

Privileged user management

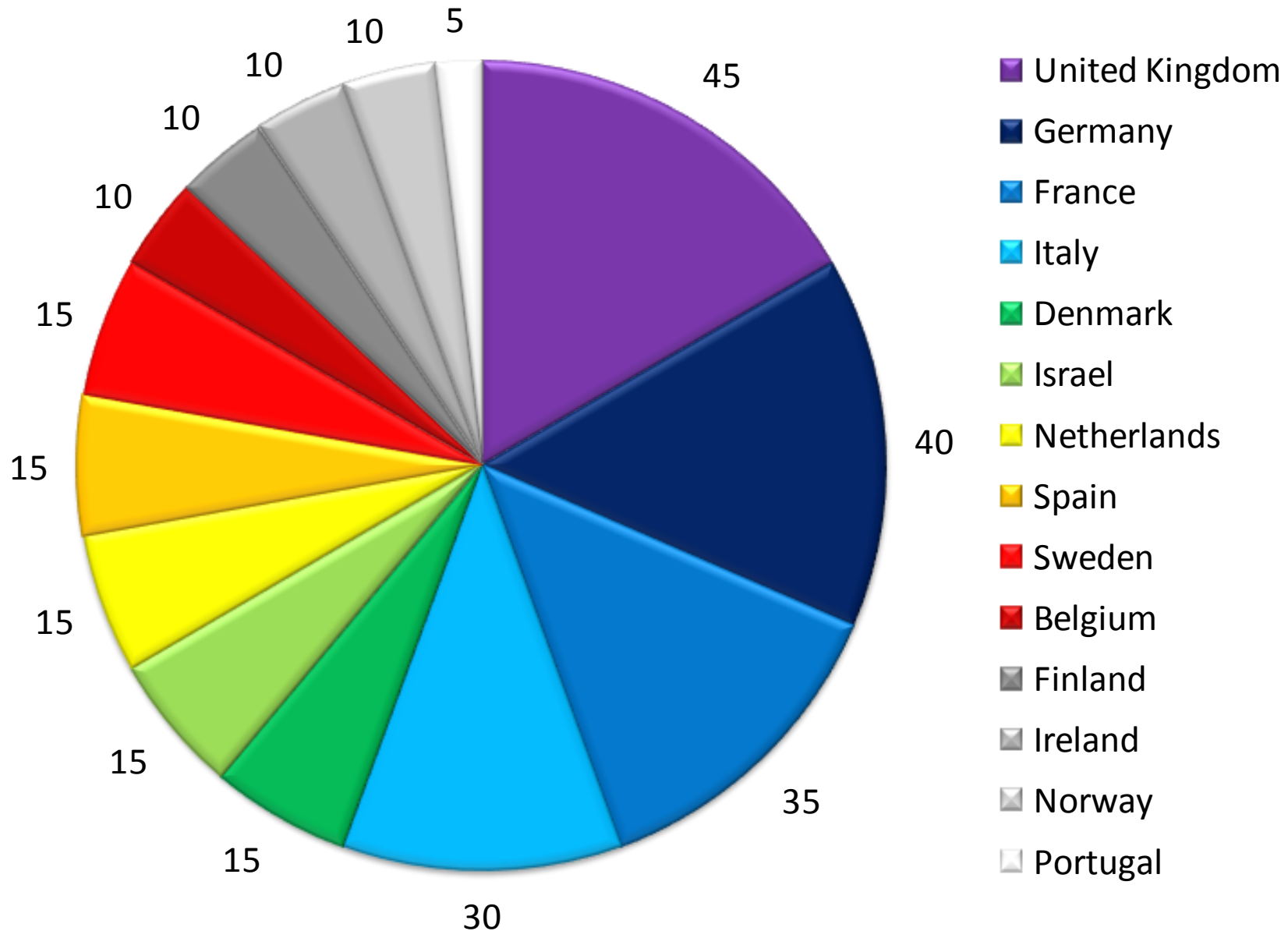
It's time to take control

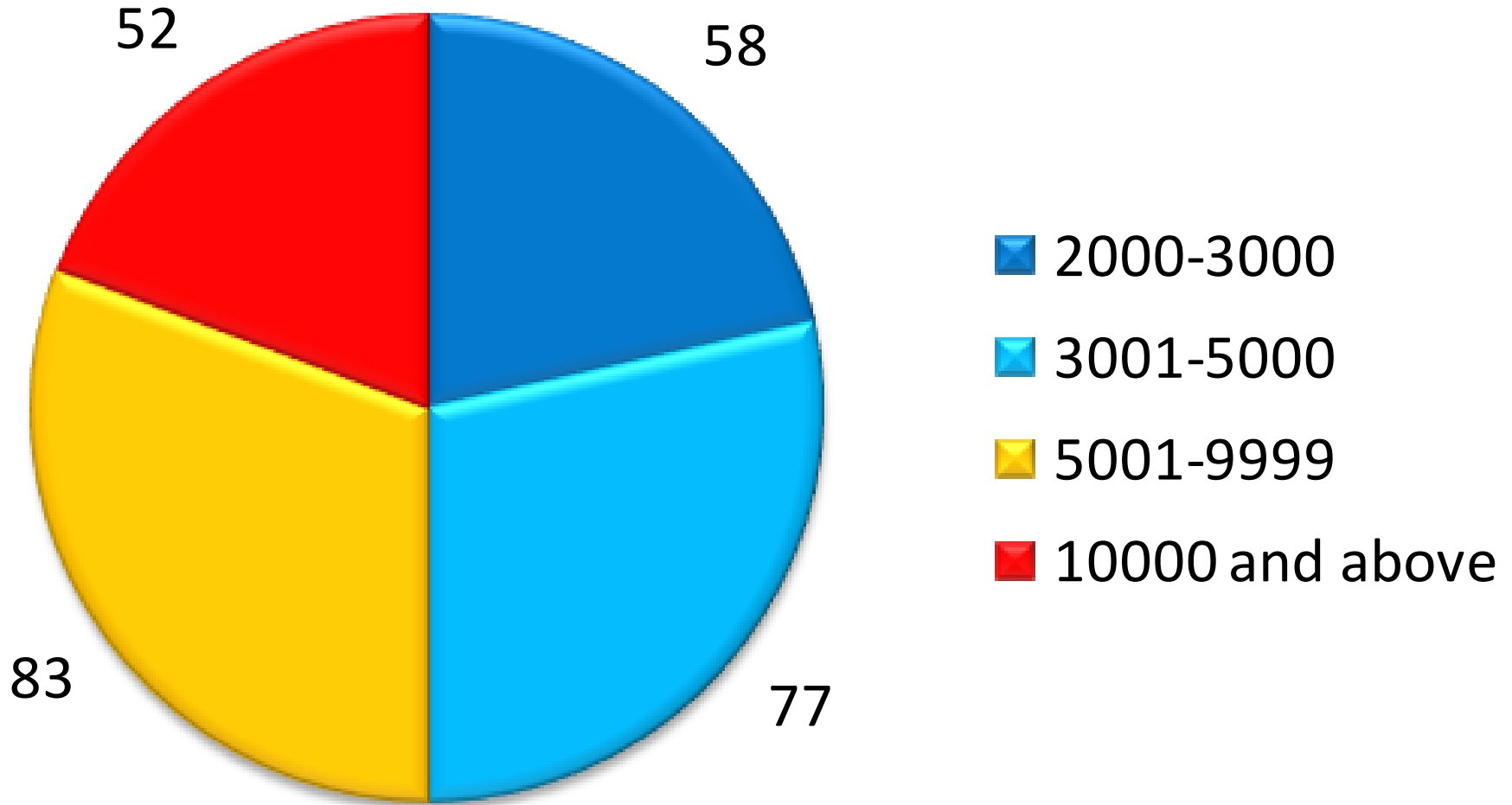
Bob Tarzey,
Analyst and Director, Quocirca Ltd

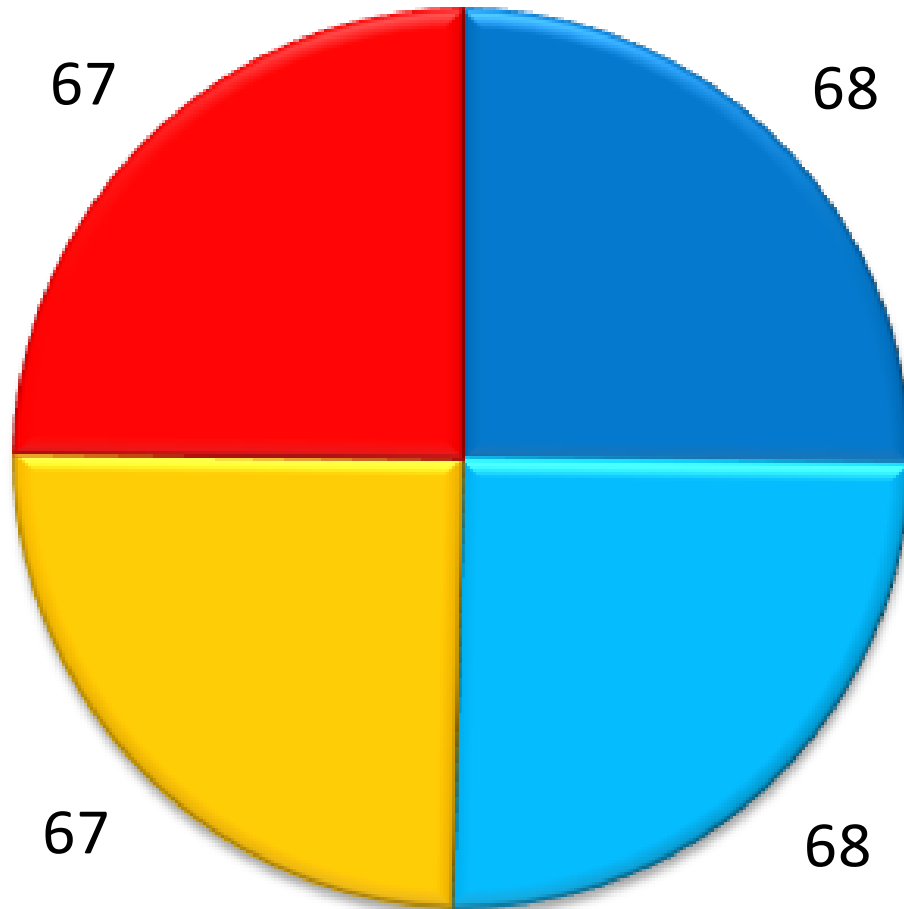
- The data presented is based on 270 telephone interviews with organisations across Europe conducted by Quocirca in June 2009
- The research was commissioned and sponsored by CA
- One aspect of the research was to look at how European organisations managed privileged user access to their IT systems and this presentation outlines the findings
- More details can be found in the associated Quocirca report available at www.quocirca.com

Privileged user management

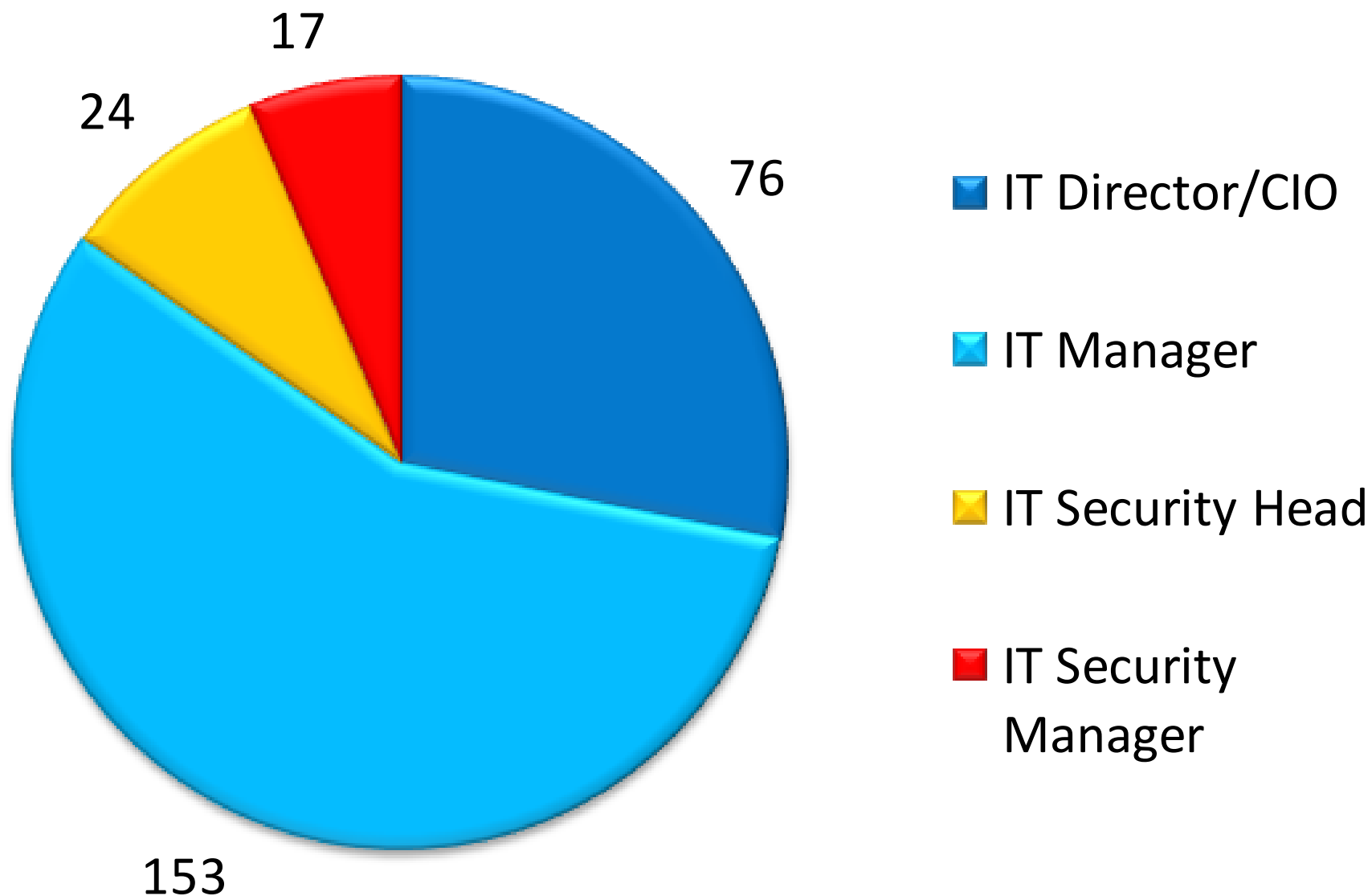
It's time to take control





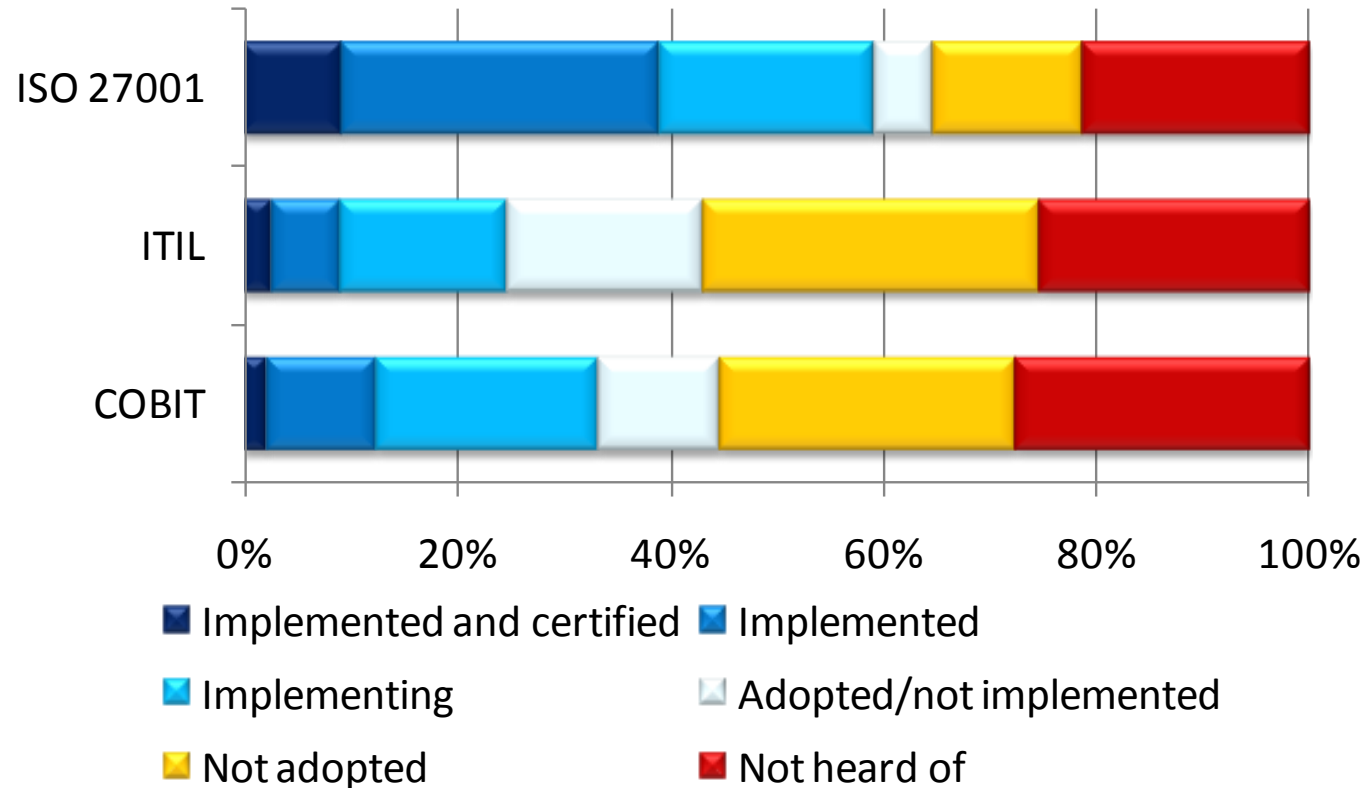


- Finance
- Government
- Manufacturing
- Telecoms & Media



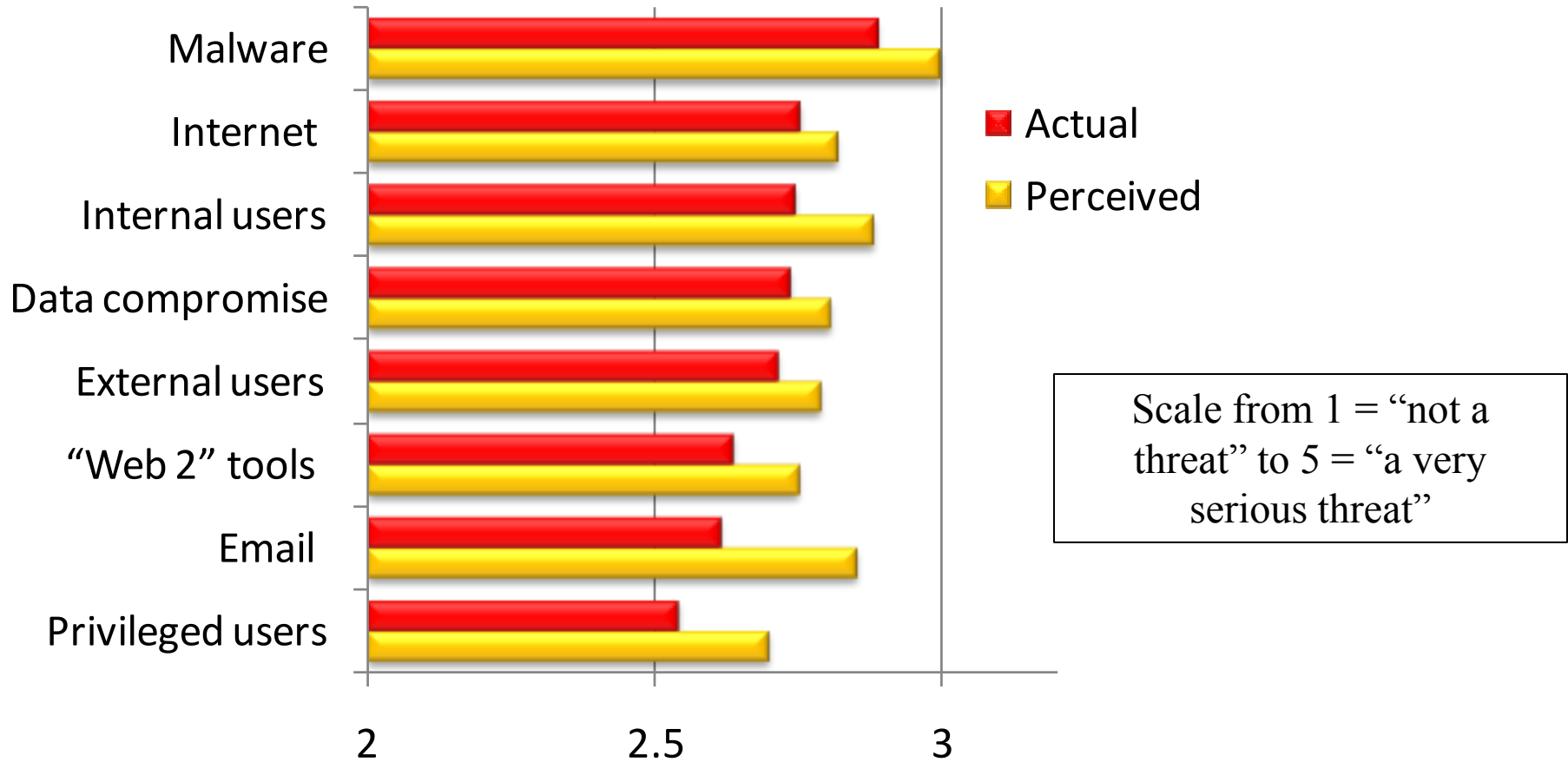
- The necessity of privileged user access
- The dangers of privileged user access
 - Accidental actions
 - Deliberate actions
 - Access by outsiders
- Controlling and monitoring their own activities is not high on the agenda of IT managers, with so many other issues to worry about
- This means there is an inherent contradiction in the confidence many businesses have in their ability to comply with certain regulations and managed their IT systems to a given standard

Deployment of security standards and methodologies?



Almost 60% of organisations say they have implemented or are planning to implement ISO27001, the widely accepted standard for the secure management of IT systems

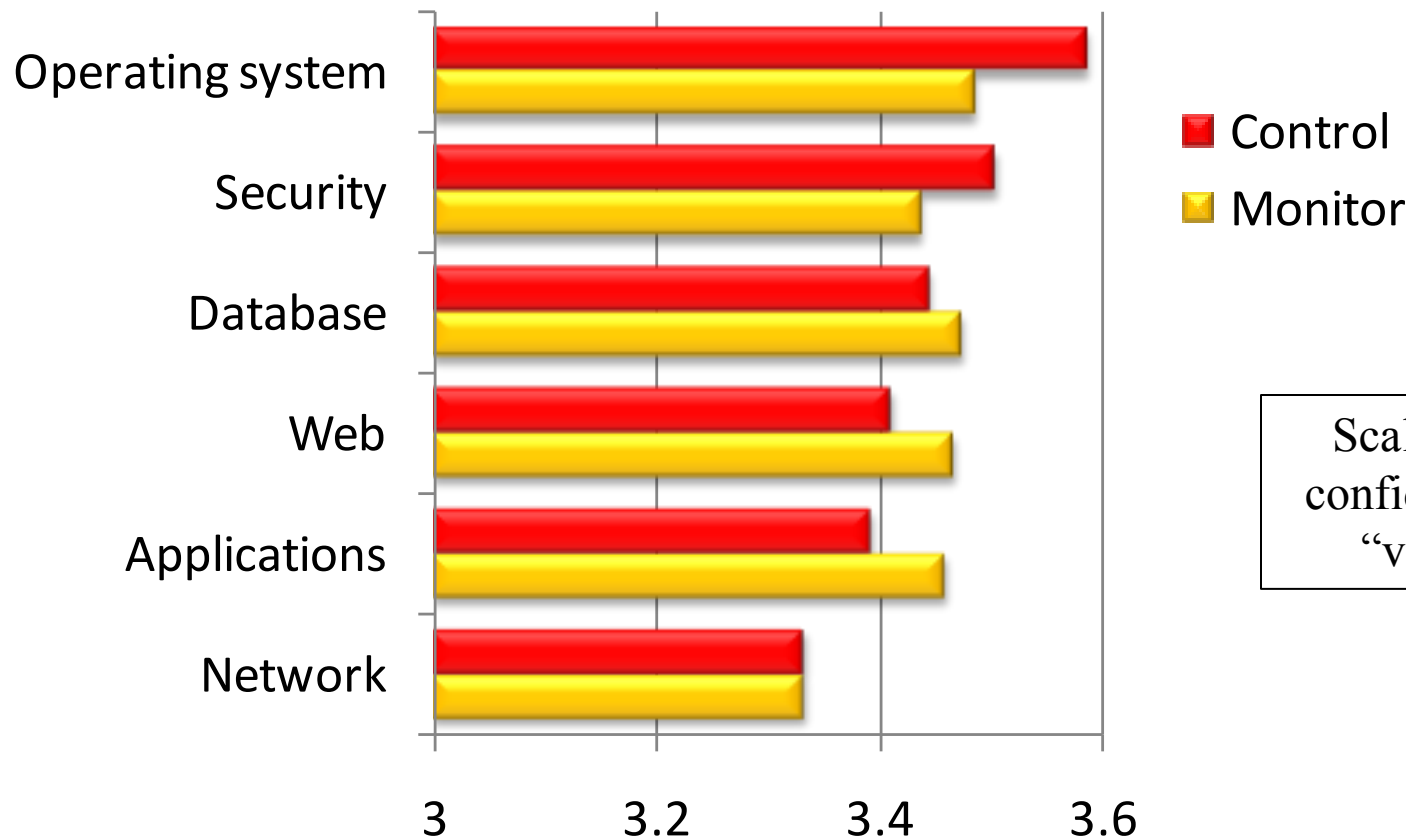
To what extent are the following a threat to IT security in your organisation?



When it comes to IT security, IT managers have many things to worry about, monitoring and controlling privileged users is not high on the list

How confident are you that you can control and monitor the following types of PU accounts?

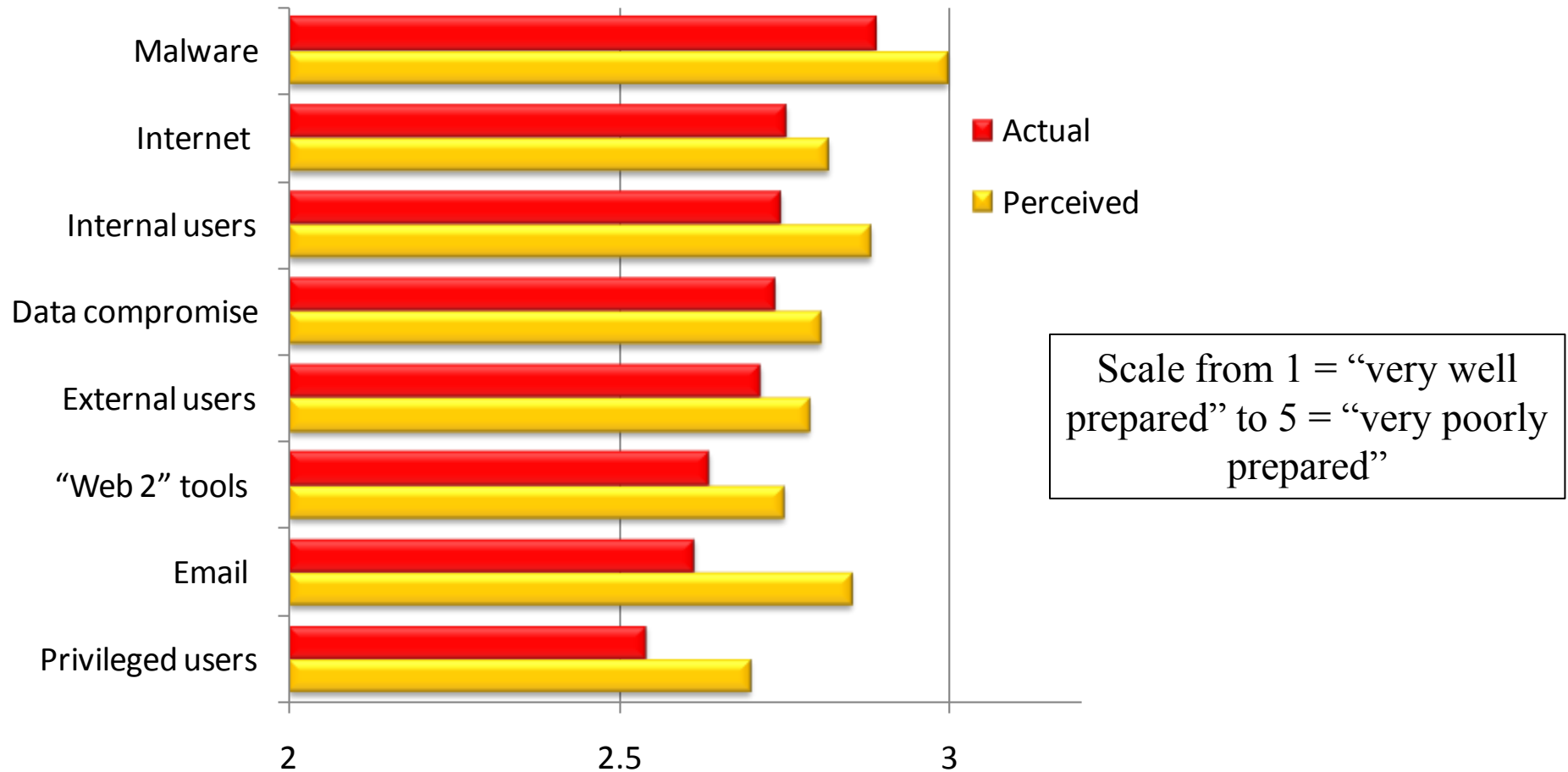
Administrators of.....



Scale from 1 = “not confident at all” to 5 = “very confident”

There is a reasonable level of confidence among IT managers that they can control and monitor privileged user activity. One might assume this is because they have the tools in place to do so, but as this research goes on to show, this is not the case

How well prepared is your organisation to protect against the following risks?



Another finding is that businesses believe they are reasonably well prepared to protect themselves against compliance audit failure, however, poor practice around privileged user shows that this confidence may be misplaced in many cases

ISO 27001

Requires: *“the allocation and use of privileges shall be restricted and controlled”*

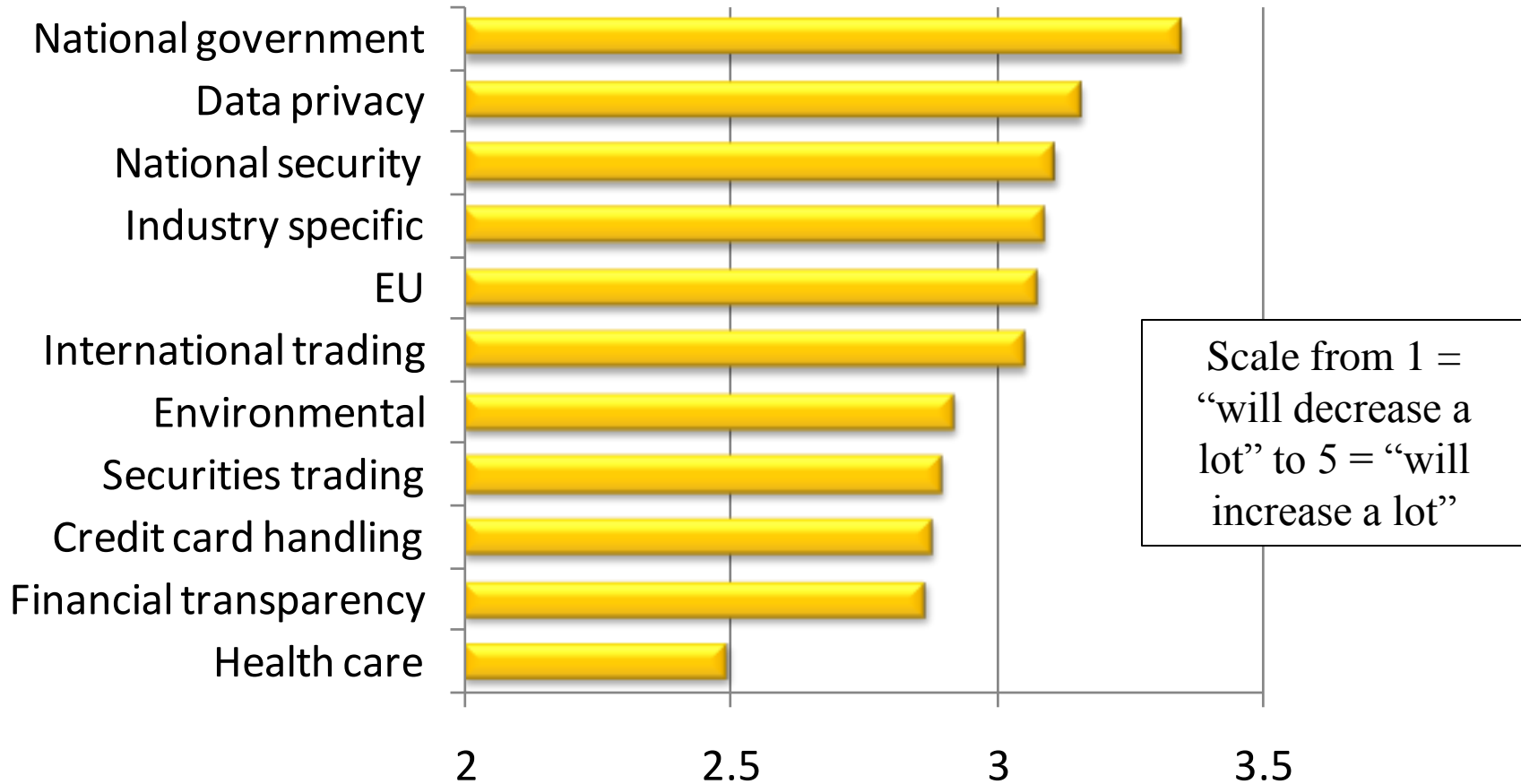
PCI DSS

Recommends: *“auditing all privileged user activity”*

Garante Privacy

Privileged users are: *“key figures for the security of data banks”*

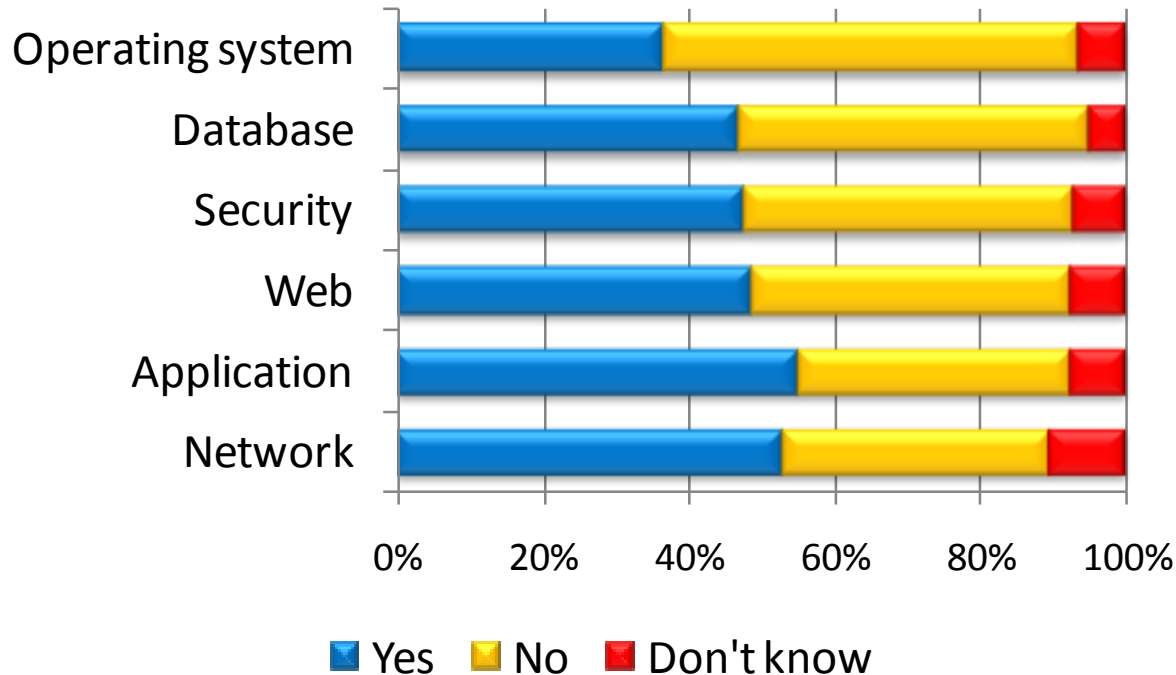
How do you see regulations in the following areas affecting your organisation over the next 5 years?



And the regulatory pressure is expected to increase in many areas, which is likely to lead any areas of bad practice in IT and data management being exposed., if they haven not been so already

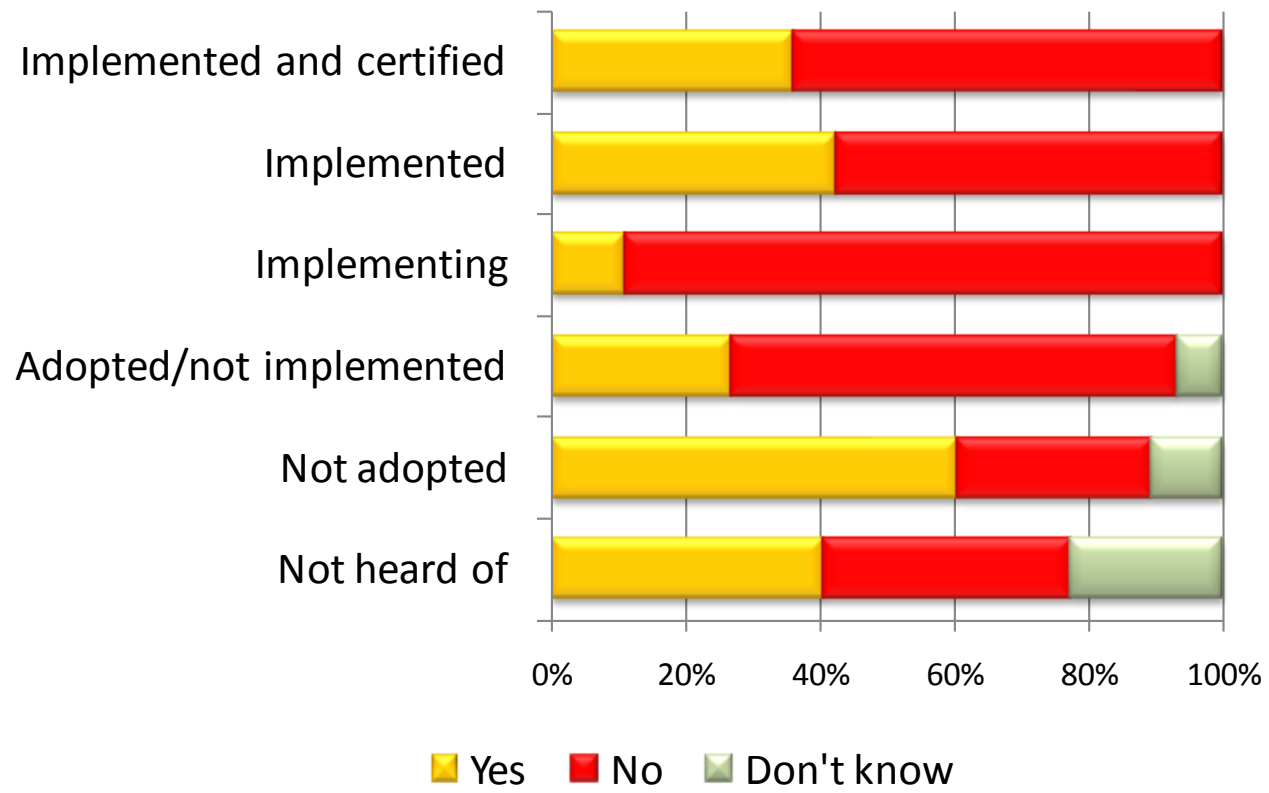
- Account sharing
- The use of default user names and
- The granting of wider access than is necessary
- Ignorance about the existence of privileged user accounts in the first place
- A failure to monitor the actions of users whilst acting under privileged

Do you share admin accounts between different individual privileged users in the following areas?



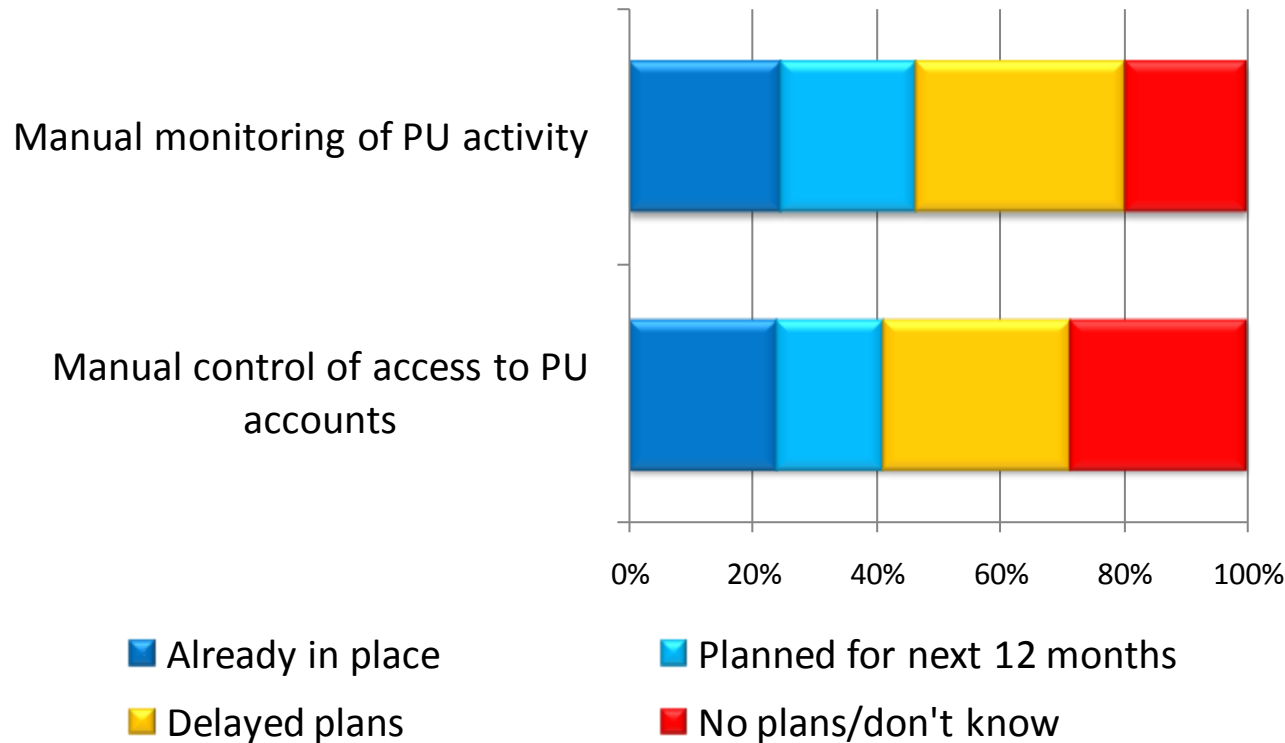
Sharing of privileged user accounts which means the activities of individual privileged users can not be tracked and is direct contravention of ISO27001 and other regulations such as PCI/DSS or national government regulations on data privacy (like Garante Privacy in Italy)

ISO27001 Status



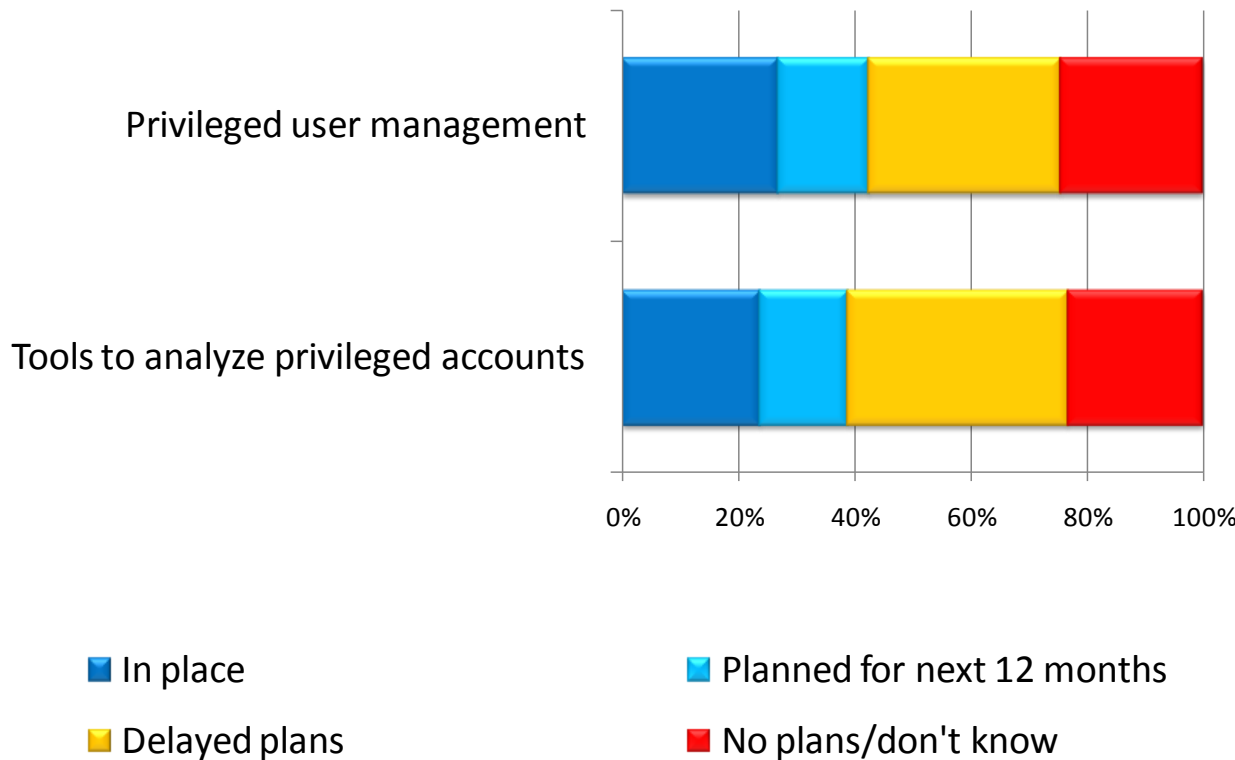
Even those that claim to have implemented ISO27001 are widely indulging in such bad practice

Do you use manual methods to manage access for privileged users?



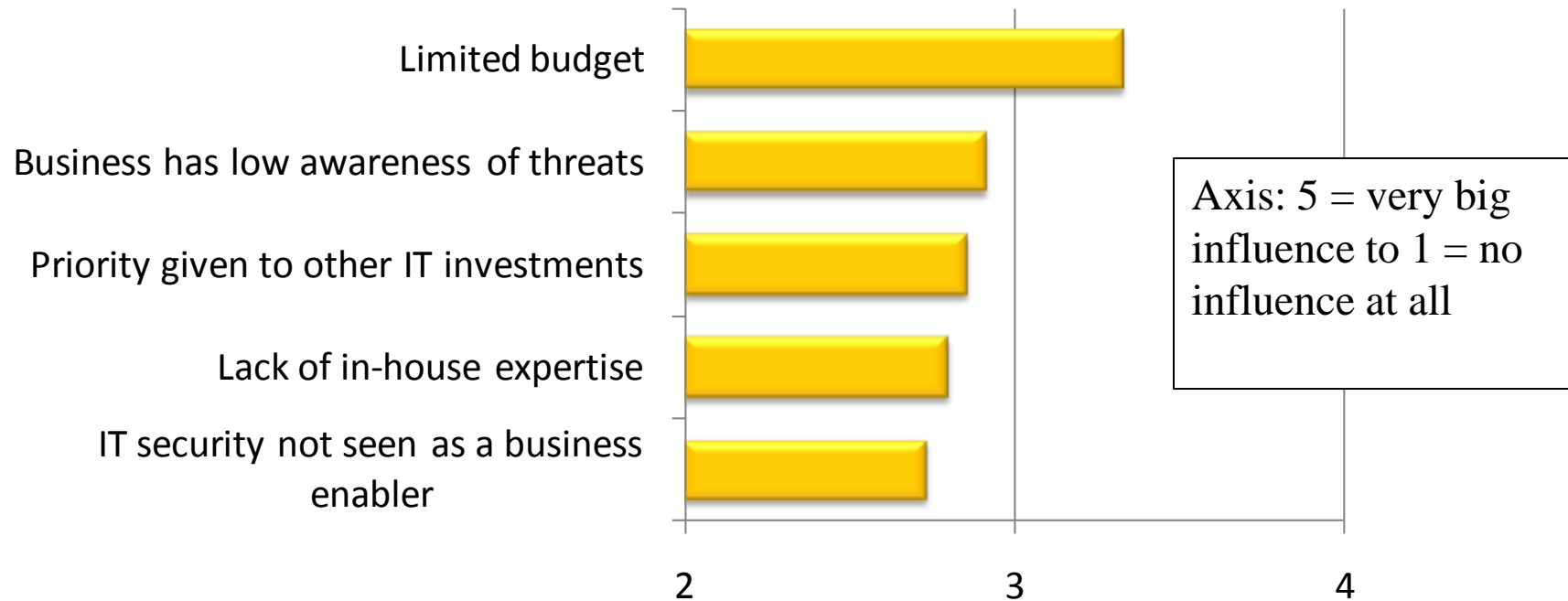
Only around 20% of organisations have manual controls in place for the management of privileged users, this includes practices such as providing one off passwords using paper based systems and does not allow for the monitoring and auditing required by regulators

Do you use any of the following types of tools for managed privileged users?



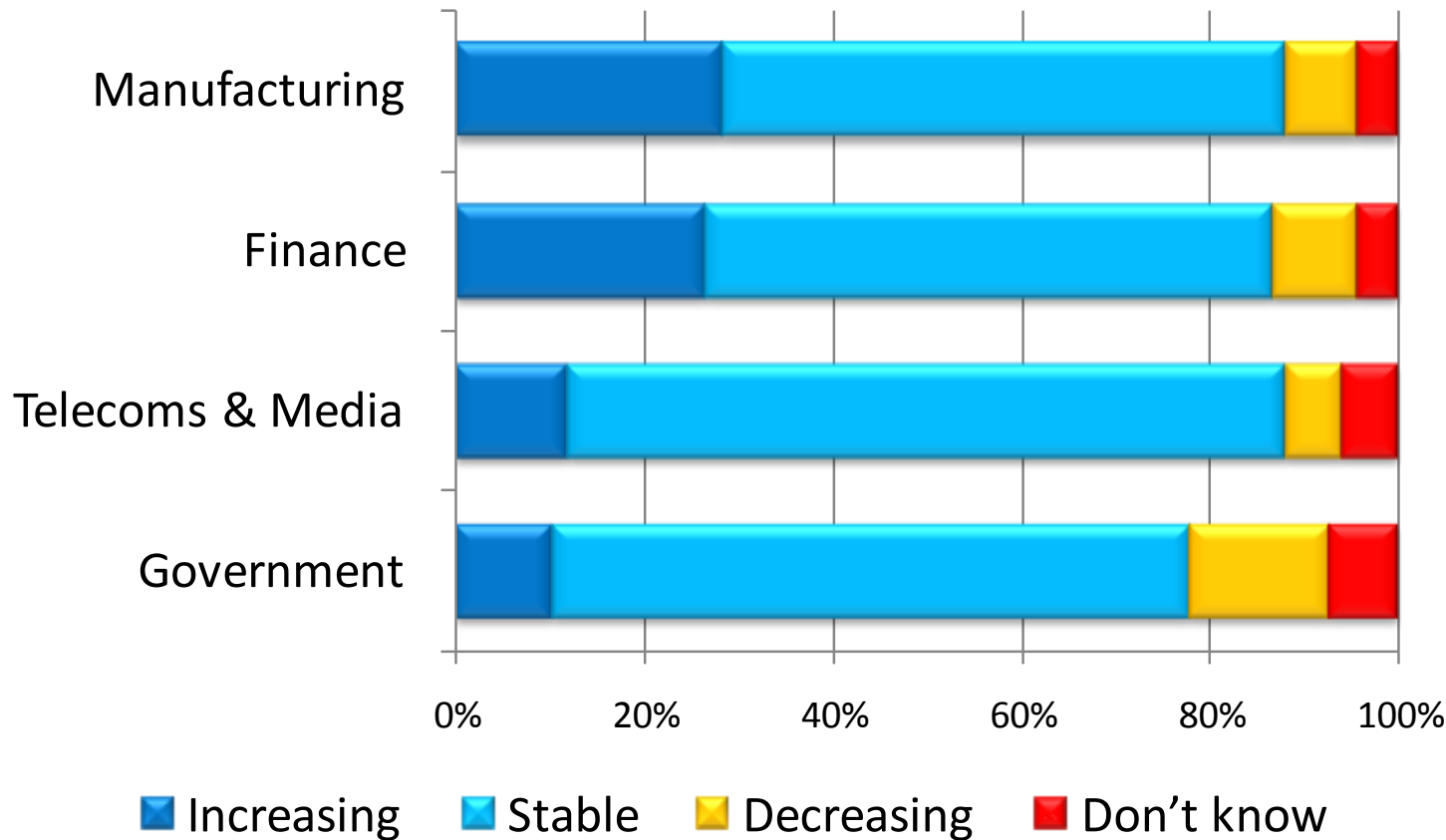
A similar percentage have put in place tools to manage and control privileged users, it is only the use of these tools that can fully satisfy the requirements of regulators and protect business from the potentially harmful actions of privileged user, whether accidental or malicious

How influential are the following factors in limiting investment in security?



One factor limiting investment is lack of budget, but another is lack of awareness of the threat – when it comes to privileged user which requires IT managers to police themselves it is all too easy to focus on other priorities and business managers will be much more aware of other high profiles risks such as malware and data loss via “normal users”

Is the proportion of your org's total IT budget is spent on IT security increasing or decreasing?



But, generally speaking IT security spending is not being compromised, despite the downturn, suggesting that if the awareness around a given threat is high enough, funds will be made available

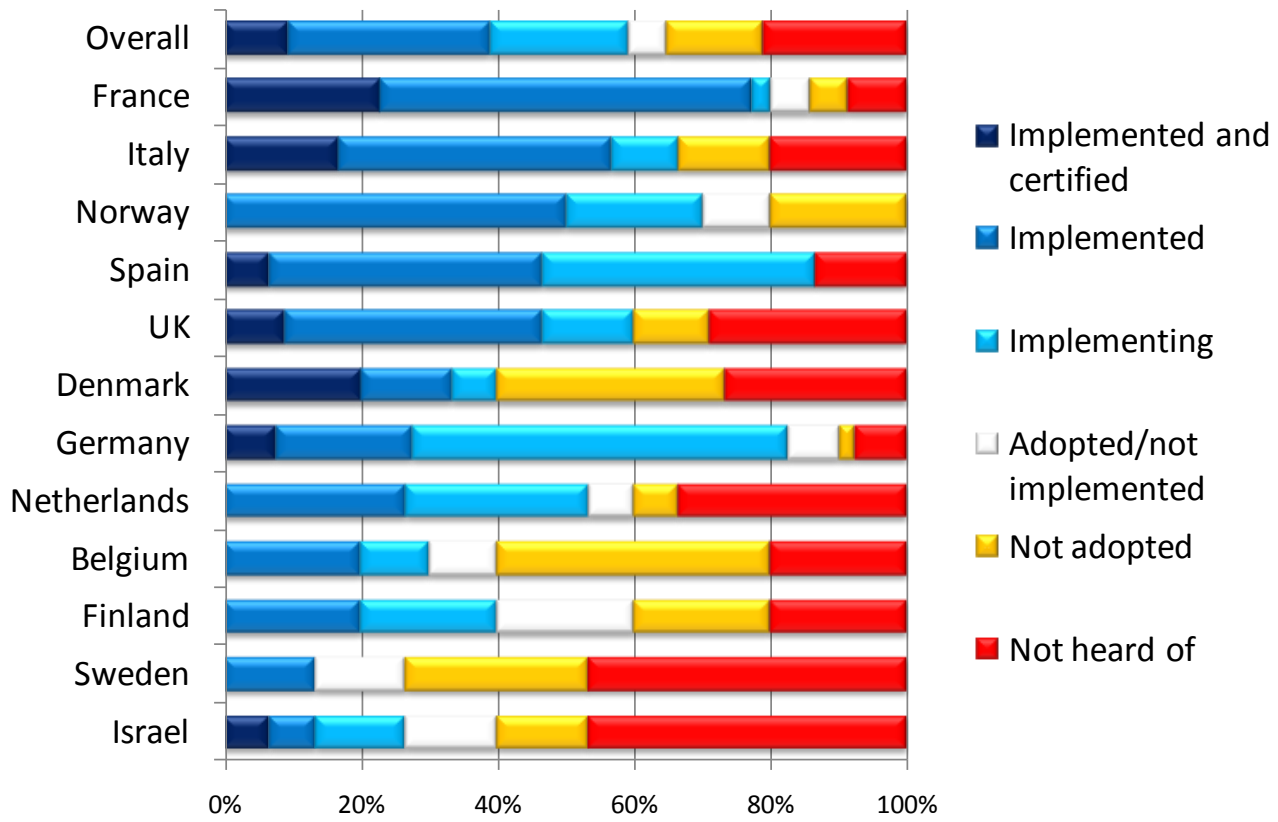
- It is in the interest of individual IT managers, the IT department as whole and the overall business to have measures in place to control and monitor privileged users
- Manual processes are ineffective and do not provide an audit trail that would satisfy regulators
- The one way to ensure this is to put in place tools that fully automate the management of privileged user accounts, the assignment of privileged user access and enable the full monitoring of their activities

Country level data

The following slides highlight some of the geographic variations in the data

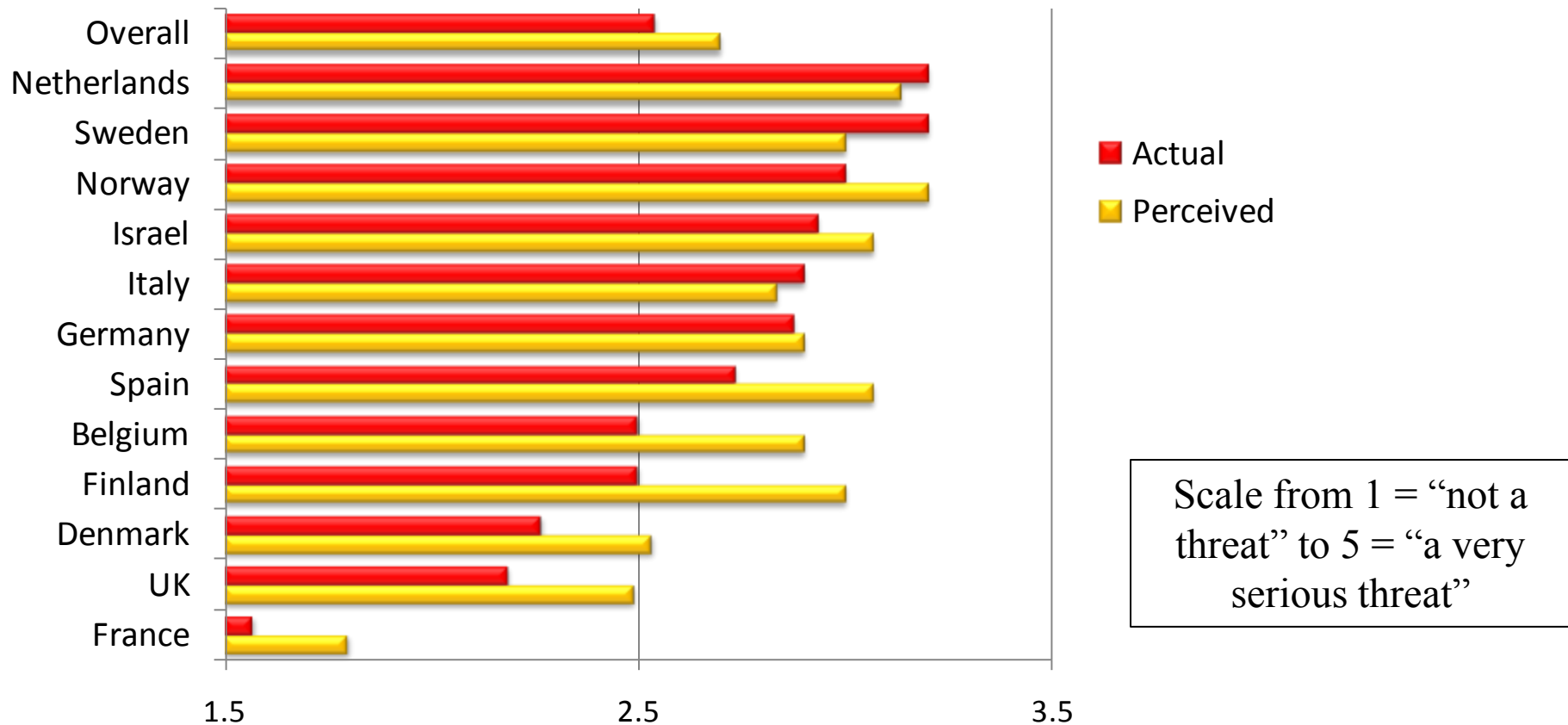
Note: the small sample sizes for all countries, with the exception of UK, Germany, France and Italy, are too small to draw anything but possible pointers for further research (see slide 3 for more details)

Deployment of ISO27001 by country



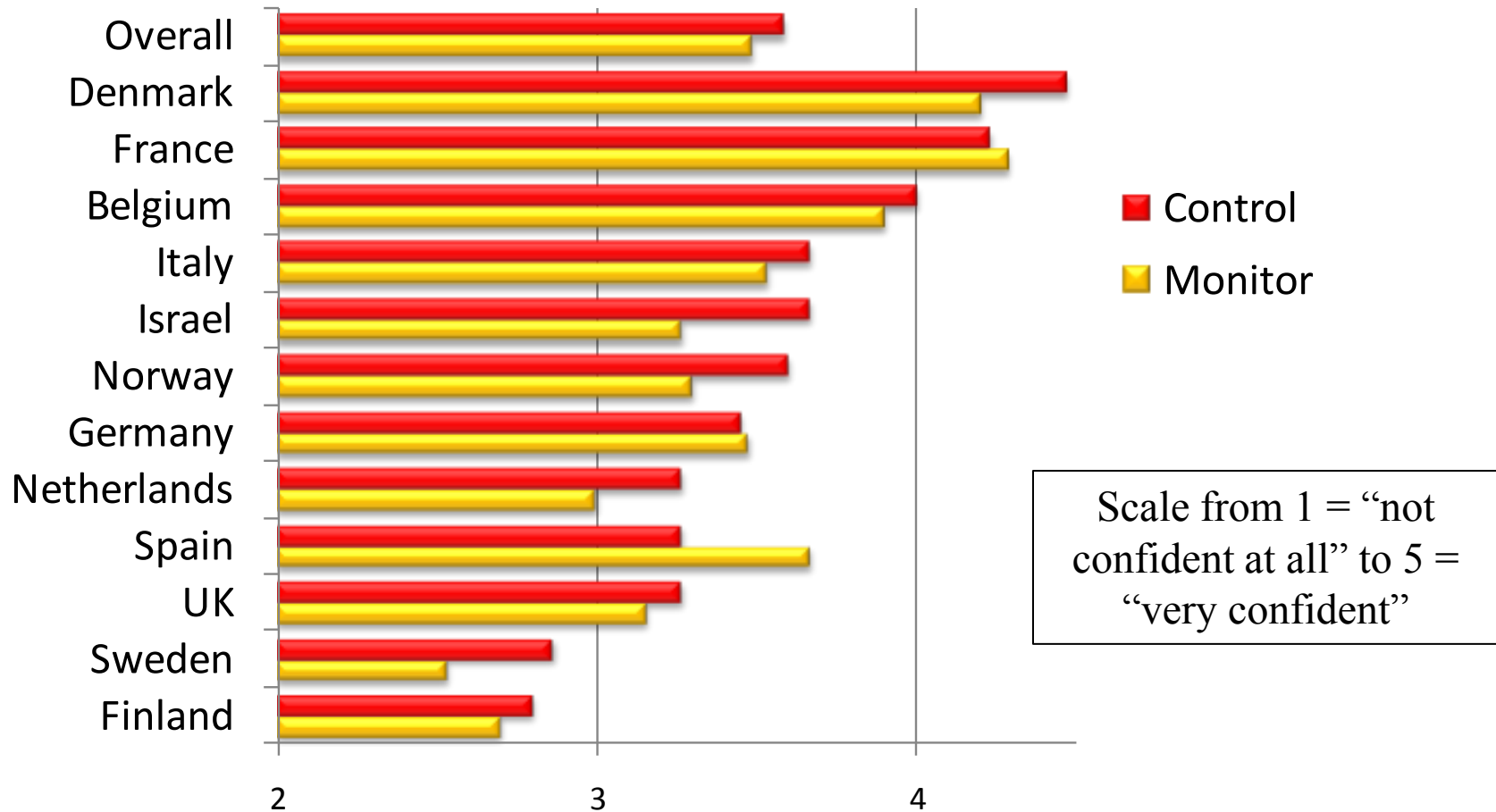
Deployment of ISO27001 varied widely. The data for France contained more interviews with IT security heads than the other samples, so there may be awareness, or even defensive, issue here, with people in such roles having more insight in to regulatory compliance or not wanting to admit to be overlooking it.

To what extent are privileged users a threat to IT security in your organisation?



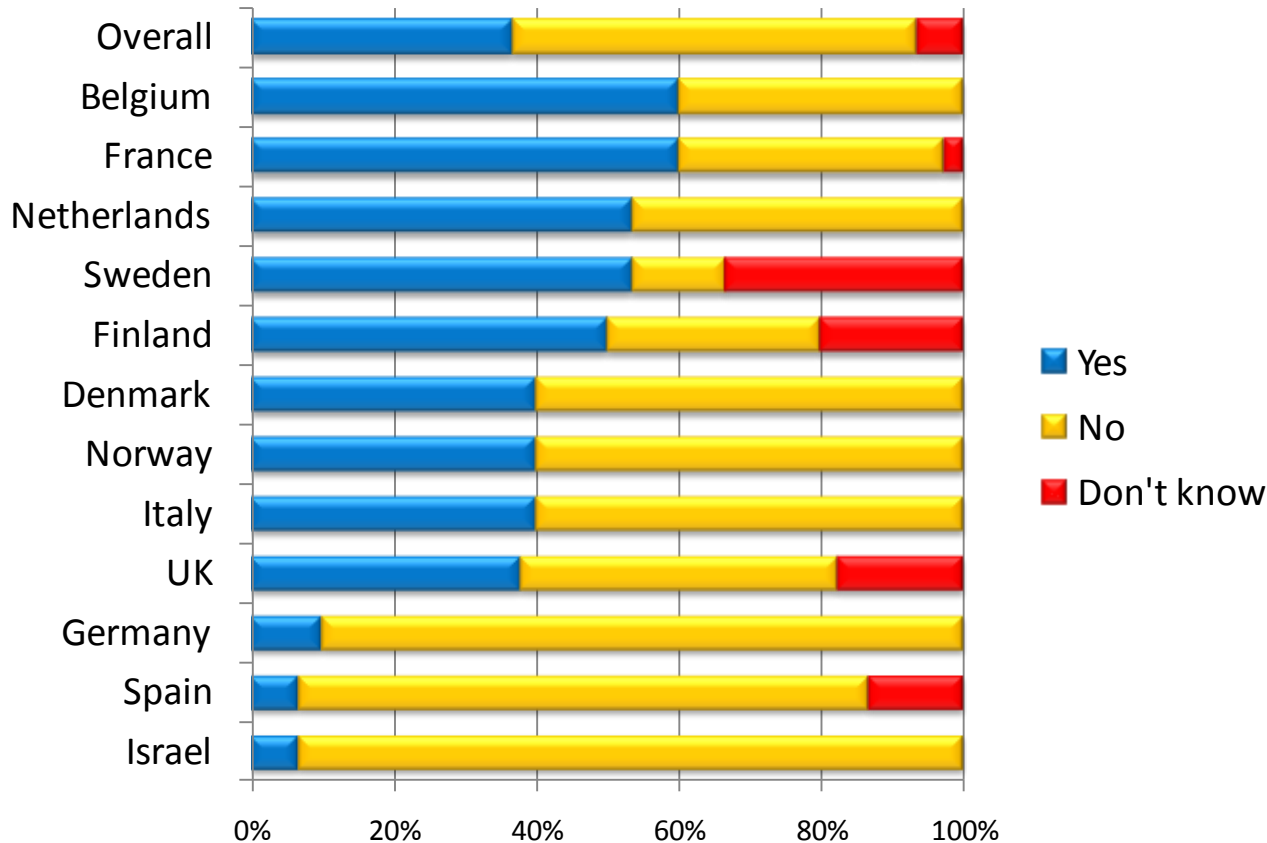
The recognised threat with regard to privileged users is roughly the inverse of ISO271001 deployment, suggesting that deployment does lead to better practice

How confident are you that you are able to control and monitor privileged user accounts at the OS level?



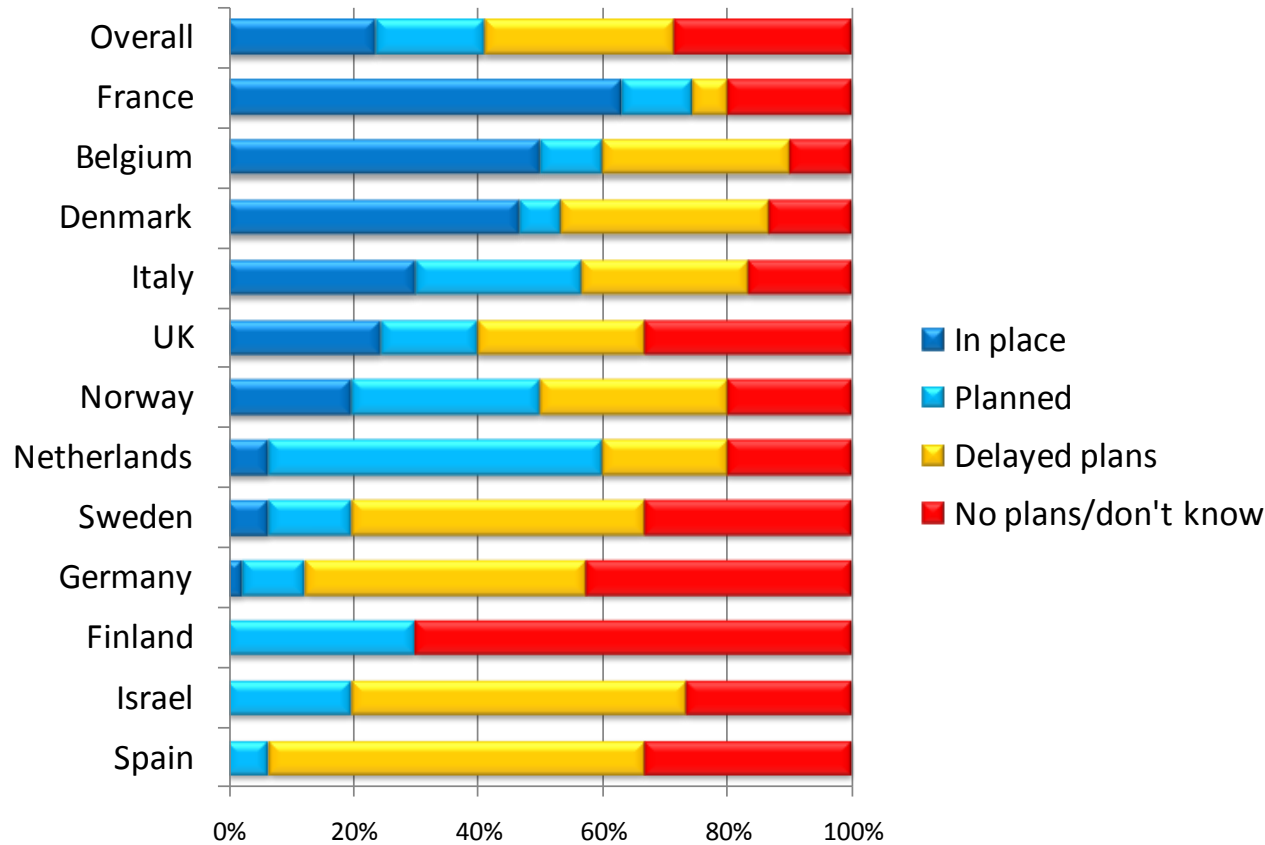
The confidence in being able to control them, is also roughly the inverse of ISO271001 deployment.

Do you share administrator accounts between different individual privileged users at the operating system level?



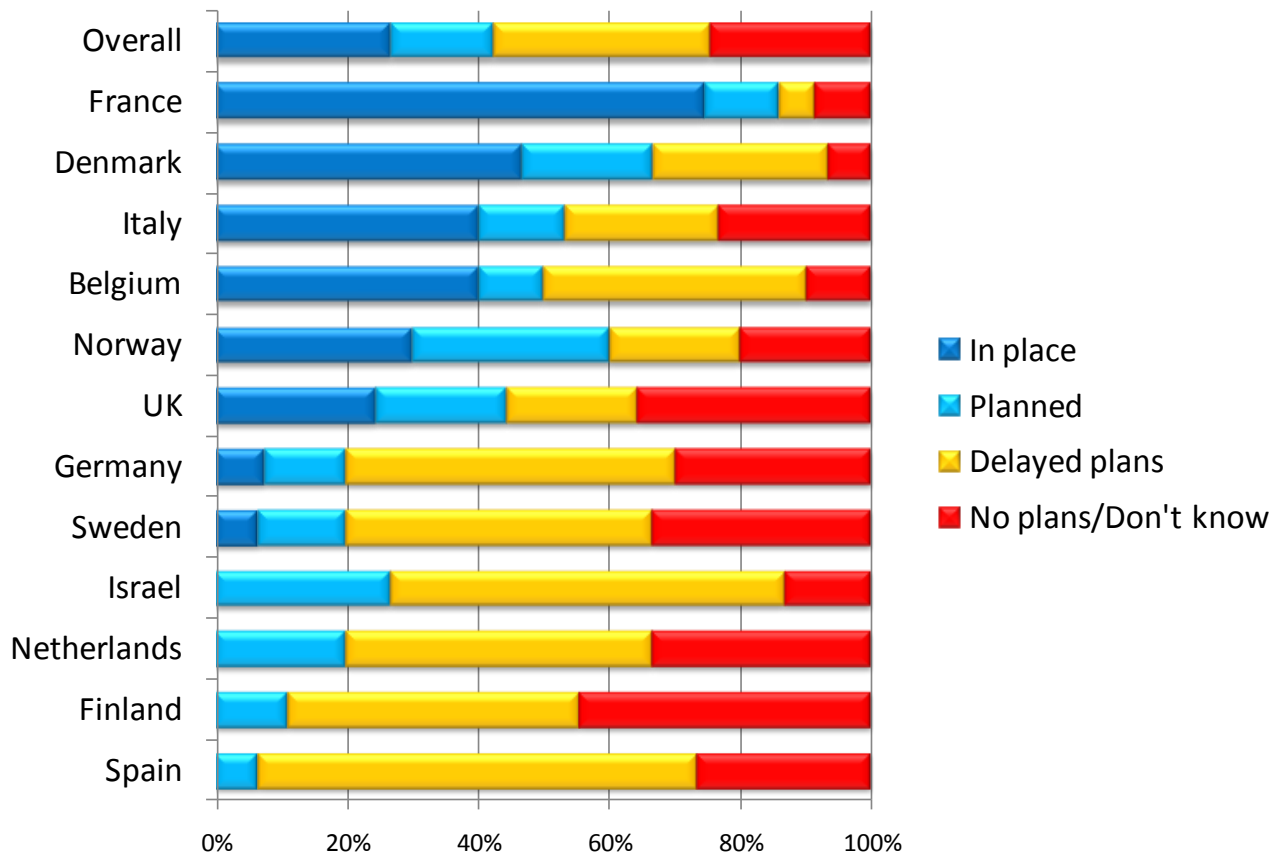
The bad practices exposed by this report should not be forgotten. There is little correlation with ISO27001 deployment and bad practices like account sharing. This suggests that the confidence conferred by the standard is general rather than specific.

Do you use manual methods to control access for privileged users?



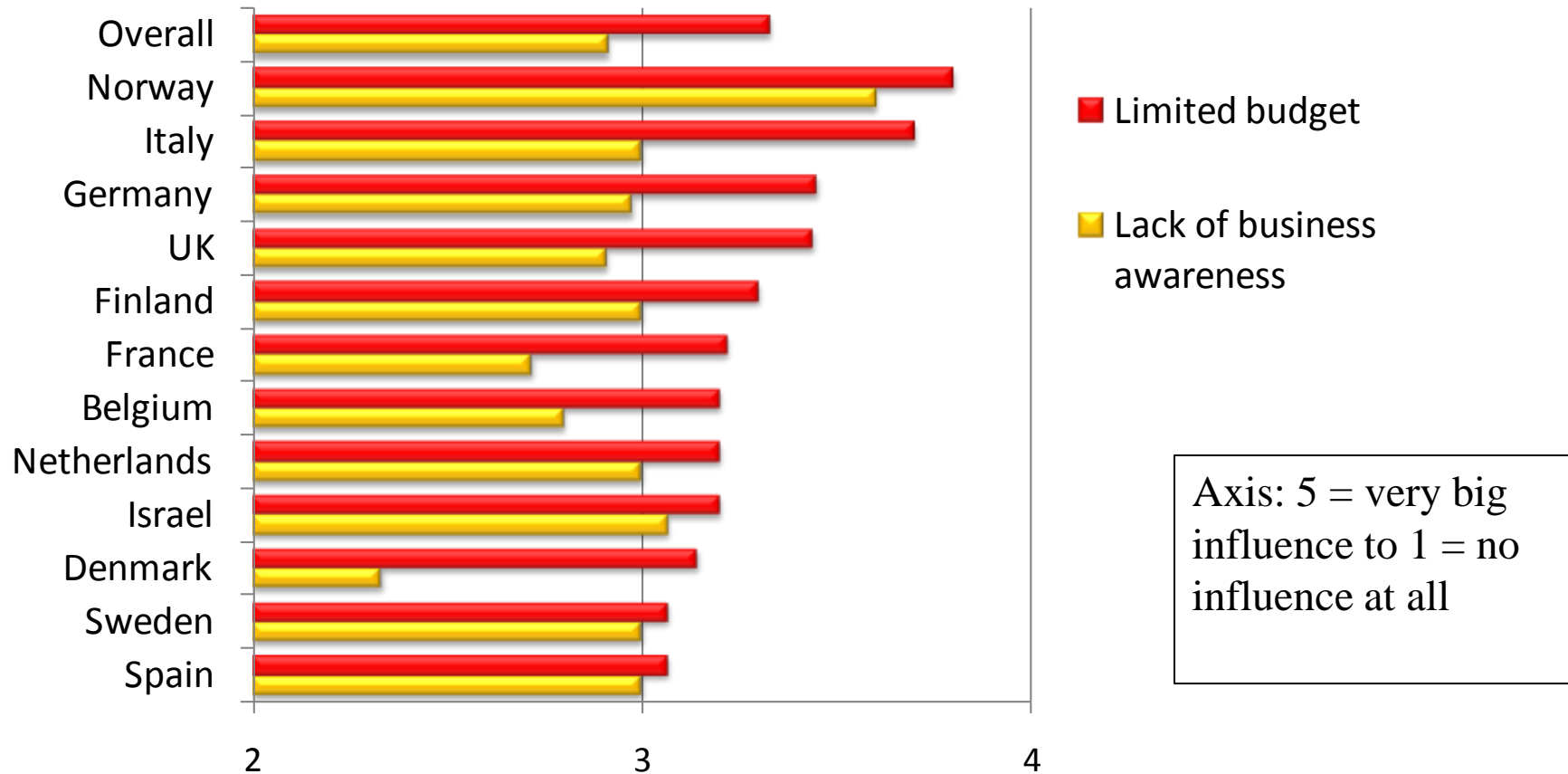
There is a rough correlation with confidence to control privileged and the use manual processes for PUM. Whilst this is a good finding, as it shows there is a payback for taking action, the benefits conferred through using and automated tools should not be forgotten.

Do you use privileged user management tools?



There is also a rough correlation with confidence to control privileged and the use of full PUM tools; an endorsement of their use.

How influential are the following factors in limiting investment in security?



Budget is always an issue, but remember, overall investment in IT security is being maintained at least as a proportion of overall IT spend. Business awareness is the next most prominent issue.

- The contacts for this project are:
 - Bob Tarzey
 - Service Director, Quocirca
 - Bob.Tarzey@Quocirca.com
 - +44 7900 275517

 - Mariateresa Faregna
 - Public Relations Manager, CA
 - Mariateresa.Faregna@ca.com
 - +39 02 90464739