isms.online

STATE OF INFORMATION SECURITY AUSTRALIA 2024

A SNAPSHOT OF THE IMPACT OF INFORMATION SECURITY ON BUSINESS RESILIENCE AND SUCCESS

PUBLIC V1.0

EXECUTIVE SUMMARY

MICHELLE MCCARTHY
HEAD OF ASIA PACIFIC
ISMS.ONLINE

This year's report, a collaborative effort of over 500 information security leaders across Australia, highlights a significant shift in the information security landscape.

As cyber threats continue to evolve, organisations are faced with the challenge of keeping pace. The introduction of new technologies, such as artificial intelligence and machine learning, has both amplified these challenges – with nearly a quarter of respondents reporting deepfake incidents – and opened up new avenues for enhanced security.

This report reveals that integrating strong information security business-wide is now a key focus and a source of business growth. Most businesses (79%) expect to increase their information security budgets for the next 12 months and 40% rank enhanced reputation as a secure and reliable entity as the best information security ROI.

Businesses prioritising a robust security posture and adhering to standards like ISO 27001 reap significant rewards. These include bolstered reputation, customer trust, and operational efficiencies. By effectively safeguarding their operations, these businesses are not only mitigating risks but also driving sustainable growth and resilience in the long run.

INTRODUCTION

Last year, the Government released the 2023–2030 Australian Cybersecurity Action Strategy and Plan, aiming to address the host of growing cyber threats and position Australia as a global leader in cybersecurity.

Aligning with this presents no small task for businesses. The strategy will inevitably require organisations to address their security posture in line with new government requirements – and for most, it's not just their own security posture they'll need to consider. Over a third of respondents to our State of Information Security report state that managing vendor and third-party risk is a key information security challenge they face.

Based on responses from 506 information security professionals working in finance, healthcare, education, technology, retail and e-commerce, the report provides an overview of Australia's current information security landscape.

We cover attitudes towards emerging technologies, how rapidly changing regulatory and compliance requirements are impacting businesses and ongoing information security challenges.

To get an in-depth view of the global information security landscape, you can read the Global State of Information Security Report 2024.

01 THE AUSTRALIAN RISK LANDSCAPE

Digitisation continues at pace, and Australian businesses are well aware of the need to manage supply chain risk. Managing vendor and third-party risk is cited as the number one information security challenge (37%) businesses are facing. Three-quarters (75%) have been impacted by a cybersecurity or information security incident caused by a third-party vendor or supply chain partner in the last 12 months.

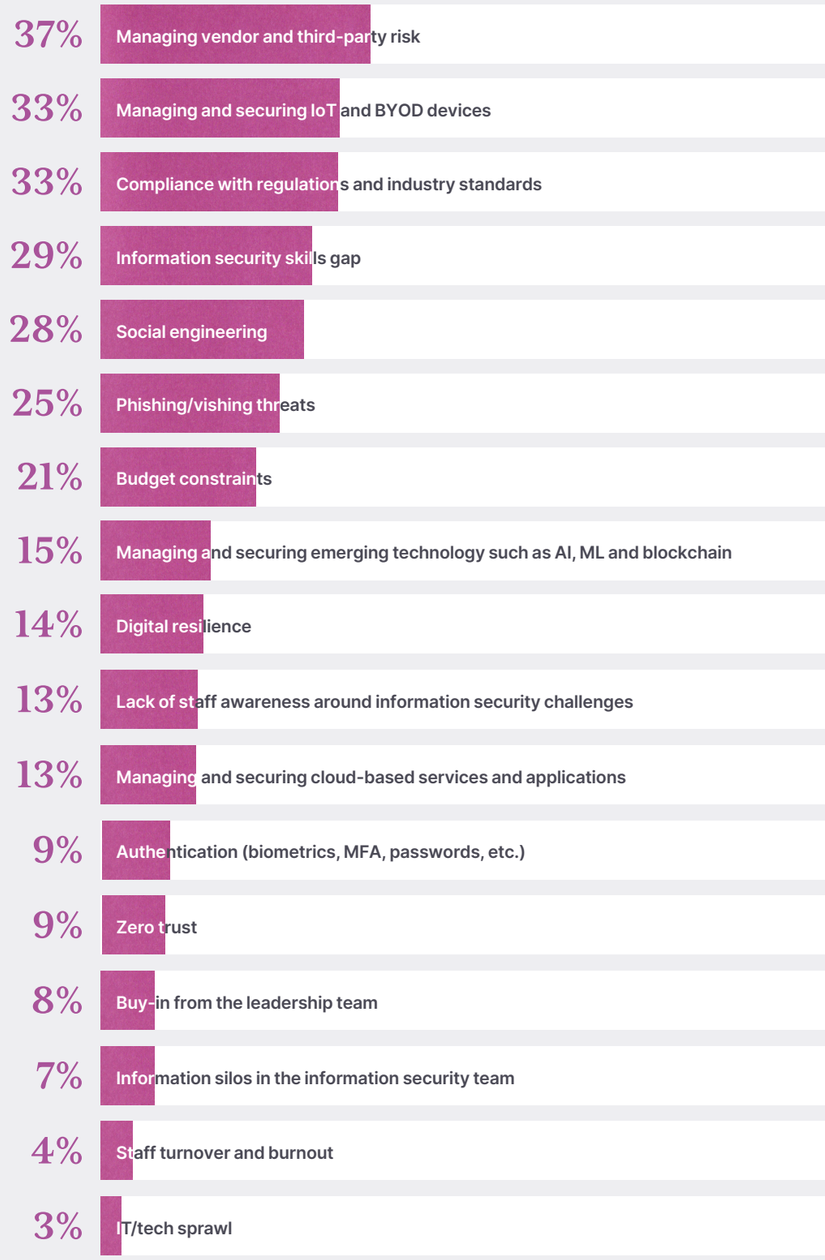
External access to systems and data poses complex issues that are not limited to vendors and supply chains. One in three organisations (33%) identify managing and securing the Internet of Things (IoT) and bring-your-own-device (BYOD) devices as a key challenge.

Businesses are still trying to address how employees use their own devices when working remotely. This includes home WiFi networks, personal mobile phones, and even public WiFi networks at cafés and other remote working locations. It's therefore unsurprising that using personal devices for work purposes without proper security measures is the top-ranking mistake made by employees, reported by over a third (36%) of respondents.

Three-quarters (75%) have been impacted by a cybersecurity or information security incident caused by a third-party vendor or supply chain partner in the last 12 months.

Compliance with regulations and industry standards (33%) also poses a significant issue for businesses. Almost three-quarters (73%) of respondents agree that the pace of regulatory change is making it hard to comply with information security best practices. Despite this, organisations clearly recognise the benefits of regulations and standards. 40% state that their enhanced business reputation as a secure and reliable entity has provided them with the best information security compliance ROI, and they're budgeting accordingly.

WHAT ARE THE CHALLENGES YOU ARE CURRENTLY FACING IN INFORMATION SECURITY?



02

THE COST OF POOR INFORMATION SECURITY

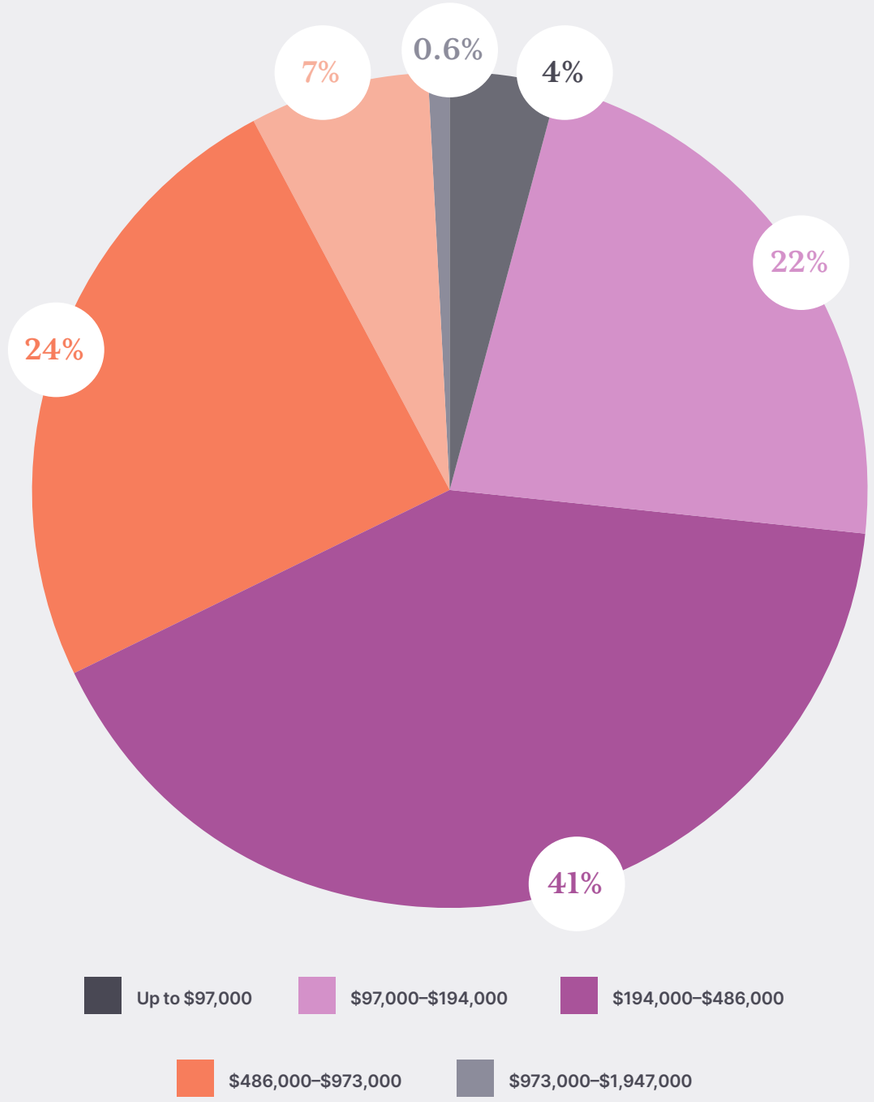
Violations of data protection rules and data breaches are leading to serious regulatory fines for businesses. Nearly three in four (72%) respondents have received fines of $194,000 or more in the last 12 months, and 7% have received fines between $973,000 and $1,947,000. This is an issue on a global scale – 75% of US respondents and 72% of UK respondents have received fines equivalent to AUS $190,000 or more.

As a result, 21% of respondents say complying with regulations to avoid penalties is motivating them to ensure strong information security and compliance. However, they ranked remaining competitive (34%) and increasing customer demand (33%) as top motivations, recognising that a robust information security posture presents key opportunities to win new business.

Nearly three in four (72%) respondents have received fines of $194,000 or more in the last 12 months

Organisations are now taking steps to address data breaches and data protection issues. Nearly half (46%) of respondents say they have increased their focus on employee education and awareness, and 42% have adopted a Zero Trust security model, using the "never trust, always verify" approach to reduce the risk of unauthorised access.

WHAT IS THE TOTAL AMOUNT YOUR BUSINESS HAS RECEIVED IN FINES FOR A DATA BREACH OR VIOLATION OF DATA PROTECTION RULES IN THE LAST 12 MONTHS?



03

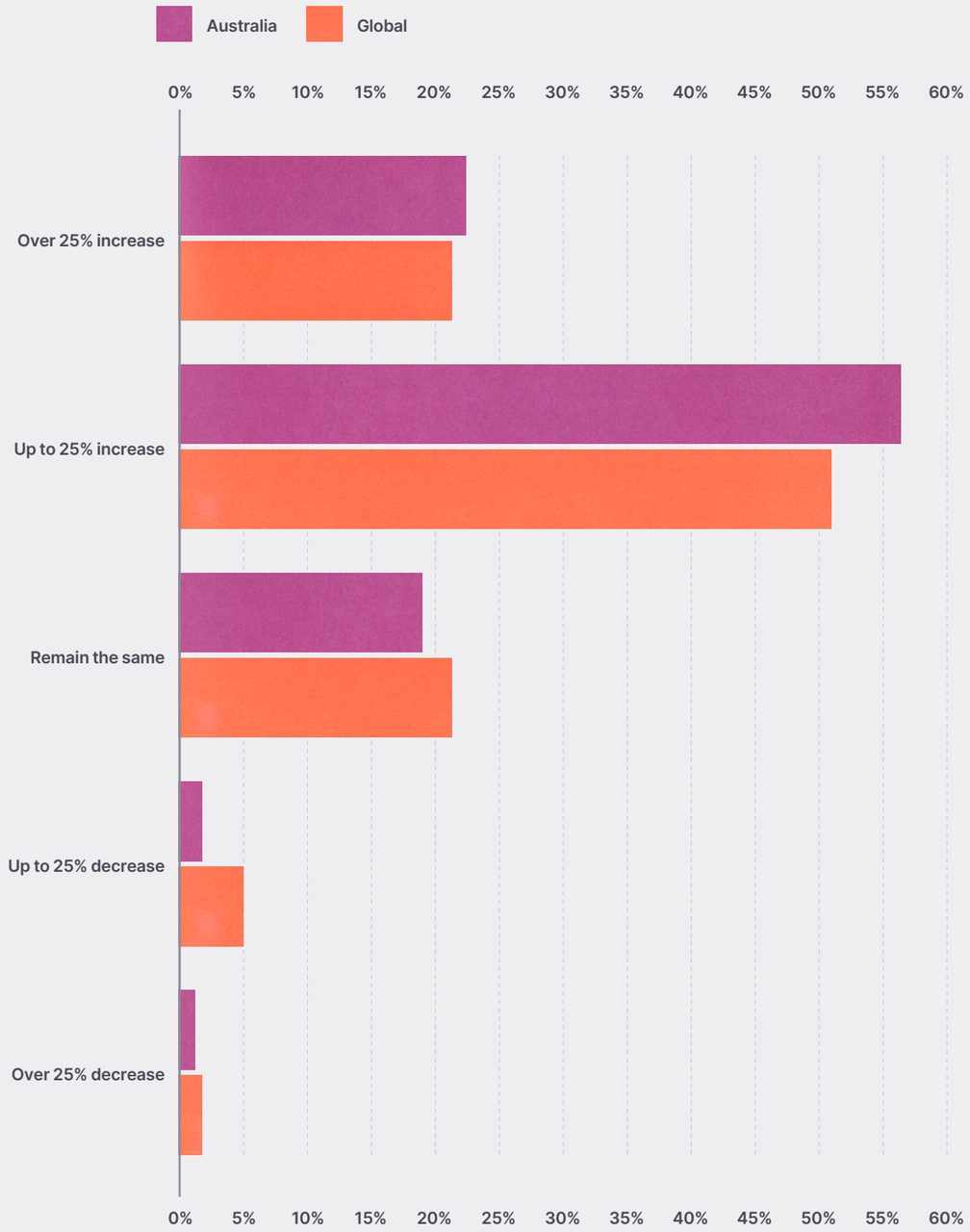
ORGANISATIONS ARE TAKING THEIR INFORMATION SECURITY SERIOUSLY

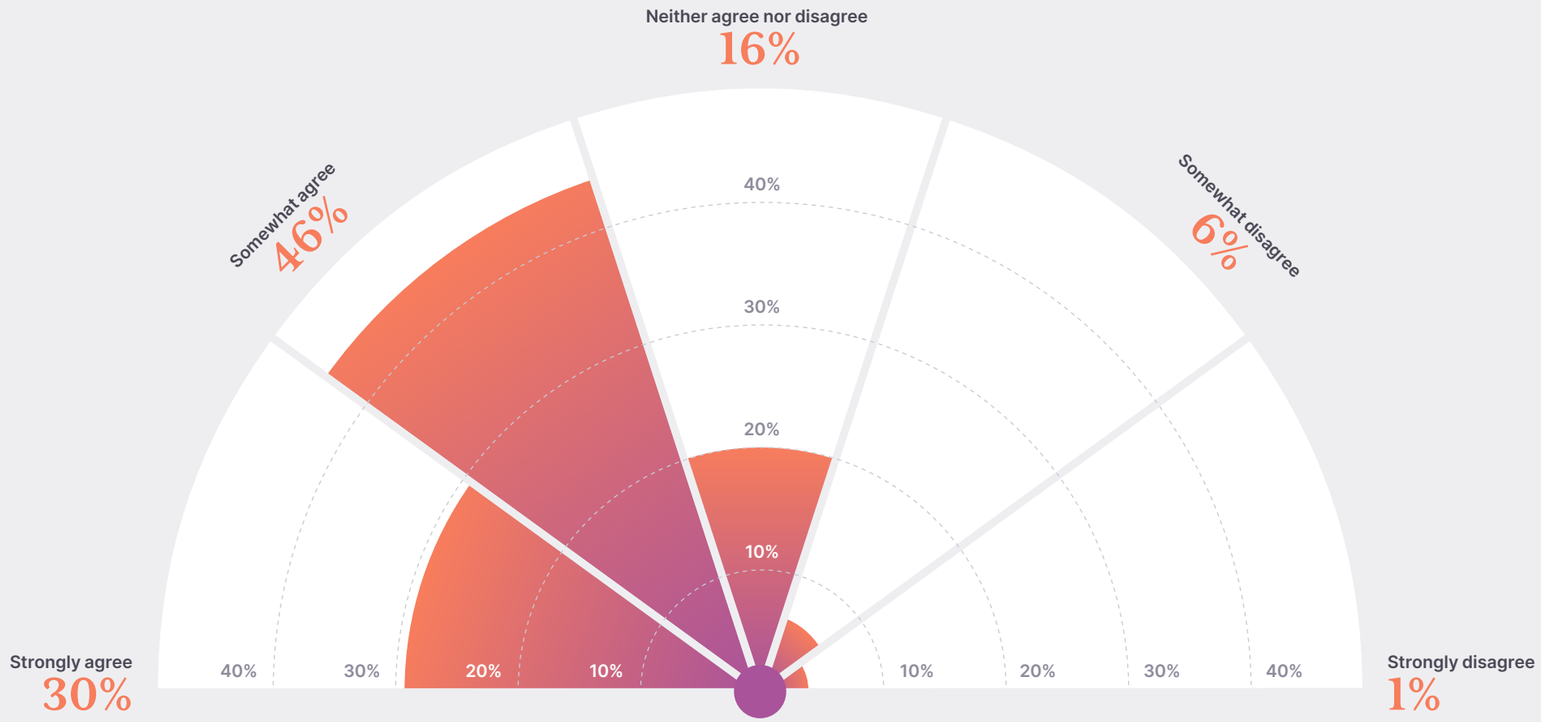
The majority of organisations surveyed (79%) expect to increase their information security spend in the next 12 months. This could be in response to the Cybersecurity Action Plan, regulatory fines or the spate of recent high-profile cyber attacks. However, it also reflects an encouraging viewpoint: confidence in information security as a vital tool to protect data and achieve a competitive advantage.

Is Australia already striding ahead in information security? Over three-quarters (76%) of respondents state that their organisation has a clear information security system or policy in place, markedly higher than the 67% global average. Encouragingly, 73% also agree senior leaders in their business understand the value of strong information security and view it as a priority, and 76% agree that every business should have an information security representative on the board.

Over three-quarters (76%) of respondents state that their organisation has a clear information security system or policy in place,

SPEND ON OVERALL INFORMATION SECURITY INITIATIVES AND RESOURCES





TO WHAT EXTENT DO YOU AGREE/DISAGREE THAT ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING TECHNOLOGY IS IMPROVING INFORMATION SECURITY?

04 EMBRACING NEW TECHNOLOGIES

Nine percent of businesses have experienced artificial intelligence (AI) privacy breaches in the last 12 months and surprisingly, 24% have been the victim of deepfake incidents. Given that deepfake technology is relatively new, it's concerning that it is both so accessible to threat actors and already presents a notable threat to nearly a quarter of businesses.

Despite this, respondents strongly support AI and machine learning (ML): 84% state that AI and ML are improving information security. In addition, 17% say that boosting their ability to adopt these new technologies securely motivates them to ensure strong information security. 69% expect to increase their spending on AI and ML security applications in the next 12 months.

With 76% of respondents also agreeing that the Cybersecurity Action Plan is realistic to achieve, this support for AI and ML reveals a real appetite for cyber innovation among Australian businesses.

Leading the way in the secure adoption of new technologies could support the Government's goal to position the country as a cybersecurity leader on the global stage.

05

ADDRESSING THE REGULATORY ELEPHANT IN THE ROOM

Nearly three-quarters (73%) of Australian businesses admit to struggling with the pace of regulatory change, agreeing that this makes it more difficult to comply with information security best practices. Despite this, Australian respondents were consistently the least likely to say that a standard or regulation named in the survey wasn't relevant to their business, showing a high level of commitment to information security best practices.

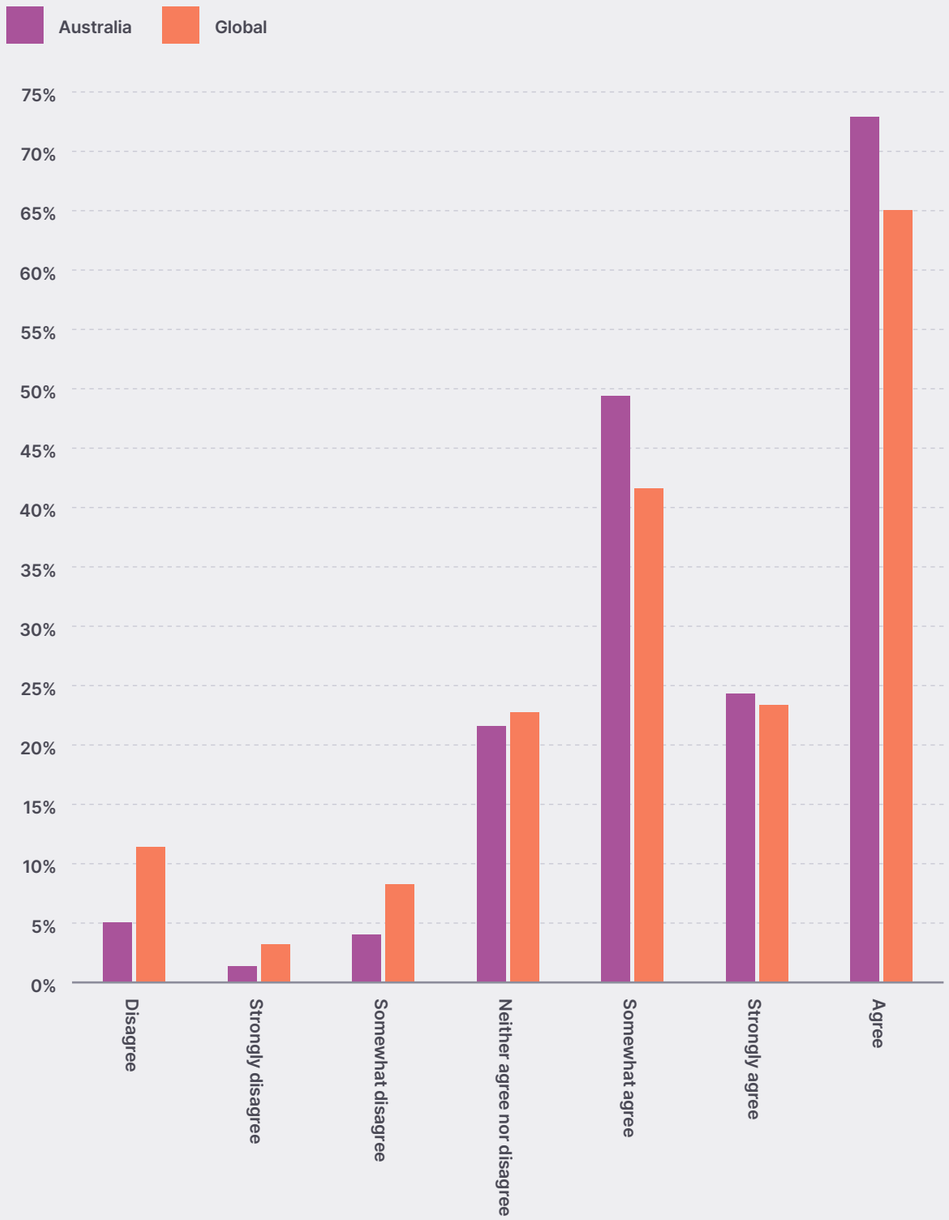
The difficulty appears to lie in the time it takes respondents to adopt existing regulations and standards, which can be vital to successful compliance. Only 38% of organisations state that Right Fit For Risk took them six months or fewer to implement, and that number lowers to 35% for Essential Eight.

Meanwhile, it took more than half (51%) of respondents six to 12 months to implement ISO 27001. Yet the ISO 27001 standard requires controls that address many of the key challenges faced by Australian businesses. Annex A includes A.5.19 Information Security in Supplier Relationships, A.6.3 Information Security and Privacy Awareness, Education and Training, and A.8.1 User Endpoint Devices. There are also 90 other organisational, people, physical and technological security controls.

The ISO 27001 standard requires controls that address many of the key challenges faced by Australian businesses.

Compliance with ISO 27001 allows organisations to implement a comprehensive, evolving information security management system (ISMS) and a set of processes to ensure data security. ISO 42001, the AI-focused standard enabling businesses to build an ethical, effective AI management system (AIMS), will also be highly relevant for proactive, tech-forward organisations in the next few years.

THE PACE OF REGULATORY CHANGE IS MAKING IT HARDER TO COMPLY WITH INFORMATION SECURITY BEST PRACTICES



06 CONCLUSION

Facing a multitude of cyber challenges, both human and machine, internal and external, organisations must now consider the most effective ways to address cyber threats. With a Government keen to establish the country as a cybersecurity leader and businesses indicating they're ready and willing to invest in information security, it's time to take action.

Key standards like ISO 27001, Right Fit For Risk, Essential Eight, and ISO 42001 provide frameworks that will help forward-thinking organisations align with the Government's ambitious Cybersecurity Strategy and reduce the impact of cyber risks. Additionally, compliance enables organisations to show customers, shareholders, and prospects that they're securing critical data.

ISMS.online is here to help ambitious organisations secure their data, achieve compliance up to five times faster, and seize the information security competitive advantage.

Get in touch

ABOUT ISMS.ONLINE

ISMS.online is revolutionising the way businesses across the globe handle data privacy and information security compliance.

The cutting-edge SaaS platform provides a comprehensive roadmap to robust and scalable governance, risk and compliance for organisations of all sizes and maturities.

With a global presence and over 25,000 users, including enterprise clients like Moneycorp, Siemens and Ricoh, ISMS.online simplifies complex processes across over 100 standards and regulations, empowering organisations worldwide to secure and scale their compliance with ease.

isms.online