Vanta



Australia State of Trust Report

Uncovering trends in security, compliance, and the future of trust

Table of Contents

Foreword 03

Key Findings 04

Part One: The Security Improvement Imperative 06

Part Two: The Trust Management Tipping Point 11

Conclusion 14

Methodology 15



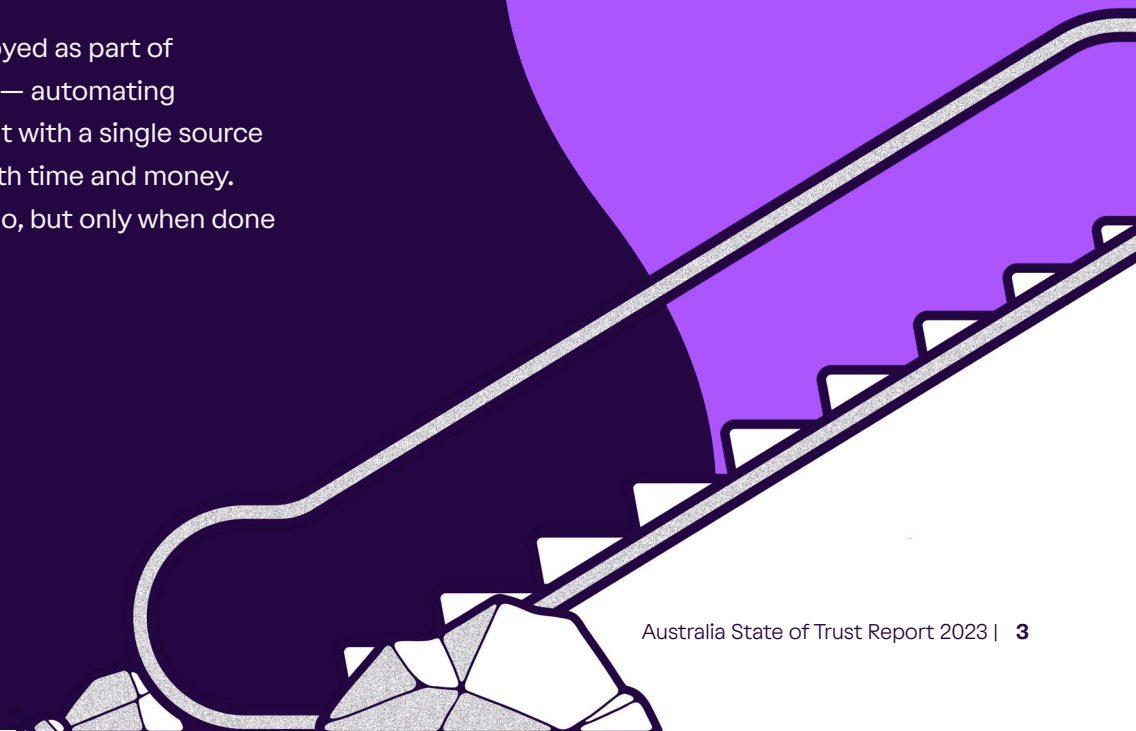
Foreword

Australian businesses today are navigating an unprecedented security landscape. The expansion of attack surfaces in a post-pandemic hybrid world, combined with shrinking teams and budgets, and the rapid rise of Generative AI, are fuelling an urgent need for companies to improve — and prove — their security posture.

Vanta's State of Trust Report (Australia edition) reveals that two-thirds (67%) of businesses say they need to improve security and compliance measures, with nearly one in four (23%) rating their organisation's security and compliance strategy as merely reactive.

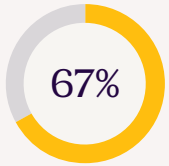
With rising risk and shrinking resources, the message is clear: businesses need new methods to improve their security. Compounding the urgency is the ever-evolving global regulatory landscape and growing compliance time-suck it entails. A KPMG study of 400 businesses found that two of the top five issues for Australian business leaders in 2023 included "dealing with cyber risks", and "evolving regulatory processes, reporting changes and impacts".[1] In a global environment where customers need proof of a company's security practices, organisations are at an impasse. So, what's the solution?

As we'll uncover, automation can accelerate security and compliance when deployed as part of a broader, proactive trust management strategy. Focusing on trust management — automating time-consuming compliance tasks, centralising security programme management with a single source of truth, and streamlining security reviews — can unlock significant savings of both time and money. Supercharging these capabilities with AI will further disrupt the security status quo, but only when done responsibly and transparently.



1 - https://kpmg.com/au/en/home/insights/2023/01/australian-business-leader-challenges-2023.html

Key Findings - Australia

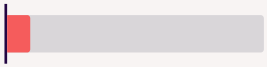


Two thirds

say their business requires improved security and compliance measures.

Only 9%

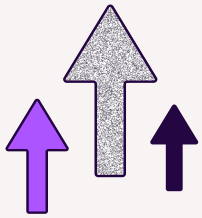
of IT budgets are dedicated to security.



Respondents say they could save at least two hours each week if security and compliance tasks were automated.

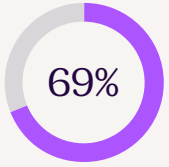


2 hours per week



73%

Nearly 3 in 4 say a better security and compliance strategy would positively impact their business through greater efficiency.



Two thirds

of businesses say that customers, investors and suppliers are increasingly looking for proof of security and compliance.



47%

Respondents believe the biggest transformation potential of AI will be improving the accuracy of security questionnaire responses and eliminating manual work.



79%

of businesses are already or planning to use AI/ML to detect high risk actions.

Respondents spend on average 7.4 hours per week on security compliance. That's 355 hours — 9 working weeks — per year.



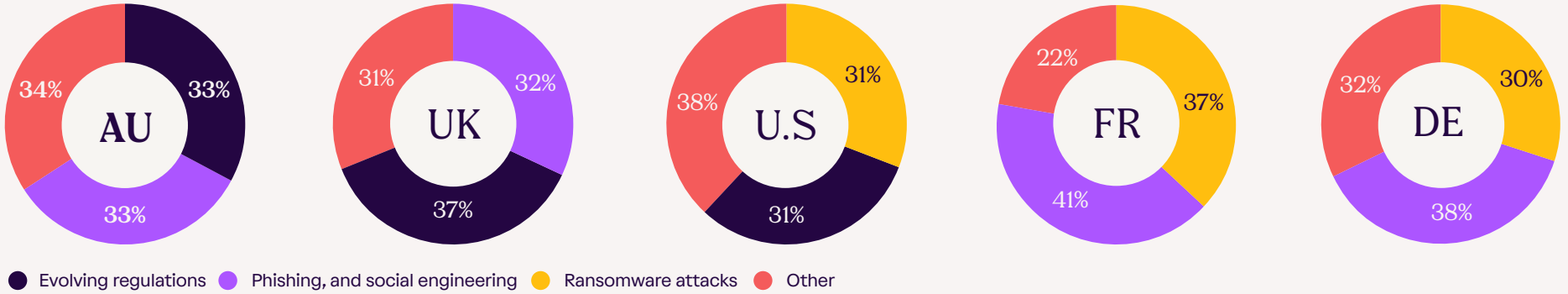
7.4 hours per week

KEY FINDINGS

Australia vs other countries

Australian leaders are most likely to say their biggest security concerns are keeping up to date with evolving regulations and phishing, and social engineering against staff, both at **33%.**

Other countries: In the UK, the biggest security concerns are also keeping up to date with evolving regulations (37%) and phishing and social engineering against staff (32%). In the U.S., evolving regulations (31%) and ransomware attacks (31%). In France, phishing and social engineering (41%) and ransomware (37%). In Germany, phishing and social engineering (38%), and ransomware (30%).



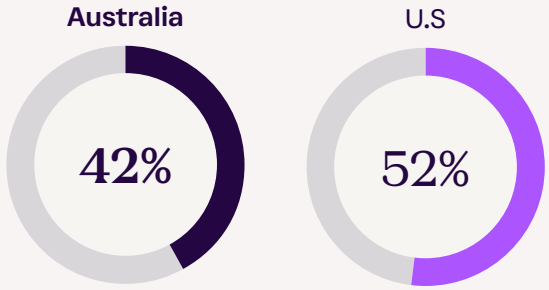
Internal audit reports (**43%**) are the most common way of proving security to customers in **Australia.**

This is matched by France and the U.S. at 43% while Germany is at 39%.

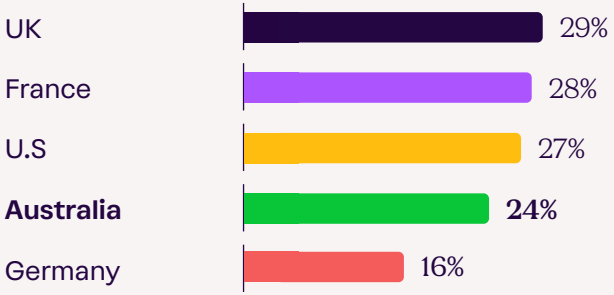


Fewer than half of **Australian** organisations (**42%**) rate their risk visibility as strong — lower than all other countries surveyed except the UK (42%).

The U.S., by contrast, rated itself at 52%.



Australian leaders feel that a lack of IT budget is less of a barrier to maintaining a robust security programme (**24%**) than all other countries except Germany (16%).



The security improvement imperative

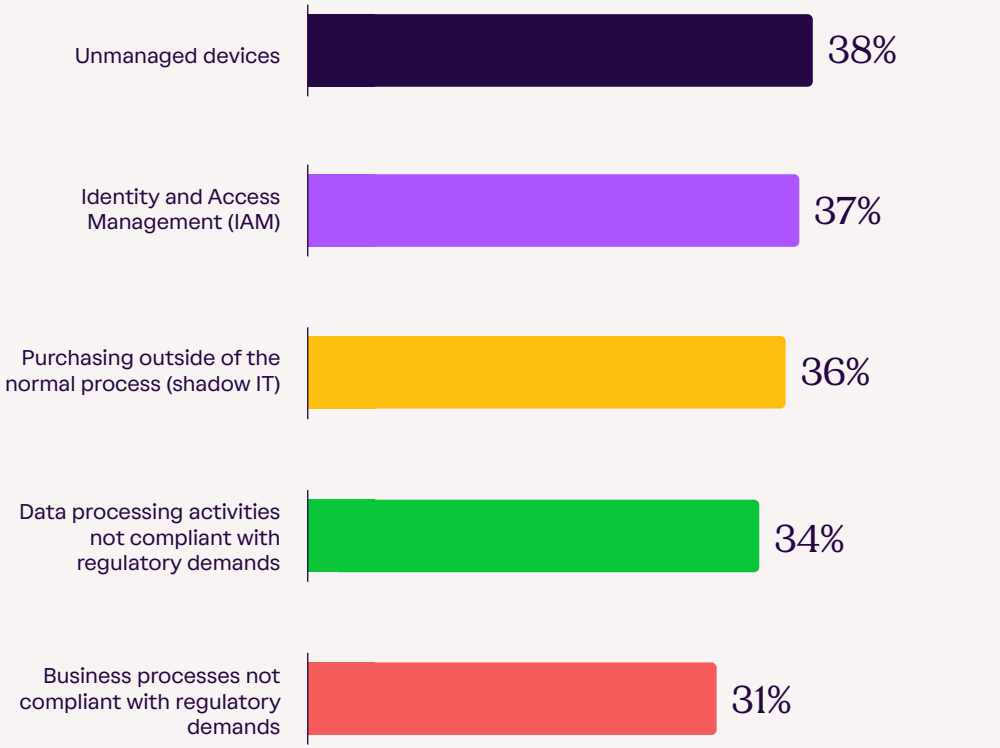
The State of Trust Report surveyed 2,500 global IT and business decision-makers (with 500 respondents from the Australia) and reveals the urgent need for businesses to improve security.

Two-thirds (67%) of Australian respondents believe their business needs to improve both security and compliance measures.

Australia's latest Annual Cyber Threat Report[2] (from July 2021 to June 2022) tracked 76,000 cybercrime reports, an increase of nearly 13% from the previous financial year. This is one report every seven minutes, accelerating from eight minutes the previous year. This cost Australian small businesses $39,000 and over $62,000 for large businesses filing a report.

For Australian companies of all sizes, limited risk visibility and blind spots accelerate this need to improve security and compliance. Only 4 in 10 (42%) organisations rate their risk visibility as strong. Meanwhile, unmanaged devices (38%) and identity and access management (37%) are the two biggest blind spots for Australian organisations.

What are your organization's biggest IT security and compliance blind spots?



2 - https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022 survey-2023

Security as a selling point

Over two-thirds (69%) say that customers, investors and suppliers are increasingly looking for proof of security and compliance.

But companies are struggling to maintain and demonstrate their security posture, even in the face of growing customer demand.

While 43% provide internal audit reports (compared to 41% globally), 36% third-party audits (matching the global average), and 35% complete security questionnaires (vs 36% globally), 16%, the highest market surveyed, admit they don't or can't provide evidence when asked. This means Australian companies are falling at the very first hurdle, costing potential revenue and growth opportunities.

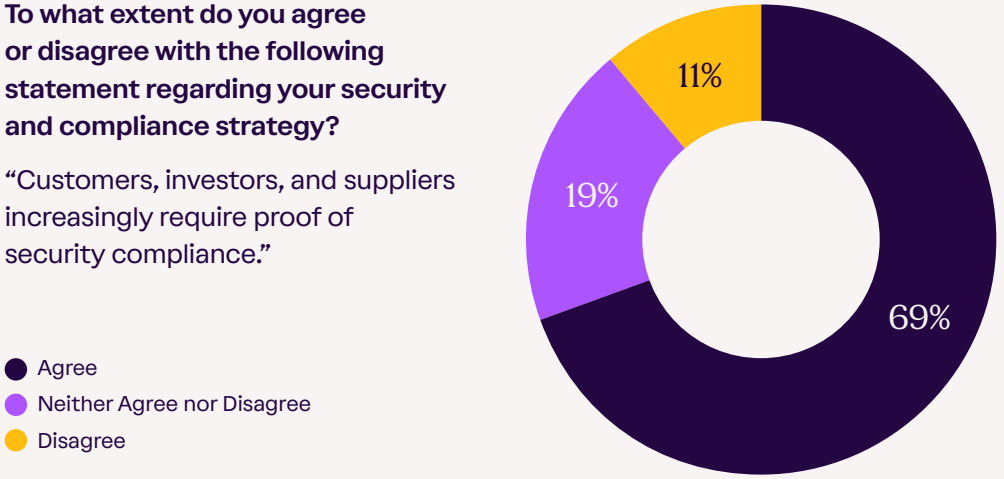
According to respondents, the biggest barriers to proving and demonstrating security externally are a lack of automation to replace manual work (34%) and the volume of customer and security and compliance requests (33%).

This comes at a time when 46% of Australian businesses surveyed say they have already, or plan to reduce IT staff. Just under a third of leaders (30%) say that their overall IT budgets have shrunk as they continue navigating the economic downturn as the Australian economy faces various threats in late 2023[3]), while 57% have either already downsized IT security budgets or are planning to.

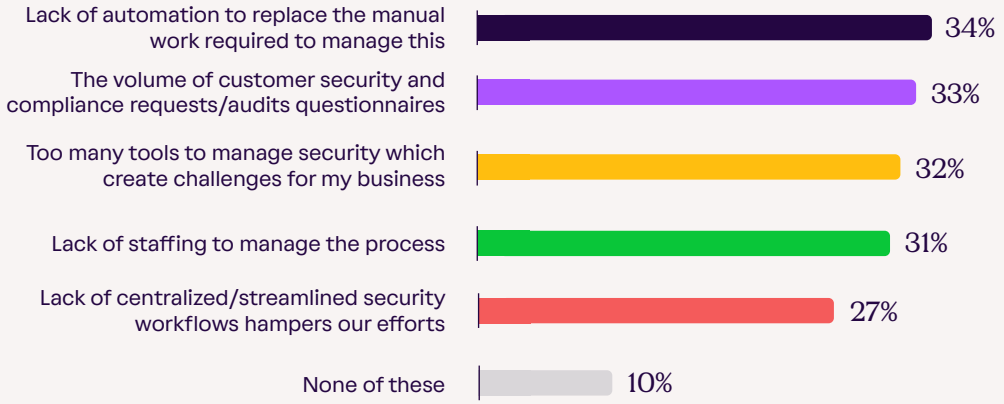
On average, only 9% of Australian IT budgets are dedicated to security, further exacerbating resource constraints.

To what extent do you agree or disagree with the following statement regarding your security and compliance strategy?

"Customers, investors, and suppliers increasingly require proof of security compliance."



What are your biggest barriers to proving and demonstrating security externally?



3 - https://www.theguardian.com/business/2023/oct/01/australian-economy-faces-multiple-threats-to-recovery-amid-global-paper-cuts

Compliance deprioritized

Given these trends, it's not surprising that respondents admit they're not prioritising compliance due to the time and financial investment. But failure to comply ultimately costs these companies potential revenue and growth opportunities, particularly in expanding to new markets.

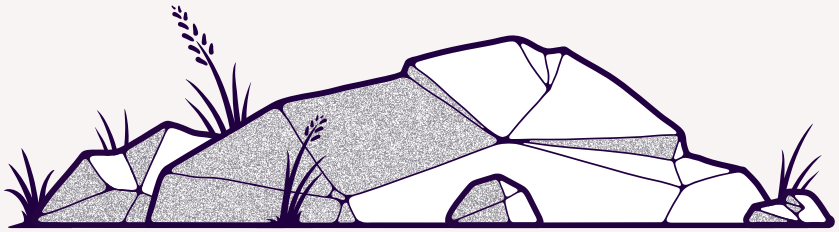
Time is being plunged into businesses' efforts to meet and maintain the demands of compliance. Respondents spend an average of 7.4 hours per week (9 working weeks per year) on compliance.

Exacerbating this time-suck, more than half (53%) of respondents say that remaining compliant with different international regulations is becoming increasingly difficult.

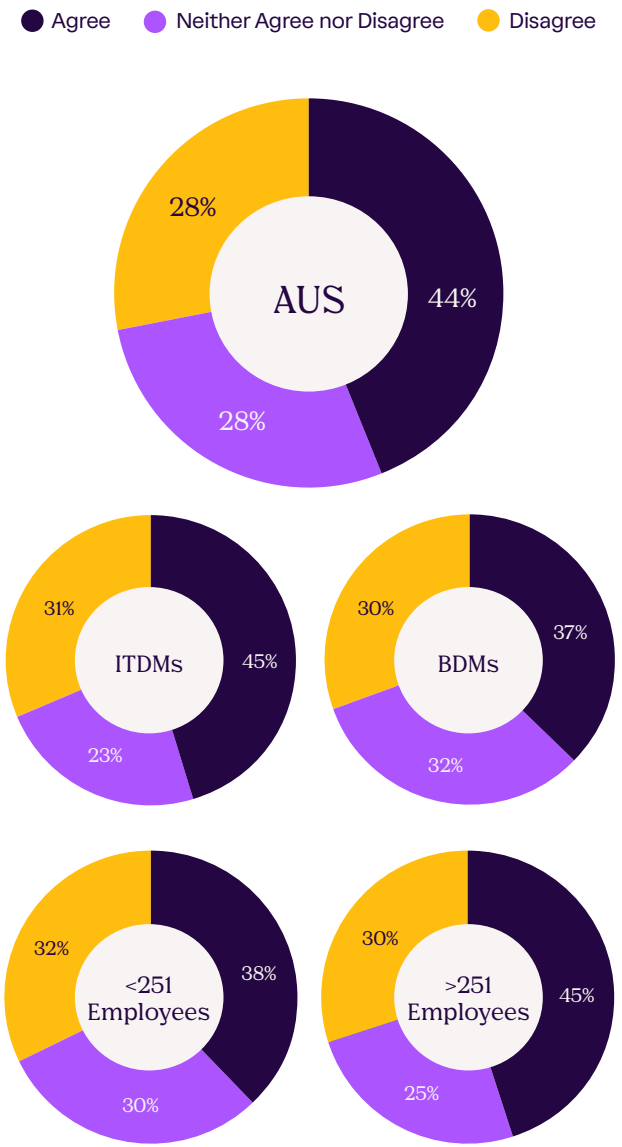
Nearly half (46%) of businesses have deprioritised compliance due to the time it takes, with 44% admitting that it's due to the required financial investment.

The two biggest barriers to proving and demonstrating security externally are a lack of automation to replace manual work (34%) and the volume of customer and security and compliance requests (33%).

But increasingly, new means to automate compliance are transforming the way companies demonstrate trust.



"My business... has deprioritized compliance due to the investment it requires."



“Having industry-recognized certification enables us to build trust and make the deal that little bit easier to close.”

Prue Burns, Head of Legal & Data Security
Josef

Keeping up with regulations in Australia

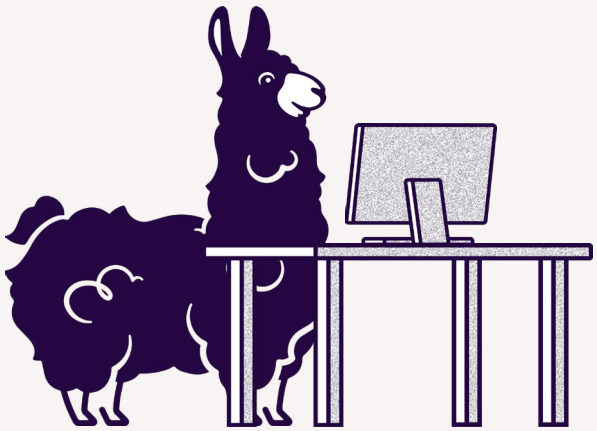
- Specific Australian regulation includes the Security of Critical Infrastructure Act 2018 (Cth)[4], applying to 22 critical infrastructure asset classes in 11 sectors — with additional Commonwealth, state, and sector-specific legislation.
- With China being Australia's biggest trade partner, major Chinese regulations include The Cybersecurity Law, Data Security Law, and Personal Information Protection Law.
- Europe's Cybersecurity Resilience Act and GDPR are the main applicable legislation across the EU.
- ISO 27001 or SOC 2 are the most common security frameworks adopted by technology companies to demonstrate their security. ISO 27001 is an international standard generally accepted globally while SOC 2 is popular in North America.

Enter AI

AI has enormous potential to reduce the repetitive, manual work needed to achieve compliance and prove security. By automating tedious tasks that teams have no choice but to perform manually, businesses have more time to focus on strategic work.

Australian businesses recognise the opportunity. 79% already or plan to use AI/ML to detect high risk actions in Australia — second only to the U.S. (82%). However, well over half (62%) are concerned that secure data management is becoming more challenging with AI adoption. And over half (58%) say that using Generative AI could erode customer trust.

As a result, 53% of businesses say regulating AI would make them more comfortable investing in it. This is particularly true for organisations with more than 250 employees who are more likely to agree compared to smaller companies (58% to 48%).



4 - https://www.legislation.gov.au/Series/C2018A00029

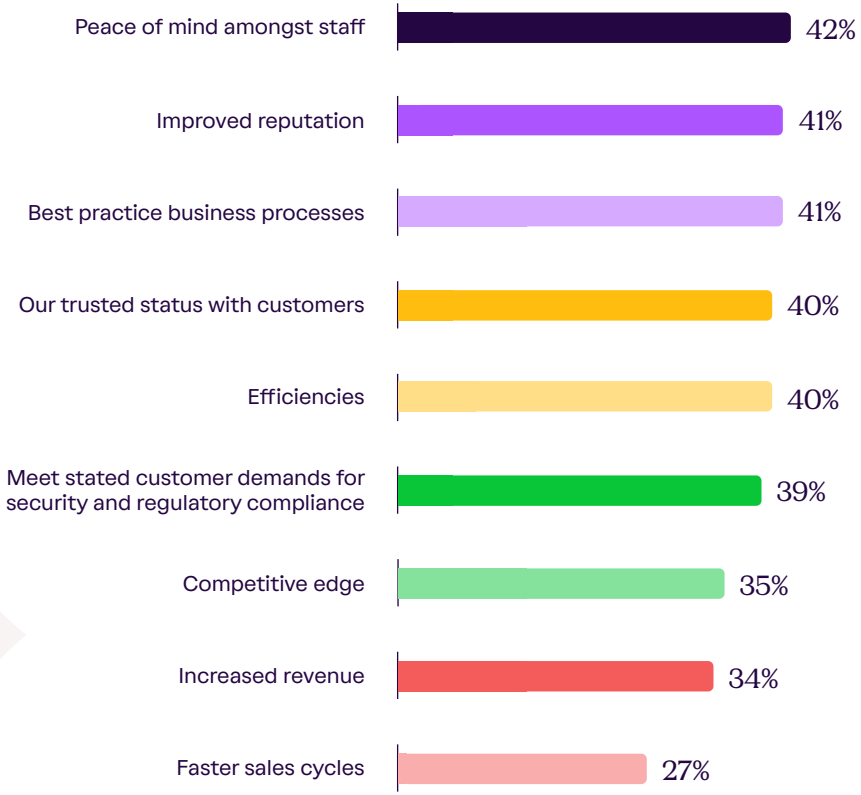
PART TWO

The trust managment tipping point

The business case for better security is plain to see. Ultimately, it improves efficiency and boosts the bottom line. Three in four (75%) Australian leaders say that a better security and compliance strategy positively impacts their businesses thanks to stronger customer trust, while nearly three in four (73%) agree that a better security and compliance strategy would make them more efficient. For 41%, the biggest value-driver of good security practices is improved reputation.



Thinking about good security practices, what value do they drive for your business?



PART TWO

Streamlining security and compliance through automation

Improving and proving security doesn't need to be a heavy lift. In fact, 66% of respondents believe that time and money could be saved by automating compliance with different regulations and frameworks.

Automation brings trust and transparency to life, and companies are taking notice. Two-thirds (67%) of businesses have increased or plan to increase their use of automation, in particular for reducing manual work and in improving the accuracy of security questionnaire responses (47% and 40%).

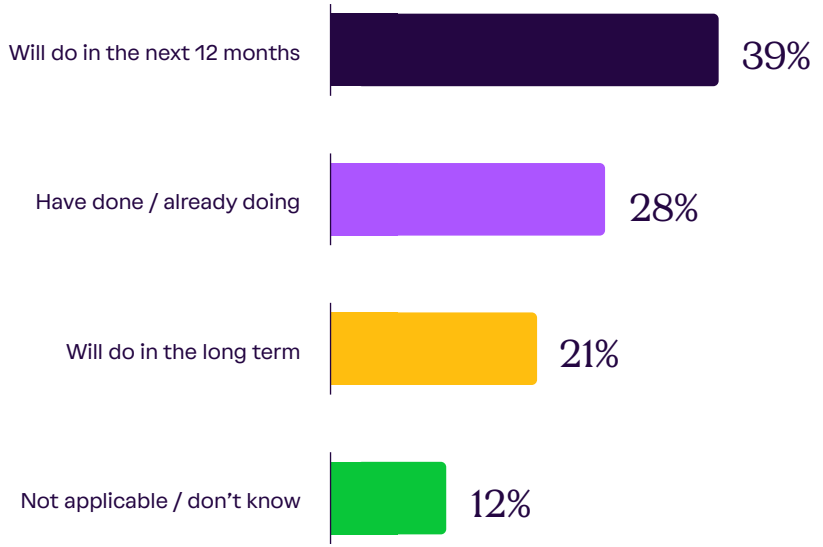
This is true for compliance as well as overall security management. On average, respondents believe they could save at least two hours per week — over 2.5 working weeks a year — if security and compliance tasks were automated.

Three-fifths (59%) agree that their business is more likely to consider automating security compliance when scaling to different markets. And one crucial way to do that is through use of a trust management platform.



Thinking about your security and compliance strategy, what steps or measures will your business take in the near future to de-risk?

"Work with vendors to automate compliance."



PART TWO

Accelerating security workflows and transforming trust with AI

While AI offers both new opportunities and new risks, when done right, it can dramatically accelerate security workflows, enabling teams to focus on strengthening their security posture and building customer trust.

Respondents in Australia think AI can be transformative to eliminating manual work (47%), improving the accuracy of security questionnaires (40%), streamlining vendor risk reviews and onboarding (35%), and reducing the need for large teams (32%).

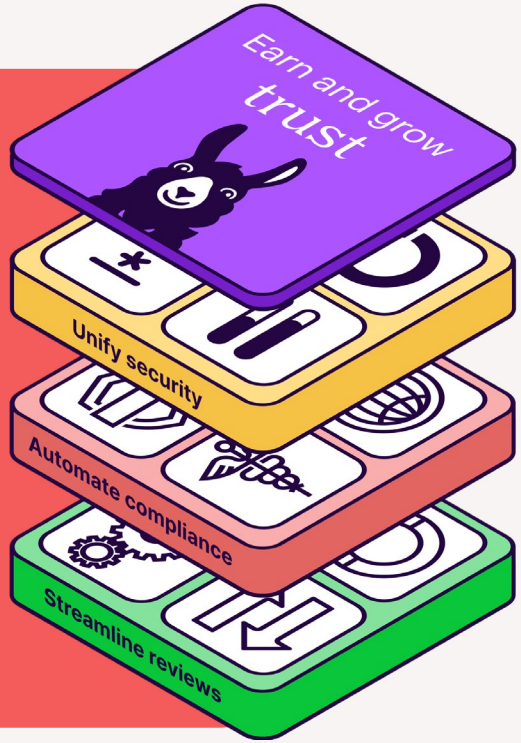
Whether that's saving time, budget or staffing resources, AI can help you do more with less: time-consuming tasks can be handed off to AI. But in a climate of growing cyber-threats, and AI tools presenting a new risk surface, it is essential to prioritise transparency and trust when deploying AI.

What is trust management?

Trust management[5] is a holistic approach to defining, managing, maturing, and proving your security and compliance commitments. It's a concerted and intentional effort to both become more secure and communicate that security to instil confidence in both prospects and customers.

A trust management platform provides a single source of truth for centralising and accelerating these efforts. Key capabilities of a trust management platform include unified security program management, automated compliance, and streamlined security reviews.

With a trust management platform, businesses of all sizes are able to move from point-in-time assessments to real-time visibility of their security posture, enabling them to increase efficiency, reduce risk, and demonstrate trust continuously.



5 - https://www.vanta.com/resources/what-is-a-trust-management-platform

Conclusion

Improving and proving security is harder than ever. The risk of attacks is rising, and AI has added another layer of complexity for Australia's IT and business leaders to navigate. In today's challenging economic climate, the data shows that companies have been forced to reduce the resources and budget to solve these very problems.

Organisations are being slowed down by manual tasks and face increased risk as they mature. Without the ability to prove their security efforts, companies can't scale, leaving themselves vulnerable to falling behind competitors.

The tipping point for trust management is here.

Supercharged by AI, trust management is critical to reducing the tedious and repetitive security tasks that pull teams away from their most strategic work. For companies at the forefront of this disruption, centralising security processes, automating compliance, and accelerating security reviews can turn trust into a truly marketable advantage.

By closing the loop on the security lifecycle from compliance through continuous monitoring and communication, businesses can transform how they build trust and ultimately unlock growth.



Trust management essentials

- **Centralise:** With 67% of Australian leaders believing their business requires improved security and compliance measures, establish a central source of truth to unify security and compliance programmes.
- **Invest:** Australian organisations dedicate only 9% of their IT budget to security. Security underpins growth — invest to unlock opportunities.
- **Automate:** Australian leaders are the least likely to provide proof of compliance to customers. Automation can reduce manual work like collecting evidence and completing security questionnaires.
- **Demonstrate:** Australian leaders are most likely to say they are concerned about AI's impact on customer trust, so lean into proactively demonstrating trust, providing transparency, and helping customers understand the power and potential of new technologies.

Vanta

Research methodology

In September 2023, quantitative research conducted by Sapio Research was commissioned by Vanta to understand the challenges and opportunities businesses are facing when it comes to security and trust management. Vanta and Sapio co-designed the questionnaire and surveyed the behaviours and attitudes of 2,500 businesses across Australia, France, Germany, the UK, and U.S. The local data in this report comes from 500 Australian organisations.

About Vanta

Vanta is the leading trust management platform that helps simplify and centralise security for organisations of all sizes. Thousands of companies including Atlassian, Autodesk, Chili Piper, Flo Health and Quora rely on Vanta to build, maintain and demonstrate their trust — all in a way that's real-time and transparent.

For more information, visit www.vanta.com