Vanta

UK State of Trust Report

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

Table of Contents

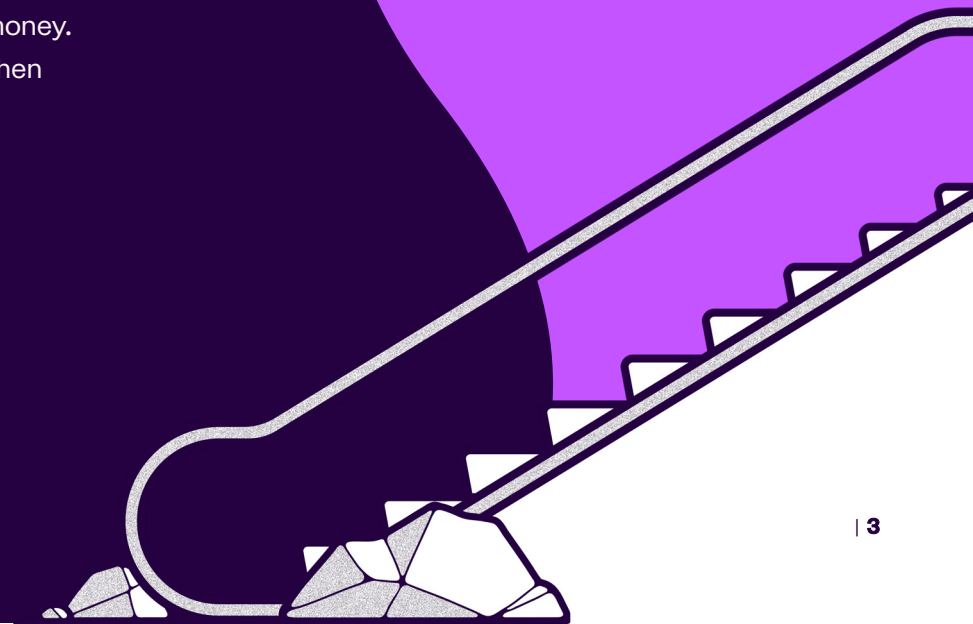
Foreword

UK 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.

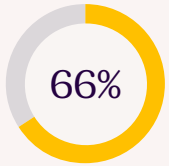
Vanta's State of Trust Report (UK edition) reveals that two-thirds (66%) of businesses say they need to improve security and compliance measures, with one in four (25%) rating their organisation's security and compliance strategy as merely reactive.

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 as UK firms are encouraged to look beyond Europe and expand globally. In an environment where customers increasingly want more 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.



Key Findings - UK

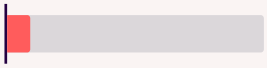


Two thirds

of business and IT leaders say their business requires improved security and compliance measures.

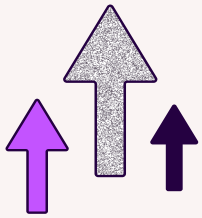
Only 9%

of IT budgets are dedicated to security.



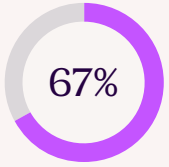
Respondents say they could save at least two hours per week – three working weeks a year – if security and compliance tasks were automated.

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.

43%

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

78%

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

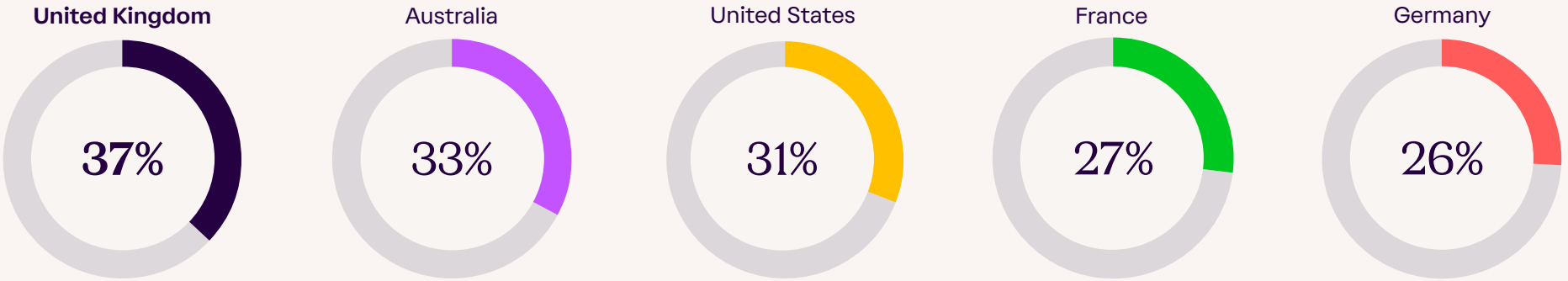
Respondents spend on average 7.5 hours each week on security compliance. That's 360 hours — over working nine weeks — per year.

7.5 hours per week

KEY FINDINGS

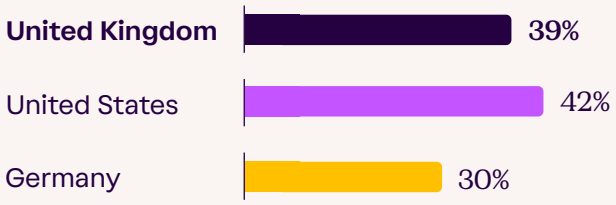
The UK vs other countries

UK leaders are most likely to say that keeping up to date with evolving regulations is their biggest security concern, at **37%.**



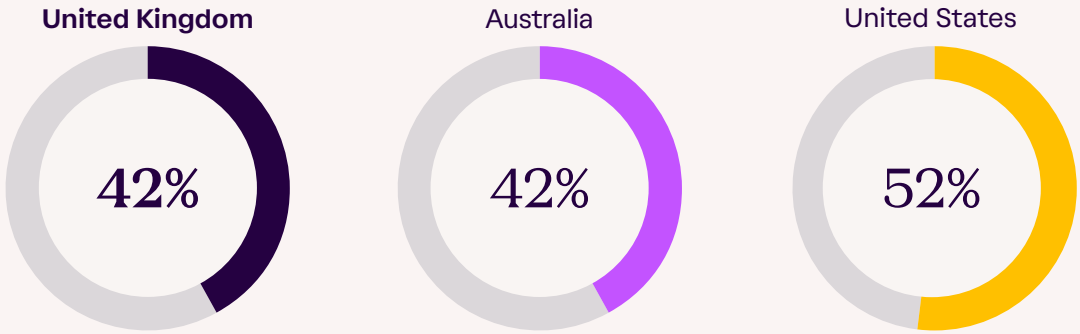
In the **UK,** filling in security questionnaires (**39%**) is the most common way of proving security to customers.

This is more common in the U.S. at 42% and less common in Germany at 30%.



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

The U.S., by contrast, was at 52%.



The security improvement imperative

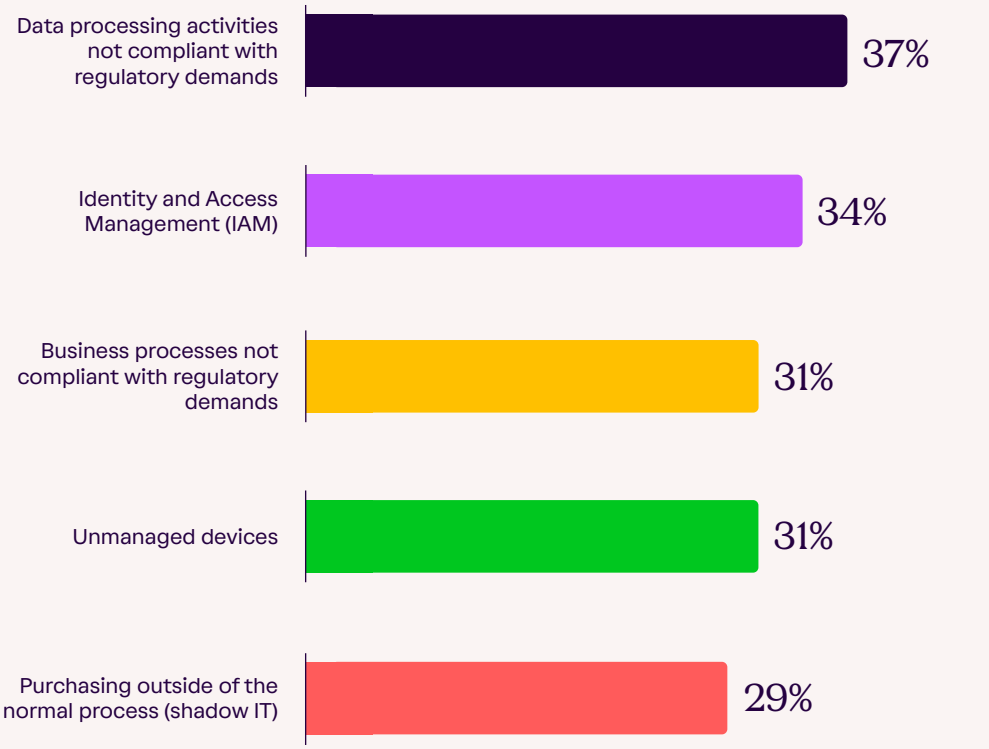
The State of Trust Report surveyed 2,500 global IT and business decision-makers (with 500 respondents from the UK) and reveals the urgent need for businesses to improve security.

Two-thirds (66%) of UK respondents believe their business needs to improve both security and compliance measures.

Cyber security is a major priority for business leaders, according to the UK's national 2023 Cyber Breaches Survey.[1] The latest results represent "an apparent decrease in prioritisation from last year".

For UK companies of all sizes deprioritization could lead to increased business risk. In fact, limited risk visibility and blind spots from Vanta's survey show an imperative to improve security and compliance. Only 4 in 10 (42%) organisations rate their risk visibility as strong. Meanwhile, data processing that doesn't comply with regulations (37%) and identity and access management (34%) are the two biggest blind spots for organisations.

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



1 - https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

Security as a selling point

Two-thirds (67%) 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 37% provide internal audit reports (vs 41% global average), 37% third-party audits (matching the global average), and 39% complete security questionnaires (compared to 36% globally), one in eight (matching the global average at 12%) admit they don't or can't provide evidence when asked. This means UK companies are falling at the very first hurdle, costing potential revenue and growth opportunities.

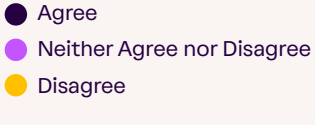
According to respondents, the biggest barriers to proving and demonstrating security externally are a lack of staffing (33%) and automation to replace manual work (30%).

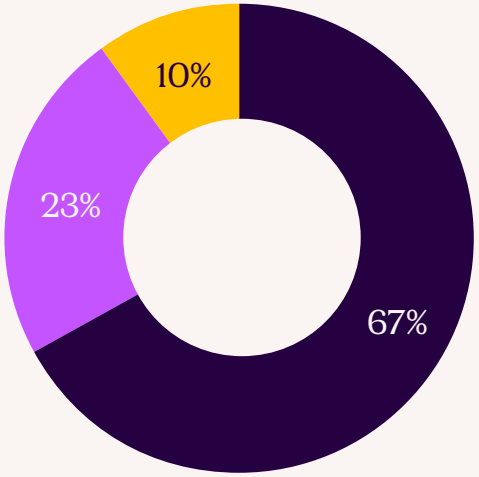
This comes at a time when 46% of UK businesses surveyed say they have already, or plan to reduce IT staff. One third of leaders (34%) say that their overall IT budgets have shrunk as they continue navigating the economic downturn, while 62% have either already downsized IT budgets or are planning to.

On average, only 10% of UK IT budgets are dedicated to security, further exacerbating resource constraints.

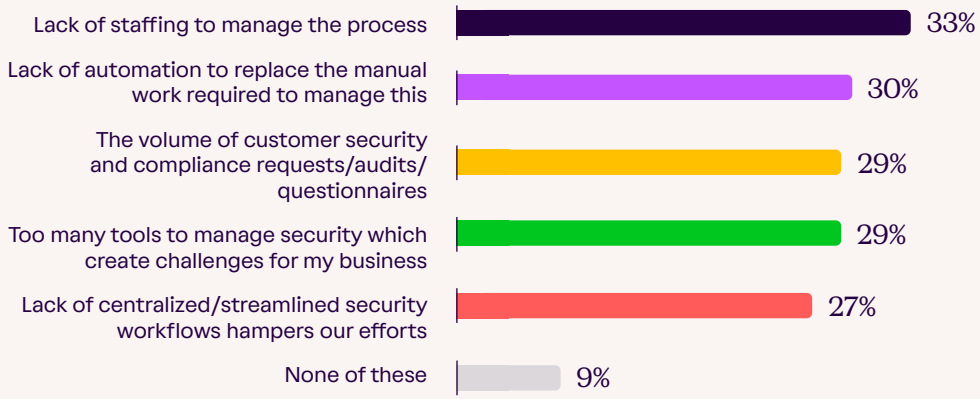
To what extent do you agree or disagree with the following statement regarding your security and compliance strategy?

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





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



“Being an AI company requires us to build an even deeper level of trust because this technology is largely unknown. We need our customers to see us as a trusted partner to help them implement this.”

Peadar Coyle, CTO and Co-Founder
AudioStack

Compliance deprioritized

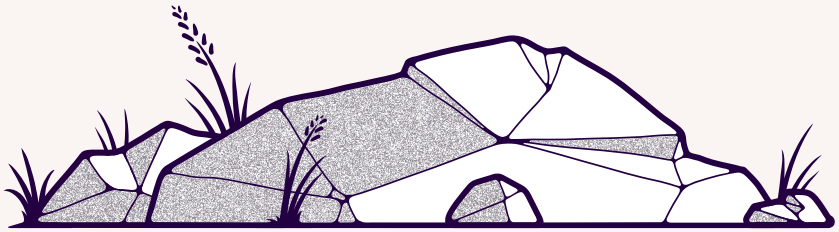
Given these trends, it's not surprising that respondents admit they're not prioritising compliance due to the time and financial investment. But failure to comply ultimately costs these companies potential revenue and growth opportunities, particularly when expanding to new markets.

Time is being plunged into businesses' efforts to meet and maintain the demands of compliance. Respondents spend an average of 7.5 hours per week (more than 9 working weeks per year) on compliance.

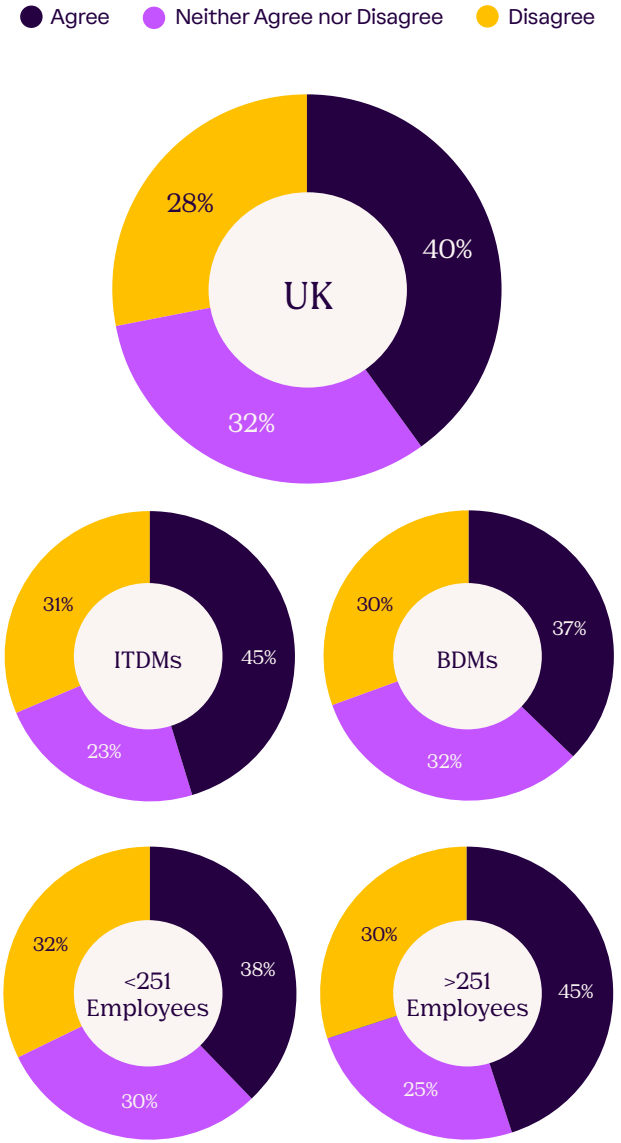
Exacerbating this time-suck, more than half (57%) of respondents say that remaining compliant with different international regulations like HIPAA and GDPR is becoming increasingly difficult.

Nearly half (45%) of businesses have deprioritised compliance due to the time it takes, with 40% admitting that it's due to the required investment.

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."



Keeping up with UK regulations

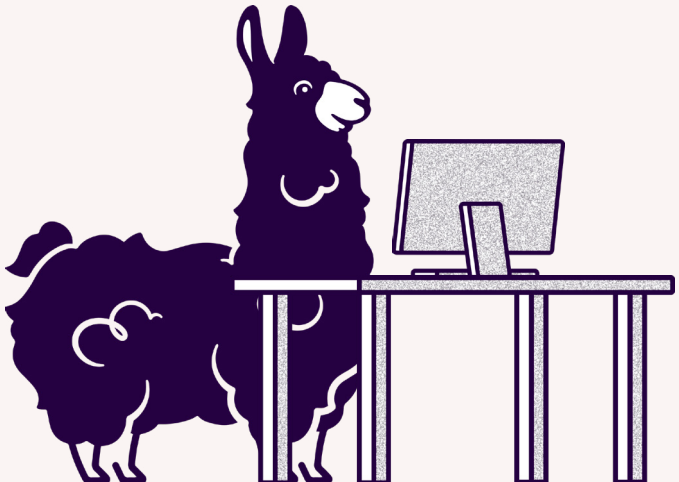
The UK General Data Protection Regulation (UK GDPR), states that personal data must be processed securely using appropriate technical and organisational measures. The Data Protection Act 2018 and the EU's Networks and Information Systems (NIS) Directive (until changed in UK law) also apply and are essential for well-managed and trustworthy business operations.

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.

UK businesses recognise the opportunity. 78% already or plan to use AI/ML to detect high risk actions. However, over half (57%) are concerned that secure data management is becoming more challenging with AI adoption. And half (51%) say that using Generative AI could erode customer trust.

As a result, 55% 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 (63% to 48%).

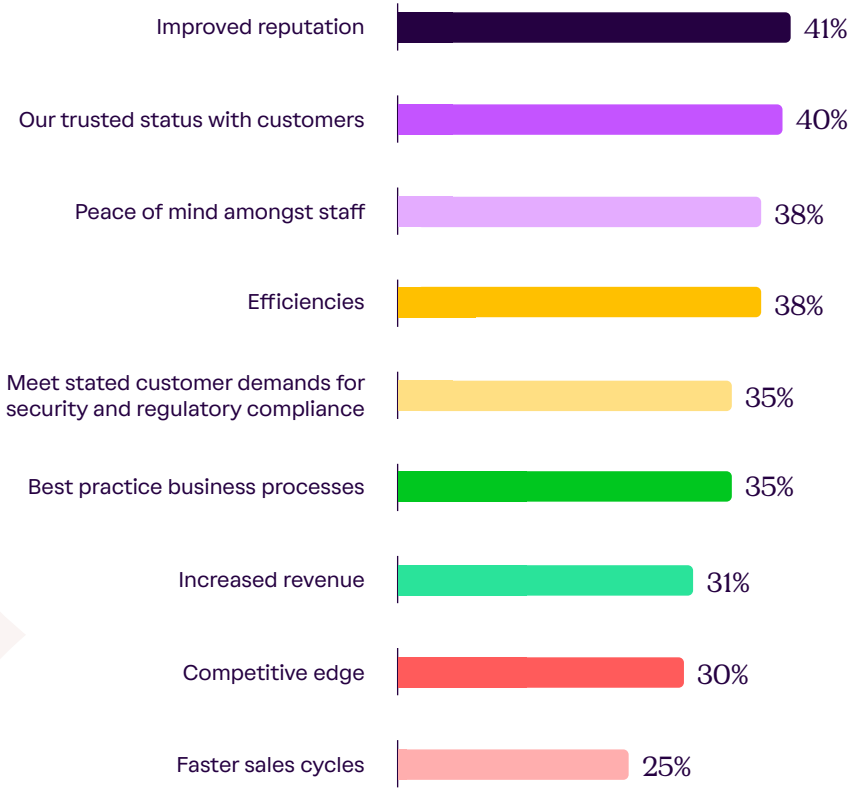


PART TWO

The trust managment tipping point

The business case for better security is plain to see. Ultimately, it improves efficiency and boosts the bottom line. Nearly seven out of ten (68%) UK leaders say that a better security and compliance strategy would positively impact their businesses, and 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

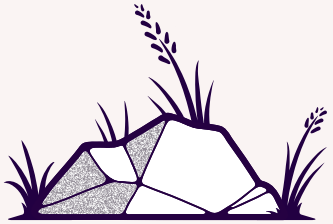
Streamlining security and compliance through automation

Improving and proving security doesn't need to be a heavy lift. In fact, 62% 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. 64% of businesses have increased or plan to increase their use of automation.

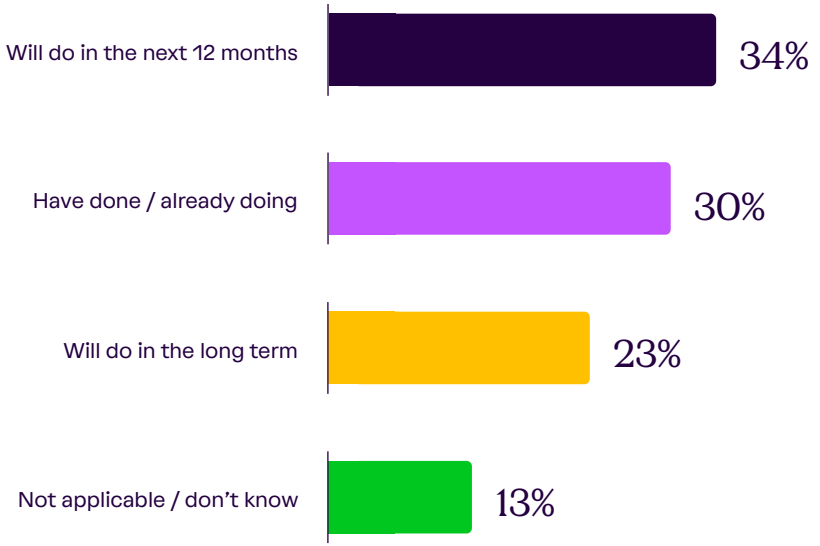
This is true for compliance as well as overall security management. On average, respondents believe they could save at least two hours per week — over 2.5 working weeks a year — if security and compliance tasks were automated.

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 the UK think AI can be transformative to improving the accuracy of security questionnaires (43%), eliminating manual work (43%), reducing the need for large teams (34%), and streamlining vendor risk reviews and onboarding (33%).

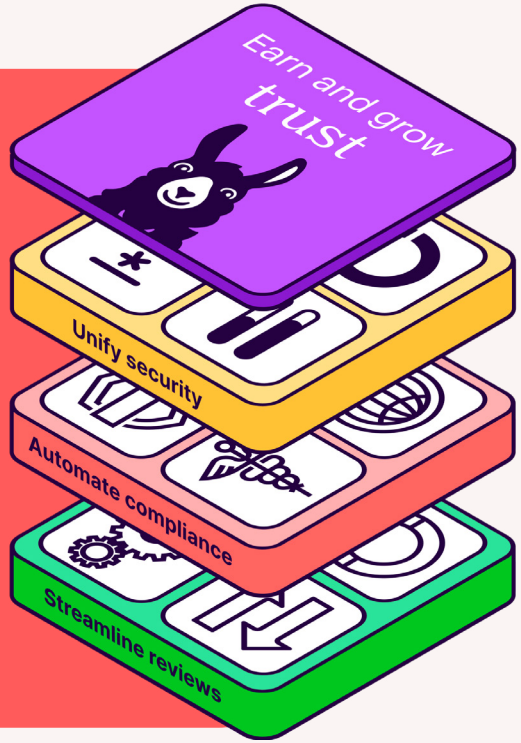
Whether that's saving time, budget or staffing resources, AI can help you do more with less: time-consuming tasks can be handed off to AI. But in a climate of growing cyber-threats, and AI tools presenting a new risk surface, it is essential to prioritise transparency and trust when deploying AI.

What is trust management?

Trust management[2] 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.



2 - 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 IT and business leaders in the UK 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 UK leaders citing blind spots around data processing and identity and access management - among others - establishing a central source of truth unifies your security and compliance programmes.
- **Invest:** The UK is the most likely market surveyed to say that lack of IT budget is a barrier to maintaining a robust security programme. Security underpins growth — invest to unlock opportunities.
- **Transparency:** UK firms are most likely to fill in security questionnaires, so showcase security measures through audits, continuous monitoring, and a public Trust Centre.
- **Automate:** UK leaders are the most likely to say that keeping up to date with evolving regulations is their biggest security concern. Automation and AI can help reduce the manual work involved and streamline efforts.

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 UK 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