REPORT

The Osirium IT Automation Survey Executive Summary

A study into how automation helps IT organisations delegate work, reduce costs and stress

OSIRIUM

Introduction

In a world where IT teams are over-stretched, it's critical that staff focus on the right tasks, and to ensure their expertise is being used in the most efficient way. Unfortunately, many IT experts are spending time on tasks that aren't adding value to the organisation.

In this report, based on independent research, we look at two specific areas of IT: delegation of routine management tasks, and compliance audits and their impact on the business. Both are important elements of IT operations that can benefit from automation. The report reveals how much automation is being done in IT, the main concerns of IT leaders when it comes to automation, and how they can be addressed. The data suggests there is room for improvement.

For more information about the research and how to safely automate IT processes, **please contact Osirium**.

> *Automation should be the top priority in IT teams, because it helps every aspect of their working life. It improves customer service and security, while reducing risk, effort and cost. The traditional Automation approach isn't always the right answer, so look out for tools that are focused, not just on the productivity benefits, but the security outcomes as well.*

David Guyatt, Co-Founder and CEO, Osirium

Part One: The challenges of delegating IT tasks

Much of the work in IT is about dealing with everyday requests for help from the business. For example, resetting a user's password, creating accounts for a new starter, or checking if a server is running.

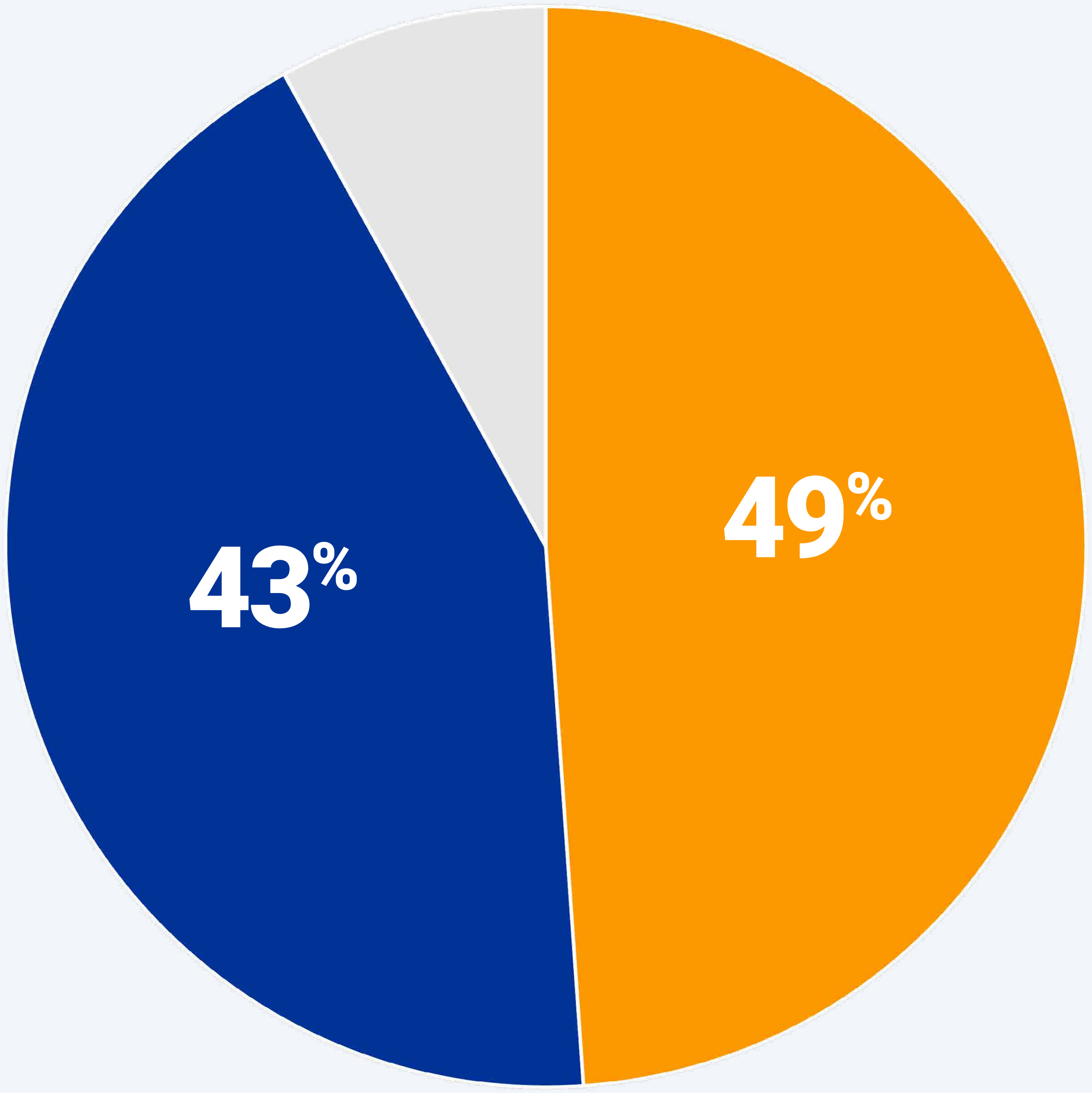
The resolution of such issues is usually straightforward but only for someone that knows how to use tools like Active Directory (AD). An expert is needed as mistakes can lead to security risks.

Ideally, such tasks could be delegated to the first IT line help desk or to the users themselves. That would provide much better service and, importantly, free up the expert's time to make progress with more strategic projects. The key to safe delegation of such jobs is automation. Automation ensures policies are followed, valuable credentials are protected, and audit trails maintained.

Delegation is widely adopted

What are the proportions of IT tasks being delegated?

A high number (**92%**) of respondents have some level of delegation of IT tasks to their help desk or users but there's a wide variance of just how much IT work is being delegated, and the tasks automation is performing. Only 43% say they delegate most of their admin tasks, so there's plenty of scope to do more.



Proportion of IT tasks being delegated

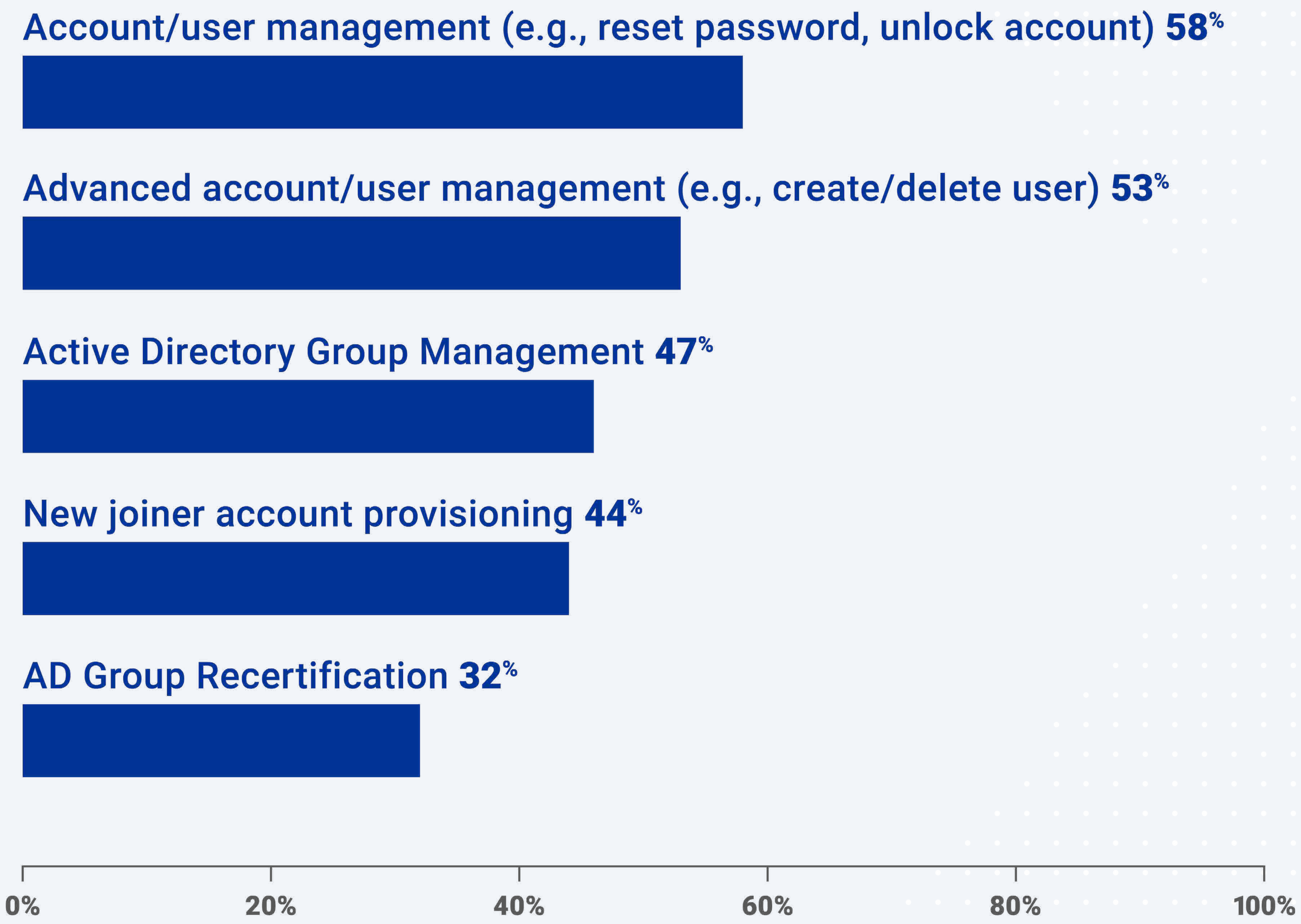
- ● Some tasks delegated **49%**
- ● Most tasks delegated **43%**
- ○ No tasks delegated **8%**

Tasks being delegated

What tasks are being delegated?

The most delegated tasks are user/account management jobs such as resetting a user's password (58% do this). Tasks like creating accounts for new starters, AD group management, and re-certification are more complex and, potentially, carry more risk. These jobs are mostly reserved for AD experts. Only 32% delegate re-certification, whilst 44% delegate account provisioning.

What is being delegated?



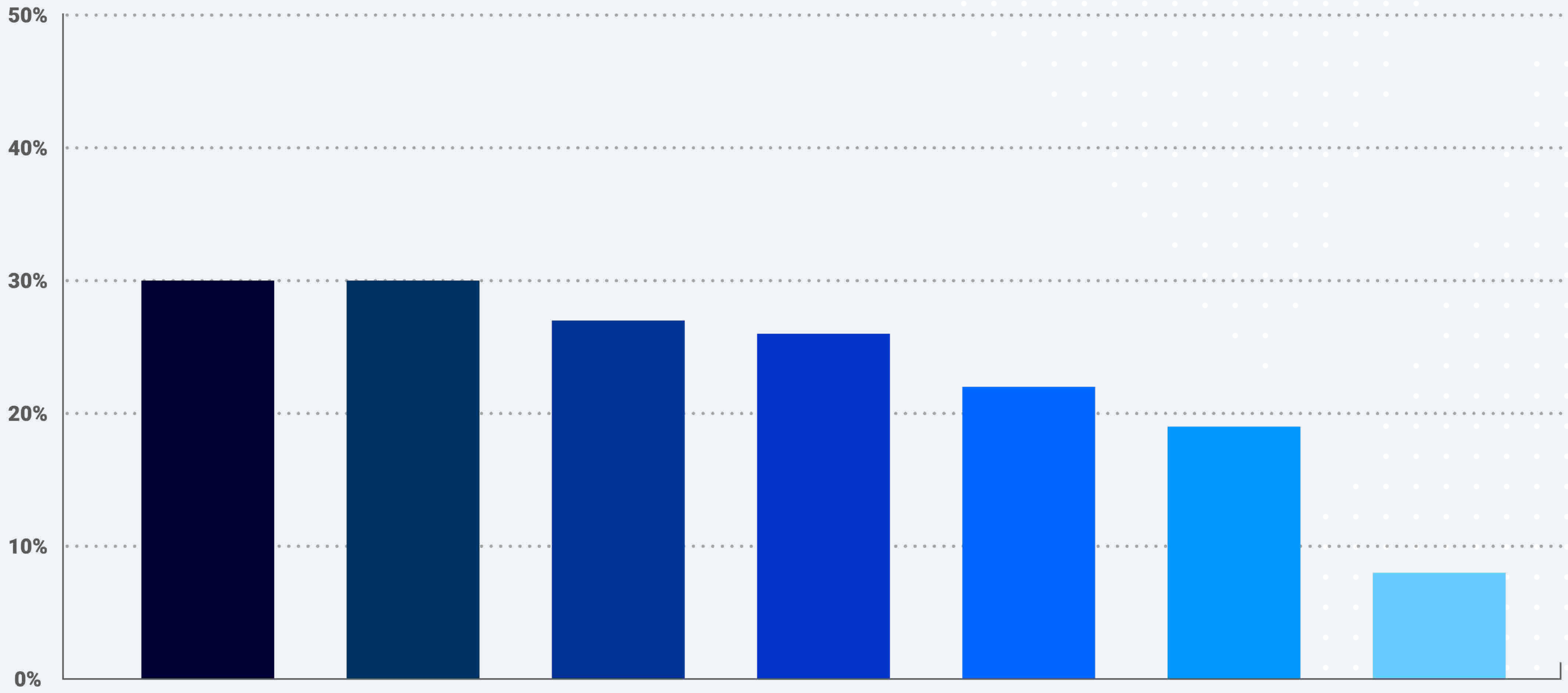
What’s holding delegation back?

Why are IT professionals reluctant to delegate their work?

Of those that say they aren’t delegating IT work, almost a third (30%) said it’s their job to do the AD management tasks, so it’s not entirely surprising that they’re not delegating that work. The same number highlighted risk as the main reason for not delegating user account management work, with trust and lack of clearance also significant. A quarter (26%) said that the help desk wouldn’t know how to do the work.

Why not delegate?

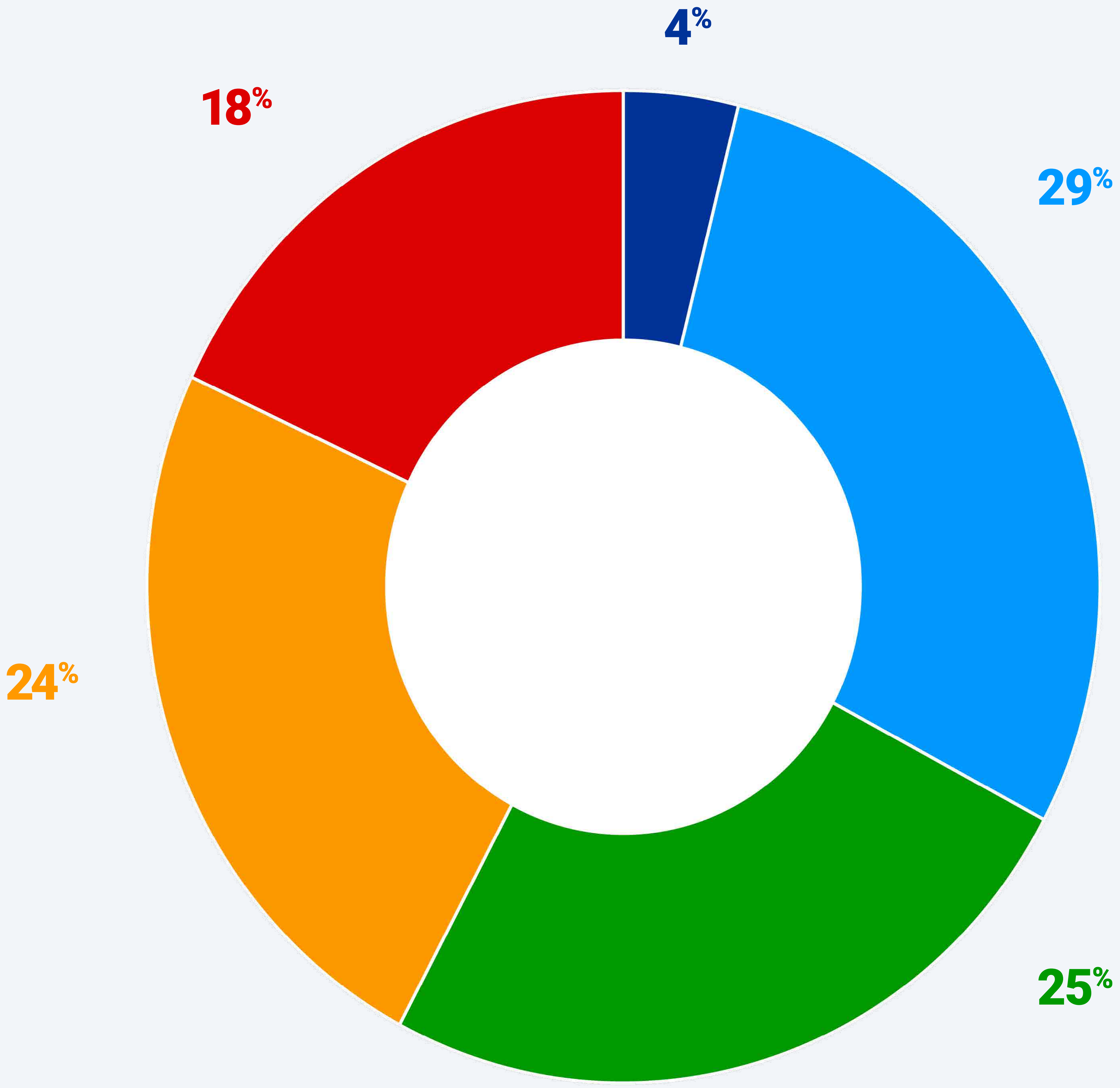
- ■ It’s part of my job responsibilities **30%**
- ■ It’s too risky **30%**
- ■ I don’t want to add to others workload **27%**
- ■ Others wouldn’t know how to perform these tasks **26%**
- ■ I don’t trust anyone else to do them **22%**
- ■ Others don’t have clearance to do these tasks **19%**
- ■ Other reasons **8%**



Risk in delegation

What are the risks concerning delegation?

When looking at all respondents, including those that are already delegating IT tasks, risk and compliance are significant concerns.



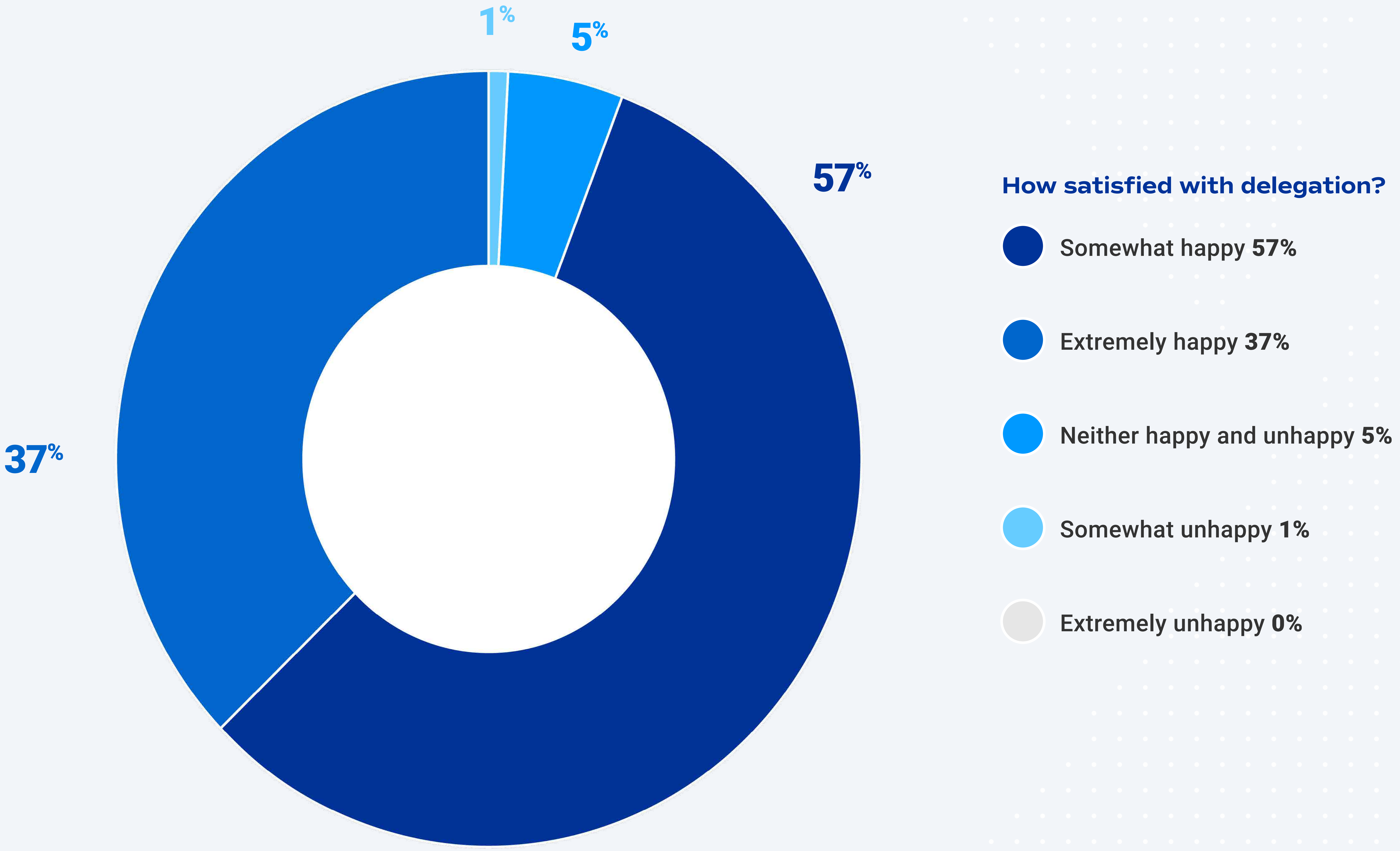
Risks in delegation?

- ● No, there are no risks **4%**
- ● Security risks **29%**
- ● Compliance risks **25%**
- ● Performance risks **24%**
- ● Cost risks **18%**
- ○ Other risks **0%**

Delegation in action

How well is delegation working?

Where user and group management tasks are being delegated, the majority (94%) are happy. However, just 37% say they are "extremely happy" so there's still plenty of room for improvement.



RPA and IT automation

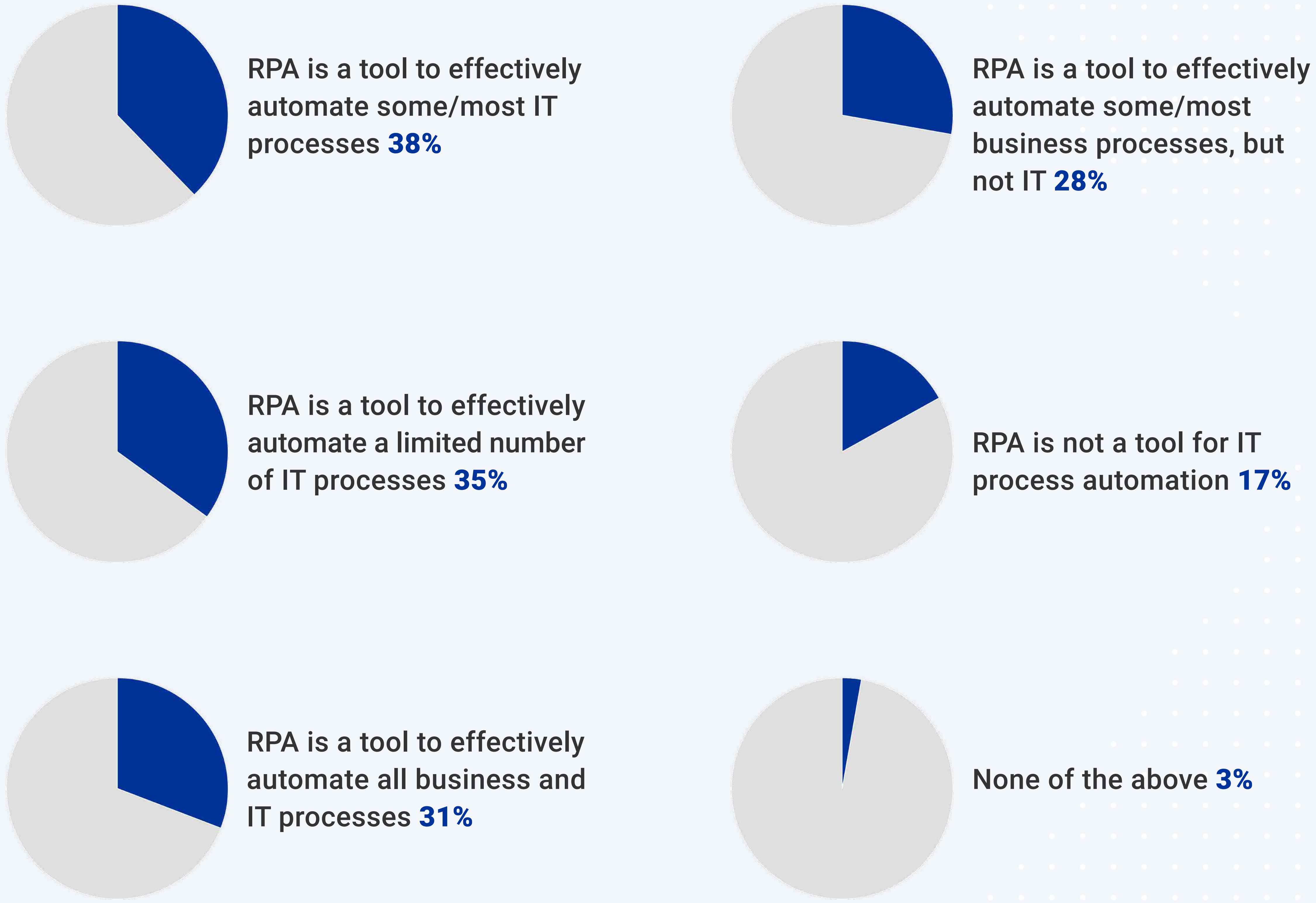
Is IT using RPA for automation?

41% of organisations say they are using RPA with a similar number (46%) saying they are considering adopting RPA in the future.

Of those with RPA, just over half (53%) use it for AD user account management, and just under half use it for new account provisioning (48%).

There is concern about using RPA for IT automation. Of those using RPA, only 38% thought it could be used for some/most IT processes, 35% thought it was suitable only for a limited set of IT operations and 17% say it is not a tool for IT automation.

Is RPA a tool for IT Automation?



Part Two: The challenges of compliance and audits

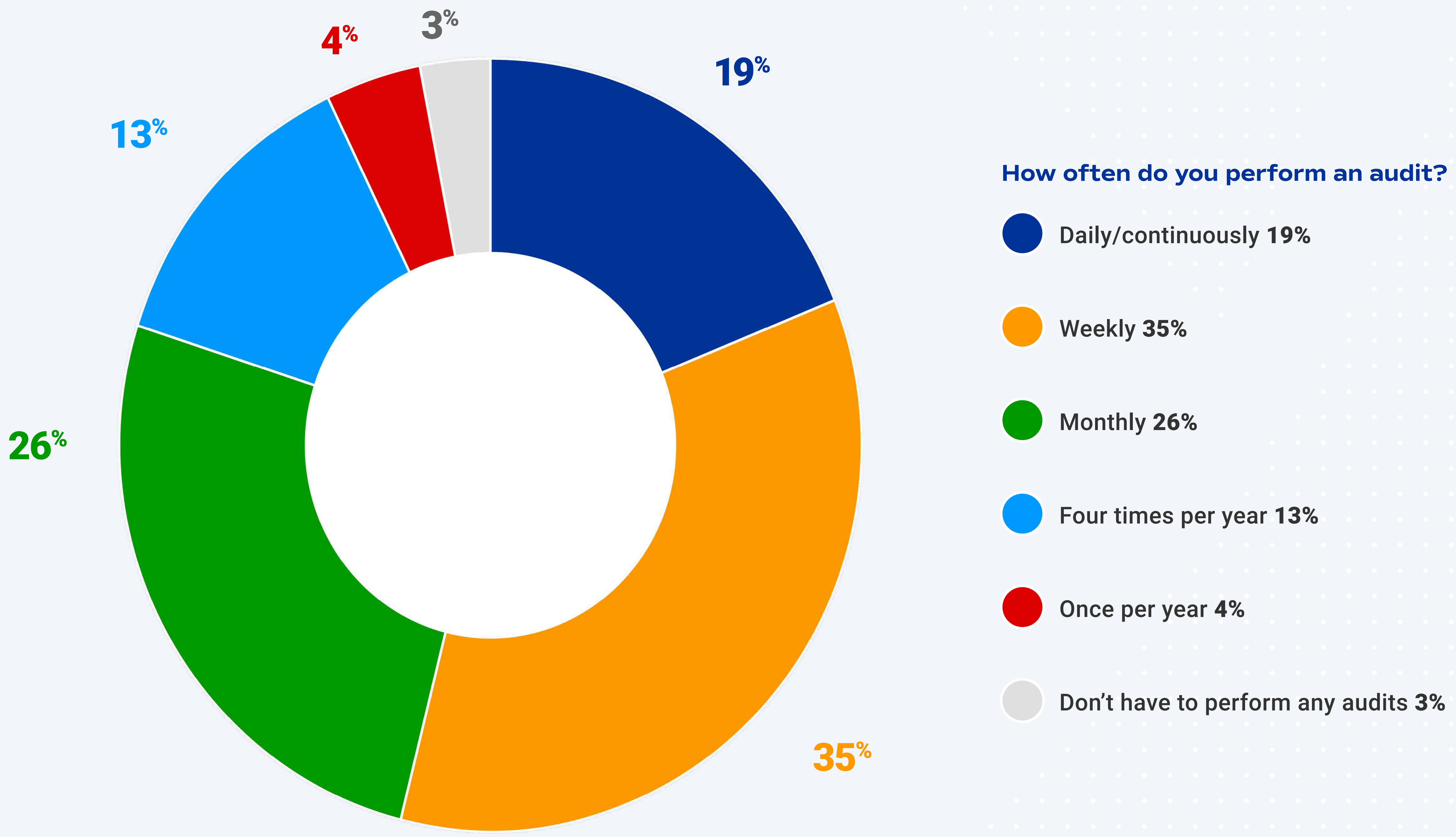
One of the activities that takes a lot of IT admin effort yet isn't directly related to delivering strategic value, is compliance enforcement and auditing. For many, especially in industry sectors with strong regulatory frameworks such as payment handling, healthcare, or critical national infrastructure, proving compliance is not optional. That said, any organisation should be applying best practices as recommended by Cyber Essentials or the National Cybersecurity Centre to protect their business, or be eligible for cyber insurance.

Audits

Audits are a frequent operation

Many standards, such as Cyber Essentials require a formal re-certification each year. However, to prove a system is in place and working, checks should be performed more frequently. For many, it's an almost daily activity. The research also shows that 54% of organisations have an audit process running at least weekly.

Even if an audit is only performed monthly, it can have a significant impact on IT resources. Building a continuous monitoring process, and ensuring best practices are always enforced, can reduce the effort significantly.

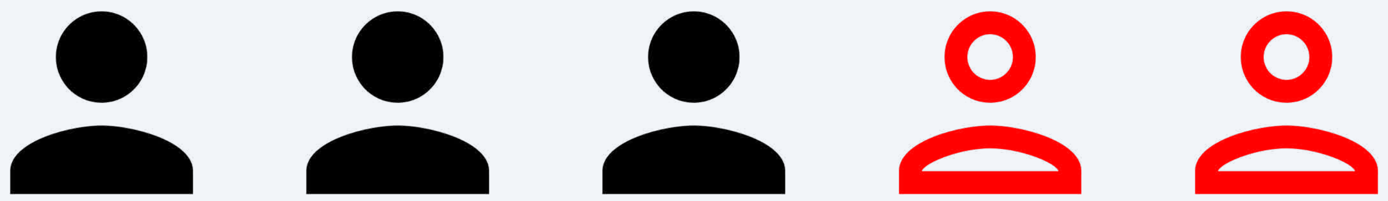


Time and money

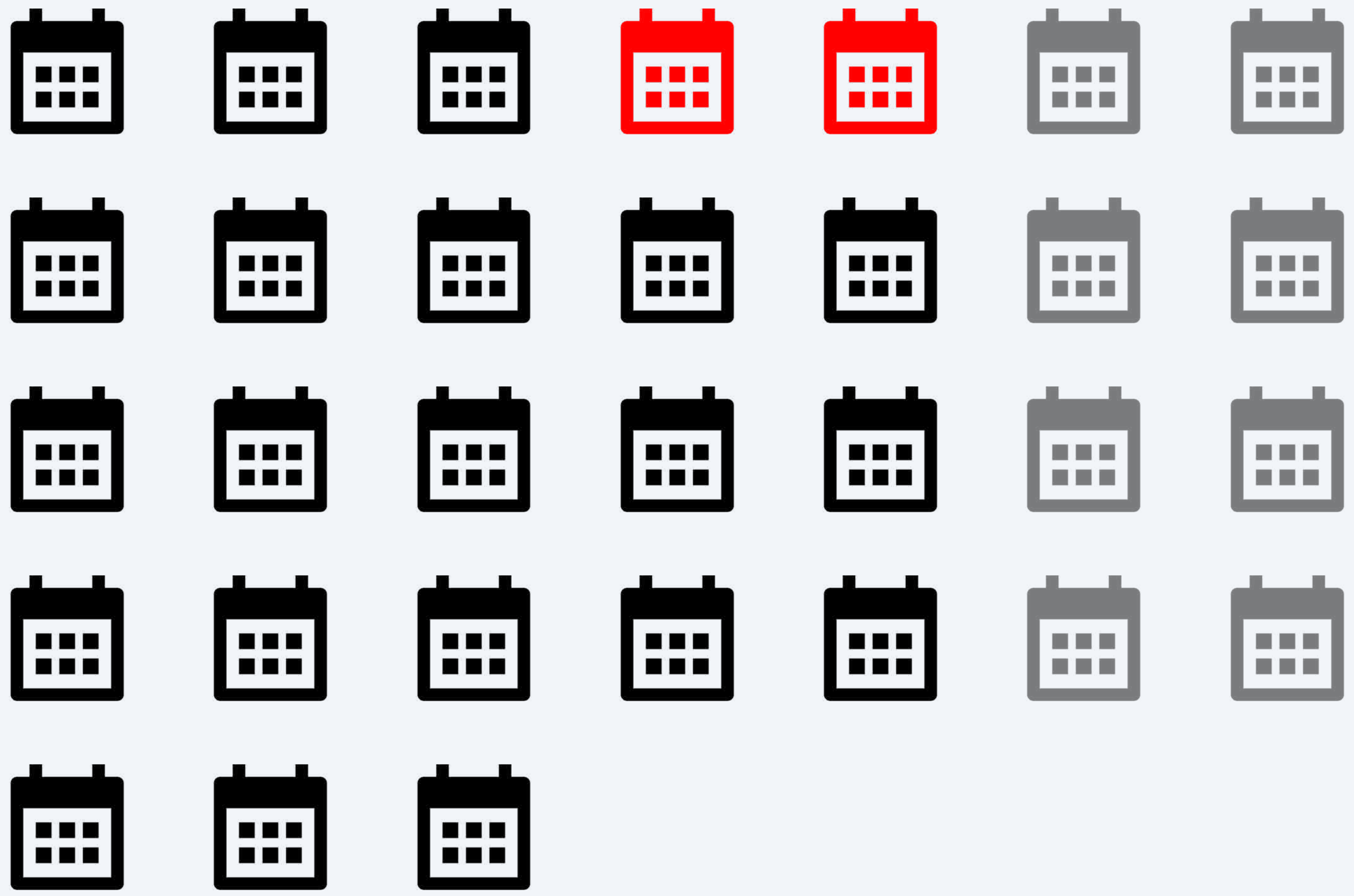
Audits are expensive

Most organisations (76%) have 2 or more people involved in audits and, on average, they each spend approximate 2 days per week on audit tasks. Worryingly, less than half (47%) of audits are completed on time. While 34% say too much time is spent on auditing, 30% don't think they spend enough.

40% of team members allocated to audit work.



At least two days in a month lost due to audits.

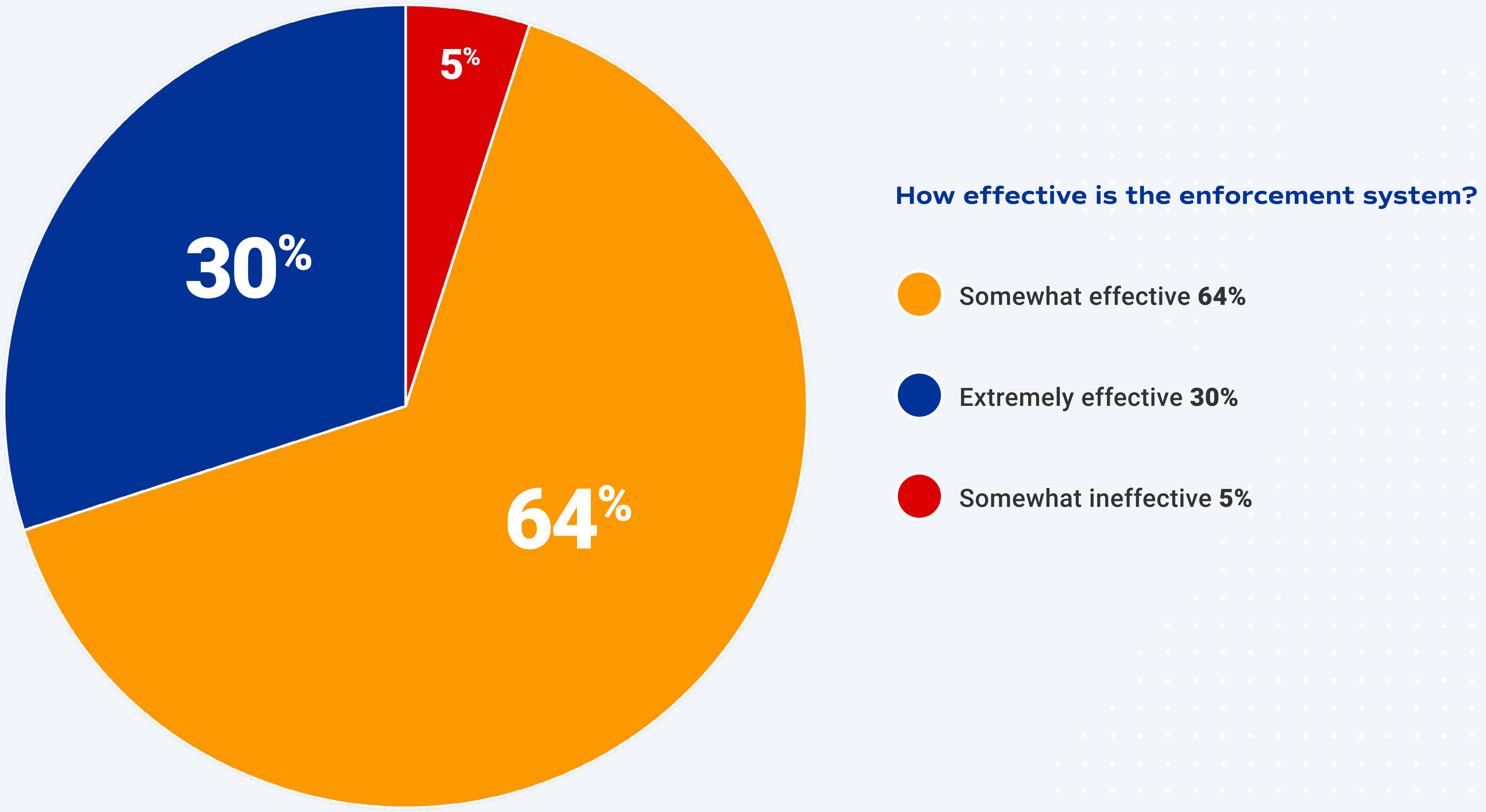


Compliance difficulties

Enforcement is hard

Most organisations (56%) use staff training as part of their compliance regime and only 32% use tools for enforcement.

Only 30% say their enforcement systems are extremely effective, but the majority (95%) are still at least somewhat satisfied. Process efficiency is highlighted as a reason for poor enforcement (40%), and the same number cite lack of staff to do the job.

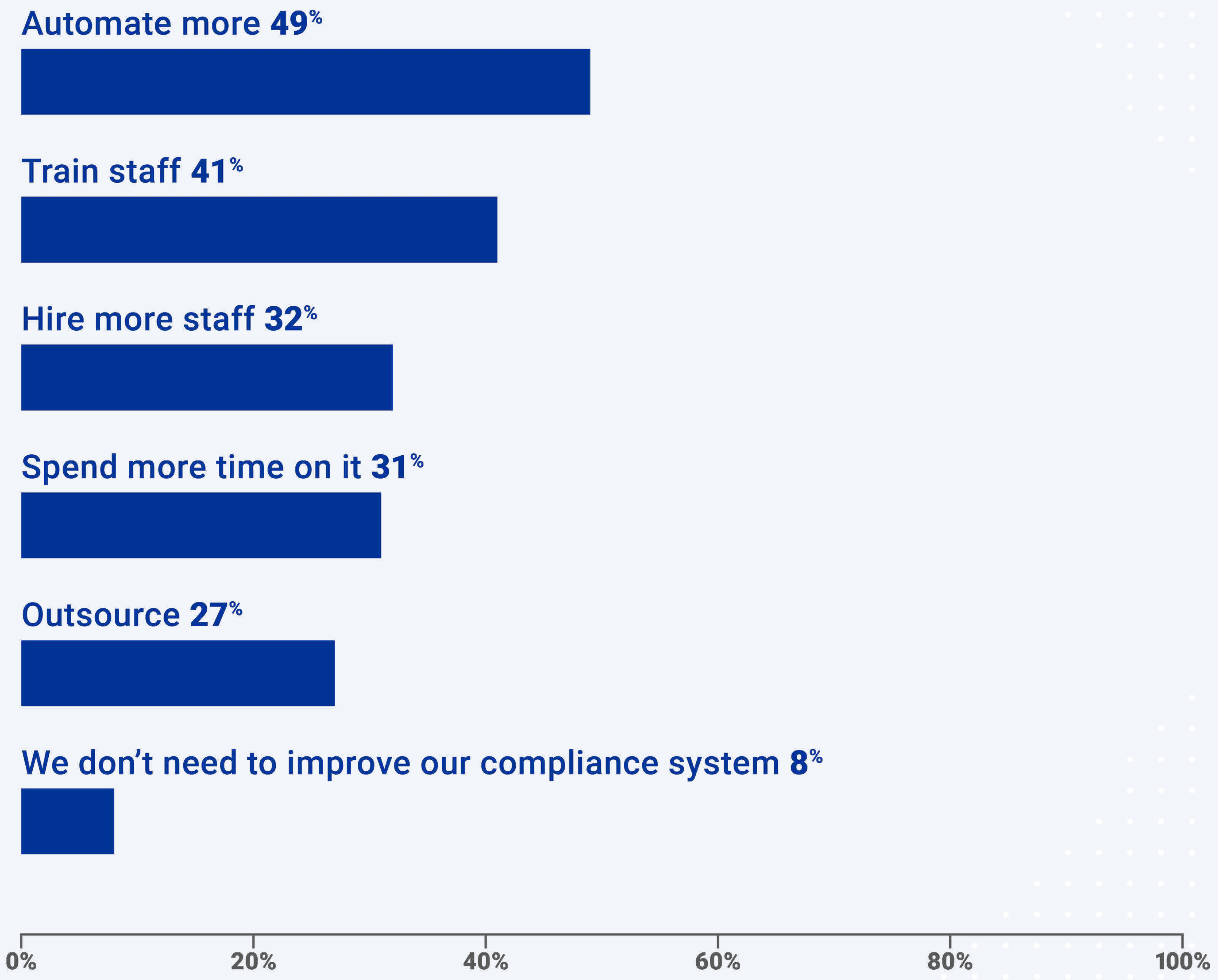


Improving compliance

Automation is a key solution

When asked “what would you do to improve compliance?” the most common recommendation was to automate more, an option chosen by almost half (49%) of respondents. That was followed by more staff training and adding more staff. Survey respondents also said they would like to automate almost 40% of their daily work, and over 40% of their team’s work.

What would you do to improve compliance?

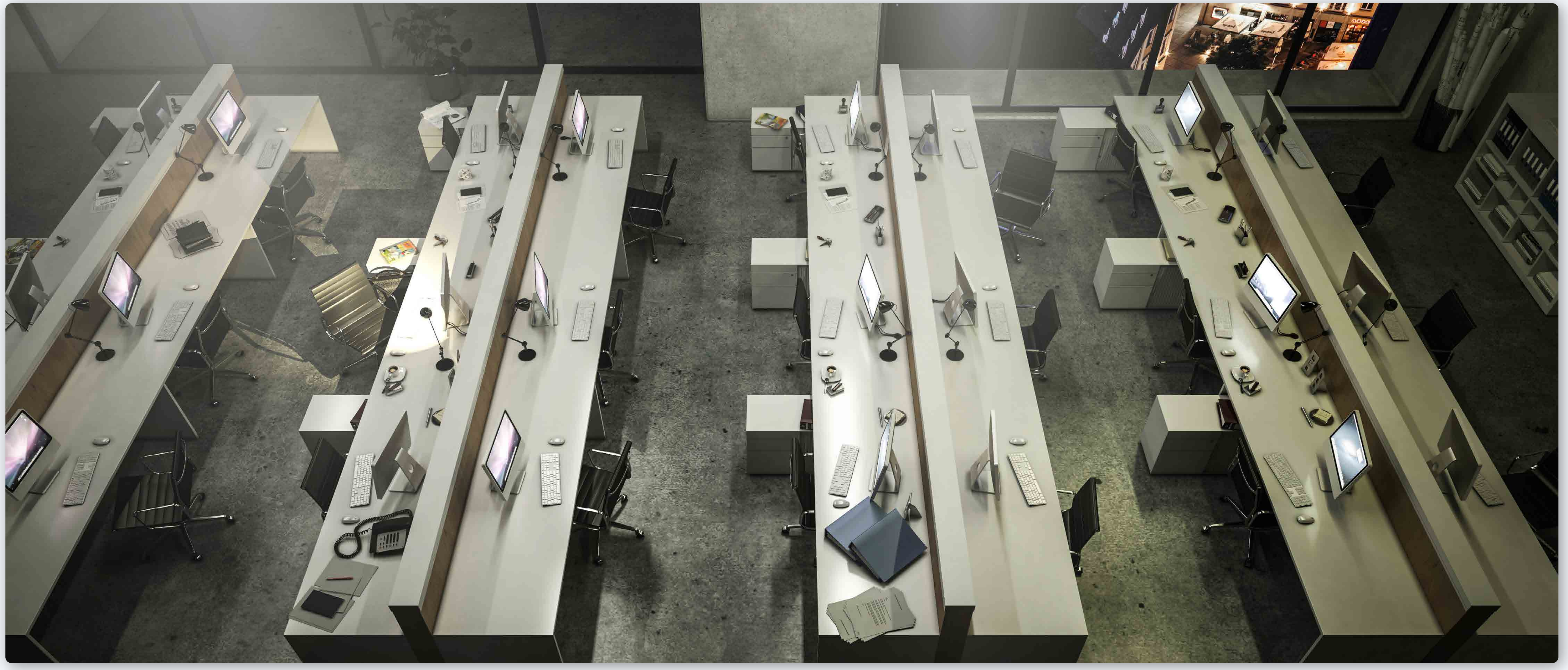


Part Three: The human cost of poor automation

The lack of automation has a negative impact on IT teams in terms of how much unnecessary time they spend on routine IT tasks and effort needed for audit compliance. It's possible to restate that impact in financial terms – take the time spent and multiply by the full-loaded cost of employing that staff.

There are however significant other costs which aren't quite so easy to calculate. IT staff end up doing work they don't enjoy, they fall behind schedule, they deliver poor service, they don't have time to spend on training and development or working on strategic projects.

The research reveals some of those hidden costs.

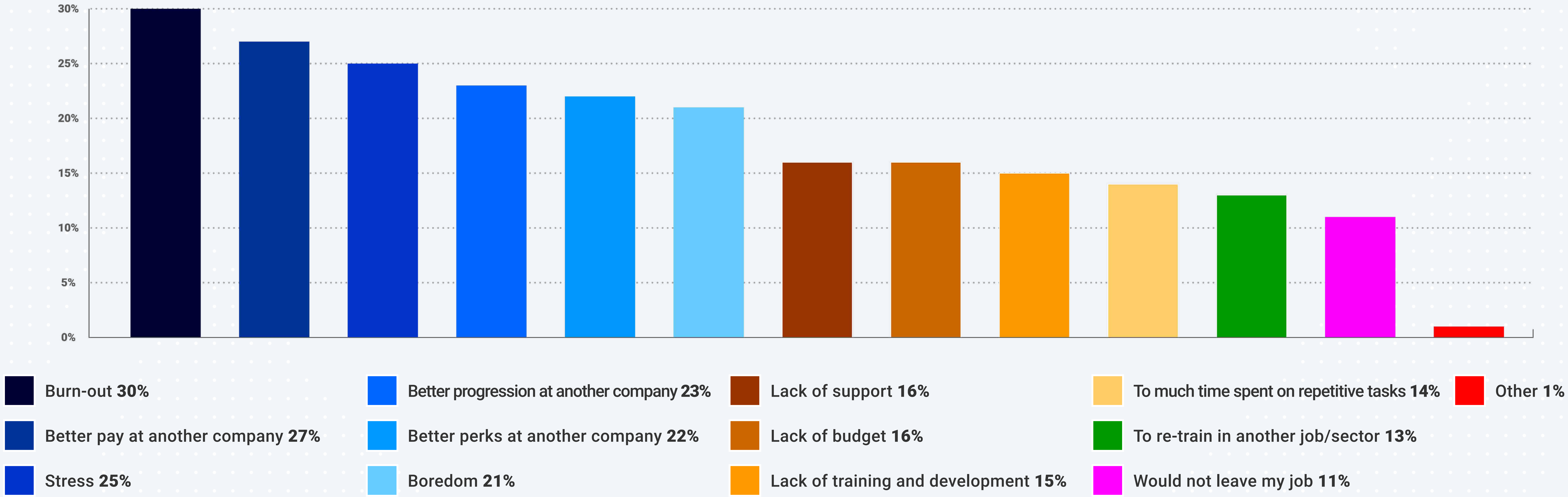


The human factor

Burn-out leads to staff departures

Burn out, closely followed by stress, are two of the biggest drivers for staff to want to change jobs. As these are highly experienced IT administrators, they can be very hard to replace.

Key factors in leaving



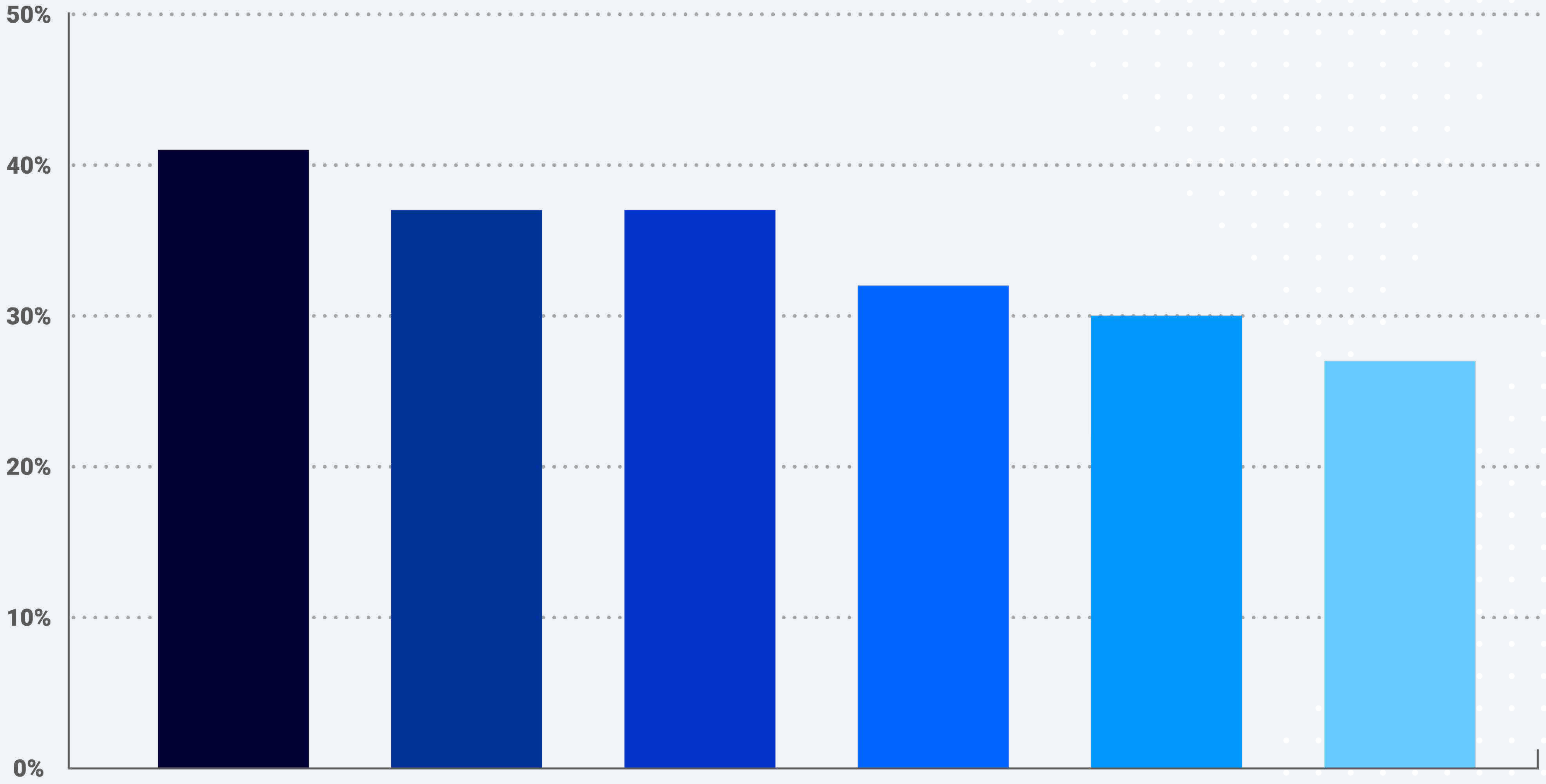
More time to retain staff

Improving skills and innovation

When asked what survey respondents would do with the time saved by automation, the number one answer was training and development (41%) with innovation and growth coming a close second (37%). A third said they'd use the time for personal time-off. It's clear that reducing manual effort has benefits for the individual and the business.

What would you do with time saved by automation?

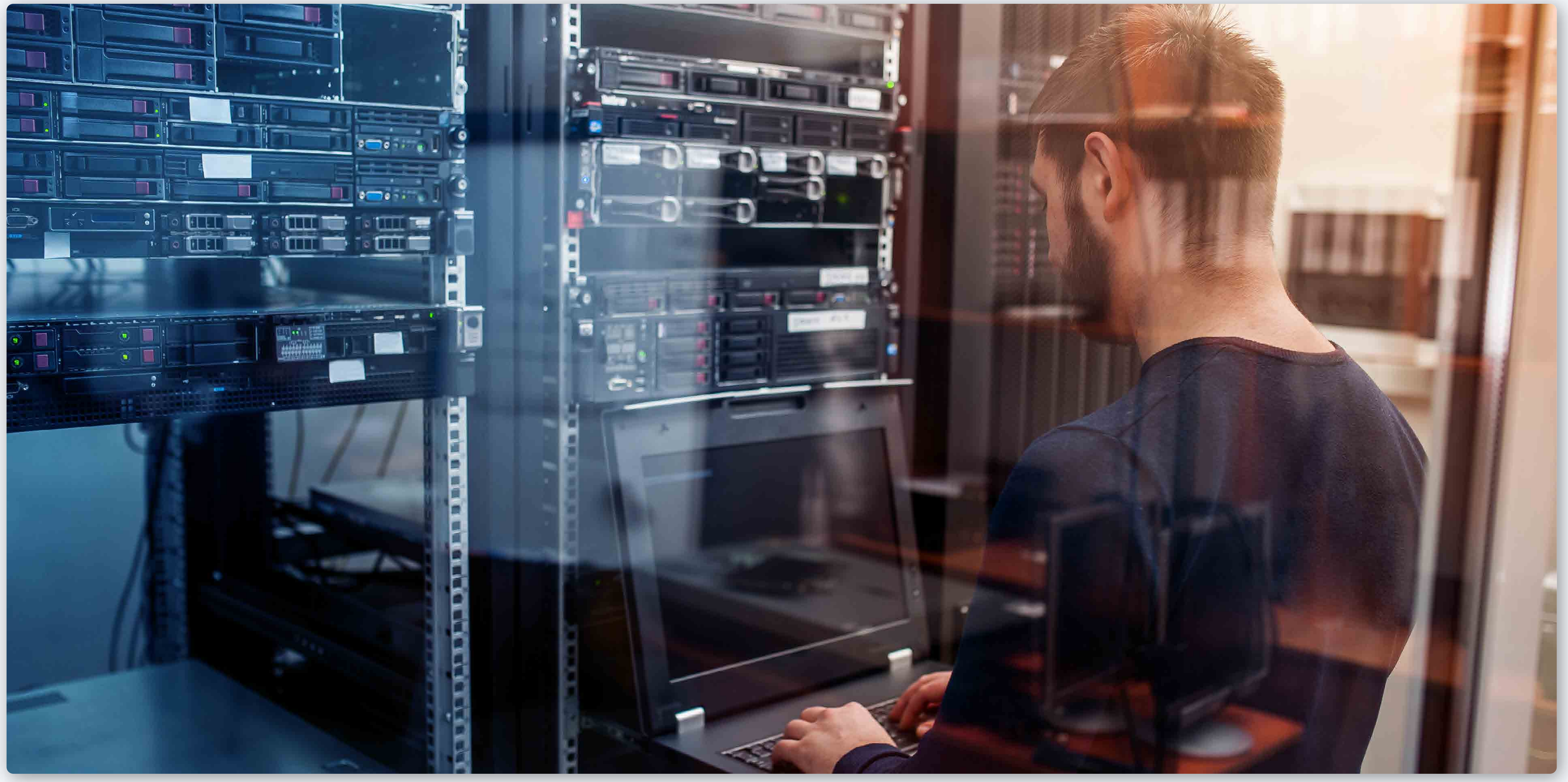
- ■ Training and development **41%**
- ■ Driving innovation **37%**
- ■ Driving growth **37%**
- ■ Taking personal time off **33%**
- ■ Catching up with industry developments **30%**
- ■ Attending webinars, conference, etc. **27%**



Recommendations

It's encouraging that delegation is being adopted and, for many, proving useful. It's also positive to see regular compliance audits being widely adopted. There is room for improvement however, particularly when secure automation is deployed. Overall, the benefits can be seen in reduced cost and risk, improved service, and reduced staff stress.

There are two key areas that IT teams should prioritise to improve automation, delegation, and compliance:



Address risk concerns

Look for secure ways to automate IT tasks that are sensitive so that more work can be delegated. Traditional automation via scripting (e.g., PowerShell or Linux/UNIX Bash), is dangerous as the scripts may include embedded administrator credentials. Robotic Process Automation (RPA) tools may need external password vaults and not guarantee that credentials are always protected. Verify the protection of the administrator credentials before delegating admin tasks to the IT help desk or end users.

Look for the right automation platform

With only just over a third of organisations that use RPA for IT automation saying it's suitable for IT operations, it's clear it is not the ideal solution for the challenges of automating IT work. **Gartner coined the term "hyperautomation"** to describe the need for different types of automation technology for different use cases.
For IT operations, look for an automation platform that makes automated script or playbook development easy, has secure connections to IT systems and devices and that makes compliance audits easy.

About this report

This online survey was conducted by Atomik Research among 1001 IT managers in the UK. The research fieldwork took place on 28 January – 4 February 2022. Atomik Research is an independent creative market research agency that employs MRS-certified researchers and abides to MRS code.

About Osirium

Osirium Technologies plc (AIM: OSI) is a leading UK-based cybersecurity software vendor delivering Privileged Access Management (PAM), Privileged Endpoint Management (PEM) and Osirium Automation solutions that are uniquely simple to deploy and maintain.

With privileged credentials involved in over 80% of security breaches, customers rely on Osirium PAM's innovative technology to secure their critical infrastructure by controlling 3rd party access, protecting against insider threats, and demonstrating rigorous compliance. Osirium Automation delivers time and cost savings by automating complex, multi-system processes securely, allowing them to be delegated to Help Desk engineers or end-users and to free up specialist IT resources. The Osirium PEM solution balances security and productivity by removing risky local administrator rights from users, while at the same time allowing escalated privileges for specific applications.

Founded in 2008 and with its headquarters in Reading, UK, the Group was admitted to the London AIM list in April 2016. For further information please visit https://www.osirium.com.