Vanta

Germany State of Trust Report

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

Table of Contents

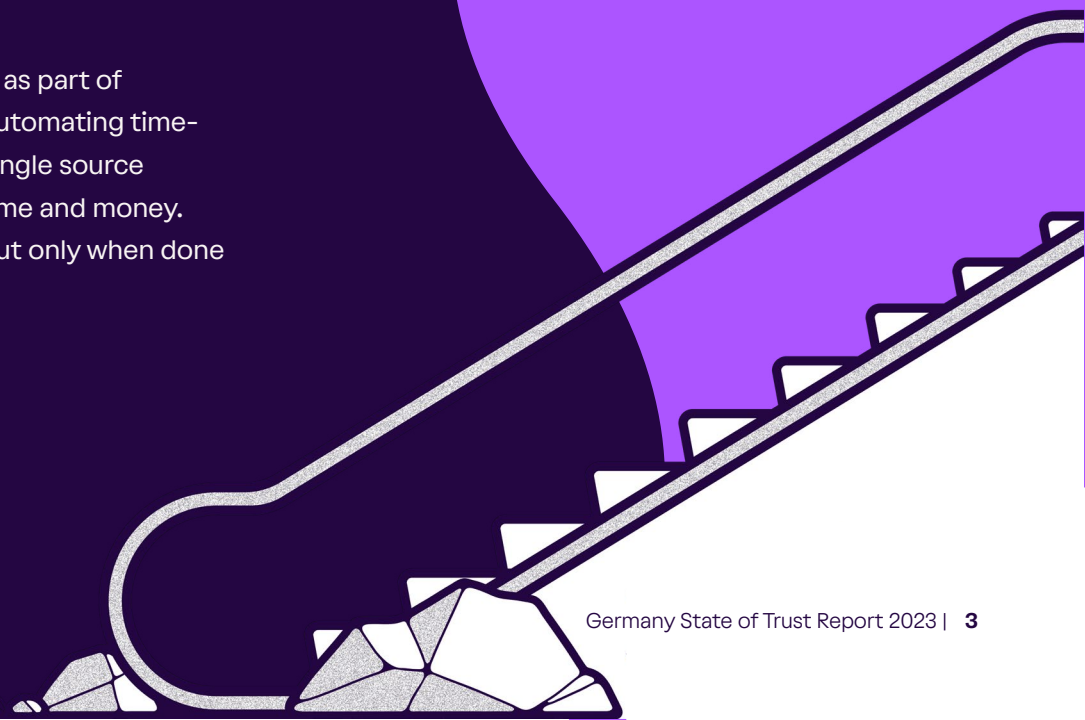
Foreword

German 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.

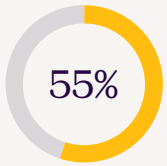
Vanta's State of Trust Report (German edition) reveals that over half (55%) of businesses say they need to improve security and compliance measures. Of the five countries surveyed — Australia, France, Germany, the UK and U.S. — German leaders are the least likely to say that their business needs this improvement. Additionally, one in five (20%) rate 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 German firms seek to expand their operations globally in a volatile economic landscape. 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 - Germany

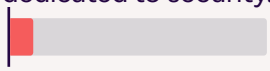


Over half

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

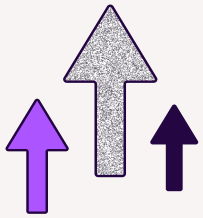
Only 9%

of IT budgets are dedicated to security.



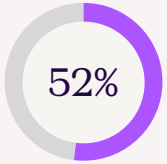
Respondents say they could save at least two and a half hours per week – nearly three working weeks a year – if security and compliance tasks were automated.

2 .5 hours per week



65%

Two thirds say a better security and compliance strategy would positively impact their business through greater efficiency.



Over half

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

41%

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

76%

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

Respondents spend on average 7.3 hours each week on security compliance. That's 350 hours — nine working weeks — per year.

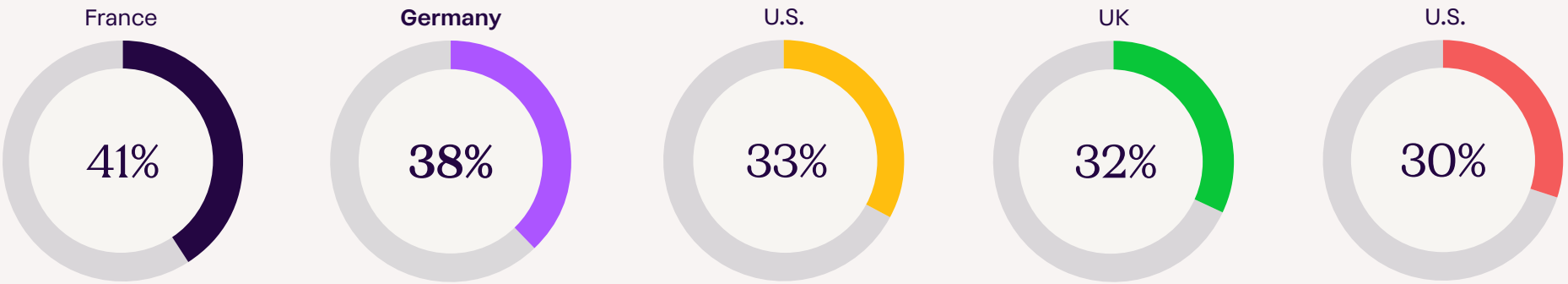
7.3 hours per week

KEY FINDINGS

Germany vs other countries

German leaders say that phishing and social engineering against their staff is their biggest security concern, at **38%.**

Other countries: France, 41%; UK, 32%; Australia, 33%; and U.S., 30%.



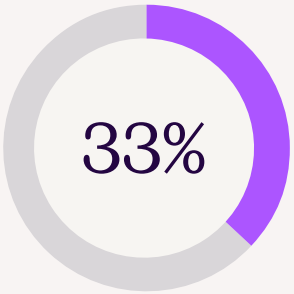
Providing an internal audit report **(39%)** is the most common way of proving security to customers in **Germany**.

43% in Australia, France, and the U.S., and 37% in the UK.

German leaders **(47%)** say they have the second strongest level of risk visibility.

The U.S., by contrast, was at 52%; France, 46%; and the UK and Australia at 42%.

German leaders are most likely to say that the volume of standards and regulations **(33%)** is the top barrier to maintaining a robust security programme.



The security improvement imperative

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

Over half (55%) of German respondents believe their business needs to improve both security and compliance measures.

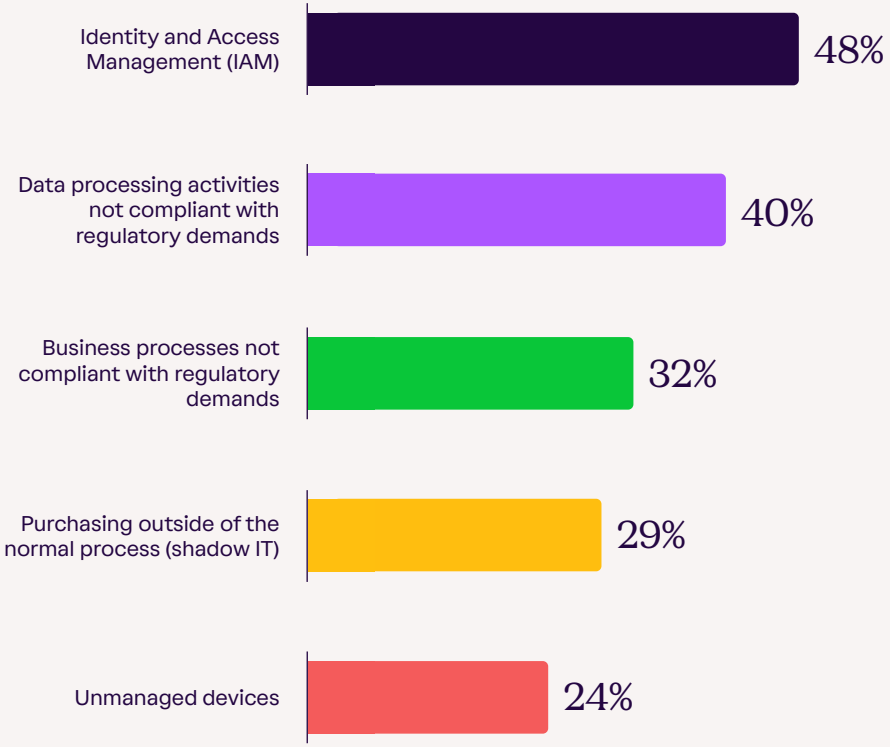
In July, the new president of the Federal Office for Information Security (BSI) Claudia Plattner, stated that Germany needed to defend itself more effectively amidst a background of escalating attacks on German organisations[1]. In November the BSI's annual report stated that hackers see local firms as easy targets for ransomware attacks[2].

Compared to their peers in other countries, German leaders are more confident in the security of their organisations (55% believe improved security and compliance measures are needed vs. 67% globally). Moreover, while they report fewer customers demanding proof of compliance (52% vs. 66% globally) and are also less likely than any other country to enter a market without being compliant (37% vs. 42% globally), they are spending just as much time on compliance workflows as their peers. On average, German organisations are spending 7.3 hours per week (vs. the global average of 7.5 hours) on compliance, and cite 'the limited amount of time available to manage compliance' just as much as other countries (27% vs. 28% globally).

Against the backdrop of attacks highlighted by the BSI — particularly against small and medium-sized enterprises, which form a strong and vital section of the economy — German organisations need to stay on top of evolving risks even as German leaders show confidence in their security and compliance compared to business leaders in other countries.

Limited risk visibility and blind spots from Vanta's survey show an imperative to improve security and compliance. While nearly half (47%) of organisations rate their risk visibility as strong, identity and access management (48%) and data processing that doesn't comply with regulations (40%) are the two biggest blind spots for German organisations.

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



1 - https://therecord.media/germany-must-defend-itself-claudia-plattner
2 - https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.pdf

Security as a selling point

Half (52%) say that customers, investors and suppliers are increasingly looking for proof of security and compliance.

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

While 39% provide internal audit reports (vs. 41% globally), 38% third-party audits (matching the global average), and 30% complete security questionnaires (36% globally), over 1 in 10 (13% compared to 12% globally) admit they don't or can't provide evidence when asked. This means German companies are falling at the very first hurdle, costing potential revenue and growth opportunities.

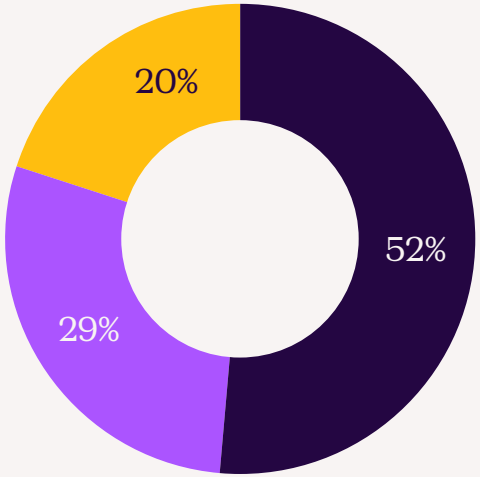
According to respondents, the biggest barriers to proving and demonstrating security externally are a lack of automation to replace manual work required to manage this (32%) and a lack of staffing to manage the process (31%).

This comes at a time when 47% of German businesses surveyed say they have already, or plan to reduce IT staff. A quarter of leaders (27%) say that their overall IT budgets have shrunk as they continue navigating the economic downturn, while 26% are still planning to shrink them.

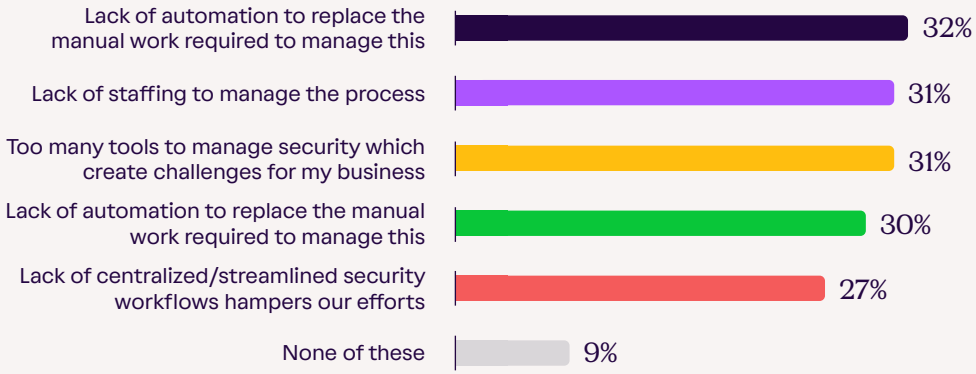
On average, only 9% of German IT budgets are dedicated to security, further exacerbating resource constraints.

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?



Compliance deprioritized

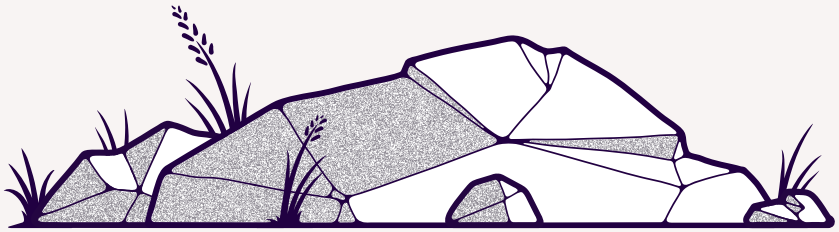
Given these trends, it's not surprising that respondents admit they're not prioritising compliance due to the time and financial investment. But failure to comply ultimately costs these companies potential revenue and growth opportunities, particularly in expanding to new markets.

Time is being plunged into businesses' efforts to meet and maintain the demands of compliance. Respondents spend an average of 7.3 hours per week (9 working weeks per year) on compliance. This is just slightly lower than the global average of 7.5 hours per week. While German leaders generally show higher confidence in their security and compliance measures, they are spending just as much time managing these efforts as other leaders, globally.

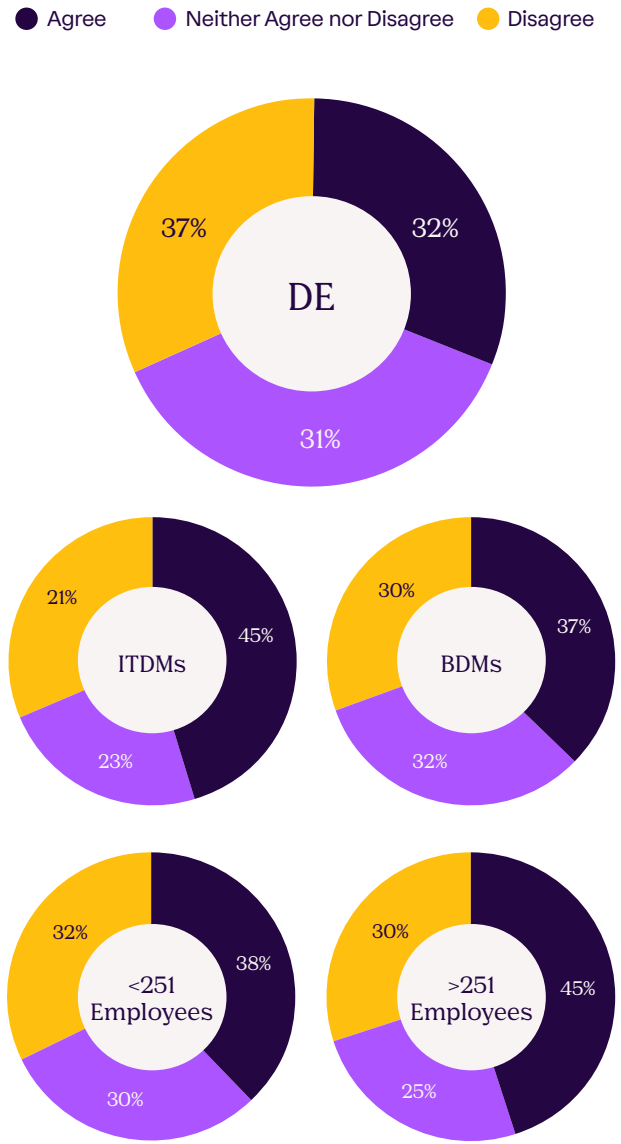
Exacerbating this time-suck, 48% of respondents say that remaining compliant with different international regulations and frameworks like SOC 2 and the UK's GDPR is becoming increasingly difficult.

Over a third (35%) of German businesses have deprioritised compliance due to the time it takes, with 32% 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 Germany regulations

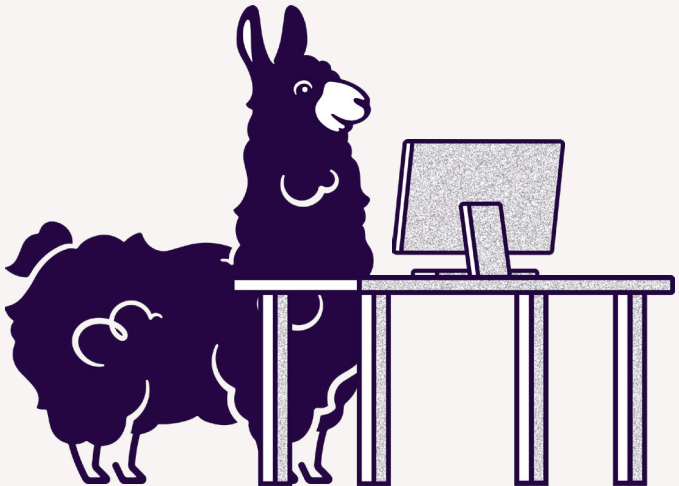
German specific regulation includes the German IT Security Act 2.0 which came into effect in May 2021. The EU's General Data Protection Regulation (GDPR), which states that personal data must be processed securely using appropriate technical and organisational measures, is also applicable. The EU's Networks and Information Systems (NIS2) Directive also passed its revisions in November 2022, considerably expanding the range of affected organisations in Germany.

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.

German businesses recognise the opportunity. 76% already or plan to use AI/ML to detect high risk actions. However, nearly half (44%) are concerned that secure data management is becoming more challenging with AI adoption. This is particularly true for IT leaders compared to their business counterparts (49% vs. 40%). Moreover, 43% of all leaders say that using Generative AI could erode customer trust.

As a result, 46% of German businesses say regulating AI would make them more comfortable investing in it.



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. 60% of leaders say that a better security and compliance strategy would positively impact their businesses thanks to stronger customer trust, and 65% agree that a better security and compliance strategy would make them more efficient. Improved reputation, a trusted status with customers, and peace of mind amongst staff were each rated at 38%.

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

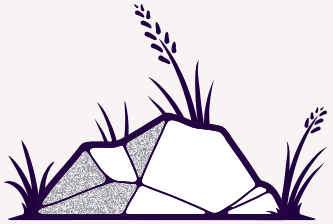
Streamlining security and compliance through automation

Improving and proving security doesn't need to be a heavy lift. In fact, 55% 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. Nearly two-thirds (64%) of businesses have increased or plan to increase their use of automation.

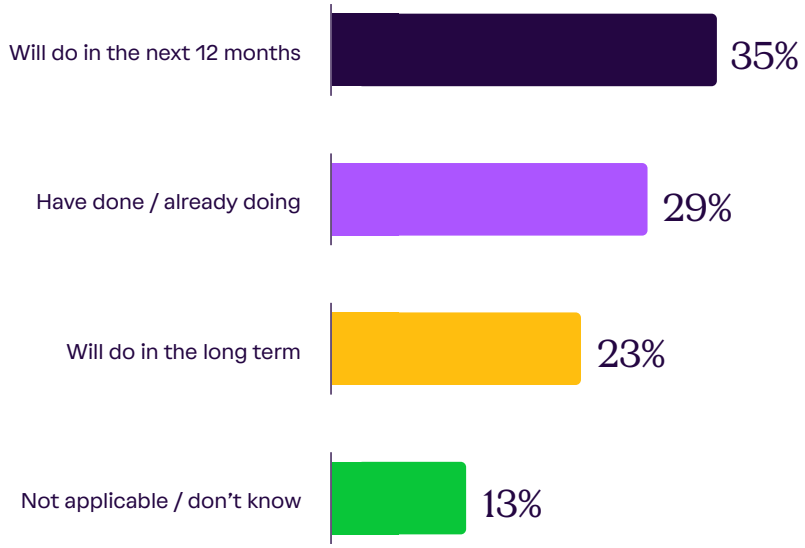
This is true for compliance as well as overall security management. On average, respondents believe they could save two and a half hours per week — nearly three working weeks a year — if security and compliance tasks were automated.

Over half (53%) 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."



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 Germany think AI can be transformative to improving the accuracy of security questionnaires (41%), eliminating manual work (47%), streamlining vendor risk reviews and onboarding (36%), and reducing the need for large teams (33%).

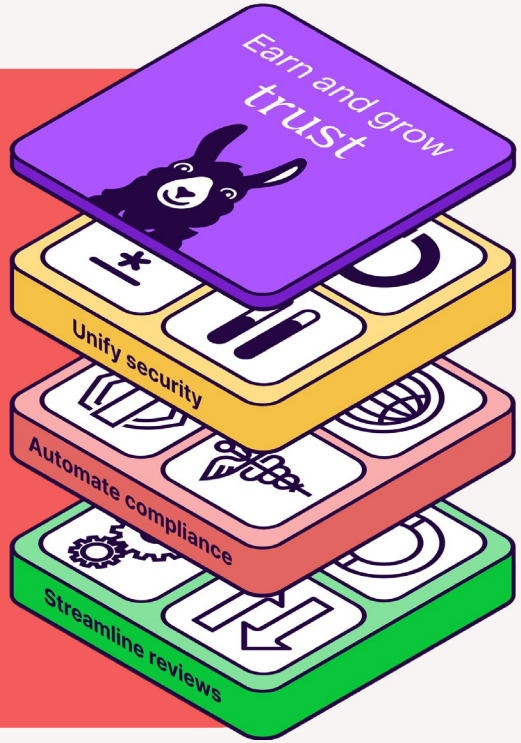
Whether that's saving time, budget or staffing resources, AI can help you do more with less: time-consuming tasks can be handed off to AI. But in a climate of growing cyber-threats, and AI tools presenting a new risk surface, it is essential to prioritise transparency and trust when deploying AI.

What is trust management?

Trust management[3] 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.



3 - 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 German 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 German leaders citing blind spots around identity and access management and data processing that doesn't comply with regulations, establishing a central source of truth unifies your security and compliance programmes.
- **Invest:** More than half of German leaders state a lack of IT budget as a barrier to maintaining a robust security programme. Remember that security underpins growth - invest to unlock opportunities.
- **Transparency:** With German organisations being asked to fill in security questionnaires as well as provide internal audit reports and third-party audits, streamline workflows by showcasing security measures through a public Trust Centre.
- **Automate:** Almost half of German leaders point to the time-suck of remaining compliant with international regulations. Automation is the quickest path to ensuring security and compliance standards are met quickly and without manual effort.

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 German 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