RMIT UNIVERSITY
Centre for Cyber Security Research and Innovation

An Overview of Cyber Security and Asset Management Standards in the Australian Mining and Minerals Sector

KEY FINDINGS REPORT

June 2023

JASANZ

Australian Government
Department of Industry, Science, Energy and Resources

What's next..

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 research has been produced as a result of the collaboration between the RMIT University 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 by the Department of Science, Industry and Resources. Special thanks to RMIT staff involved in the study: 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.

Terminology

The following terms and acronyms are used in this report:

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), outlines a cyber security framework an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats (ACSCc).

International Electrotechnical Commission (IEC) 62443 Security for Industrial Automation and Control Systems series specifies the process requirements for the secure development of products used in industrial automation and control systems.

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 that 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.

Contents

ACKNOWLEDGEMENTS **3**

TERMINOLOGY **3**

EXECUTIVE SUMMARY **6**

1 WHY IS THIS STUDY NEEDED? **8**

1.1 BACKGROUND 8

1.2 OBJECTIVES OF THE STUDY 9

1.3 PHASES OF THE STUDY 10

1.4 KEY QUESTIONS OF THE STUDY 10

2 HOW WAS THIS STUDY UNDERTAKEN? **11**

2.1 PHASE 1: LITERATURE REVIEW 11

2.2 PHASE 2: SURVEY 11

2.3 PHASE 3: WORKSHOPS 12

2.4 PHASE 4: INTERVIEWS 12

3 KEY FINDINGS **13**

3.1 KEY INSIGHTS: WHAT CAN WE LEARN FROM THIS RESEARCH? 13

3.2 LITERATURE REVIEW FINDINGS 13

3.3 SURVEY FINDINGS 15

3.4 WORKSHOP AND INTERVIEW FINDINGS 22

3.5 KEY INSIGHTS 24

4 RECOMMENDATIONS **28**

REFERENCES **30**

APPENDIXES **31**

APPENDIX 1: DEMOGRAPHIC DATA OF SURVEY RESPONDENTS 31

APPENDIX 2: SURVEY QUESTIONS 33

APPENDIX 3: COMPARISON OF STANDARDS AND FRAMEWORKS 36

APPENDIX 4: CRITICAL MINERALS LIST 37

APPENDIX 5: MAP OF AUSTRALIAN CRITICAL MINERALS IN MINES 39

Executive Summary

The Joint Accreditation System of Australia and New Zealand (JASANZ) commissioned the RMIT University Centre for Cyber Security Research and Innovation (CCSRI) to undertake a study to gain a comprehensive understanding of three international standards in the Australian mining and minerals industries, namely:

- AS ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements;
- AS ISO 55001:2014 Asset Management – Management Systems – Requirements;
- AS ISO 22301: 2019 Security and Resilience – Business Continuity Management Systems – Requirements.

CCSRI conducted in-depth research through an extensive gap analysis literature review, surveying industry practitioners, and conducting focus groups and one-on-one interviews with industry experts and experienced practitioners.

As a result of this research, this report examines how ISO and ISO-EC Standards perform against other frameworks such as the NIST Cybersecurity Framework, the Information Security Manual and Essential Eight in the mining and minerals industries in Australia. It identifies the strengths of ISO and ISO-IEC Standards and how to best promote it as the tool of choice for protection against cyber incidents and protection of assets. The objective is to gain an understanding of the applicability and flexibility of ISO and ISO-IEC Standards and certification as a means to protect information and assets and to promote business continuity and resilience, as well as how domestic application of international standards related to digital, critical technologies and critical minerals sectors can be improved.

The report gives the Australian mining and minerals sector a clearer picture of the uptake of the three ISO and ISO-IEC Standards, the benefits of implementing these Standards, as well as the barriers to implementation.

Making positive change is not easy. Understanding barriers and resistance to change, is part of the challenge of improving the uptake of ISO and ISO-IEC Standards in the mining and minerals sector. This report provides the sector with insights to help navigate these challenges.

Key issues and findings that this report highlights include:

- Uptake of the ISO and ISO-IEC Standards is relatively low, particularly in small and medium-sized organisations, and organisations do not necessarily see the benefits in implementing ISO and ISO-IEC Standards due to perceived complexity of the standards, the costs of the standards and difficulty of implementation, and the availability of other standards and frameworks.
- Organisations have poor visibility and understanding of cyber security and related areas, and cyber security is generally not considered a priority in a mining context.
- Organisations do not have the required funding to effectively implement cyber security, asset management and business continuity, including ISO and ISO-IEC Standards.
- 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. Mining companies can take additional measures such as supplementing ISO/IEC 27001 conforming ISMS with the Australian Informational Security Manual controls or supplementing the ISO 55001 conforming AMS with additional practices such as ‘open systems’ and ‘systems evolution’ as prescribed by the Living Asset Management Think Tank (Hardwick et al., 2020).

The recommendations for action documented in this report point towards adopting a holistic whole-of-sector approach to change and emphasise the importance of marshalling key stakeholder groups – government, industry bodies, and mining and minerals organisations – to take concerted and aligned action to improve the cyber security posture and asset management practices of organisations in this important sector of the Australian economy.

1 Why is This Study Needed?

1.1 Background

The impetus to undertake this critical research stems in part from data showing that between 2019 and 2020, there was a four-fold increase in the number of reported cyber breaches among mining companies (Verizon, 2019). Furthermore, according to the latest EY Global Information Security Survey (GISS), 71 per cent of mining respondents stated that they had seen a significant increase in the number of disruptive cyber attacks over the past 12 months and 55 per cent of mining and minerals industry executives were worried about their organisation's ability to manage a threat (Mitchell, 2022).

Mining and mineral resources are significant sources of wealth and income that play a crucial role in the Australian economy. The mining industry creates thousands of jobs and provides essential materials for all sectors of the economy, boosting economic growth. The Australian mining industry employs 1.2 million people and generates $50 billion average earnings per year and generates $160 billion of resource exports (AusIMM, 2023). It is anticipated that this figure has likely increased with the mining and minerals industries becoming increasingly reliant on automated and connected operational technologies (OT) to support remote workforces and control operations without being on-site. In turn, this has increased the urgency and importance of organisations adopting cyber security, asset management and business continuity management standards to protect themselves from the growing presence of cyber attacks and data breaches.

Cyber security is becoming an increasingly critical issue for governments, businesses, and everyday citizens in Australia. Highly sophisticated cyber-attacks are proliferating at an alarming pace, and some industries are becoming more exposed to risks than others. The nature of the mining industry, for instance, enhances the magnitude of risk as a cyber-attack could easily result in the loss of life.

As a result, JASANZ has commissioned RMIT University CCSRI to gain a better understanding of the awareness and use of the following three international standards in the Australian mining and minerals industry as shown by Table 1.

Table 1: International standards on cyber security, asset management, and business continuity.

ISO	Description
AS ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems - Requirements	This standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation.
AS ISO 55001:2014 Asset Management – Management Systems - Requirements	This standard specifies requirements for the establishment, implementation, maintenance and improvement of a management system for asset management.
AS ISO 22301: 2019 Security and Resilience – Business Continuity Management Systems - Requirements	This standard specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise.

The study also examines other similar standards and frameworks that organisations may utilise to enhance cyber security and manage assets. These include:

- The **NIST Cybersecurity Framework**, a framework based on existing standards, guidelines, and practices for organisations to better manage and reduce cybersecurity risk (NIST);
- The **Information Security Manual** (ISM) produced by the Australian Cyber Security Centre (ACSC) that outlines a cyber security framework an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats (ACSCc);
- The **Essential Eight**; 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);
- The **IEC 62443** Security for Industrial Automation and Control Systems series specifies the process requirements for the secure development of products used in industrial automation and control systems (ISA, 2020).

1.2 Objectives of the study

The major objectives of this study were to:

- Assess how AS ISO/IEC 27001 certification performs against other frameworks such as NIST, ISM and Essential Eight in the mining and minerals industries in Australia;
- Identify the strengths of AS ISO/IEC 27001 certification to best promote it as the tool of choice for protection against cyber incidents and protection of assets;
- Gain an understanding of the applicability and flexibility of AS ISO/IEC 27001 certification, AS ISO 55001 and AS ISO 22301 standards and extension to certification and record pathways as solutions to remedy problems associated with the protection of information and assets in promoting business resilience to the mining and mineral industries in Australia;
- Increase domestic application of international standards related to digital, critical technologies and critical minerals sectors.

1.3 Phases of the study

This project has been undertaken in four phases (as shown by Table 2).

Table 2: Phases of the Overview of Cyber Security and Asset Management Standards in the Australian Mining and Minerals Sector Project.

Project Phase	Description
Phase 1: Literature review	A gap analysis literature review to build an understanding of the comparison between international standards and other similar frameworks, and to determine the drivers and barriers to adoption of international standards.
Phase 2: Survey	A survey of mining and minerals industry executives and senior management was conducted to determine the awareness and use of international standards and frameworks, as well as the benefits of and barriers to adopting the international standards.
Phase 3: Workshops	Three workshops across Australia with senior industry executives and management designed to gain an understanding of Australian mining and minerals industry attitudes towards international standards and frameworks relating to cyber security and asset management.
Phase 4: Interviews	Ten one-one-one interviews with industry experts and practitioners designed to supplement the workshop insights and explore in detail some of the key issues raised in the workshops.

Further detail regarding how the project was undertaken is provided in section two of this report.

1.4 Key questions of the study

The key questions that are addressed in this study that are designed to meet the project objectives as shown by Table 3 are:

Table 3: Key questions of the study

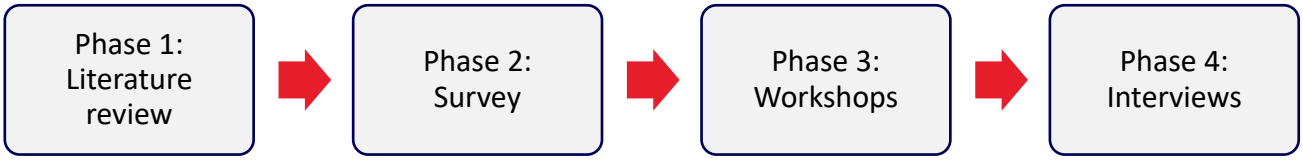
Key questions this study investigates

• What are the strengths of the three ISO and ISO-IEC Standards and how do they complement each other?
• What are the benefits from having ISO and ISO-IEC Standards and certification?
• What are the risks associated with ICT and with outsourcing information security and asset management systems in the mining and minerals industries? Including:
  o What are the potential reasons for data breaches?
  o What are the implications on business continuity?
• What action can be taken to promote the uptake of the three ISO and ISO-IEC Standards by the Australian mining and minerals industry?

2 How Was This Study Undertaken?

The RMIT University CCSRI conducted a review of Australian mining and mineral companies' cyber security, asset management and business continuity capabilities, their current state of operations and their implementation of ISO and ISO-IEC Standards and other relevant standards and frameworks. The study was conducted in four phases (as shown by Figure 1):

Figure 1: Phases of the study.



In undertaking this study, CCSRI consulted a range of experts from across Australia, ranging from mining practitioners, expert consultants, industry networks and government agencies.

2.1 Phase 1: Literature review

In the first phase of the study, CCSRI undertook a gap analysis literature review to understand the range of cyber security frameworks used in the mining and minerals industry, and any barriers to adoption of these frameworks and standards.

This gap analysis research considered the utility of the three ISO and ISO-IEC Standards relating to the mining and minerals industry sector:

- AS ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements;
- AS ISO 55001:2014 Asset Management – Management Systems – Requirements; and
- AS ISO 22301:2019 Security and Resilience – Business Continuity Management Systems – Requirements.

The research also considered how these standards compared against other similar frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Information Security Manual and the Australian Cyber Security Centre's (ACSC's) Essential Eight.

2.2 Phase 2: Survey

In the second phase of the study, CCSRI conducted a survey of executive and senior management representatives currently employed in various roles and organisations in the Australian mining and minerals industry sector in order to understand current practices, and the workforce's understanding of international standards relating to cyber security and asset management.

Refer to Appendix 1 for demographic data of survey participants.

Survey participants were recruited through the professional networks of the CCSRI and JASANZ. Survey responses were collected via an online platform from November 2022 – April 2023. The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey generated 36 responses. The survey encompassed questions on the relative merits of the ISO and ISO-IEC Standards, when compared with other cyber security and asset management standards; and how they could be improved upon.

Refer to Appendix 2 for details of the survey questions.

2.3 Phase 3: Workshops

In phase three, CCSRI undertook three in-person workshops with eighteen experts (from academia, industry, and government) across Australia in Melbourne, Brisbane and Perth. The purpose of these workshops was to gain an understanding of Australian mining and minerals industry attitudes towards international standards and frameworks relating to cyber security and asset management.

RMIT CCSRI engaged in a national consultation process holding three workshops in Melbourne, Brisbane and Perth respectively and ten interviews. Through the workshops and interviews, the Centre consulted 28 experts and practitioners across industry, policy, regulation, and academia.

In the first part of each workshop, the Director of CCSRI presented key findings from the literature review around the benefits and problems of each of the three standards: ISO /IEC 27001 (Information Security), ISO 55001 (Asset Management), and ISO 22301 (Business Continuity Management).

In the second part of each workshop, four questions were posed to participants:

- What are the current practices in the mining and minerals industry, regarding cyber security, asset management and business continuity?
- What are some of the gaps in your experience that need to be addressed?
- How can practices, standards and frameworks be enhanced to improve cyber security, asset management and business continuity?
- What resources/changes are required to get there?

2.4 Phase 4: Interviews

In the fourth phase of the project, ten key industry personnel were interviewed to supplement the workshop insights and explore in detail some of the key issues raised in the workshops.

The CCSRI consulted ten experts in a series of one-to-one 30-minute interviews. Most of these experts were middle-level managers or technical experts in cyber and/or mining. The interviews provided an opportunity to gain a deeper-level understanding of the cyber security and asset management practices, and barriers to the adoption of the ISO and ISO-IEC Standards.

3 Key Findings

3.1 Key insights: What can we learn from this research?

The key findings of the study provide valuable insights into the current practices of the Australian mining and minerals industry and the drivers and barriers to the adoption of international standards and similar frameworks.

The following sections show the key findings and insights from the study literature review, survey, workshops and interviews.

3.2 Literature review findings

The gap analysis literature review completed in the first phase of the study focused on understanding the cyber security frameworks and standards used in the mining and minerals industry, the strengths of these frameworks and standards, and any barriers to adoption.

The findings of the literature review identified the strengths and weaknesses of the ISO and ISO-IEC Standards (Table 4). These findings were used to inform the questions and focus of the survey, workshop and interview questions in the other phases of the study.

Table 4: Gap analysis literature review key findings on strengths of ISO and ISO-IEC Standards and barriers to adoption.

ISO standard	Strengths	Barriers
AS ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements	• Creating a proactive security posture for the organisation. • Reducing vulnerabilities, threats and risks associated with information systems. • Determining roles and responsibilities regarding information 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.	• Lack of adequate information security procedures and policies. • Insufficient staff awareness. • Costs issues to implement cyber security. • Inadequate risk management process. • Poor asset identification and inventory.
AS ISO 55001:2014 Asset Management – Management Systems – Requirements	• 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 quality of products.	• Lack of a formally defined strategy. • Inefficient use of resources. • Lack of funds to implement systems. • Absence of reporting and auditing systems. • Poor communications internally.
AS ISO 22301: 2019 Security and Resilience – Business Continuity Management Systems - Requirements	• Improving organisational security. • Minimising cyber security incidents. • Reducing unplanned interruptions. • Ensuring continued critical operations. • Financial savings.	• Limited funds for implementation of standard. • Insufficient testing of BCM systems Lack of training around BCM. • Lack of higher management support.

The findings of the gap analysis literature review are detailed in project deliverable, *the Gap Analysis Report of the Australian Mining and Minerals Industry to Understand the Uptake of International Standards*.

3.3 Survey findings

The phase two survey findings included insights into awareness of ISO and ISO-IEC Standards and frameworks, implementation, accreditation, barriers to adopting the standards, as well as the benefits of adoption.

A general note: survey respondents were primarily from larger organisations which, in our assessment, reflects larger organisations' greater capacity to investigate risks surround cyber security and asset management.

3.3.1 Awareness

Awareness of ISO and ISO-IEC Standards is relatively high amongst large organisations but not amongst small and micro-organisations:

- A large number of respondents (71.4 per cent) are aware of ISO/IEC 27001 Information Security, followed by 42.9 per cent of respondents being aware of ISO 22301 Business Continuity Management.
- Two-thirds (66.7 per cent) of respondents from large organisations (200 or more employees) were aware that ISO and ISO-IEC Standards exist.
- 66.7 per cent of respondents from large organisations (200 or more employees) were aware of the three specific ISO and ISO-IEC Standards (AS ISO 55001, AS ISO/IEC 27001 and AS ISO 22301) relevant to this study.
- 28.57 per cent of respondents from small organisations (5-19 employees) were aware of ISO 27001 Information Security and ISO 22301 Business Continuity Management respectively.
- Similarly, only 14.3 per cent of micro-organisations (0-4 employees) were aware of ISO /IEC 27001 Information Security.
- Awareness of ISO 55001 Asset Management (28.6 percent) and other ISO and ISO-IEC Standards is relatively low (28.6 per cent)

3.3.2 Implementation

Implementation of ISO and ISO-IEC Standards across the industry is relatively low:

- One third of survey respondents reported that they had implemented ISO 55001 Asset Management.
- ISO 22301 Business Continuity Management is the least implemented ISO-IEC standard with only 11.1 per cent reporting that it had been implemented in their organisation.
- Almost 30 percent (28.6 per cent) reported implementing ISO/IEC 27001 Information Security in their organisation.
- More than 14 per cent of respondents (14.3 per cent) indicated that no ISO and ISO-IEC Standards have been implemented in their organisation.

3.3.3 Accreditation

The question relating to accreditation of ISO and ISO-IEC Standards was answered by only 27.7 per cent of survey respondents. Amongst the 27.7 per cent who responded to the question, 30 per cent reported that their organisation had no accreditation. Of those who reported their organisation being accredited:

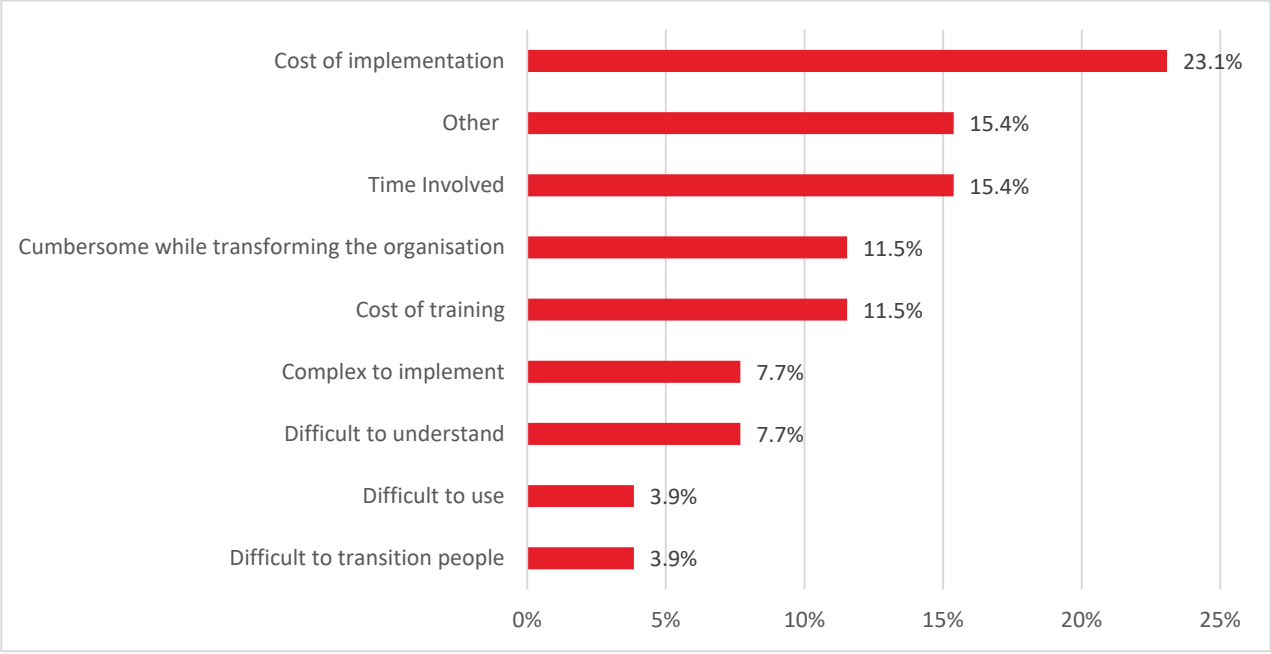
- None were accredited in ISO 22301 Business Continuity Management.
- 20 per cent reported accreditation in ISO/IEC 27001 Information Security.
- 40 per cent held accreditation in ISO 55001 Asset Management.
- Only 10 per cent were accredited in other ISO-IEC Standards.
- A general note: given the high rate of certification amongst survey respondents, and the actual rate of certifications to ISO/IEC 27001 and ISO 55001 being low (as stated by JASANZ), it is hypothesised that this might be the result of multiple respondents from a single accredited organisation.

3.3.4 Barriers to implementation

Respondents indicated a wide range of barriers to implementing standards and frameworks generally, however, the two main barriers to implementation appear to be cost and the amount of time involved in implementation (Figure 2).

Lower ranked barriers to adopting standards and frameworks included the cumbersomeness of ISO-IEC Standards implementation while transforming the organisation (11.5 per cent), the cost of training (11.5 per cent), the difficulty of understanding the ISO-IEC Standards (7.7 per cent), and the complexity of implementation (7.7 per cent).

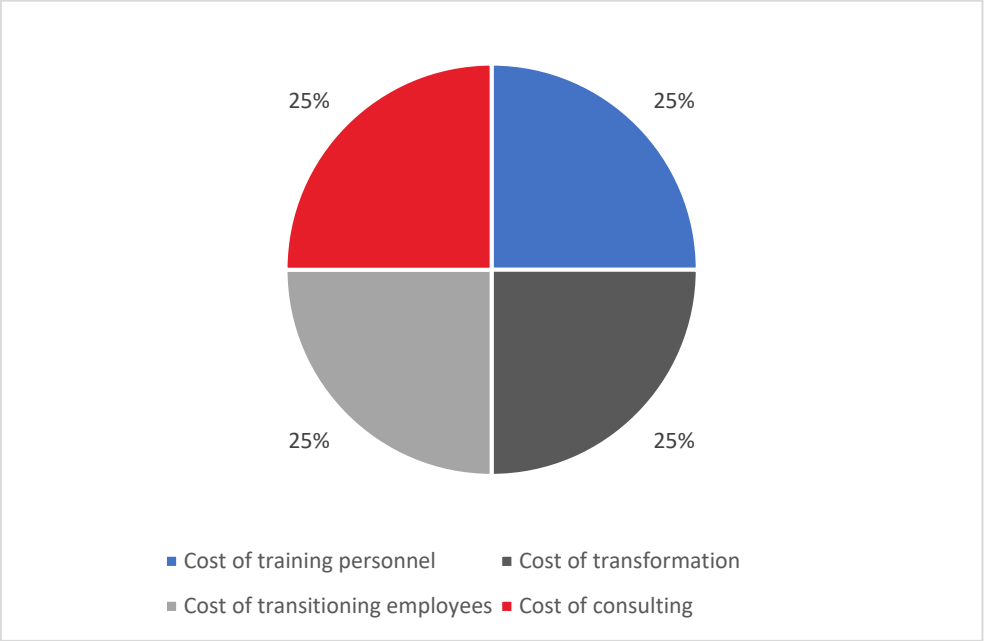
Figure 2: Factors impacting organisation's choice of and ability to implement standards and frameworks.



(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

Drilling down into the cost barriers associated with implementation of ISO and ISO-IEC Standards specifically, respondents equally ranked the costs of transformation, transitioning, training and consulting (Figure 3) as significant barriers.

Figure 3: Cost barriers that affect choice of ISO.



(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

3.3.5 Benefits of implementing ISO and ISO-IEC Standards

As shown in Figure 4, survey respondents highlighted four main benefits of implementing the **ISO /IEC 27001 Information Security Standard**: maintaining a proactive security posture; enhanced availability, confidentiality and integrity of information; providing a framework for risk management; and, helping to maintain the organisation's reputation with key stakeholders.

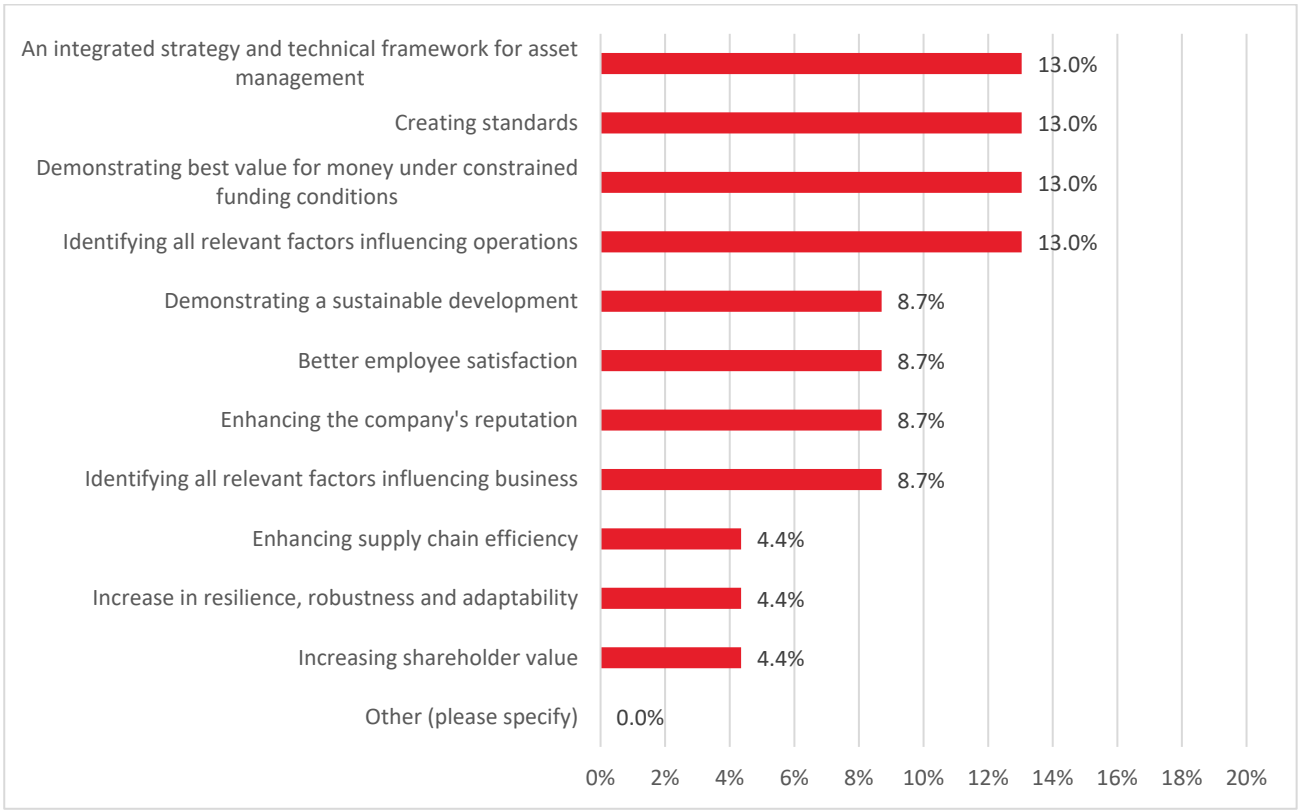
Figure 4: The benefits to organisations of implementing ISO/IEC 27001 Information Security.

(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

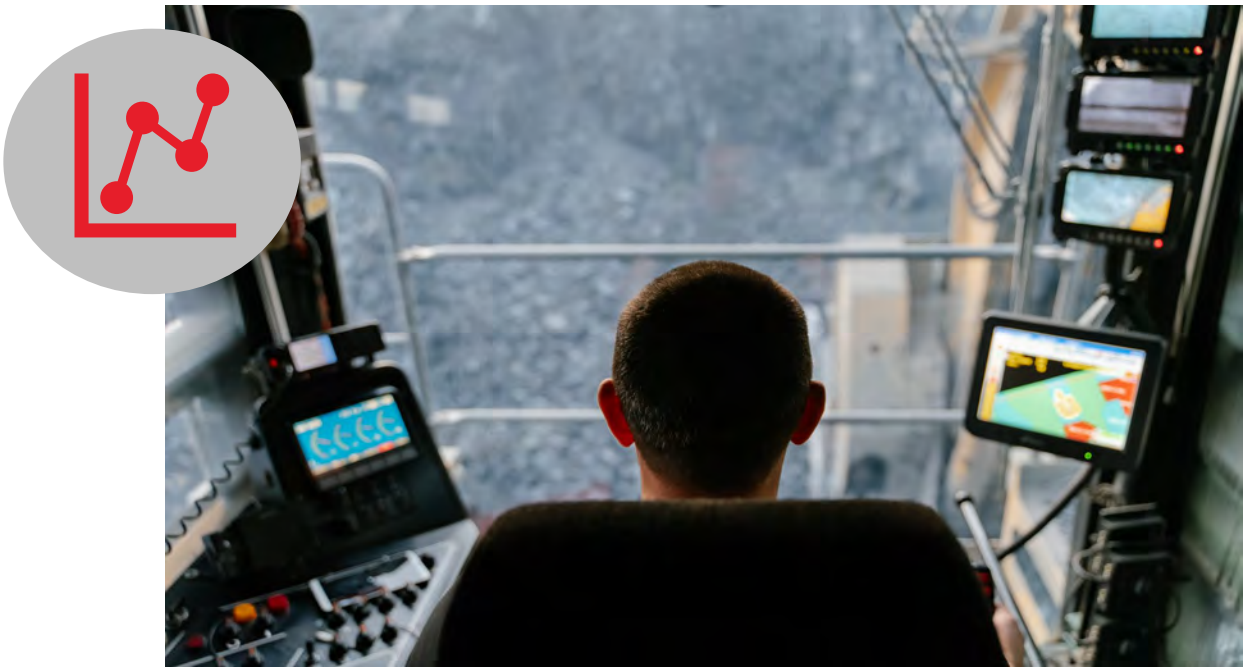
Survey respondents highlighted four main benefits of using the **ISO 55001 Asset Management Standard**: It provides an integrated strategy and technical framework for asset management; it helps to identify all relevant factors influencing operations; it demonstrates best value for money under constrained funding conditions; and, it also assists in creating standards within organisations as shown by Figure 5.

It is also worth noting that only 4.4 per cent of respondents believed using the ISO 55001 Asset Management standard would increase the organisation's resilience and adaptability.

Figure 5: Benefits to organisations of implementing ISO 55001 Asset Management.

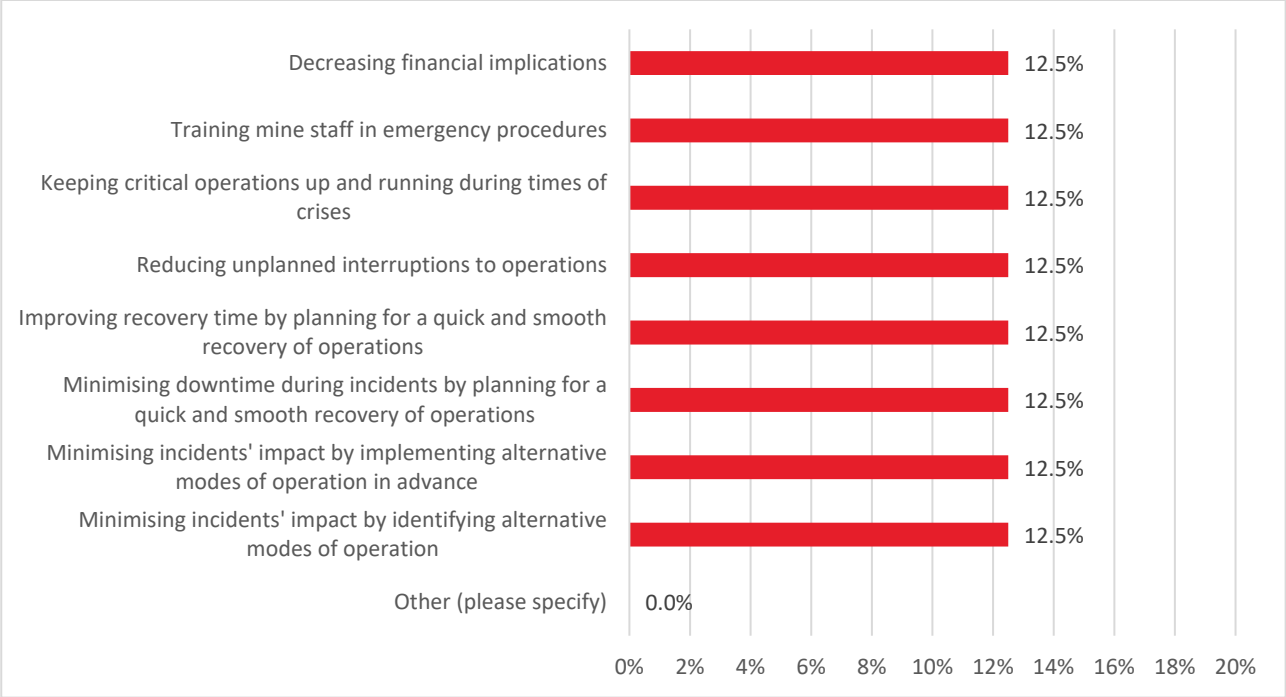


(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)



Survey respondents did not rank one benefit over another, with respect to using the **ISO 22301 Business Continuity Management Standard**. The responses highlight multiple benefits associated with implementing ISO22301 (Figure 6).

Figure 6: Benefits to organisations of implementing ISO 22301 Business Continuity Management.

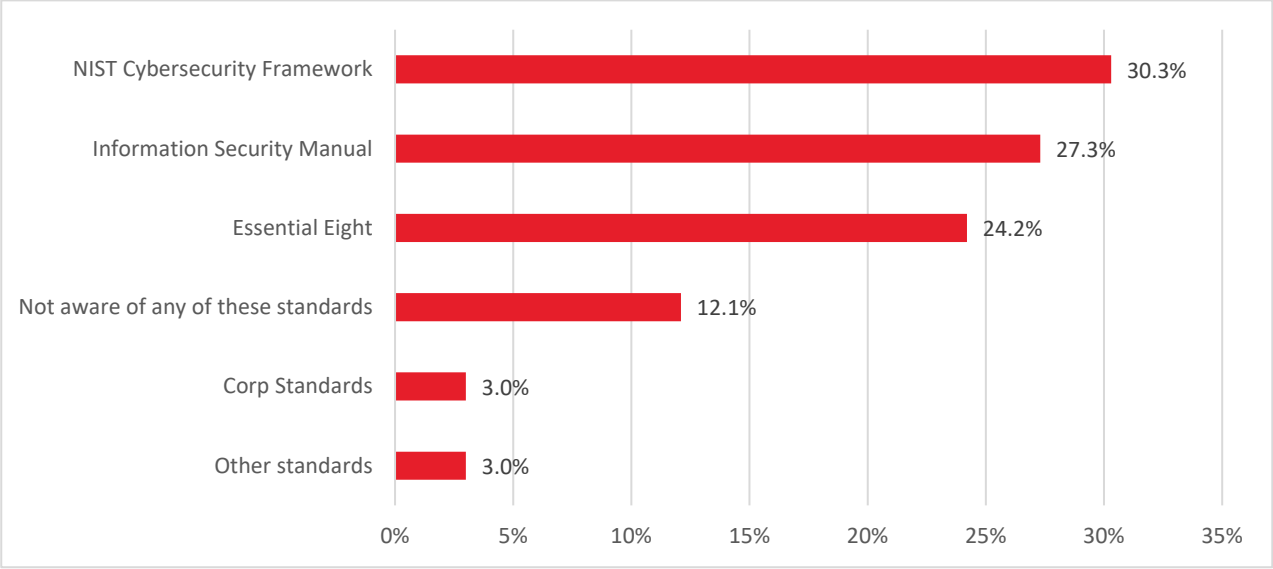


(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

3.3.6 Awareness, use and benefits of other standards

Respondent awareness of other standards and frameworks was relatively low, with the most well-known being the NIST Cybersecurity Framework (30.3 per cent), followed by the Information Security Manual (27.3 per cent). Almost a quarter of respondents (24.2 per cent) were aware of the Essential Eight (Figure 7).

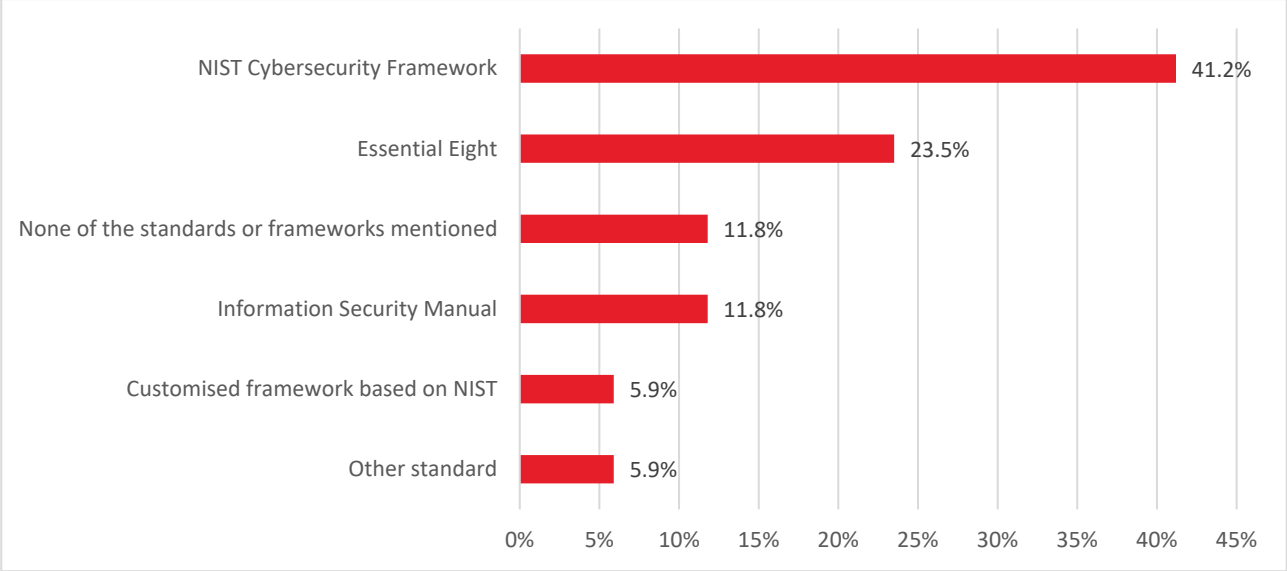
Figure 7: Awareness of other standards and frameworks.



(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

In terms of implementing other standards, the NIST Cybersecurity Framework was the standard / framework that was most commonly implemented, followed by the Essential Eight and ISM. Only six per cent of respondents (5.9 per cent) had implemented some other standard, which relied upon NIST as a guide (Figure 8).

Figure 8: Implementation of other standards or frameworks.

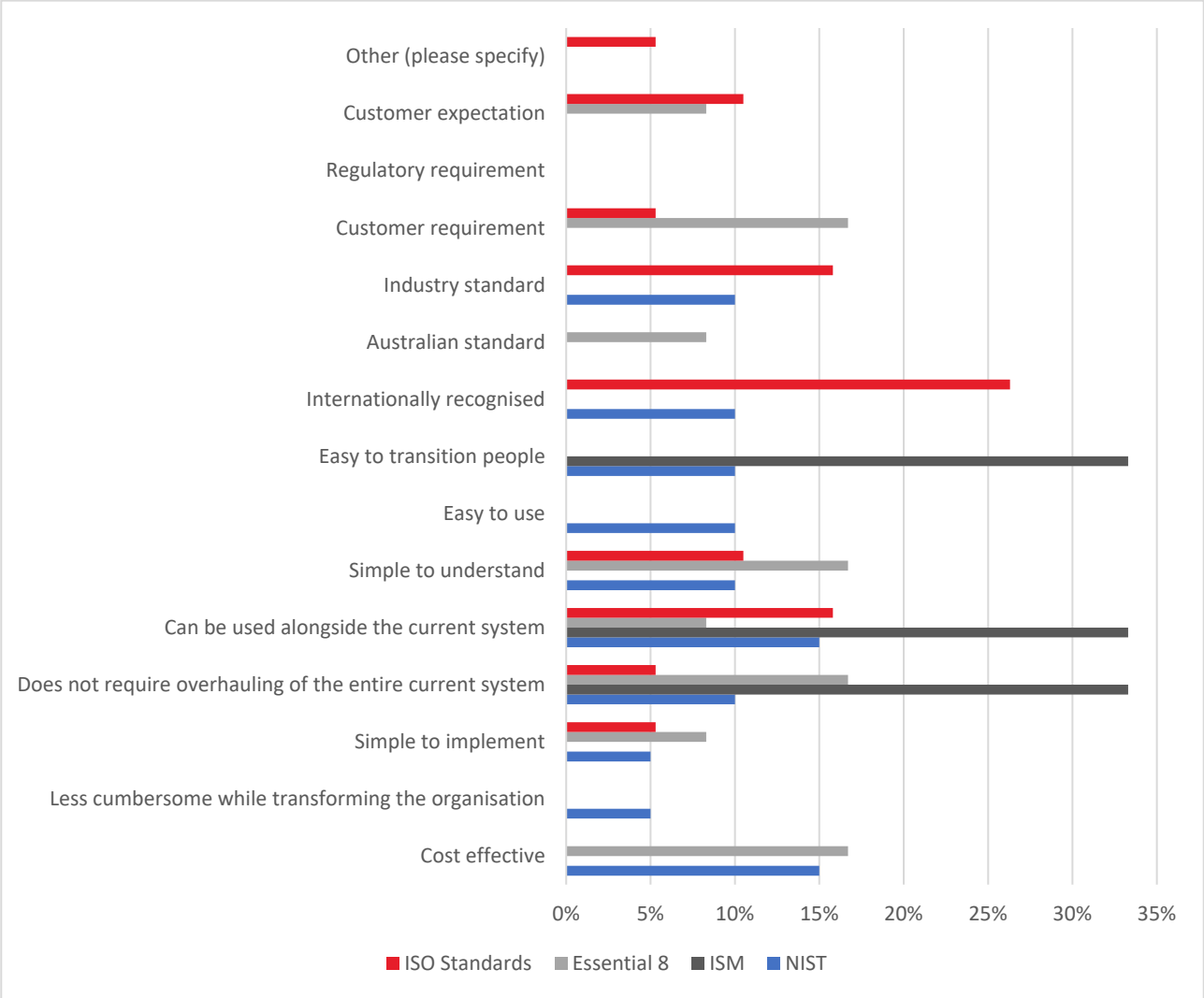


(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

When considering the reasons for implementing ISO and ISO-IEC Standards when compared to other standards and frameworks, international recognition of the ISO and ISO-IEC Standards, and the fact that the ISO and ISO-IEC Standards are industry standards and can be used alongside the organisation's current system were all highlighted by respondents as important reasons for choosing implementation of this type of framework (Figure 9).

Similarly, respondents indicated a wide range of reasons for implementing the NIST Cybersecurity Framework and the Information Security Manual. However, in relation to the Essential Eight only three reasons for choosing this framework for implementation were identified: ease of transitioning people, the ability to use the framework along current system, and the framework does not require overhaul of the organisation's entire current system.

Figure 9: The reasons for choosing to implement parts or all of the ISO and ISO-IEC Standards or other frameworks.



(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

Refer to Appendix 3 for full details of reasons choosing to implement the ISO and ISO-IEC Standards or other frameworks.

3.3.7 Strategy and management of cyber and information security

The following are key issues identified by the study:

- The ISO and ISO-IEC Standards were deemed to have added value to organisation's business goals and operations mainly by maintaining international level of quality in operations and by providing guidance to middle management;
- Respondents consistently reported that ISO and ISO-IEC Standards were expensive, complex to implement, and difficult to understand. By contrast, NIST and Essential Eight were both cited as more adaptable, and easier to implement alongside organisations' existing systems. That is, they were considered less disruptive to the business' operations;
- NIST was nominated as being the most useful standard in terms of cost, change management, ease of understanding (language) and being internationally recognised;
- Thirty-three per cent of respondents nominated that they implemented ISO and ISO-IEC Standards because they were internationally recognised;

- Another key reason for implementation cited by respondents (33.3 per cent) was customers' expectation as a key driver for using ISO and ISO-IEC Standards;
- A key insight was that 60 per cent of respondents stated that they used a third-party vendor to assist in applying standards or frameworks, which alludes to the cost and complexity of using the ISO and ISO-IEC Standards.

3.4 Workshop and interview findings

The findings from the workshops and interviews have been integrated due to the complementary nature and consistency of the findings. This is a positive indicator as the intention of the interviews was to build a deeper understanding of the issues raised in the workshops.

The key insights from the three workshops and ten one-on-one interviews conducted with practitioners from industry, policy, regulation and academia include:

- **Lack of knowledge** of ISO and ISO-IEC Standards (and other frameworks) is one of the key reasons for standards not being utilised within organisations;
- The **cost of ISO and ISO-IEC Standards** is too high ($170US) and not perceived to be of significant value, especially for middle managers who are responsible for cyber and/or asset management. Participants report that they cannot convince their company (or in practice, their procurement area or manager) to pay for the ISO and ISO-IEC Standards. Instead, they opt to **use freely available standards** such as the NIST Cybersecurity Framework or may utilise complementary standards such as the IEC 62443 for cyber security of industrial automation and control systems, which is widely used globally for ICSs and is the de facto standard in the oil and gas industry;
- The ISO and ISO-IEC Standards are **not suitable for small to medium-sized organisations**. These organisations prefer to use the Essential Eight because it is more concise and easier to follow;
- Participants indicated that **cyber security is not a priority** for companies; knowledge, awareness and training on cyber security and asset management is relatively low. However, participants also indicated that in the aftermath of large-scale data breaches, such as the Optus and Medibank data breaches affecting millions of Australians and causing major reputational damage to both companies, companies are now seriously reviewing their data handling and cyber security practices;
- Many participants reported that the ISO and ISO-IEC Standards **are legacy-based**, and do not sufficiently foresee future threats, especially given the rapidly evolving nature of cyber threats. International standards such as the ISO and NIST are perceived to be static and therefore not particularly helpful, as a resource, to combat the rapidly changing nature of these threats;
- The ISO and ISO-IEC Standards were deemed to be **overly complex** in language, and were difficult to understand for middle-level managers and practitioners. The standards contained too much jargon;
- There are two distinct types of technologies amongst companies, especially larger organisations such as informational technology and operational technology that warrant distinctly **different cyber and asset management strategies**;
- **Smaller organisations do not have the funding and resources** to allocate to cyber security and asset management. They view the standards as compliance documents, rather than being a useful tool to help improve and protect their business;

- Many small to medium sized companies **opt to use other standards** such as the Essential Eight rather than NIST or the ISO and ISO-IEC Standards, as the Essential Eight is more concise and simpler to use;
- **No substantial legislative framework**: While there are substantial legislative requirements around cyber security standards in the mining and minerals industry, the industry is not deemed 'critical' under the *Security of Critical Infrastructure Act 2018*. If the industry is deemed to be 'critical' under the *SOCI Act*, the industry would need to comply with these legislative requirements, not the ISO and ISO-IEC Standards. This would entail a significant amount of work to be done by organisations to ensure compliance with the legislation and some participants indicated that this could turn cyber security into a 'compliance' activity rather than a means to improve companies' operational practices. If SOCI Act compliance requirement eventuates, it is likely that companies will forgo the use of other standards, such as the ISO and ISO-IEC Standards;
- **Regulation is not a ready-made solution:** Whilst regulation can be useful, it could force companies to view cyber security as a compliance activity, thereby diverting organisational resources away from upskilling staff in cyber and asset management standards;
- Cyber security and asset management are **not deemed to have a direct impact on citizens** and the community, unlike physical safety in the mining and minerals sector. Therefore, mining and minerals companies especially smaller and medium sized entities do not place an emphasis on cyber security risks in their businesses;
- **Boards and management have little or no understanding or visibility** of the cyber security threats facing their business. This is particularly acute with respect to vulnerabilities prevalent in operational technology equipment in their companies. They also do not have a consolidated understanding of third-party vendor/service providers' cyber security practicesp
- There is a **lack of advocacy** by boards and management regarding cyber standards being critical in order for organisations to be well-prepared for cyber incidents
- **Use of certification in supply chain and procurement.** Large organisations often use international standards such as ISO and ISO-IEC Standards as a filtering mechanism to vet smaller firms when procuring services, as part of their supply chain. Conversely, smaller entities often subscribe to ISO and ISO-IEC Standards as a method of proving their 'forward' cyber security posture.
- Most companies have relationships with and outsource to **third-party services** that host their data (databases) in the cloud. These third-party vendors hold data (sometimes commercially sensitive data), however there are no strict or uniform standards on how these potential vulnerabilities are managed;
- Larger organisations have little to no visibility of the cyber security practices used by their **supply chain** (i.e. third-party auditing or compliance requirements);
- Large organisations have their own **in-house standards, frameworks and practices** and are not necessarily interested in a standardised framework for the mining and minerals sector. These organisations prefer to custom design their own technical standards and frameworks rather than apply international standards because they are generic and not deemed to be relevant to their industry and organisational circumstances. For the relatively few organisations that want to embark on improving discrete domain elements of their operations (security of their information, management/maintenance of assets, business continuity measures, etc.), only a subset see the ISO or IEC Standards as relevant to this;

- Participants regarded people as often being the weakest link when it comes to data management and security. Changing **company culture** to embed cyber awareness, safety and security is pivotal to strengthening cyber security;
- **Attitudes, brand and reputation:** Companies' attitudes are rapidly shifting in an increasingly digital commercial environment; they are taking cyber security seriously and they recognise the potential damage of a cyber incident to their business, brand and reputation, especially following recent data breaches at major ASX companies;
- Organisations in this industry sector use a large number of **legacy systems** which are more easily compromised and pose major vulnerabilities to potentially sophisticated attackers. While upgrading these systems is not currently an industry priority, this does highlight the importance of upgrading technologies;
- **Lack of cyber security training** leads to data breaches;
- Some participants suggested that **cyber insurance** could be a way of integrating liability, and costing cyber security risks, within a product/service;

3.5 Key insights

In relation to the key questions that this study focuses on (see section 1.4), the following key insights were evident from the quantitative and qualitative data analysis.

3.5.1 What are the strengths of ISO and ISO-IEC Standards and how do they complement each other?

The strengths of the three ISO and ISO-IEC Standards were clearly identified (Table 5) as being:

Table 5: Strengths of ISO and ISO-IEC Standards.

ISO-IEC Standard	Identified strengths
AS ISO/IEC 27001 Information Security Management Systems	• Encourages companies to document and assess their main processes which can increase productivity and ensure a better security posture. • Greater stability of systems, lower malfunctions and vulnerabilities, and improved risk management. • Enhances availability, confidentiality and integrity of information. • Provides a framework for risk management. • Improves stakeholders' perception of the company and its reputation.
AS ISO 55001 Asset Management	• Provides an integrated strategy and technical framework for asset management based on rigorous scientific and technical principles. • It assists in identifying all relevant factors influencing operations. • Improves asset financial returns. • Improves working environment by improving health, safety and environmental performance.
AS ISO 22301 Business Continuity Management	• Minimises incidents' impact by identifying alternative modes of operation and proactively implementing them. • Minimises downtime during incidents and improves recovery time by foreseeing and planning for a quick and smooth recovery of operations. • Keeps critical operations up and running during times of crises and reducing unplanned interruptions to operations.

In the survey, workshops and interviews, the CCSRI found that the ISO/IEC 27001:2013 – Information Security and the ISO/IEC 22301:2019 – Business Continuity were often used together in a complementary manner. In particular, information security was found to facilitate business continuity.

However, the standards are often not applied in an integrated way because the three ISO and ISO-IEC Standards were utilised by different departmental areas within organisations. This resulted in the three standards being applied independently of each other.

3.5.2 What are the benefits of ISO and ISO-IEC Standards and certification?

What are the benefits, and who benefits, from having ISO and ISO-IEC Standards and certification. These are:

- ISO and ISO-IEC Standards and certification benefit the organisation in general. In all three workshop discussions, it was found that within companies, areas focusing on Information Technology and Operations Technology particularly benefitted from applying the ISO and ISO-IEC Standards;
- Implementation of ISO and ISO-IEC Standards led to organisations adopting a proactive security posture with respect to risk management;
- ISO and ISO-IEC Standards and certification enhanced availability, confidentiality and integrity of information, which led to an increase in organisations' reputation. Internally, use of ISO and ISO-IEC Standards amongst staff in organisations, was deemed to lead to greater collaboration;
- Implementation of ISO and ISO-IEC Standards also led to an increase in stakeholders' confidence regarding an organisation's commitment to protecting data, and organisations that used ISO and ISO-IEC Standards were perceived by stakeholders to be more resilient;
- Workshop participants indicated that ISO and ISO-IEC Standards can be useful as a tool to vet/screen whether vendors or third-parties sufficiently manage cyber security and asset risks, particularly for large organisations.

3.5.3 What are the risks associated with ICT and with outsourcing information and asset management?

Respondents identified a number of risks associated with ICT and with outsourcing information security and asset management systems in the mining and minerals industries. These risks included:

- Slippage of information during handovers;
- Manpower turnover with the outsourced body reverberates with outdated software being used;
- People's risky behaviour which compromises cyber security, including lack of knowledge on how data breaches occur;
- Lack of initiative by management and board to avoid operation downtime during software upgrades and installations;
- Data security is not always a board and management priority;
- Lack of knowledge on system vulnerabilities; and
- People's lack of digital hygiene.

Respondents also identified implications for business continuity in relation to ICT and in outsourcing information and asset management. These implications include:

- Business continuity is complemented and facilitated by information security and works in tandem with information security;
- Multiple outsourced bodies creates complexity in operations;
- Multiple outsourced bodies not working in alignment, and not exchanging or sharing knowledge; and
- The different business agendas of multiple outsourced bodies adversely affects operations.

3.5.4 What IoT/SCADA systems do mining and minerals companies use?

In workshops, participants stated that mining companies used IoT (Internet of Things) and SCADA (Supervisory Control And Data Acquisition) systems extensively in their field operations.

Programmable Logic Controller (PLC) based systems are used for:

- Enabling tele-monitory and control of drilling equipment;
- Electronic detonation;
- Explosive handling;
- Seamless mine transportation systems;
- Positioning and navigation.

In terms of the hazards relating to the use of IoT/SCADA systems in the mining and minerals industry, workshop participants stated that the key issues in the sector are:

- There are no uniform standards on how they are utilised in in the industry;
- Legacy systems make it difficult to update software regularly, thereby making these systems vulnerable to attack. A related issue is that due to the extensive nature of third-party contracting arrangements in the sector, when larger companies change vendors, the larger companies have no viable option to upgrade their software;
- The complexity, time and resource intensity of updating software is a major hurdle for most organisations; they therefore opt not to update their software regularly, leaving them more vulnerable to cyber attacks;
- Organisations often opt to use technical controls but do not spend resources on training key personnel; people are often the weakest link.

3.5.5 Which minerals are deemed ‘critical minerals’?

Workshop participants stated the critical minerals were those that were essential for Australia’s economy. These include: iron ore, bauxite, alumina, lithium, uranium, lead, zinc, thermal coal, black coal, manganese, nickel, aluminum, brown coal, diamonds, silver, and copper. Australia is a major producer of many of these minerals. Australia is the largest exporter of iron ore, thermal coal, alumina, metallurgical coal, and liquefied natural gas (NLG) and the second-largest exporter of thermal coal in the world.

A full list of critical minerals is provided in Appendix 4.

The mining and minerals industry accounts for 75 per cent of the country's exports and is a major source of economic development. (See Appendix 5: Map of Australian Critical Minerals in Mines).

Workshop participants stated that it was highly likely that in the near future the mining industry would be deemed ‘critical infrastructure’ under the *SOCI Act.*

3.5.6 What action can be taken to improve the uptake of the three ISO and ISO-IEC Standards?

A list of recommendations for action that can be taken to promote the uptake of the three ISO and ISO-IEC Standards by the Australian mining and minerals industry is provided in the following section, Section 4: Recommendations. Further discussion and information regarding recommended actions is contained in the *Overview of Cyber Security and Asset Management Standards in the Australian Mining and Minerals Sector White Paper* that accompanies the Key Findings Report.

4 Recommendations

Looking toward the future and the ways in which cyber security and asset management postures can be enhanced, the following recommendations are put forward in Table 6 to improve the uptake of ISO and ISO-IEC Standards and other similar frameworks in both large and small organisations in the Australian mining and minerals industry sector.

Table 6: Recommendations for improving the uptake of ISO and ISO-IEC Standards and frameworks in the Australian mining and minerals sector.

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	a) 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. b) 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.
	Recommendations 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

Recommendations	
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 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.

Note: Further information on each of the above recommendations can be found in the *Overview of Cyber Security and Asset Management Standards in the Australian Mining and Minerals Sector White Paper* that accompanies this report.

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.

AusIMM n.d., Australia's Mining Industry, https://www.ausimm.com/insights-and-resources/mining-industry/australian-mining-industry/, viewed 18 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.

Department of Industry, Science, Energy and Resources, *2022 Critical Minerals Strategy*, March 2022, https://webarchive.nla.gov.au/awa/20220603113601/https://www.industry.gov.au/data-and-publications/2022-critical-minerals-strategy, viewed 21 April 2023.

Hardwick, J, Kerr, M, Killeen, M, Kohler, P, Lafraia, J and Sally Nugent, S 2020, *Living Asset Management Maturity*, Living Asset Management.

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

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.

Mitchell, P 2022, *Does cyber risk only become a priority once you've been attacked?*, EY, 8 March 2022, https://www.ey.com/en_us/mining-metals/does-cyber-risk-only-become-a-priority-once-you-ve-been-attacked, viewed 20 April 2023.

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

Verizon 2019, *Data Breach Investigations Report and 2016 Data Breach Investigations Report*; cited in PWC Mine 2020 Report, pp.19-20, https://www.pwc.com.au/industry/mining/pwc-mine-2020.pdf, viewed 18 April 2023.

Appendixes

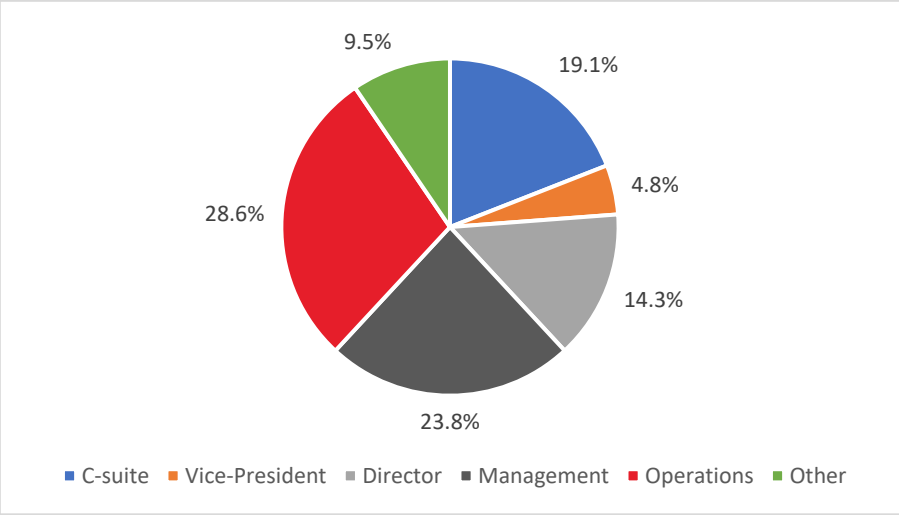
Appendix 1: Demographic data of survey respondents

The demographics of the respondents is described through distribution collated into four categories: current role, size of organisations, jurisdiction of organisations, and number of sites of each organisation as shown in the following figures (Figures 10, 11, 12 and 13 respectively).

Current job role

Over 50 per cent of survey respondents were either in Operations or Management roles (52.4 per cent combined), with the other almost 50 per cent in C-suite, Director, and Vice-President roles (Figure 10).

Figure 10: Current job role of all respondents.

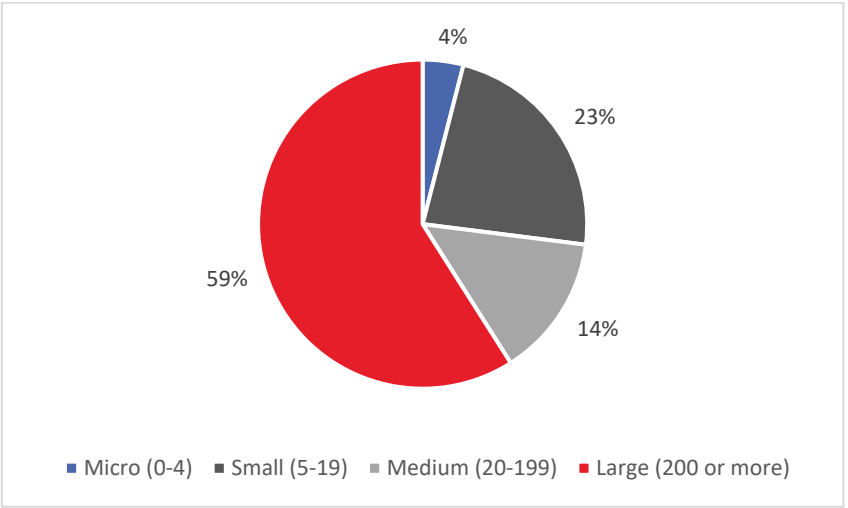


(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

Size of organisation

The majority of survey respondents (59 per cent) were employed in large mining and minerals industry companies that employed 200 or more employees (Figure 11).

Figure 11: Approximate size (number of employees) of organisation in which respondents are employed.

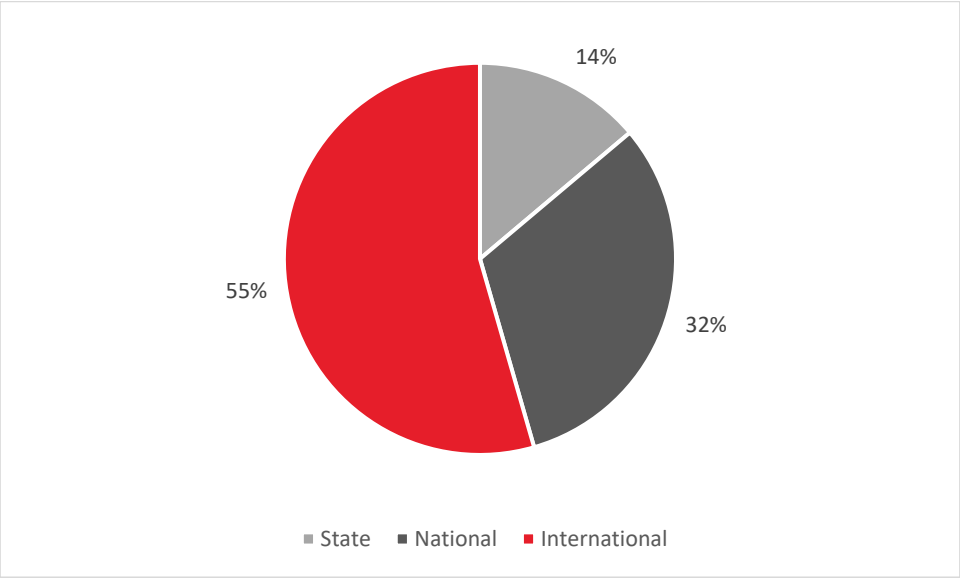


(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

Jurisdiction

The majority of survey respondents (55 per cent) were employed in organisations that operated international jurisdictions (Figure 12).

Figure 12: Jurisdiction in which the organisation operates.

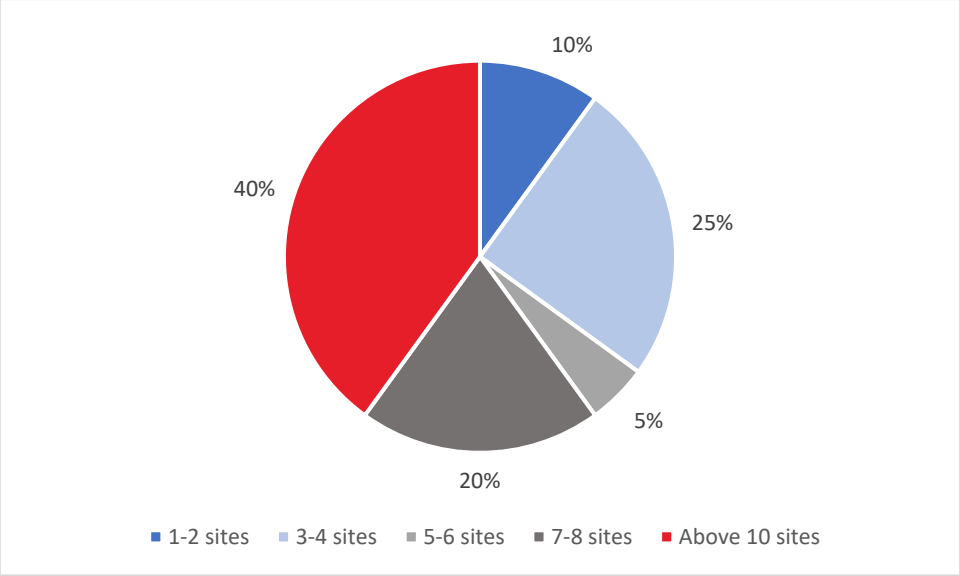


(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

Number of sites

The data shows that 40 per cent of the organisations represented in the survey operated from more than 10 sites/offices, followed by 25 per cent of respondent organisations operating from 3 to 4 sites (Figure 13).

Figure 13: The number of sites/offices that the organisation operates from.



(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

Appendix 2: Survey questions

The Engaging with Australian Mining and Minerals Industries on the Use of International Standards survey included the following questions (Table 7).

Table 7: Engaging with Australian Mining and Mineral Industries on the Use of International Standards survey questions.

No.	Question:
Demographics	
Q2:	Which of the following best describes your current job role/title? • Chief Technology Officer (CTO) • Chief Operations Officer (COO) • Chief Executive Officer (CEO) / President • Chief Information Officer (CIO) • Chief Information Security Officer (CISO) • Owner / Proprietor • Vice President • Director • Other (please specify)
Q3:	What is the approximate size (no. of employees) of your organisation?
Q4:	In what jurisdiction does your organisation operate in?
Q5:	How many sites/offices does your organisation operate from?
International Organization for Standardization (ISO) Standards	
Q6:	Are you aware of ISO (International Organization for Standardization) standards?
Q7:	Are you aware of any of the standards listed below? (Select all that apply) • AS ISO/IEC 27001:2013 – Information Security • AS ISO 22301:2019 – Business Continuity • AS ISO 55001:2014 – Asset Management • Other ISO and ISO-IEC Standards (please specify) • None
Q8:	Have any of the following ISO and ISO-IEC Standards been implemented in your organisation? (Select all that apply) • AS ISO/IEC 27001:2013 – Information Security • AS ISO 22301:2019 – Business Continuity • AS ISO 55001:2014 – Asset Management • Other ISO standards (please specify) • None at all

No.	Question:
Q9:	Does your organisation hold accredited certification for any of these ISO standards? (Select all that apply): • AS ISO/IEC 27001:2013 – Information Security • AS ISO 22301:2019 – Business Continuity • AS ISO 55001:2014 – Asset Management • Other ISO standards (please specify) • None
Q10:	How has implementing ISO/IEC 27001:2013 benefited your organisation? (Select all that apply)
Q11:	How has implementing ISO 55001:2014 benefited your organisation? (Select all that apply)
Q12:	How has implementing ISO 22301:2019 benefited your organisation? (Select all that apply)
Q13:	How has implementing these standards added value to your organisation's business goals and operations? (Select all that apply)
Q14:	When ISO was adopted in your organisation, how would you describe/classify the cost of the ISO implementation? (Select one)
Q15:	What factors made it expensive to adopt ISO in your organisation? (Select all that apply)
Q16:	My organisation chose to implement ISO standards for the following reasons (Select all that apply)
Comparison with other frameworks	
Q17:	Are you aware of any of the following standards or frameworks? (Please select all that apply) • National Institute of Standards and Technology (NIST) • Information Security Manual (ISM) • Essential Eight • Other (please specify) None of the above
Q18:	Has your organisation implemented in full or part any of the following standards/frameworks? (Select all that apply) • National Institute of Standards and Technology (NIST) • Information Security Manual (ISM) • Essential Eight • Other (please specify) • None of the above
Q19:	My organisation has implemented parts or all of NIST for the following reasons: (Select all that apply)
Q20:	My organisation has implemented parts or all of ISM for the following reasons: (Select all that apply)
Q21:	My organisation has implemented parts or all of Essential Eight for the following reasons: (Select all that apply)

No.	Question:
Application of other system	
Q22:	Does your organisation adhere to any other standards/frameworks relevant to Information Security? If yes, please name the system or standard.
Q23:	Does your organisation adhere to any other standards/frameworks relevant to Business Continuity? If yes, please name the system or standard.
Q24:	Does your organisation adhere to other standards/frameworks relevant to Asset Management? If yes, please name the system or standard.
For all frameworks/standards	
Q25:	What factors impact your organisation's choice of and ability to implement standards/frameworks? (Select all that apply)
Q26:	Does a third party assist you in applying standards/frameworks in your organisation?
Q27:	Who in your organisation makes the decision to adopt frameworks/standards? (Select all that apply)
Further opportunities to participate in this project	
Q28:	We would like to learn more about your experience. Would you be open to continuing your participation in this study?
Q29:	We will be holding focus groups and one-to-one interviews, where you can share your knowledge and experience of your organisation and the industry. Would you be open to being involved in these stages? (Select all that apply)

Appendix 3: Comparison of standards and frameworks

The rationale for selecting different standards and frameworks, as identified by survey respondents, is shown in Table 8.

Table 8: The reasons for choosing to implement parts or all of the ISO and ISO-IEC Standards or other frameworks.

Reasons for choosing to implement parts of all of Standards and Frameworks	NIST	ISM	Essential 8	ISO
Cost effective	15.0%	0.0%	16.7%	0.0%
Less cumbersome while transforming the organisation	5.0%	0.0%	0.0%	0.0%
Simple to implement	5.0%	0.0%	16.7%	5.3%
Does not require overhauling of the entire current system	10.0%	33.3%	8.3%	5.3%
Can be used alongside the current system	15.0%	33.3%	8.3%	15.8%
Simple to understand	10.0%	0.0%	16.7%	10.5%
Easy to use	10.0%	0.0%	0.0%	0.0%
Easy to transition people	10.0%	33.3%	0.0%	0.0%
Internationally recognised	10.0%	n/a	n/a	26.3%
Australian standard	n/a	0.0%	8.3%	n/a
Industry standard	10.0%	0.0%	0.0%	15.8%
Customer requirement	0.0%	0.0%	16.7%	5.3%
Regulatory requirement	0.0%	0.0%	0.0%	0.0%
Customer expectation	0.0%	0.0%	8.3%	10.5%
Other (please specify)	0.0%	0.0%	0.0%	5.3%
Total	**100.0%**	**100.0%**	**100.0%**	**100.0%**

(Source: RMIT 2022, The Engaging with Australian Mining and Minerals Industries on the Use of International Standards Survey.)

Appendix 4: Critical minerals list

Australia's critical minerals list highlights priority critical minerals. The list is based on global technology needs, particularly around electrification, advanced manufacturing and defence. The list below (appearing as Table 1 in the government's 2022 Critical Minerals Strategy) shows Australia's current list of 26 critical minerals.

Table 9: Australian critical minerals list

Critical mineral	On US list[6]	On EU list[7]	On Japan list[8]	On India list[9]	Australian geological potential[10]	Australian economic demonstrated resources (2020)[11]	Australian production (2020)	Global production (2020)[12]
High-Purity Alumina	✓[13]	✓[14]			Moderate	No data	No data	No data
Antimony	✓	✓	✓	✓	Moderate	125.2 kt	3.9 kt	155 kt
Beryllium	✓	✓	✓	✓	Moderate	No data	No data	240 t
Bismuth	✓	✓	✓	✓	Moderate	No data	No data	17 kt
Chromium	✓		✓	✓	Moderate	0	0	40,000 kt
Cobalt	✓	✓	✓	✓	High	1,495 kt	5.6 kt	135 kt
Gallium	✓	✓	✓	✓	High	No data	No data	300 t
Germanium	✓	✓	✓	✓	High	No data	No data	130 t
Graphite	✓	✓	✓[15]	✓	Moderate	7,970 kt	0	1,100 kt
Hafnium	✓	✓	✓		High	14.5 kt	No data	No data
Helium					Moderate	No data	4 hm^3	140 hm^3
Indium	✓	✓	✓	✓	Moderate	No data	No data	900 t
Lithium	✓	✓	✓	✓	High	6,174 kt	40 kt	82 kt
Magnesium	✓	✓	✓		High	Magnesite: 286,000 kt	Magnesite: 799 kt	Magnesite: 26,000 kt

6 J Burton, 'U.S. Geological Survey Releases 2022 List of Critical Minerals', United States Geological Survey (USGS), U.S. Department of the Interior, Federal Government of the United States, 2022, accessed 3 March 2022.
7 Joint Research Centre, 'The Fourth List of Critical Raw Materials for the EU', European Commission, 2020, accessed 3 March 2022.
8 J Nakano, translation of a Ministry of Economy, Trade and Industry (METI) publication as presented in The Geopolitics of Critical Minerals Supply Chains, Centre for Strategic & International Studies (CSIS), 2021, p 22, accessed 3 March 2022.
9 V Gupta, T Biswas and K Ganesan, Critical Non-Fuel Mineral Resources for India's Manufacturing Sector—A Vision for 2030, Council on Energy, Environment and Water (CEEW), 2016, pp 73–74, accessed 3 March 2022. Minerals that are identified as of high economic importance, high supply risk, or both for 2030 are highlighted here.
10 Geoscience Australia, Australia's Identified Mineral Resources 2021, Geoscience Australia, Australian Government, unpublished, accessed 3 March 2022.
11 Geoscience Australia, Australia's Identified Mineral Resources 2021, [dataset], Geoscience Australia, Australian Government, accessed 3 March 2022.
12 Geoscience Australia, using estimated world production from USGS Mineral Commodity Summaries 2021, adjusted with reported Australian production in the dataset of Australia's Identified Mineral Resources 2021, accessed 17 January 2022.
13 The US identifies aluminium as a critical mineral.
14 The EU identifies bauxite (an ore of aluminium) as critical.
15 Japan identifies carbon (which forms graphite) as a critical mineral.

Critical mineral	On US list[6]	On EU list[7]	On Japan list[8]	On India list[9]	Australian geological potential[10]	Australian economic demonstrated resources (2020)[11]	Australian production (2020)	Global production (2020)[12]
Manganese	✓		✓		High	Manganese ore: 276,000 kt	Manganese ore: 4,800 kt	17,200 kt
Niobium	✓	✓	✓	✓	High	216 kt	No data	78 kt
Platinum-group elements	✓	✓	✓	✓	Moderate	107 t	0.522 t	380 t
Rare-earth elements	✓	✓	✓	✓	High	4,200 kt	20 kt	240 kt
Rhenium			✓	✓	Moderate	No data	No data	53 t
Scandium	✓	✓			High	30.34 kt	No data	No data
Silicon		✓[16]	✓	✓	High	No data	No data	8 kt
Tantalum	✓	✓	✓	✓	High	99.4 kt	0.1 kt	1.8 kt
Titanium	✓	✓	✓		High	Ilmenite: 274,000 kt Rutile: 35,300 kt	Ilmenite: 1,100 kt Rutile: 200 kt	Ilmenite: 12,000 kt Rutile: 1000 kt
Tungsten	✓	✓	✓		High	577 kt	<1 kt	84 kt
Vanadium	✓	✓	✓	✓	High	7,408 kt	0	86 kt
Zirconium	✓		✓	✓	High	Zircon: 79,300 kt	Zircon: 400 kt	Zircon: 2,000 kt

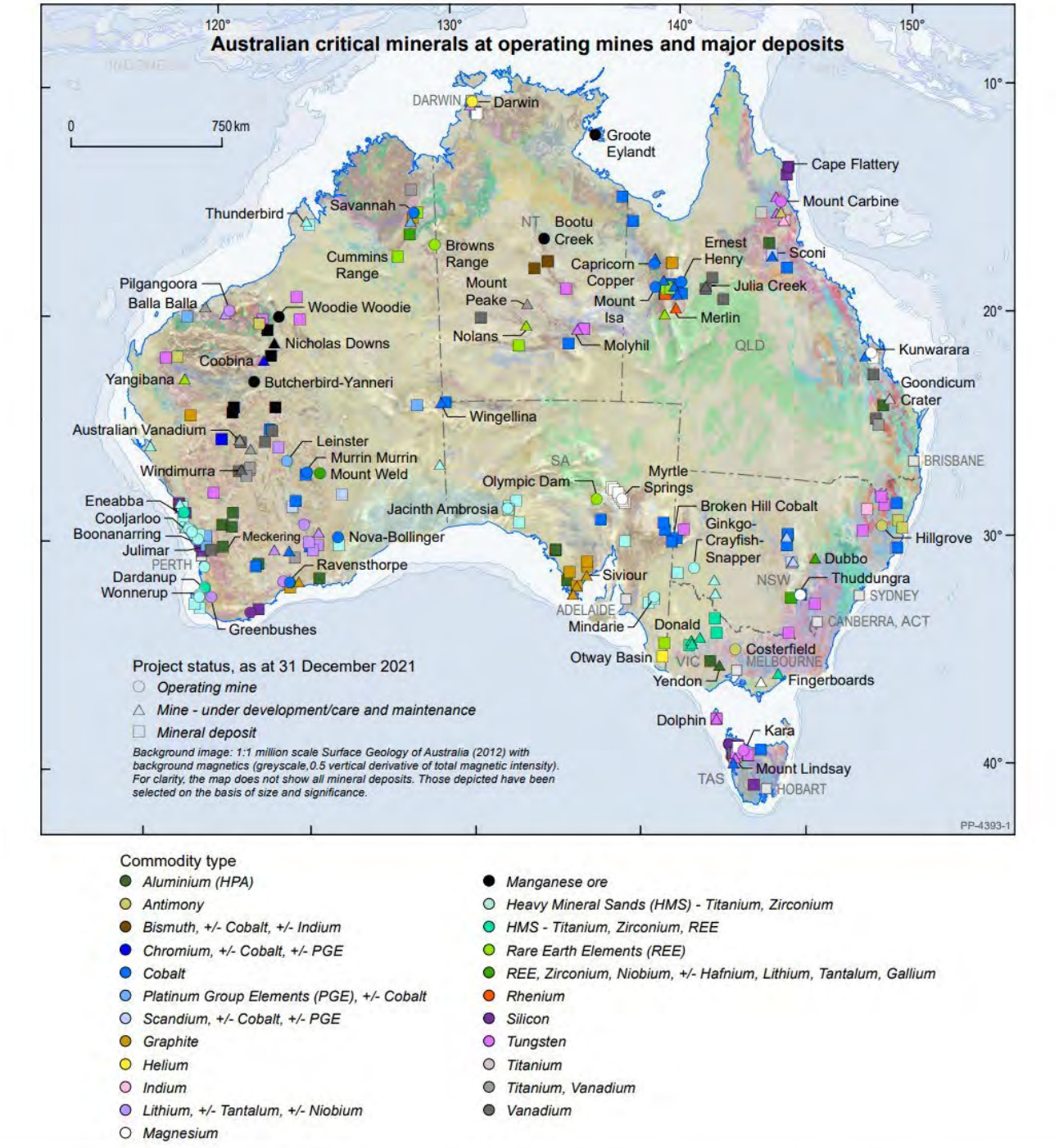
16 The EU identifies silicon metal as a critical mineral.

(Source: Department of Industry, Science, Energy and Resources 2022, 2022 Critical Minerals Strategy, March 2022).

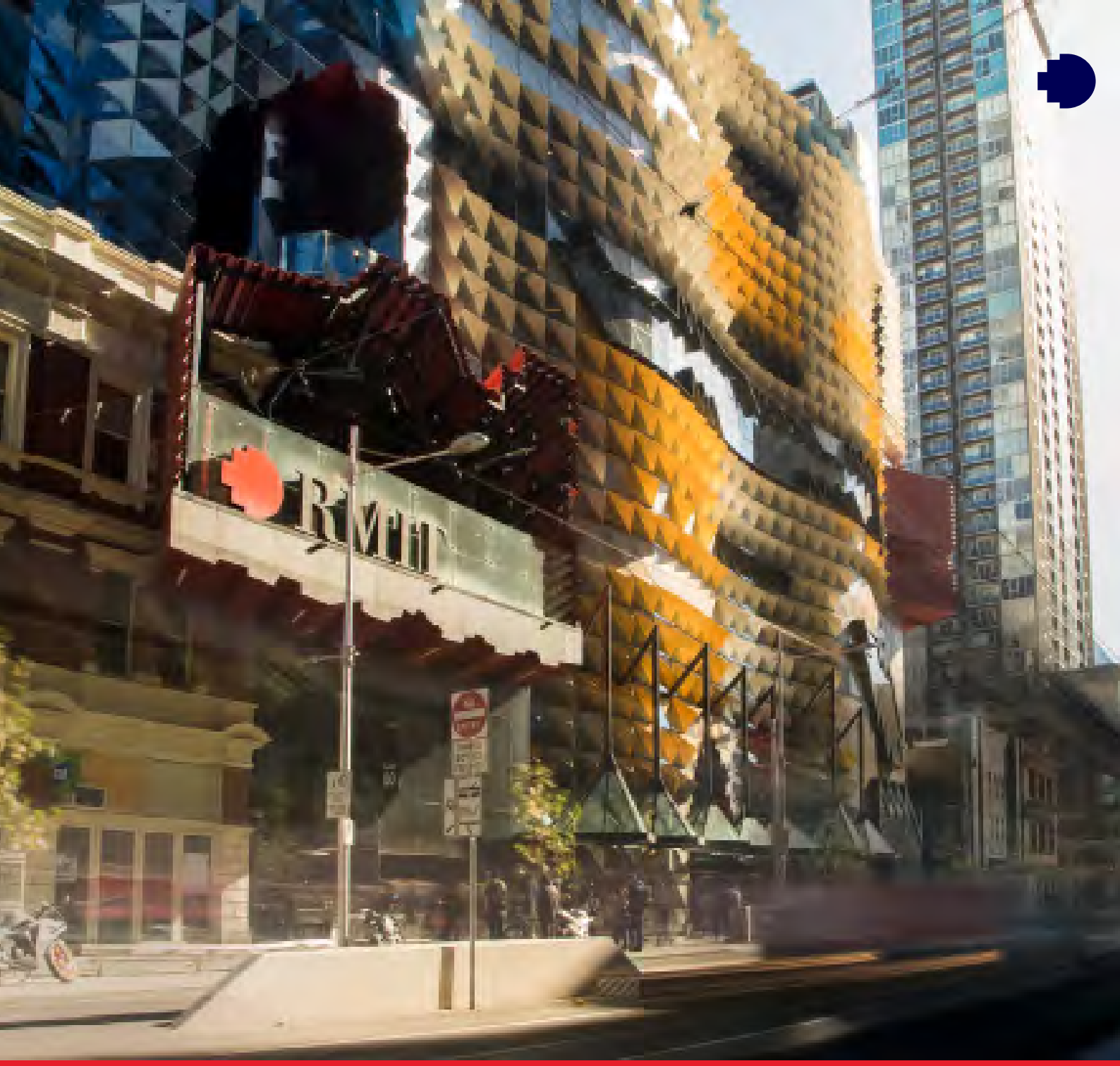
Appendix 5: Map of Australian critical minerals in mines

The following map, from the 2022 Critical Minerals Strategy, identifies Australian critical minerals (see Appendix 4 above) at operating mines in Australia and also identifies the major deposits of the commodity types.

Figure 14: Map of Australian critical minerals at operating mines and major deposits.



(Source: Department of Industry, Science, Energy and Resources 2022, 2022 Critical Minerals Strategy, March 2022).



Connect with us

By email

ccsri@rmit.edu.au

Website

rmit.edu.au/cyber

RMIT UNIVERSITY

Centre for Cyber Security Research and Innovation