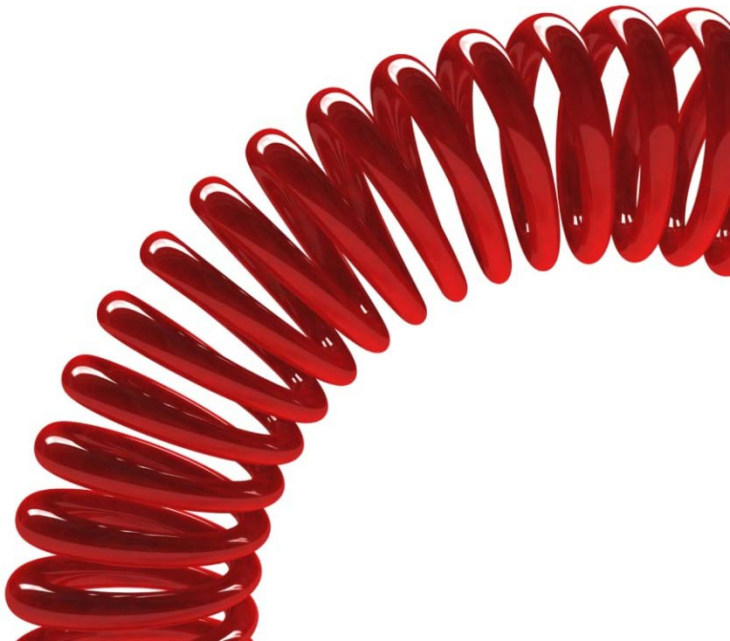
Deloitte.

2010 Global TMT Security Study

Bounce Back

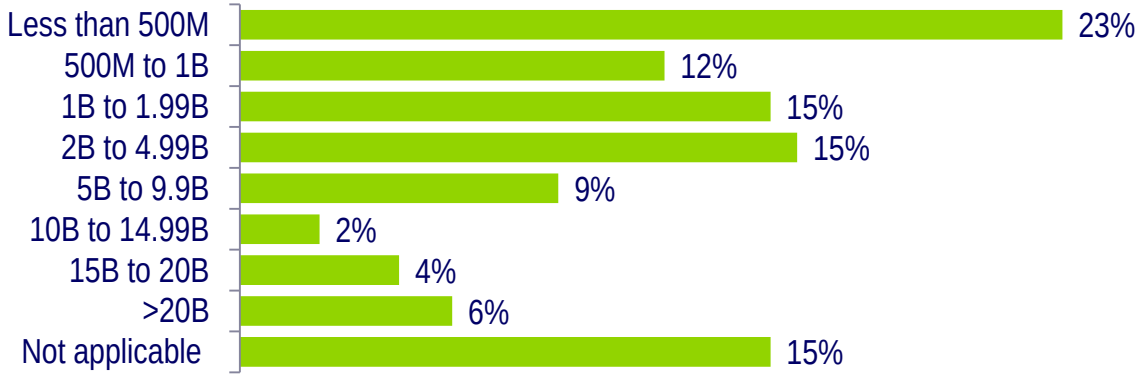


Audit . Tax . Consulting . Financial Advisory .

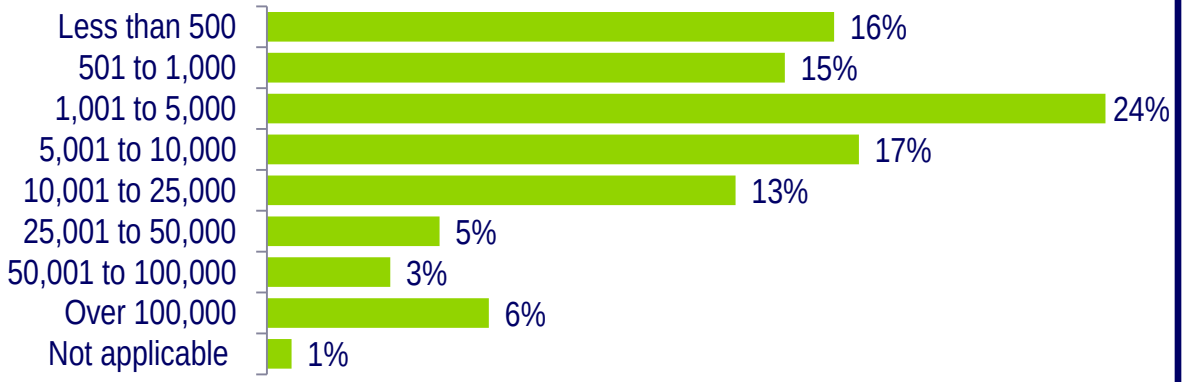
About the Study

Participant profile

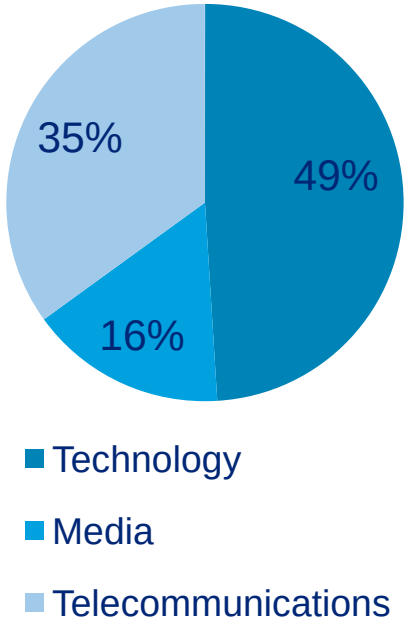
Annual Revenue (USD)



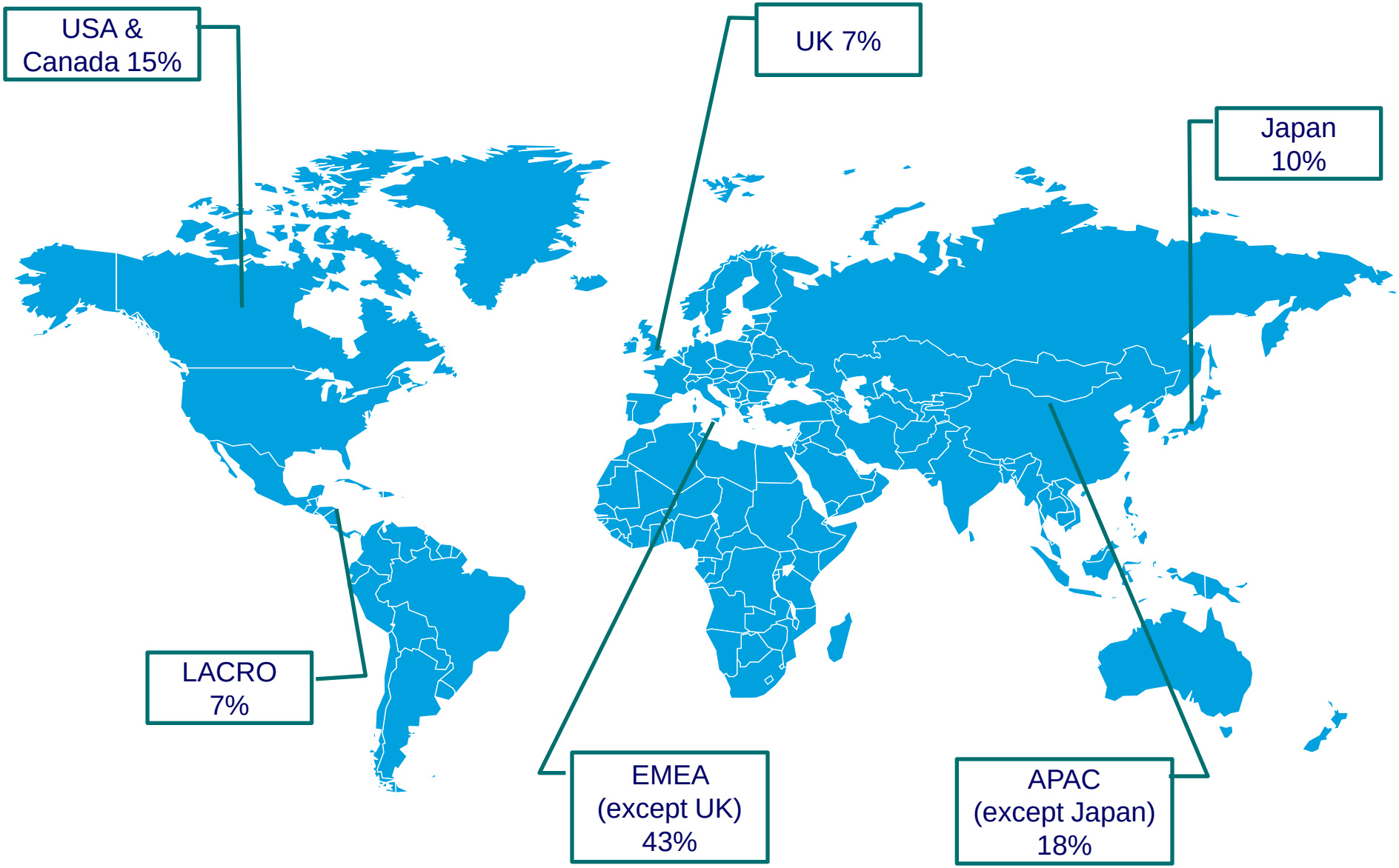
Number of employees



Industry Breakdown



Participants by Region



Key Finding

Bounce Back - Key finding

2. Cloud in the forecast

- Cloud computing could fundamentally change how IT Services are delivered

- Cloud computing may in many scenarios be a more efficient way to deliver and manage IT services

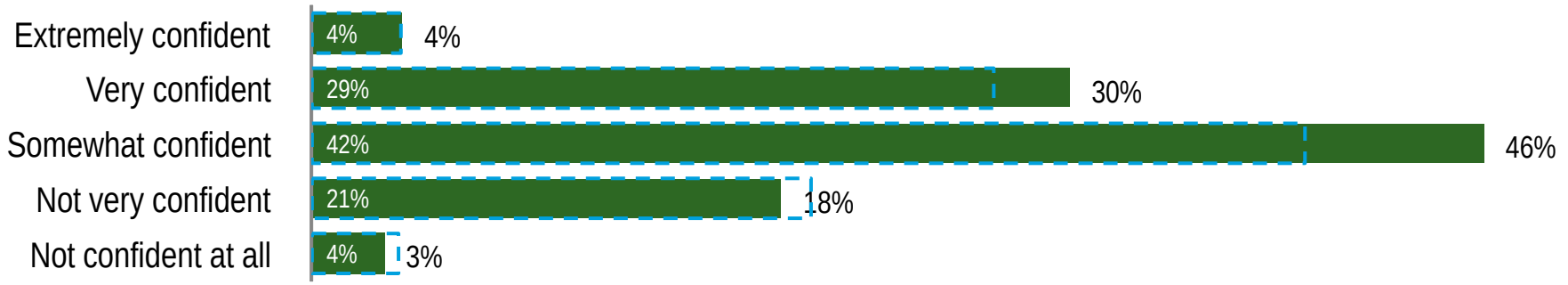
- But TMT organizations must address the security & privacy challenges

Confidence in the level of protection from an external attack

62% of respondents believe that their organizations are well protected against external attacks involving information systems. Another 31% is only somewhat confident.

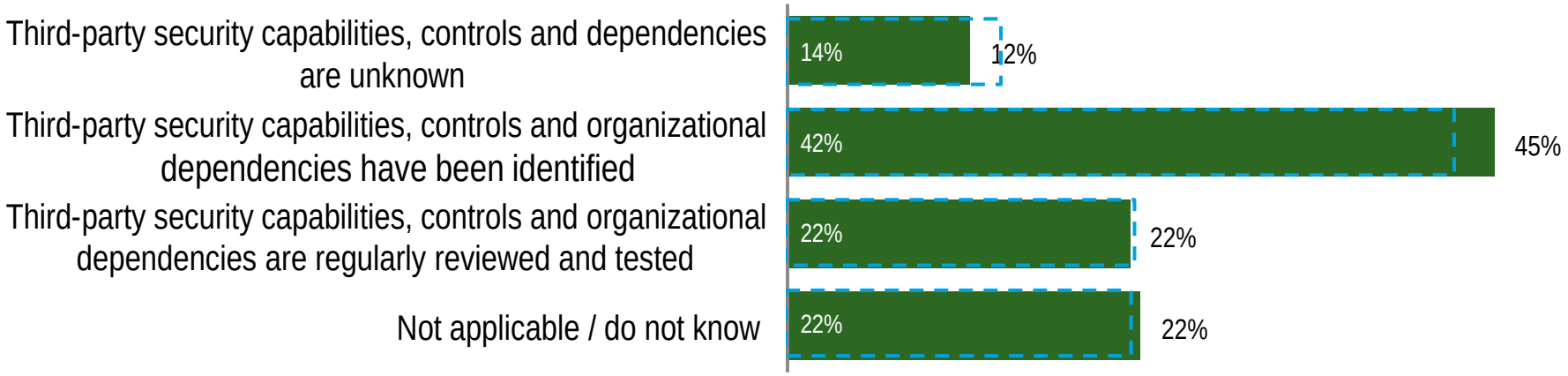
Confidence in the level of protection from an internal attack

34% of respondents believe that their organization is protected against internal attacks involving information systems. Another 46% are somewhat confident, indicating that attacks originating internally are still a concern for organizations.



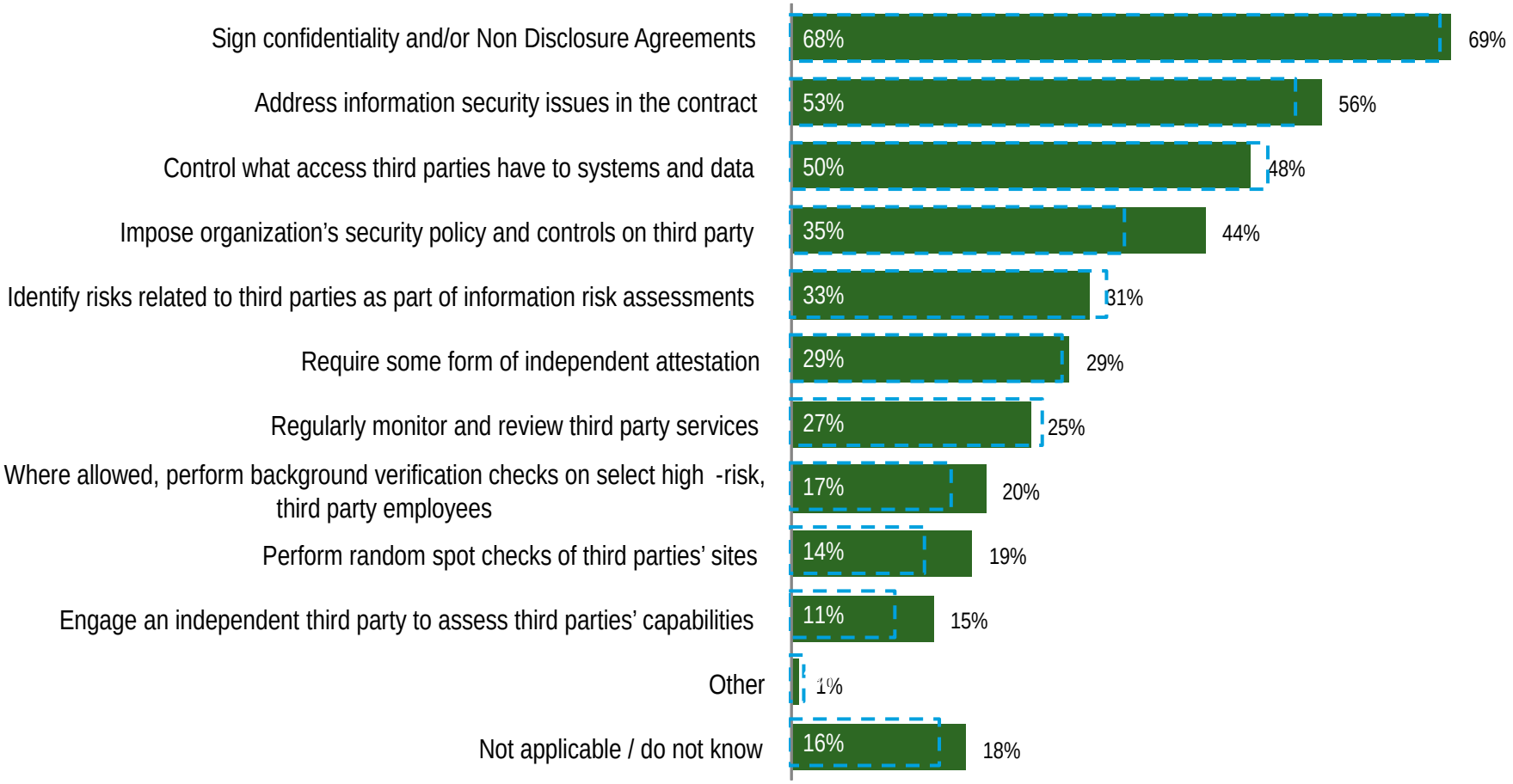
Dealing with third-party capabilities and dependencies

Third-party capabilities and dependencies should be reviewed and tested periodically to ensure these extended business relationships are delivering as promised. Yet only 22% of respondents do such reviews and testing on a regular basis.



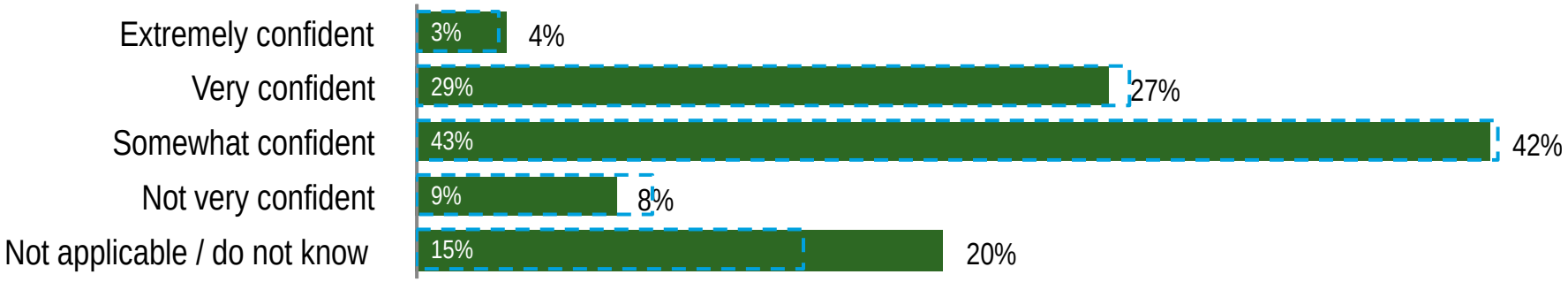
Ensuring that security practices of third parties are adequate

The top three methods are “Sign confidentiality / Non-disclosure agreements” (69%), “Address information security issues in the contract” (56%), and “Control what access third parties have to systems and data” (48%) .



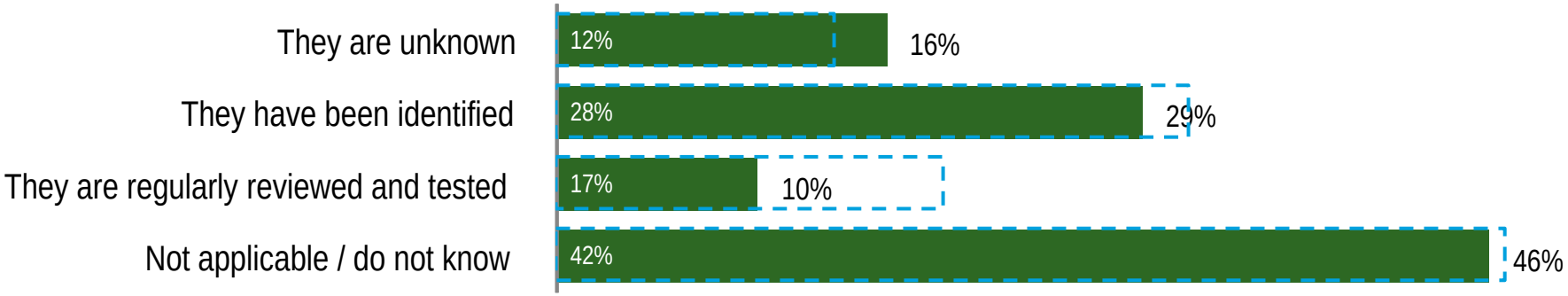
Confidence in third-party security practices

Only 27% of respondents are “Very confident” in their third parties’ information security practices, while 50% of respondents are “Not very confident” or “Somewhat confident.” Only a few technology companies (7%) are “Extremely confident” in their third parties’ security practices.



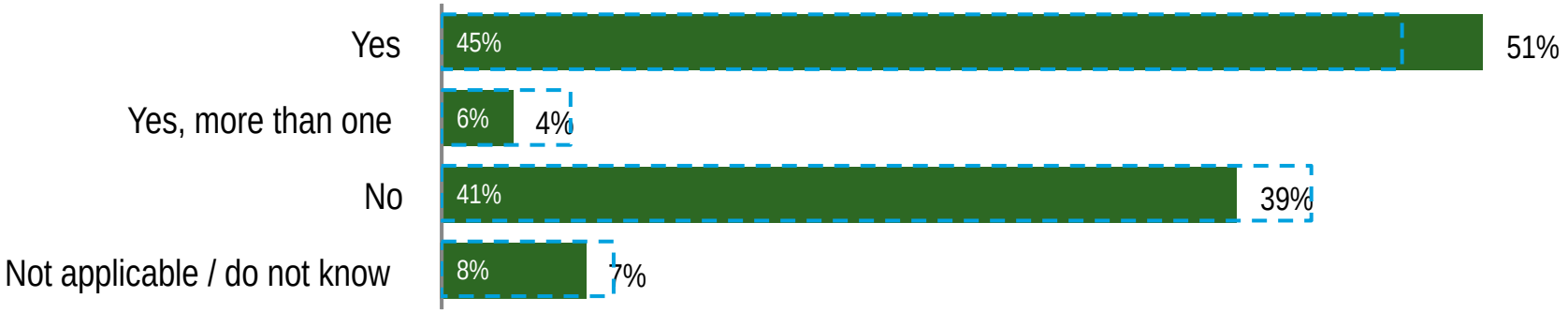
Dealing with third-party business continuity management capabilities, controls, and organizational dependencies

Third-party business continuity management capabilities, controls, and dependencies should be reviewed and tested periodically to ensure these extended business relationships are delivering as promised. Yet only 10% of TMT respondents do such reviews and testing on a regular basis, compared with 17% across all industries.



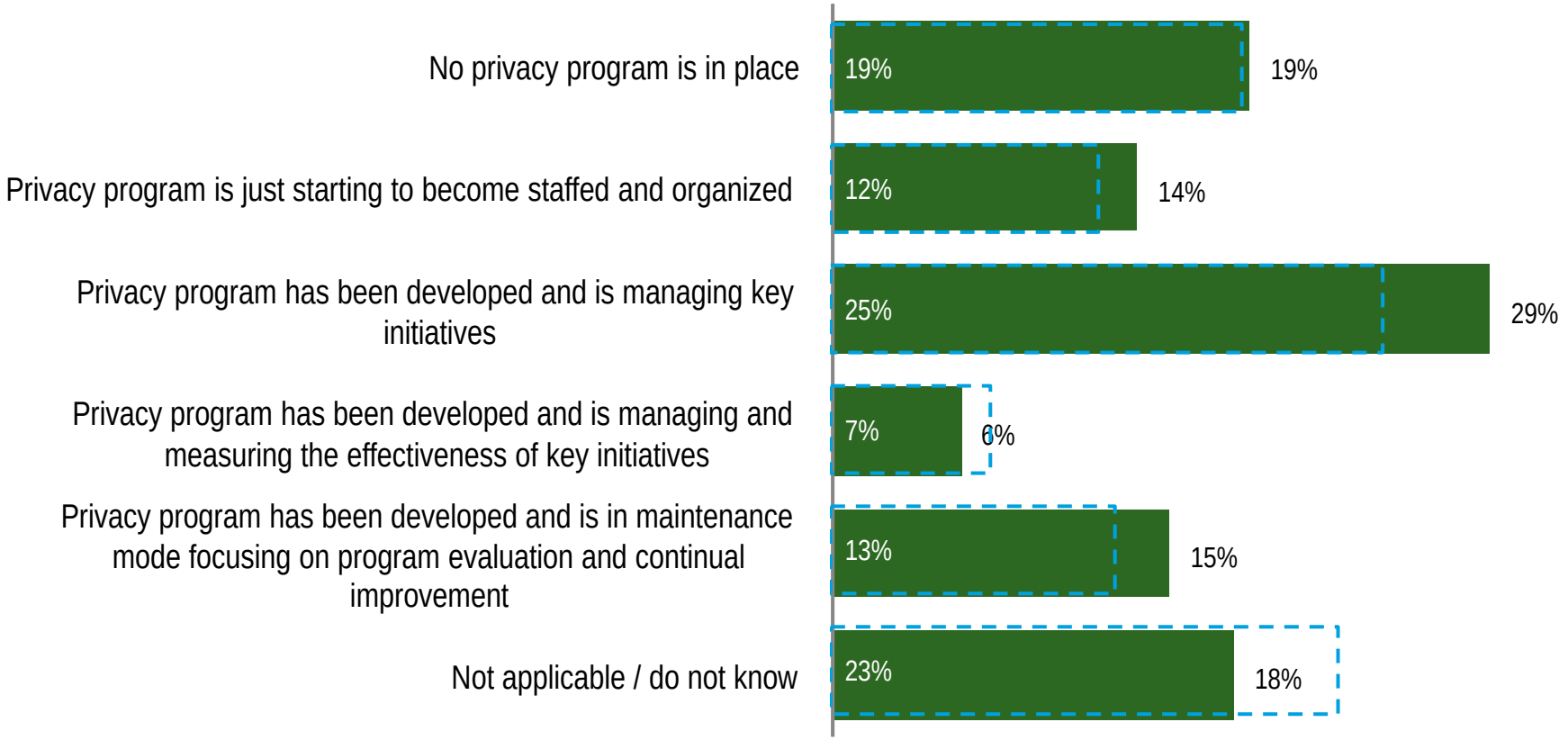
Presence of an executive responsible for privacy

This year's study shows that 51% of the technology, media, and telecommunications companies has appointed an executive responsible for privacy. The technology sub-industry was most likely to have an executive responsible for privacy (56%).

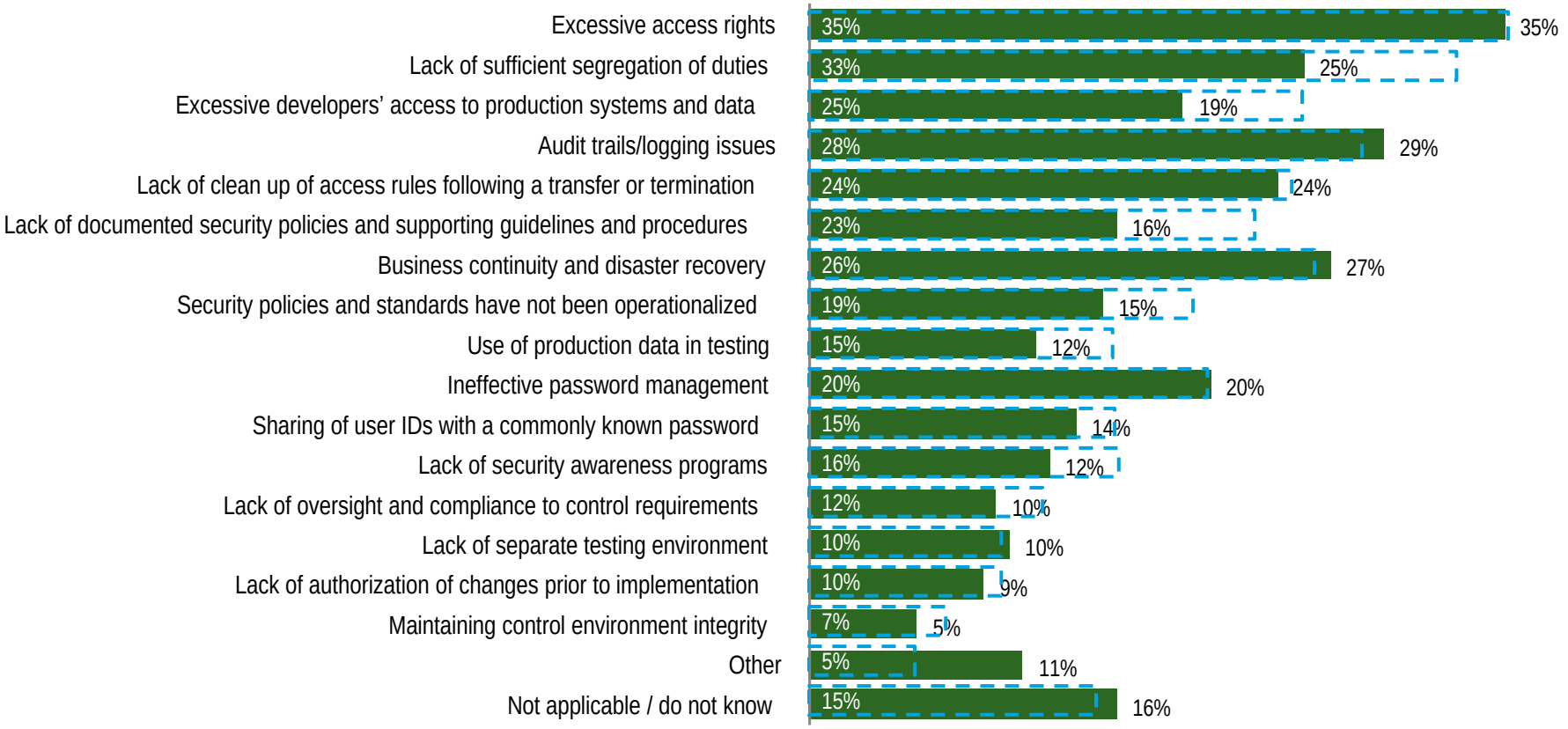


Privacy program maturity

Almost one-fifth of respondents indicated that they have no privacy program in place. Almost one-third however indicate that a privacy program has been developed and is managing key initiatives. The state of privacy programs varies greatly per respondent.



Audit findings



Most common audit findings for TMT industry:

1. Excessive access rights
2. Audit trails/logging issues

Most common audit findings across all industries:

1. Excessive access rights
2. Lack of sufficient segregation of duties

Contacts Details

Contact details

François Vergez: fvergez@deloitte.fr

www.deloitte.fr

Deloitte.