recommendations	
Recommendations to Government and Associated Bodies	
Recommendation 1	Government should consider a legislative/regulatory framework for mining companies to comply with to ensure the sector is prepared and can adequately respond to, and recover from, cyber incidents.
Recommendation 2	JASANZ should map what obligations mining and mineral companies, and their supply chains, will be required to undertake if the sector is included as a critical sector in the *Security of Critical Infrastructure Act 2018* (SOCI Act).
Recommendation 4	Government should consider holding boards accountable for cyber breaches and incidents from poor asset management practices, where those breaches result in serious harm to the community.
Recommendation 6	c) Government(s) could better promote ISO and ISO-IEC Standards through national roadshows where, as an incentive, ISO and ISO-IEC Standards are distributed at no cost to mining and minerals companies. d) JASANZ should consider subsidising the cost of ISO and ISO-IEC Standards for small and medium-sized mining and minerals organisations.
Recommendation 7	JASANZ should develop case studies and strategies for adoption, targeted at small and medium-sized enterprises to illustrate how using ISO and ISO-IEC Standards will have a positive impact on their business.
Recommendation 8	JASANZ should investigate how small organisations work with larger mining and minerals companies, and the reasons why larger companies do not use the ISO and ISO-IEC Standards.
Recommendation 10	JASANZ should create an industry network of ISO Champions to help promote the ISO and ISO-IEC Standards within the mining and minerals industry.
Recommendation 11	JASANZ should develop a scheme to better integrate the ISO 27001, ISO 55001 and ISO 22301 standards and develop a mapping tool to show how the standards complement each another.
Recommendation 14	JASANZ and Standards Australia should seek to influence more regular updating of ISO and ISO-IEC Standards to ensure that they are able to address emerging security concerns.
Recommendation to Industry Bodies	
Recommendation 9	Industry bodies should run cyber security and asset management awareness, training, and skills programs at minimal or no cost, to upskill the mining and minerals sector.
Recommendations to Mining and Minerals Companies	
Recommendation 3	Boards and senior company officers should be encouraged to undertake training around cyber security and asset management risks.
Recommendation 5	Mining and minerals companies Chief Information Security Officers' (CISOs) should be required to report on the cyber security and asset management status of the company

Recommendations	
	through annual reports to ensure the company is adequately managing cyber security risks.
Recommendation 15	Mining and minerals companies should require third-party suppliers to be ISO Certified by a certification body holding appropriate IAF Member Body accreditation where possible.
Recommendation 16	Mining and minerals companies should consider applying ISO and ISO-IEC Standards in their organisation as a way to develop a more robust security culture and to build trust with the wider community.
Recommendation 17	Mining and minerals companies should review legacy systems and invest in newer systems and/or consider implementing compensating controls.

Conclusion

In summary, RMIT CCSRI has undertaken extensive research, conducted surveys, and engaged with experts across Australia through a series of workshops and interviews. In total, the CCSRI received survey responses from thirty-eight professionals, and engaged with 28 cyber security experts in one or more domains around cyber security, asset management, business continuity and mining and minerals.

The CCSRI found ten key challenges as to why the uptake of ISO and ISO-IEC Standards in the mining and minerals industry remains relatively low, particularly amongst smaller and medium sized companies. This can be attributed to their not seeing the benefits of using the ISO and ISO-IEC Standards, their complexity, high cost, and the availability of competing frameworks. Further, cyber security is not considered a key priority in the industry and boards and senior company officers often do not have visibility of the cyber and asset management risks in their enterprise, particularly with regard to Operational Technologies (OT) in the field, and amongst their third-party contractors.

RMIT CCSRI's has made 17 recommendations to improve cyber security in terms of enhancing the practices of Australian mining and minerals companies around cyber security, asset management and business continuity.

References

ACSCa n.d., *Essential Eight*, Australian Cyber Security Centre, https://www.cyber.gov.au/resources-business-and-government/essential-cyber- security/essential-eight, viewed 21 April 2023.

ACSCb n.d., *Glossary – C*, Australian Cyber Security Centre, https://www.cyber.gov.au/acsc/view-all-content/glossary/c, viewed 20 April 2023.

ACSCc n.d., *Information Security Manual*, Australian Cyber Security Centre, https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism, viewed 21 April 2023.

Cyber and Infrastructure Security Centre 2022, Register of Critical Infrastructure Assets Guidance, September 2022, https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/register-critical-infrastructure-assets.pdf, viewed 21 April 2023.

Federal Register of Legislation, *Corporations Act 2001*, https://www.legislation.gov.au/Series/C2004A00818, viewed on 20 April 2023

International Electronic Commission 2020, ISA/IEC 62443:2020 *Security for industrial automation and control systems,* International Society of Automation (ISA).

International Standards Organization 2013, *AS ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements*, International Standards Organization.

International Standards Organization 2014, *ISO 55000:2014 Asset management — Overview, principles and terminology*, International Standards Organization.

International Standards Organization 2019, *AS ISO 22301:2019 Security and Resilience – Business Continuity Management Systems – Requirements*, International Standards Organization.

Minerals Council of Australia, *Pre-Budget Submission 2022-23*; https://treasury.gov.au/sites/default/files/2022-03/258735_minerals_council_of_australia.pdf; 25 January 2022, viewed on 20 April 2023

NIST n.d., *National Institute of Standards and Technology (NIST) Cybersecurity Framework*, https://www.nist.gov/cyberframework, viewed 18 April 2023.

Connect with us

By email

ccsri@rmit.edu.au

Website

rmit.edu.au/cyber

RMIT UNIVERSITY

Centre for Cyber Security Research and Innovation