CIO PULSE REPORT

Identity and access management revisited

A changing world demands simplification and an urgent focus on security

FREEFORM DYNAMICS

CIO WaterCooler

in association with

XALIENT accelerate your business

okta

About this Report

Why did some organisations respond better than others to the lockdown-driven challenge of getting people working from home? According to a survey of CIO WaterCooler members, a key factor could be how far they had got towards implementing coherent and comprehensive identity and access management capabilities, or IDAM as it's known.

Before Covid-19, better IDAM was often seen as merely 'nice to have,' but the pandemic has stripped away that illusion. As the 73 responses to our online survey show, while some organisations dealt well with the jump in demand for secure remote access to business IT and for cloud and SaaS applications, other organisations had problems.

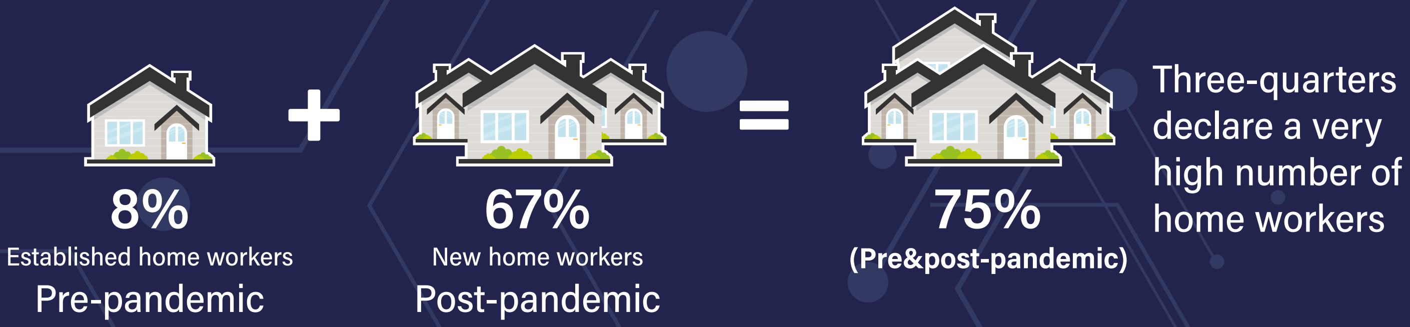
Their IDAM capabilities are one thing that sets these two groups apart, with the pandemic revealing a hidden truth: today, coherent IDAM is not 'nice to have,' it is 'need to have.'

Change came Urgently and Suddenly

At the start of 2020, IT landscapes were already pretty complicated. We had office-based workers, mobile workers and people who worked from home at least some of the time, all in significant numbers, and we had cloud and SaaS solutions alongside 'traditional' applications. Managing multiple IT identities could be complex and time-consuming, and it sometimes introduced errors, but at least it was a regular and familiar task, and one we believed we understood.

Then, almost overnight, the way that the majority of businesses functioned was turned upside down.

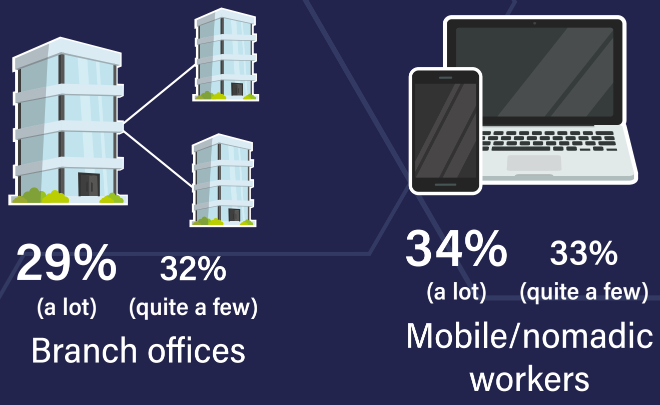
Impact of Covid-19 on home working



Ensuring secure user access to on-site applications and services, wherever those users were based, was a significant challenge even before the pandemic. So too was the trend towards using cloud-based solutions and SaaS applications, as organisations strove for greater agility and flexibility.

With huge numbers of people ordered to work from home, those challenges were multiplied several times over.

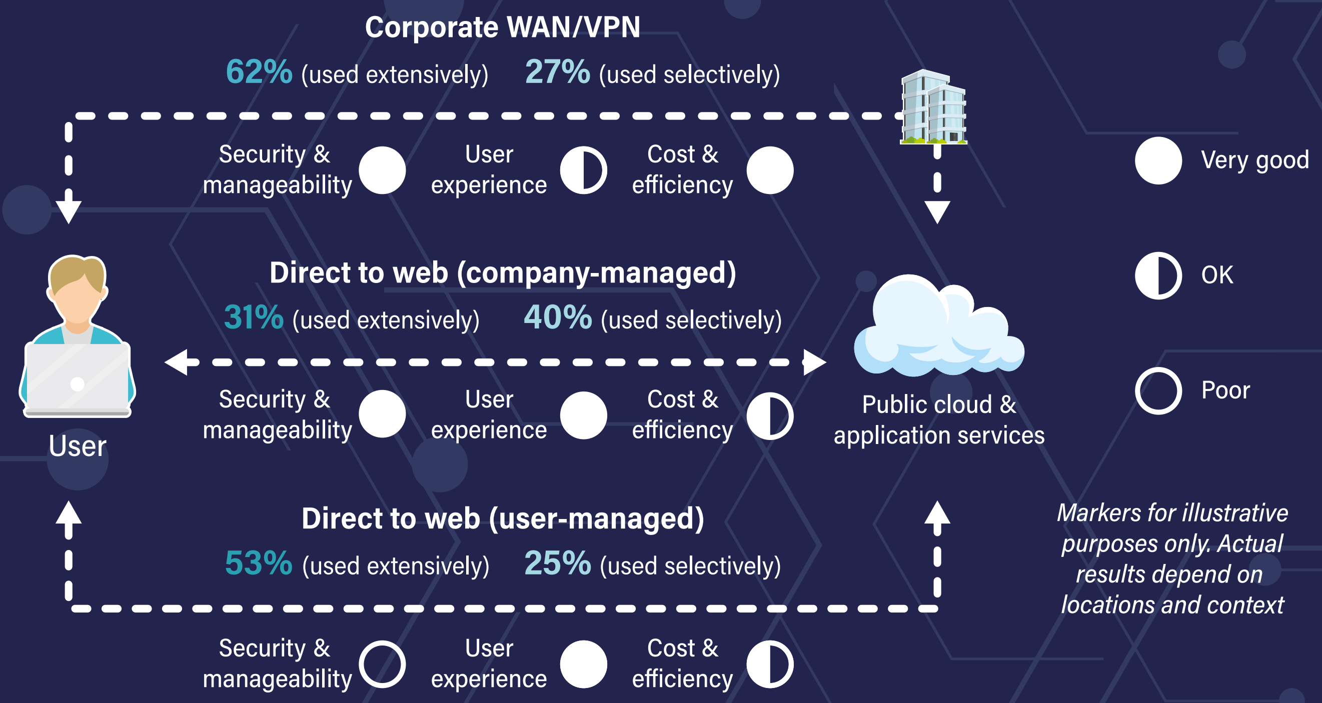
Other forms of remote working in use



Not only did working locations and work hours become far more diverse and flexible, but our secure access processes had to incorporate people using multiple devices, some personal, others borrowed, and some taken from business offices. And all this needed to happen without over-reliance on a limited pool of IT skills and resources.

The Cloud Connectivity Conundrum

Your remote users - who may well be the majority of the organisation now - need to connect safely, securely and efficiently to applications running both inside and outside the data centre. Today, enterprises use a variety of methods and mechanisms to link users both to the Internet and their on-site systems while maintaining a good user experience.



Corporate WAN/VPN

62% (used extensively) 27% (used selectively)

Security & manageability ● User experience ◐ Cost & efficiency ●

Direct to web (company-managed)

31% (used extensively) 40% (used selectively)

Security & manageability ● User experience ● Cost & efficiency ◐

Direct to web (user-managed)

53% (used extensively) 25% (used selectively)

Security & manageability ○ User experience ● Cost & efficiency ◐

User

Public cloud & application services

● Very good

◐ OK

○ Poor

Markers for illustrative purposes only. Actual results depend on locations and context

The one thing common to all these mechanisms is of course the need for security, which in turn translates to the need for identity and access controls. You need to know who is connecting and from where, what user rights they have, and so on. However, they address security in different ways.

For example, traditional WANs, corporate VPNs, and connections from branch offices are usually managed and secured by the organisation itself. Conversely, the use of home networks is widespread but it relies on the user for security. For many users this will not be a problem, but there are always likely to be some who lack the skills to adequately secure their WiFi network, say.

Then there are newer mechanisms, most notably the various SD-WAN (Software Defined Wide Area Network) solutions. Some of these focus solely on connectivity, while others also incorporate full network security. Our survey finds relatively low SD-WAN usage today, but with considerable growth potential (right).

This variety of connectivity means we ideally need a single IDAM tool or overlay that is consistent and can cover all approaches. Only in this way can we maintain both service access and enterprise security. And because large numbers of staff are likely to continue working flexibly into the future, the use of web-based conferencing and communications tools - and the need for IDAM - can only grow.

The emerging role of SD-WAN

Basic services

Focused mostly on connectivity

10%	24%	28%
Used extensively	Used selectively	Would be desirable

Advanced services

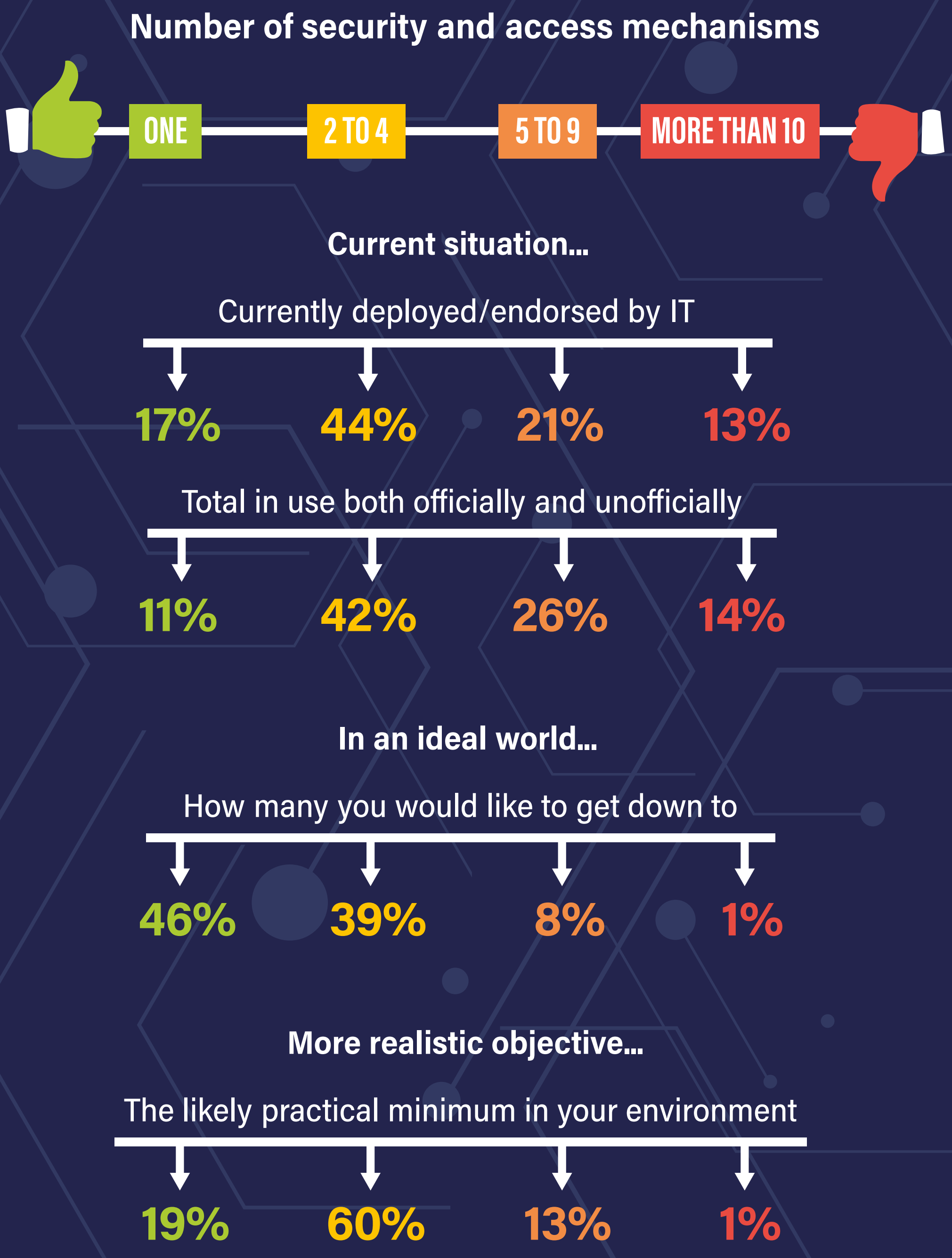
Incorporating full network security

7%	24%	32%
Used extensively	Used selectively	Would be desirable

The Threat of Identity Sprawl

The survey highlights the huge challenge facing organisations as they grapple both with managing identities and with controlling access to applications, systems and data. A big part of the problem is that most organisations run multiple security and access mechanisms, resulting in users having multiple identities.

Around one-third use more than four officially sanctioned IDAM schemes, and one in seven organisations say that they use more than 10. The numbers are even higher when we add 'shadow' log-in systems to the count.



Number of security and access mechanisms

	ONE	2 TO 4	5 TO 9	MORE THAN 10
Current situation...				
Currently deployed/endorsed by IT	17%	44%	21%	13%
Total in use both officially and unofficially	11%	42%	26%	14%
In an ideal world...				
How many you would like to get down to	46%	39%	8%	1%
More realistic objective...				
The likely practical minimum in your environment	19%	60%	13%	1%

Having multiple mechanisms and identity administration tools will clearly create operational friction. Experience shows that friction of this kind inevitably increases the risk of manual errors, any one of which could cause security headaches, never mind the high probability of users experiencing delays and frustration.

Survey respondents clearly recognise the problem: almost half (46%) say that they would ideally like to get down to using just one IDAM system - a 'one-stop-shop' for identity, in other words.

However, many of those currently using multiple systems clearly regard one as an unrealistic ambition. If we deduct the 11% who say they already run a single IDAM system, just 8% more believe that getting multiple systems down to one is a practical possibility. Instead, most believe that a target of two to four IDAM systems is realistic, while a significant minority would settle for between five and nine.

Taken together, these results indicate a poor awareness of the capabilities of modern IDAM tools. For example, they can replace multiple legacy IDAMs on-site, be deployed as managed services, or run as cloud-based overlays to consolidate existing identity mechanisms into a single IDAM layer.

Challenges and Risks

The research very clearly shows the need for IDAM simplification. That is because many of the practical challenges and issues around identity and access can be a direct consequence of using more than one IDAM system.

Many organisations experience hassles trying to manage separate identities when using multiple cloud services, for example, or when internal IDAM systems need to be integrated with those of cloud service providers.

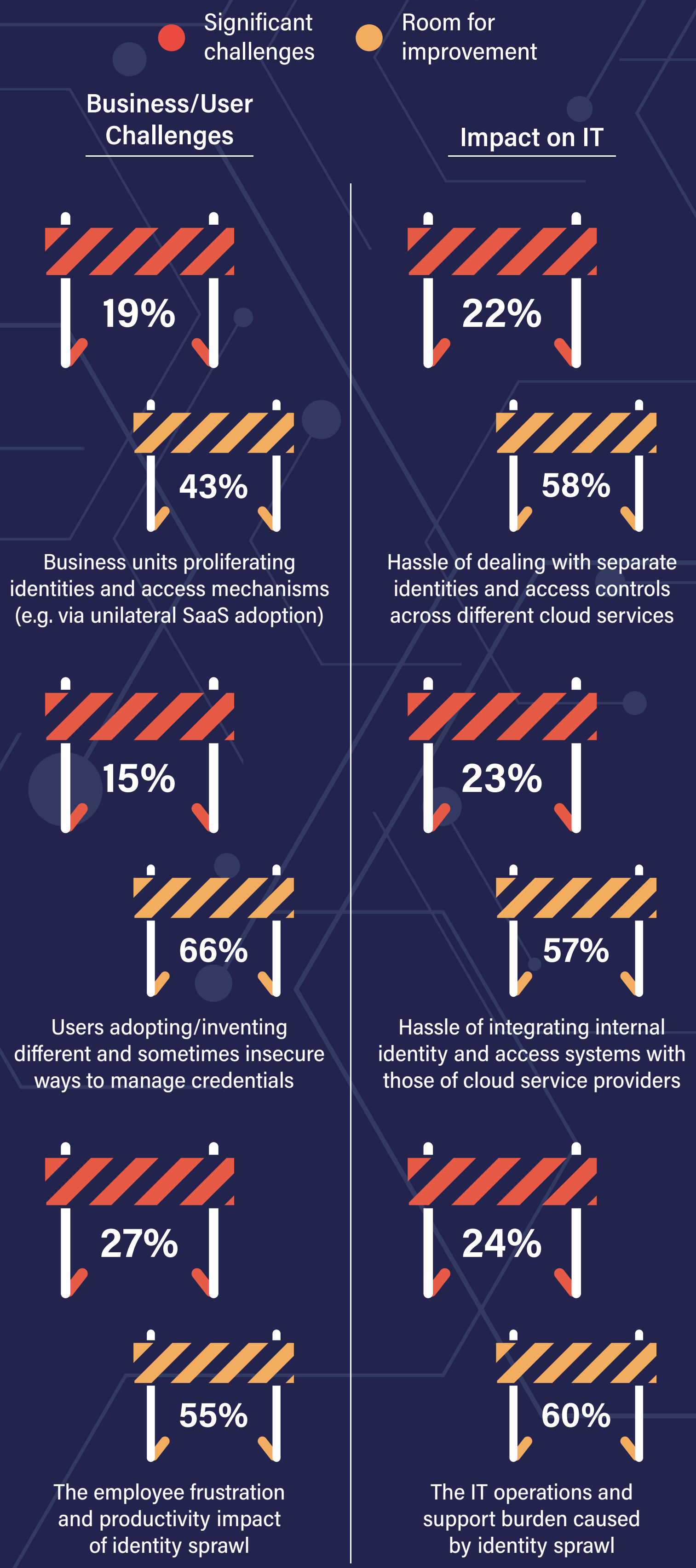
Indeed, one of the things that brings identity and authentication issues to the surface is the proliferation of identities that can occur when business units take on cloud services and Software as a Service (SaaS) offerings.

It is also common for users to adopt or invent different, sometimes insecure, ways to manage credentials. This is not too surprising at a time when SaaS usage is expanding greatly, and when users are having to adopt new systems while also working from home, perhaps for the first time. However, the detailed results showed fewer than one in five respondents could report that they had no issues here.

All these issues clearly cause challenges for IT staff. If we drill down further, only around 15% of respondents said that IT Operations and Support have no issues at all with identity sprawl. Conversely more than four in every five have at least some issues or challenges in this area.

And the daily challenges and issues managing IDAM are not theoretical, nor are they problems only for IT. The final result shows that IDAM challenges can directly cause employee frustration, and this in turn can lead to user productivity problems, both of which are boardroom-level issues.

To what degree are the following a challenge at the moment in relation to identity and access?



Business units proliferating identities and access mechanisms (e.g. via unilateral SaaS adoption)

Hassle of dealing with separate identities and access controls across different cloud services

Users adopting/inventing different and sometimes insecure ways to manage credentials

Hassle of integrating internal identity and access systems with those of cloud service providers

The employee frustration and productivity impact of identity sprawl

The IT operations and support burden caused by identity sprawl

The IDAM Capability Scorecard

Given the challenges that Identity and Access Management presents, it is interesting to look at how effective are the capabilities that organisations have in place to help with routine operations and administration. The need for comprehensive and coherent IDAM solutions has never been in doubt, and the dramatic shift in working patterns driven by the pandemic and the mass switch to home working has shone a bright light on this.

	● Coherent and comprehensive	● Gaps and disjoints exist	● Generally patchy	● Little/nothing in place
IDAM fundamentals (directory, SSO, MFA, etc) on-premise & cloud	30%	52%	14%	1%
Automated access lifecycle provisioning/ removal (joiners, movers, leavers)	14%	44%	27%	14%
Customer/partner ID and access management to your systems	14%	45%	22%	11%
Facilities to integrate new apps & cloud services into your IDAM	24%	40%	24%	10%
'Non-human' ID management, e.g. IoT, autonomous AI, etc	14%	30%	26%	18%
API management (programmatic access to systems & data)	12%	41%	27%	15%
IDAM-related analytics and reporting	8%	36%	32%	18%

On the positive side, it is clear that a significant proportion of respondents recognise the importance of IDAM, including the opportunity to deploy cloud-based IDAM - this typically overlays legacy systems to provide a coherent identity solution. And almost a quarter already use IDAM to ease the adoption of new SaaS applications and cloud services.

However, IDAM capabilities remain patchy or disjointed for the vast majority. In addition, few have fully implemented capabilities to automate the access lifecycle, despite automation being widely recognised as a key enabler of efficiency, as well as a great way to minimise human error and ensure security. Improving your capabilities in these areas can bring significant benefits, as we will see shortly.

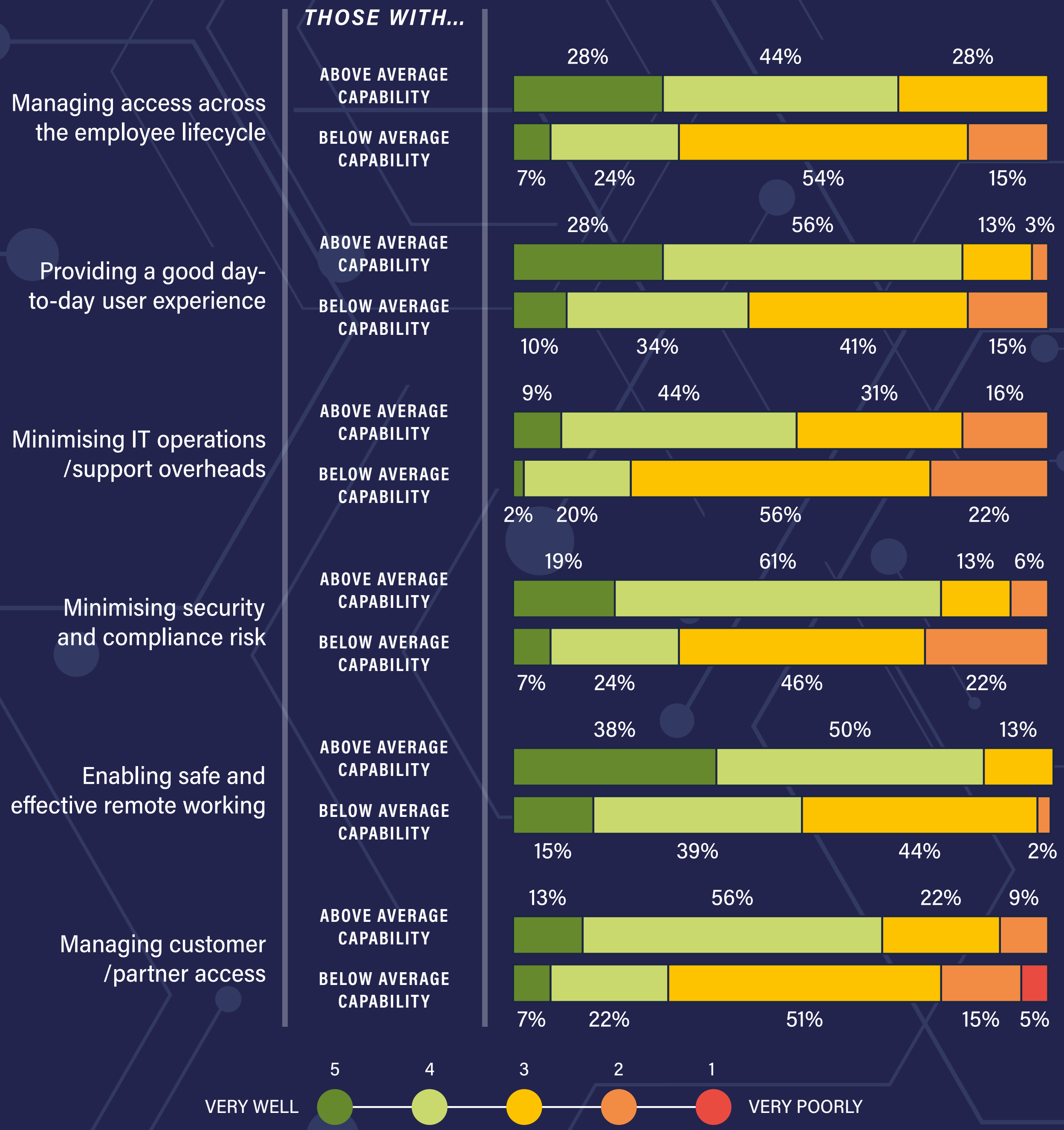
But IDAM capabilities are also lacking in less well-established areas. It is troubling for example that only around one in eight respondents said that they have coherent and comprehensive capabilities to manage API access to systems and data. As has already been mentioned, cloud and SaaS usage is increasing rapidly and APIs are often used to integrate between SaaS solutions and systems running in-house. IDAM for APIs should therefore be a priority to ensure security is maintained.

It is also puzzling to see how few said that they had comprehensive analytics and reporting capabilities. It seems that the value of knowing what's going on is not widely appreciated, at least by budget holders, which is worrying in this fast-changing world where privacy and security are high profile matters.

The Capability Advantage

It can be difficult for individual CIOs and IT organisations to demonstrate a solid business case for investment in IDAM capabilities. However, deeper analysis of our survey responses offers significant promise here. We used our IDAM Capability Scoreboard (page 6) to generate a total score for each respondent and separated them into two groups, one of those who reported above-average IDAM capabilities and the other below. We could then compare the two groups' performance on a range of IT and business requirements and look for correlations between IDAM capability and IT success.

How well do your current Identity and Access Management mechanisms support the following?



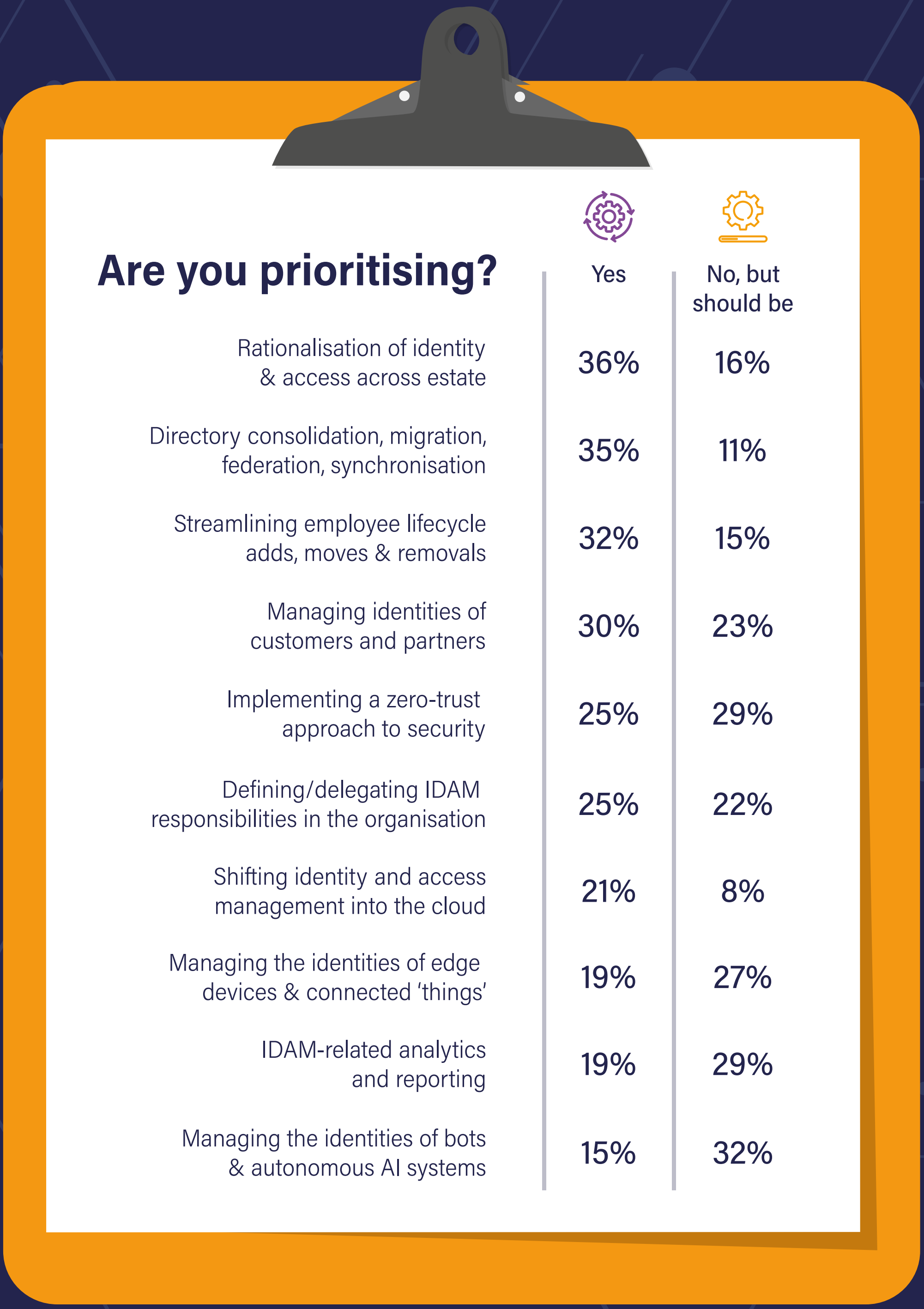
While the results do not confirm causality between good IDAM and effective IT operations, the correlations are unlikely to be a coincidence: organisations with above-average IDAM are likely to provide better support for a number of IT and business operations. Many, such as minimising IT and support overheads, offer obvious advantages when making a business case. Some, such as minimising security and compliance risk, are also essential when it comes to enabling the safe and effective remote working that so many organisations now need.

Upping Your Game

Given the importance of IDAM and the operational benefits that correlate with better IDAM capabilities, it is interesting to see how our survey respondents ranked their priorities. Of course, in each case there were others who had no plans for action, for example because they had already acted. or because they saw no need.

Having already seen just how many IDAM tools that some organisations have deployed, it is no surprise to see that directory consolidation and identity rationalisation are high priorities. Identity sprawl also helps explain the priority given to streamlining of identity lifecycle management and managing the identities of customers and partners.

Given the uptake of SaaS services, it should also be no shock that significant numbers plan to move identity and access management to the cloud.



Are you prioritising?

	Yes	No, but should be
Rationalisation of identity & access across estate	36%	16%
Directory consolidation, migration, federation, synchronisation	35%	11%
Streamlining employee lifecycle adds, moves & removals	32%	15%
Managing identities of customers and partners	30%	23%
Implementing a zero-trust approach to security	25%	29%
Defining/delegating IDAM responsibilities in the organisation	25%	22%
Shifting identity and access management into the cloud	21%	8%
Managing the identities of edge devices & connected 'things'	19%	27%
IDAM-related analytics and reporting	19%	29%
Managing the identities of bots & autonomous AI systems	15%	32%

But alongside those plans of action, it is encouraging to see that there are many areas where survey respondents think they should be doing something, even if they have no active projects yet. High on this list are managing the identities of bots, autonomous AI systems, edge devices and 'connected things,' all of which are likely to grow in importance as usage expands. Could the same happen with the often overlooked reporting and analytics? Clearly IDAM has considerable potential for change, if only good business cases can be made.

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we help busy IT and business professionals get up to speed on the latest technology developments and make better-informed investment decisions.

For more information, visit www.freeformdynamics.com or follow us on Twitter @FreeformCentral

About CIO WaterCooler

The CIO WaterCooler is a free, open and supportive community that supports its users in sharing their knowledge and experience with their peers around the around. We help our members raise their profile, share their news and views and allow to keep up to date with the developments fast pace of change and technology.

For more information, visit www.ciowatercooler.co.uk

About Xalient

Xalient empowers forward-thinking enterprises to innovate, differentiate and accelerate their business through the application of advanced technology. Combining transformative, software-defined network, security and Identity technologies with intelligent managed services, we help the world's top brands to become more resilient, adaptable and responsive to change. Driven by a passion for putting customers first, our forward-thinking, no-nonsense approach enables organisations to build secure networks for the future. We help them optimise cloud-based application performance, ensuring the highest levels of security for their people and their organisations, whilst providing a dependable and positive customer experience that accelerates their business today and into the future.

For more information, visit www.xalient.com

About Okta

The foundation for secure connections between people and technology. Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to both secure and manage their extended enterprise, and transform their customers' experiences. With over 5,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely adopt the technologies they need to fulfil their missions.

For more information, visit www.okta.com

Terms of Use