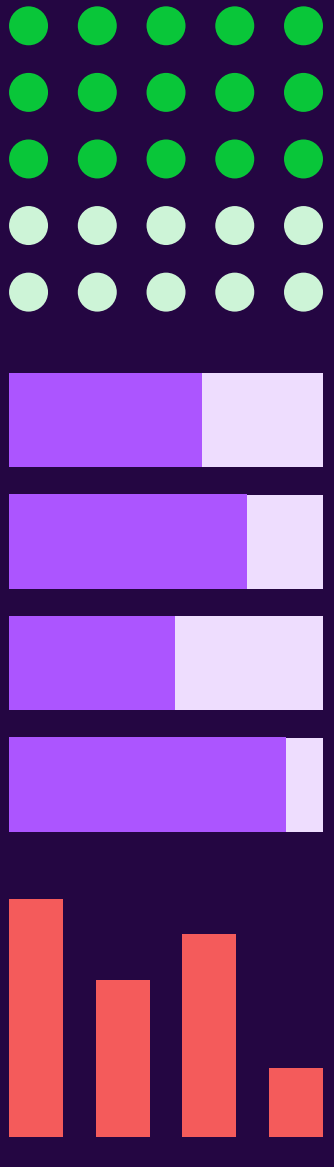
UNITED KINGDOM

The State of Trust Report 2024



Vanta

Table of contents

Introduction

Trust is critical to the success of every business. But building, scaling and demonstrating trust is getting harder for UK organisations.

To meet customer expectations, security leaders and their teams must address complex threats, a growing compliance burden, and increasing risk from their third-party vendor footprint. The rapid adoption of AI technologies only adds to the challenge, requiring more oversight and governance.

Vanta's second annual State of Trust Report uncovers key trends across these areas of security, compliance and the future of trust. Based on a survey of 2,500 IT and business leaders (with 1,000 of the respondents from the UK), our research found that more than half (54%) of UK organisations say that security risks for their business have never been higher.

But as risks increase, so do the opportunities. Automation and AI can significantly minimise the manual security and compliance tasks that prevent security teams from focusing on mission-critical work. According to our research, in the UK just 11% of a company's IT budget is dedicated to security — but in an ideal world, leaders say it would be 17%.

This is where automation and AI can play a transformative role in unlocking efficiencies for security teams and ultimately, business value for UK organisations.

Key findings - UK

54%

of UK organisations think that security risks for their organisation have never been higher.

#1

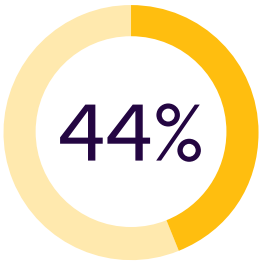
Cybersecurity threats are the number one concern for UK businesses in 2024, higher than financial and operational risk.

12 working weeks

a year are spent on compliance tasks — increasing by 2 weeks since last year.

6 working weeks

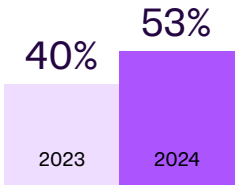
a year could be saved if security and compliance tasks were automated.



of UK organisations say that a vendor of theirs has experienced a data breach since they started working together.

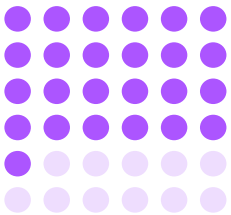
7.2 hours

IT decision makers in the UK spend an average of 7.2 hours per week — the equivalent of 8.9 working weeks a year — assessing and reviewing vendor risk.



More than half

of UK organisations believe good security practices drive customer trust for their business, an increase of 13% from 2023.

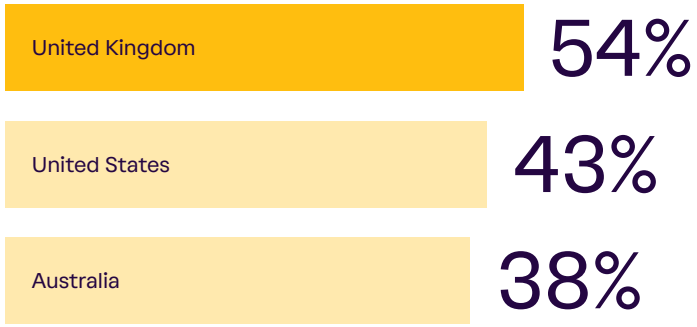


More than two-thirds

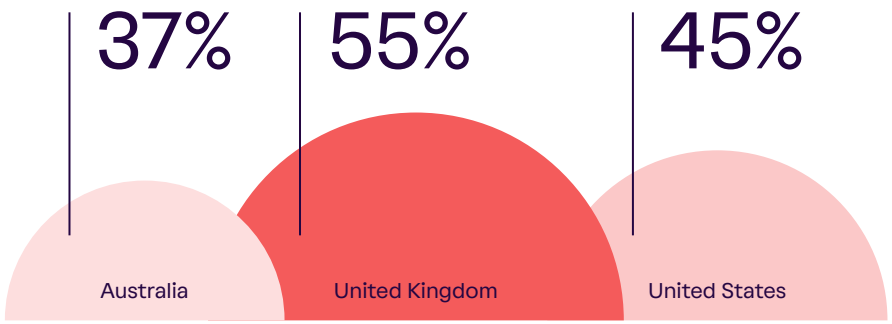
(69%) of UK organisations say that customers, investors and suppliers increasingly require demonstration of compliance.

The UK vs other countries

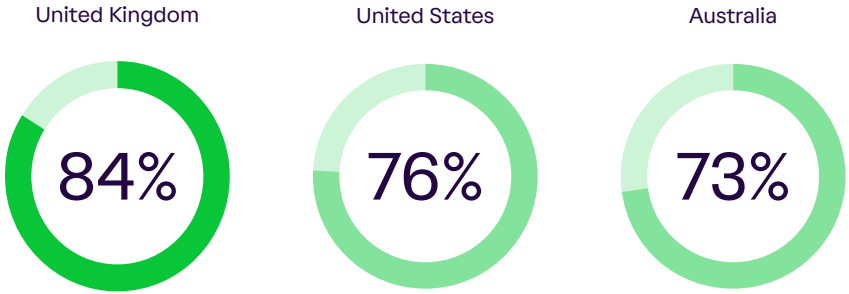
Organisations in the UK are more likely to have increased their investment in automation for IT operations



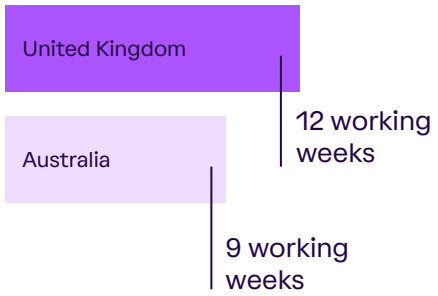
More than half of organisations in the UK have increased their investment in AI for security operations – higher than all other countries



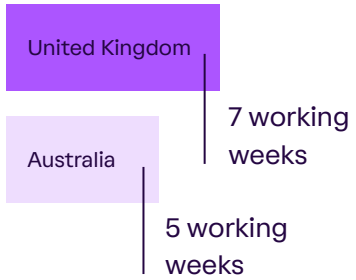
UK organisations are more likely to say they have a dedicated security budget



Organisations in the UK spend the most time on compliance tasks



UK organisations are spending more time on vendor security reviews and risk assessment than other countries



1.

The state of trust today

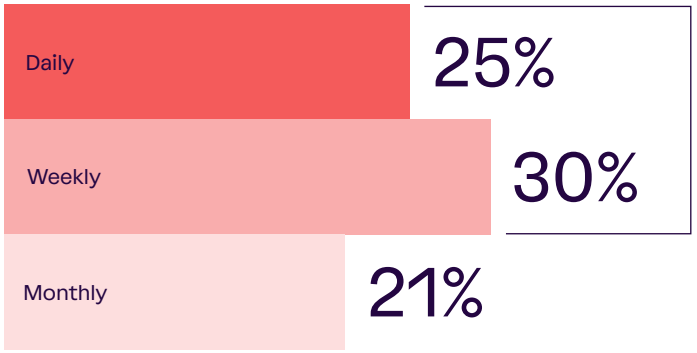
The security landscape — compounded by third-party risk and AI — has never been more challenging

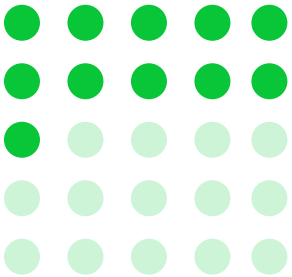
Cybersecurity threats are the number one concern for UK businesses in 2024, higher than financial and operational risk. And more than half (54%) of UK organisations say that security risks have never been higher, with 55% of UK organisations detecting and responding to cybersecurity threats at least once a week.

Further complicating security is vendor risk — almost half of UK organisations say that a vendor of theirs has experienced a data breach since they started working together.

At the same time, half (49%) of UK organisations have concerns around the use of AI and the risks it poses for the security of the organisation.

Frequency of detecting and responding to cybersecurity threats





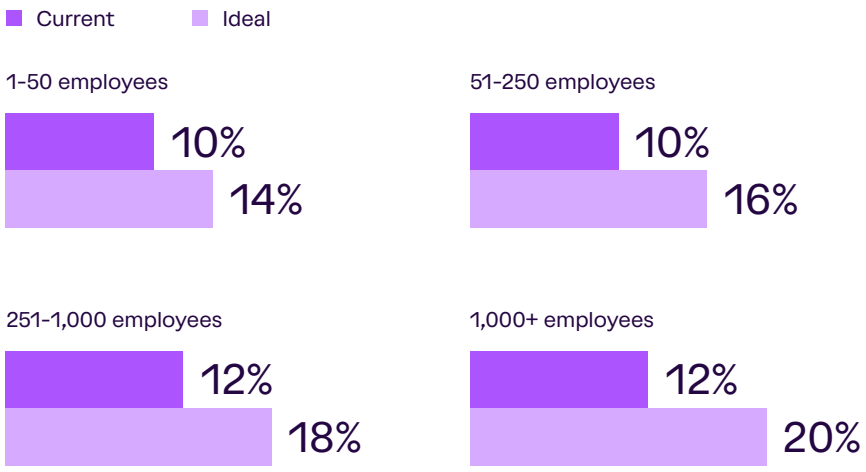
44%

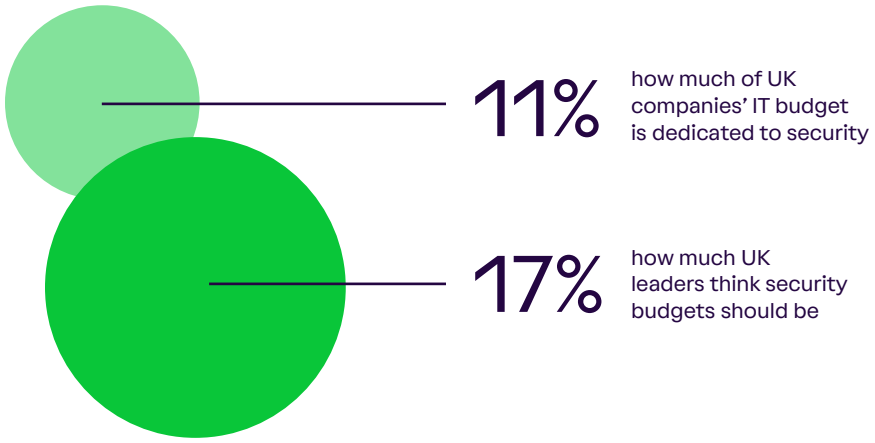
of UK organisations have had a vendor experience a data breach since they started working with them.

“Security doesn’t need to be complex. It needs to scale the business, be a business enabler and it needs to be there at the very beginning. Without it, it’s only a matter of time before there’s a serious issue.”

Leo Cunningham, Former Chief Information Security Officer
Flo Health

Current and ideal security budget percentage climbs with organisation size





Security budgets and investment are not where leaders think they should be, especially in larger UK organisations

Despite increasing security risks, just 11% of a company's IT budget in the UK is dedicated to security — but in an ideal world, leaders say it would be 17%.

The larger the organisation, the more of its IT budget is spent on security. However, for UK organisations with over 1,000 employees, leaders say that 20% of their organisation's security budget would ideally be dedicated to security when it is currently just 12%.

Compounding this challenge is the fact that almost 1 in 10 (9%) UK organisations have decreased their investment in hiring cybersecurity staff — an ongoing consequence of a tough economy, budget constraints and talent shortages.

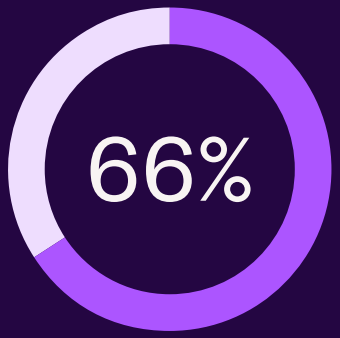
While threats are increasing, businesses are also facing growing security expectations. More than two-thirds (69%) of UK organisations say that customers, investors and suppliers are increasingly requiring proof of compliance. To establish and deepen trust with customers, businesses need to prioritise security resourcing.

As AI adoption accelerates, governance and risk management stall

At the same time that AI is becoming increasingly common in the tech stack, security concerns are also on the rise. A majority (66%) of UK businesses plan to invest more in security around the use of AI within their organisation in the next year. And over the last 18 months, cyber risks and threats have gone up, with UK businesses experiencing more phishing attacks (35%), a rise in AI-based malware (34%) and more compliance violations (27%).

AI governance and risk management, however, are still relatively nascent. Just over 2 in 5 (43%) UK organisations currently conduct, or are in the process of conducting, regular AI risk assessments. When it comes to formal policies for governing AI usage, only 42% of UK organisations have or are in the process of putting a company AI policy in place despite the increased use of AI tools.

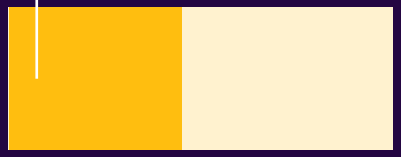
Building trust in AI



of UK organisations plan to invest more in AI security in the next 12 months

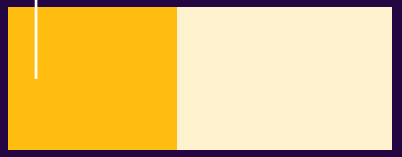
43%

of UK organisations have conducted, or are in the process of conducting, regular AI risk assessments



42%

of UK organisations have, or are in the process of putting, a company AI policy in place



“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

Protecting customer trust in a AI world

Building and maintaining trust is even more critical as UK organisations accelerate their usage of AI to develop and deliver new products. This means committing to safe and ethical AI practices and prioritising transparency, particularly when it comes to training AI models.

Over one-third of UK organisations (37%) use a mix of customer and synthetic data to train AI models, while 30% use anonymised customer data. Further, while 29% of UK organisations require opt-in from customers to use their data for AI training, 74% of companies don’t offer an opt-out option.

While the future of AI is far from set, UK organisations can maintain trust by giving customers control over their data through an informed consent model. This vigilance should extend to third parties too, and companies should require a formal data processing agreement (DPA) stipulating that vendors not use customer data to train their AI models.

Training AI with customer data

29%
of UK organisations require customer opt-in

74%
of UK organisations don’t offer an opt-out option

2.

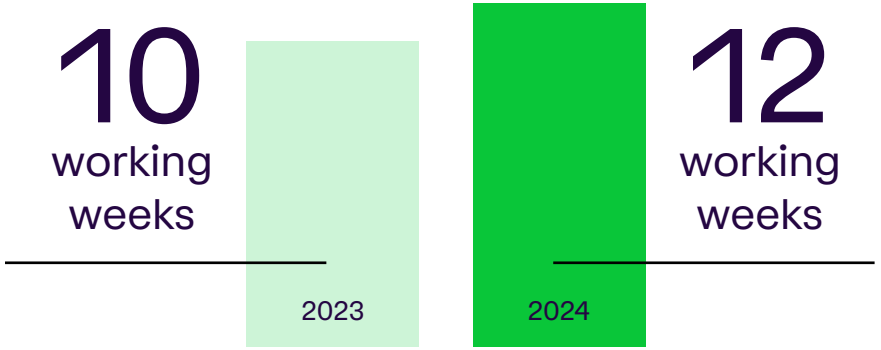
Easing the compliance burden

The compliance burden has never been higher

Time spent on compliance tasks increased to over 12 working weeks in 2024 — from 10 working weeks in 2023. This is the most time spent on compliance out of all regions and an increase of two hours a week compared to 2023. And 1 in 10 (10%) respondents are spending over 21 hours each week — 25 working weeks a year — on security compliance.

When it comes to security programme management across UK organisations, IT decision makers spend an average of 7.2 hours per week — 8.9 working weeks a year — assessing and reviewing vendor risk.

Time spent on manual compliance per year is going up



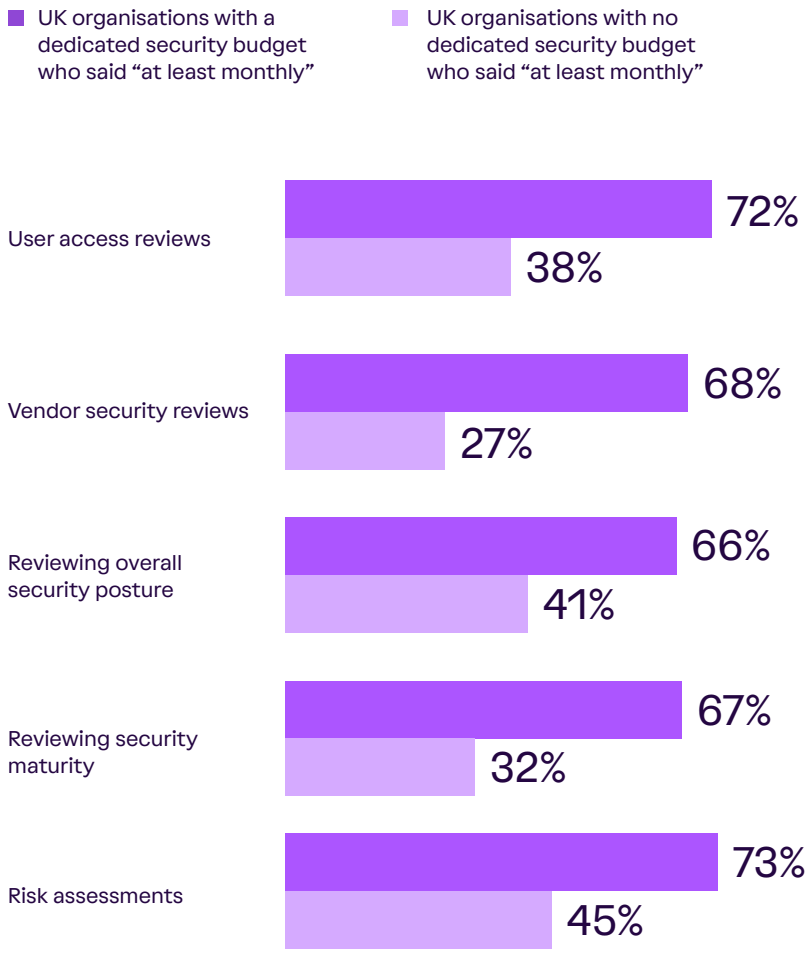
The average time IT decision makers spend on assessing and reviewing vendor risk

“We noticed an increased interest in our security posture — we were getting a lot of security questionnaires, often with questions that weren’t relevant to us. That took up time that would be better spent on more crucial work.”

Dimitrios Stergiou, Director of IT and Information Security,
Taptap Send

There is also a significant gap in the frequency of foundational security activities depending on whether UK organisations have a dedicated security budget.

How budgets impact the frequency of security activities



Security and compliance automation frees up time and improves efficiency for security teams

The scale of activities required for compliance is extensive. But with automation, UK security professionals could save 12% of the working week. In 2024, UK organisations also estimate that they could save more time through automation than they did in 2023.

Automation is of growing importance to security teams, with 51% of UK organisations saying that their investment in automation for security operations has increased over the past year. And 6 in 10 (60%) say that the automation of manual work is a priority for their security and compliance strategy.

On average, security teams in the UK could save between 4-5 hours a week by automating activities like user access reviews, employee management and answering security questionnaires — allowing them to focus on strategic security initiatives.

While 77% of UK IT decision makers say that their company could save time and money through automation, just 60% of business decision makers say the same. Leaders from the frontlines of security can help bridge this 17% gap by getting buy-in for automation that reduces time-consuming processes. Automation not only benefits the business but also improves employee wellbeing, with 41% of respondents in the UK agreeing that good security practices bring peace of mind.

6 in 10

UK organisations say that the automation of manual work is a priority for their security and compliance strategy

Estimated hours saved through automation per working week

3.

Trust and third-party risk

Third-party risk increases as companies scale

Managing vendor risk is a challenge for any business, and this only becomes more difficult as a company scales. The larger the business, the more vendors they have — and the bigger the associated risk.

At the same time, less than a quarter (24%) of UK organisations rate their visibility into vendor risk as "very strong". With half (50%) of UK organisations saying that a vendor they work with has previously experienced a breach, businesses need to implement a proactive approach that reduces risk and enables continuous visibility into their third-party landscape.

The average number of vendors according to organisation size

"We have an ever-growing and ever-changing list of vendors, and we need to stay on top of them while having finite resources. Vanta's Vendor Risk Management helps me stay on top of all of our vendors and see at a glance which ones need an updated review."

Quentin Berdugo, Chief Information Security Officer
Pigment

Confidence in vendor compliance is high, but third-party breaches undermine overall security and trust

The majority of UK organisations (70%) feel confident that their vendors comply with relevant industry standards and regulations. But breaches are still prevalent, and regardless of their security maturity, 44% of UK businesses say that a vendor of theirs has had a data breach since they started working with them or using their products.

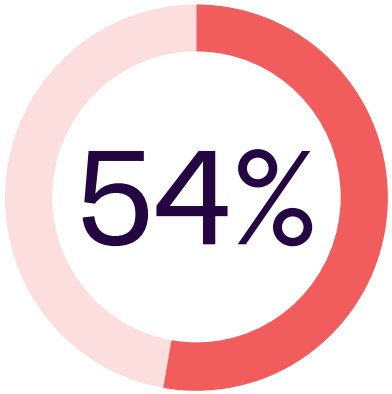
These types of breaches have a serious impact on customer trust, with 63% agreeing that third-party breaches negatively impact their organisation's reputation. One in two (54%) UK businesses say they've terminated a vendor relationship due to security concerns.

To maintain and scale trust — both across their own organisations and their third-party vendors — forward-thinking leaders need to go beyond the standard of point-in-time checks towards a holistic and continuous approach to monitoring.

AI can transform vendor risk management and security reviews

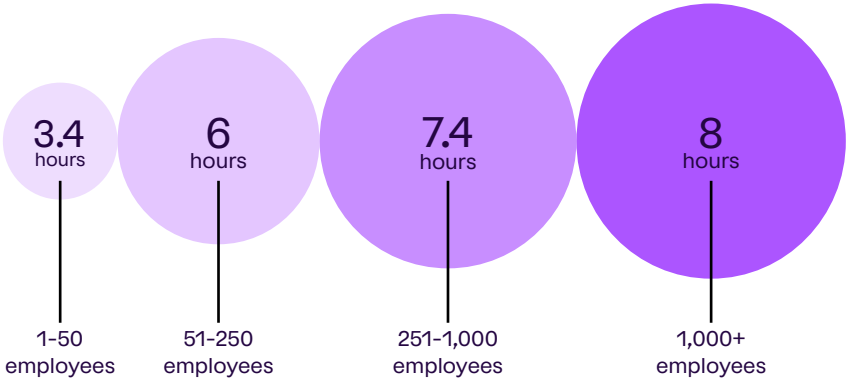
On average, UK organisations spend 6 hours per working week — the equivalent of 7 working weeks a year — on vendor security reviews and risk assessments. But UK organisations now see even more potential in AI to streamline vendor risk reviews and onboarding than they did last year — up from 33% in 2023 to 43% in 2024.

IT and business leaders in the UK say the most transformative areas for AI are improving the accuracy of security questionnaires (45%), streamlining vendor risk reviews and onboarding (43%), eliminating manual work (37%) and reducing the need for large teams (32%).



More than one in two businesses say they have terminated a vendor relationship due to security concerns

Hours per week spent on vendor security reviews in the UK by organisation size



4.

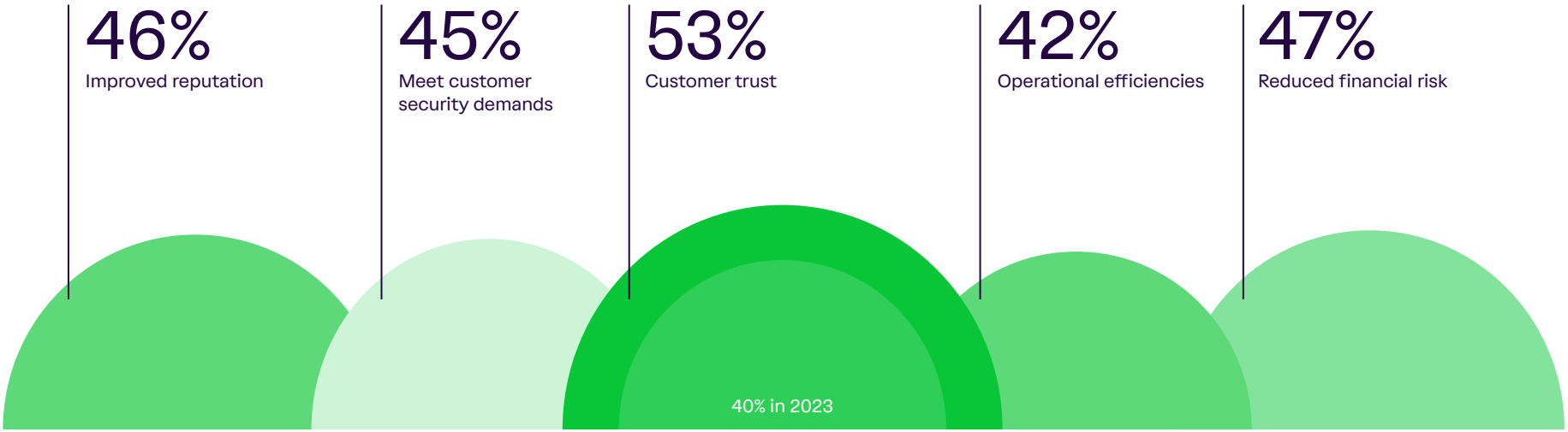
Good security is good business

Demonstrating trust continues to drive business value

As the security expectations of customers grow, UK leaders continue to recognise the business value of investing in security — and demonstrating it. Close to two-thirds (69%) of UK organisations say that customers, investors and suppliers increasingly require demonstration of compliance.

More than half (53%) of UK organisations believe good security practices drive customer trust for their business (up 13% from last year) and 47% recognise that good security practices lead to reduced financial risks.

The value of good security practices



“Strengthening our security posture has enabled our growth, allowing us to target new sectors, and enter new geographical regions.”

Joshua Dent, Business Strategy, and Partnerships Manager
ComplyCube

Confidence in reporting on security programme outcomes is high, but measuring the ROI of trust is more challenging

An overwhelming 84% of UK organisations are confident in their team's ability to show the impact of their security programme on the business. Further, 9 in 10 (91%) UK organisations quantify and measure the impact of their programme in some capacity.

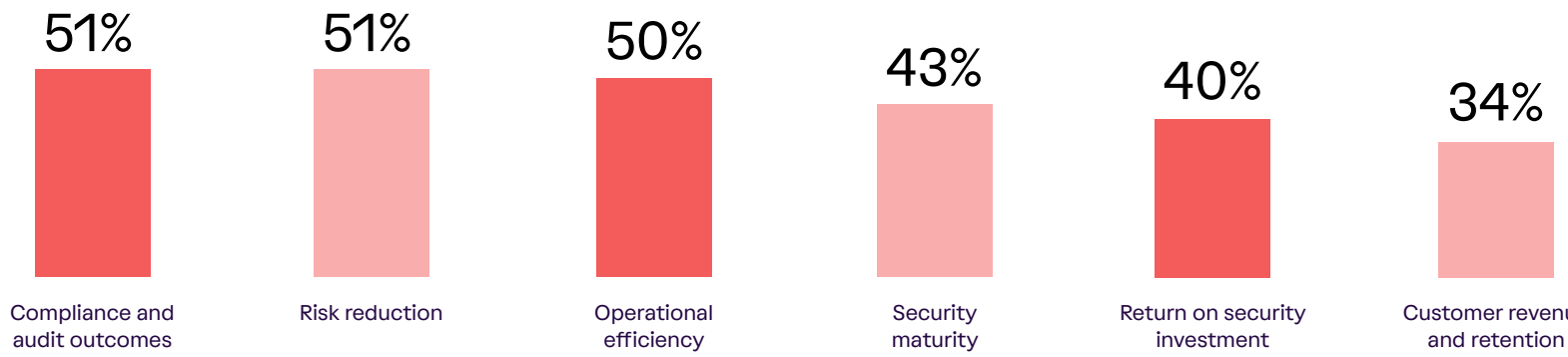
The top three ways that UK organisations measure impact are: compliance and audit outcomes, risk reduction and operational efficiency.

While teams are quantifying and measuring impact, only 40% are measuring actual ROI. And even fewer are tracking the security programme's impact on customer revenue and retention. With increasing pressure on security teams to demonstrate measurable impact — in addition to reduced risk — leaders need actionable reporting capabilities that centralise visibility across their security programme.

84%

of organisations are confident in their team's ability to show the impact of their security programme on the business

How UK organisations are measuring a security programme's impact



Conclusion: Go beyond the standard with trust management

For UK organisations of all sizes, building and scaling trust is difficult. Greater reliance on third-party vendors and the growing usage of AI technologies mean that security leaders face an increasingly complex threat landscape while also navigating resource constraints.

But the tools available today only make this work more challenging. Teams are stuck with solutions that rely on screenshots and spreadsheets and only provide point-in-time visibility into their security posture.

To keep pace with where the future of trust is headed, security leaders need to go beyond the standard way of doing things. They need to make trust continuous, collaborative and automated across every part of their business. With a holistic trust management strategy, UK organisations can not only reduce risk, but also build customer confidence and accelerate revenue growth.

Here are three ways that UK organisations can start to make this shift:

01

Build a trust programme powered by automation

The tools you use to manage your trust programme should help rather than hold you back. Implement trust management platforms that automate key workflows, continuously monitor your security and compliance and provide centralised visibility and insights across your programme.

02

Demonstrate trust in real time

Go beyond point-in-time compliance certifications and create opportunities to proactively demonstrate and maintain trust with customers. This looks like showcasing your security controls through a public Trust Center and instantly and accurately responding to security questionnaires with the help of AI.

03

Strengthen your entire trust network

Trust isn't just a reflection of your organisation. It also reflects your network of vendors, partners and business ecosystem. Raise the bar for your security by building a bespoke standard of trust that centralises visibility and allows you to define what good security looks like for those that do business with you.

Methodology

In July and August 2024, 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 Research co-designed the questionnaire and surveyed the behaviours and attitudes of 2,500 business and IT leaders across Australia, the UK and U.S. Year-over-year comparisons for relevant questions were calculated using only the Australia, UK and U.S. datasets from The State of Trust Report 2023.

About Vanta

Vanta is the leading trust management platform that helps organisations of all sizes automate compliance, manage risk and prove trust. Thousands of companies including Atlassian, Omni Hotels, Quora and ZoomInfo rely on Vanta to build, maintain and demonstrate trust — all in a way that's continuous and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, London, New York, San Francisco and Sydney.

For more information, visit www.vanta.com.

Vanta