gemalto
security to be free

The 2016 Global Cloud Data Security Study

Independently conducted by Ponemon Institute LLC
Publication Date: July 2016

Contents Page

Introduction

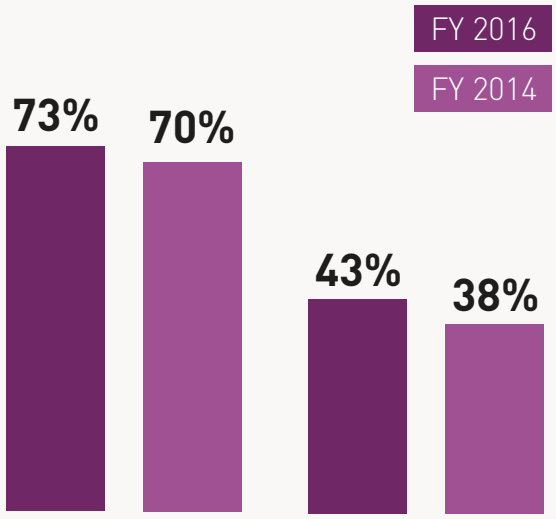
We are pleased to present the findings of The 2016 Global Cloud Data Security Study sponsored by Gemalto. The purpose of this research is to understand trends in cloud governance and security practices since the study was first conducted in 2014.

We surveyed 3,476 IT and IT security practitioners in the United States, United Kingdom, Australia, Germany, France, Japan, Russian Federation, India and Brazil who are familiar and involved in their company's use of both public and private cloud resources. Seventy-three percent of respondents say their organizations are heavy (25 percent) or moderate (48 percent) users of cloud resources.

Participants in this study estimate that cloud use will increase over the next two years. Today respondents estimate that 36 percent of their organizations' total IT and data processing requirements are met using cloud resources. This is expected to increase to an average of 45 percent of IT and data processing requirements in the next two years. However, the findings reveal that organizations have difficulty managing the risk without applying the correct governance and security practices. Since 2014, there has been little change in the belief that management of privacy and data protection regulations are more complex in the cloud than on-premises, as shown in Figure 1. On a positive note, slightly more respondents in this year's study say their organizations have established clearly defined roles and accountability for safeguarding confidential or sensitive information stored in the cloud.

Figure 1. Perceptions about cloud governance

(Strongly agree and agree responses combined)



The following are trends in cloud governance and security:

Cloud usage continues to grow in importance without the support of necessary governance practices. Cloud computing applications and platform solutions are considered very important or important to their organizations' operations, according to 73 percent of respondents. Eighty-one percent of respondents say cloud solutions will become very important or important over the next two years. The use of cloud computing resources for total IT and data processing requirements is expected to increase from an average of 36 percent to an average of 45 percent in the next two years.

More consumer data is stored in the cloud and is the data most at risk. Since 2014, the storage of customer information has increased significantly from 53 percent of respondents to 62 percent of respondents. While more customer information is moving to the cloud, it is also considered the information most at risk in the cloud.

Confidence in knowing all cloud computing services in use is increasing. Fifty-four percent of respondents are either very confident (24 percent) or confident (30 percent) that the IT organization knows all cloud computing applications, platform or infrastructure services in use today. This is an increase from 45 percent of respondents in the previous study.

The difficulty in protecting confidential or sensitive information when using cloud services has decreased slightly. In the previous study, 60 percent of respondents said it is more difficult to protect confidential or sensitive information when using cloud services. This year, the percentage has decreased to 54 percent of respondents. However, organizations still face challenges in the protection of confidential information when using cloud services. The difficulty in controlling or restricting end-user access has increased from 48 percent of respondents to 53 percent of respondents.

Responsibility for cloud security is moving to the cloud user. Fewer respondents (31 percent of respondents) say cloud security is a shared responsibility between the cloud provider and user. More respondents (36 percent) say the cloud user should be responsible for cloud security, an increase from 33 percent of respondents in the previous study.

Efficiency and cost are the most important factors for selecting a cloud provider. The primary reasons for selecting a particular cloud provider are efficiency (41 percent of respondents) or cost (37 percent). However, more respondents say security is a consideration when selecting a cloud provider (22 percent vs. 15 percent in the previous study).

Evaluation of cloud provider security is shifting to the end-user. Sixty percent of respondents say their organizations evaluate the security capabilities of cloud providers prior to engagement or deployment. More respondents believe the end-user is responsible for security evaluations (30 percent vs. 25 percent of respondents in the previous study).

Security evaluations of cloud providers rely increasingly on contractual negotiations and legal reviews. This year's research reveals a significant increase in the use of contractual negotiation and legal reviews to evaluate cloud providers from 51 percent to 62 percent of respondents. Fewer organizations look at proof of security compliance (42 percent), a selfassessment security questionnaire (34 percent) and an assessment by in-house security team (25 percent). Similar to the previous study, only 19 percent of respondents say their organizations conduct a third-party assessment by security expert or auditor.

The inability to control end-users is resulting in more cloud resources deployed without evaluation. Increasingly, it is the loss of control over end-users that results in cloud resources deployed without security scrutiny. Other reasons are not enough resources to conduct an evaluation (58 percent of respondents) and increasingly that no one is in-charge (41 percent vs. 35 percent in the previous study).

Encryption in the cloud is increasing. Seventy-two percent of respondents say the ability to encrypt or tokenize sensitive or confidential data is important, and 86 percent say it will become more important over the next two years, an increase from 79 percent in the previous study. More respondents than in the previous study say their organizations use encryption, tokenization or other cryptographic solutions to secure sensitive or confidential information at rest (36 percent vs. 42 percent of respondents in 2016).

Strong authentication measures continue to be important. Sixty-seven percent of respondents say the management of user identities is more difficult in the cloud than the onpremise environment. However, organizations are not adopting measures that are easy to implement and could increase cloud security. Since 2014, the ability to control strong authentication prior to accessing data and applications in the cloud increased from 73 percent of respondents to 78 percent of respondents.

Key Findings

In this section we provide an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. The report is organized according to the following topics:

- As the cloud's popularity grows, so does the risk to sensitive data
- Cloud security is stormy because of Shadow IT
- Data security governance practices ignore the security practitioners
- Protection of data in the cloud is important but not practiced
- Cloud complicates identity and access management

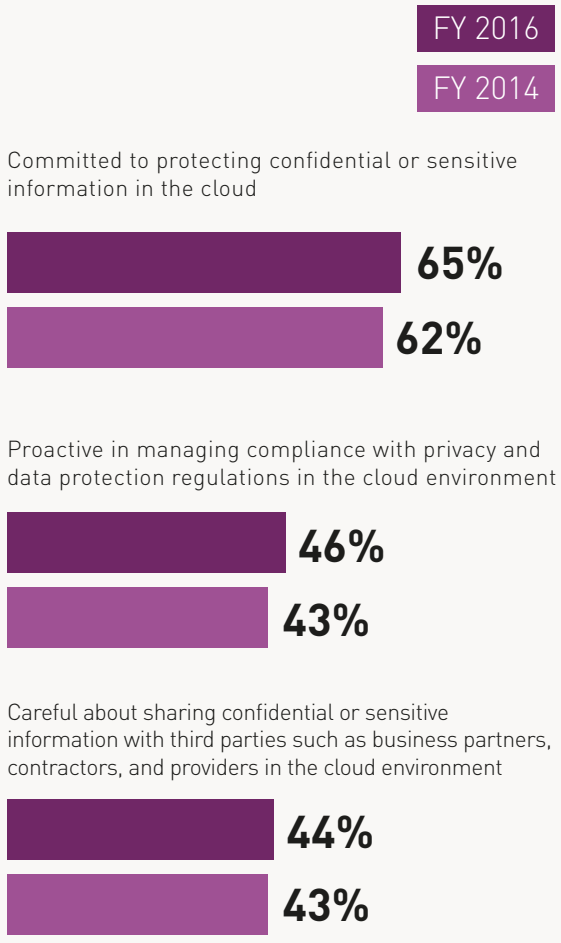
As the cloud's popularity grows, so does the risk to sensitive data

Cloud usage continues to grow in importance without the support of necessary governance practices. Cloud computing applications and platform solutions are considered very important or important to their organizations' operations, according to 73 percent of respondents. Eighty-one percent of respondents say cloud solutions will become very important or important over the next two years. The use of cloud computing resources for total IT and data processing requirements is expected to increase from an average of 36 percent to an average of 45 percent in the next two years.

Does the growth and importance of the cloud mean there is an increase in policies and procedures to safeguard data? Despite the finding that 65 percent of respondents say their organizations are committed to protecting confidential or sensitive information in the cloud, Figure 2 reveals that similar to the 2014 study, 54 percent of respondents (100 minus 46 percent) do not agree their organizations have a proactive approach to managing compliance with privacy and data protection regulations in the cloud environment. Fifty-six percent of respondents (100 minus 44 percent) do not agree that their organization is careful about sharing sensitive information with third parties such as business partners, contractors and providers in cloud environments.

Figure 2. Perceptions about governance practices in the cloud

(Strongly agree and agree responses combined)

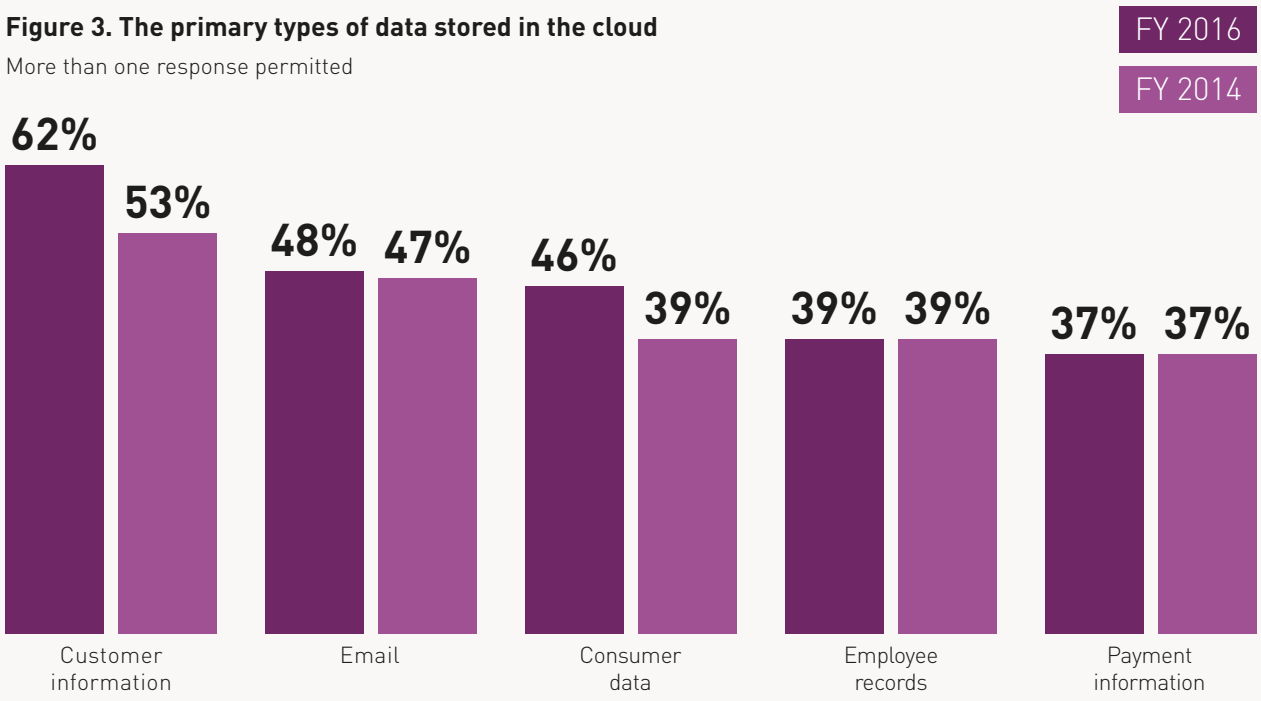


The type of corporate data stored in the cloud is also the data most at risk.

As shown in Figure 3, customer information, emails, consumer data, employee records and payment information are most often stored in the cloud. Since 2014, the storage of customer information has increased significantly from 53 percent of respondents to 62 percent of respondents.

Figure 3. The primary types of data stored in the cloud

More than one response permitted

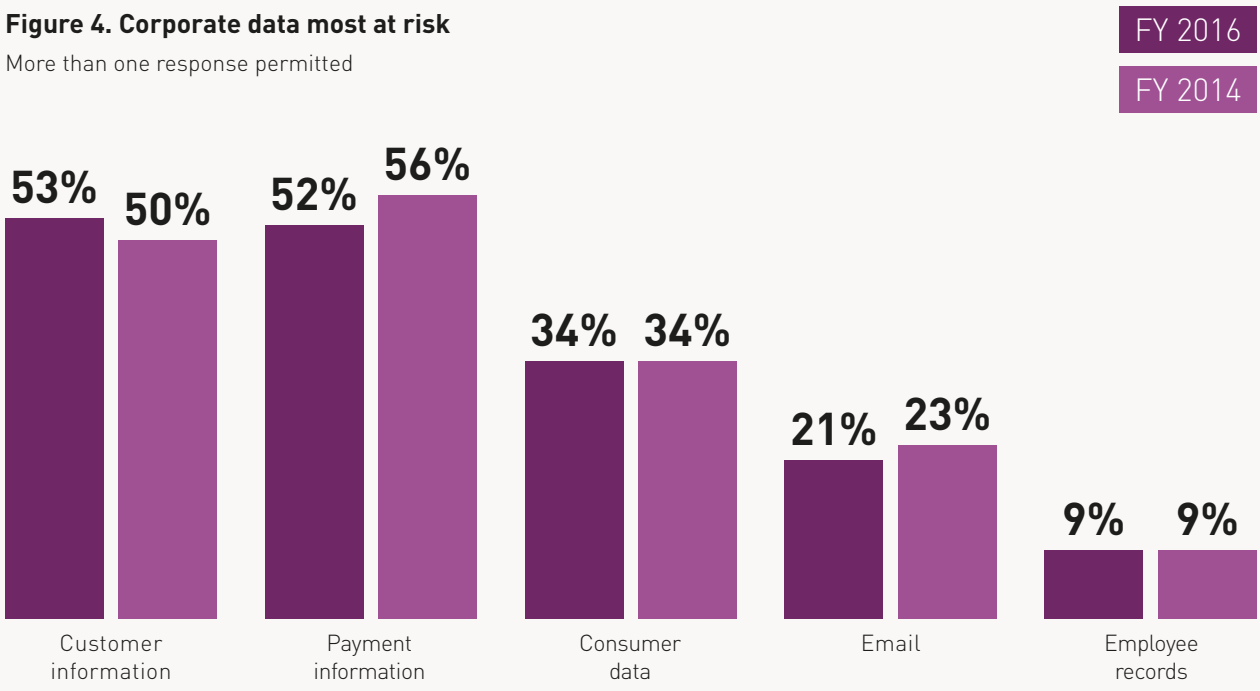


The type of corporate data stored in the cloud is also the data most at risk.

While more customer information is moving to the cloud, it is also considered the information most at risk in the cloud, as revealed in Figure 4. Perceptions that payment information is at risk in the cloud have decreased from 56 percent of respondents in the previous study to 52 percent of respondents.

Figure 4. Corporate data most at risk

More than one response permitted

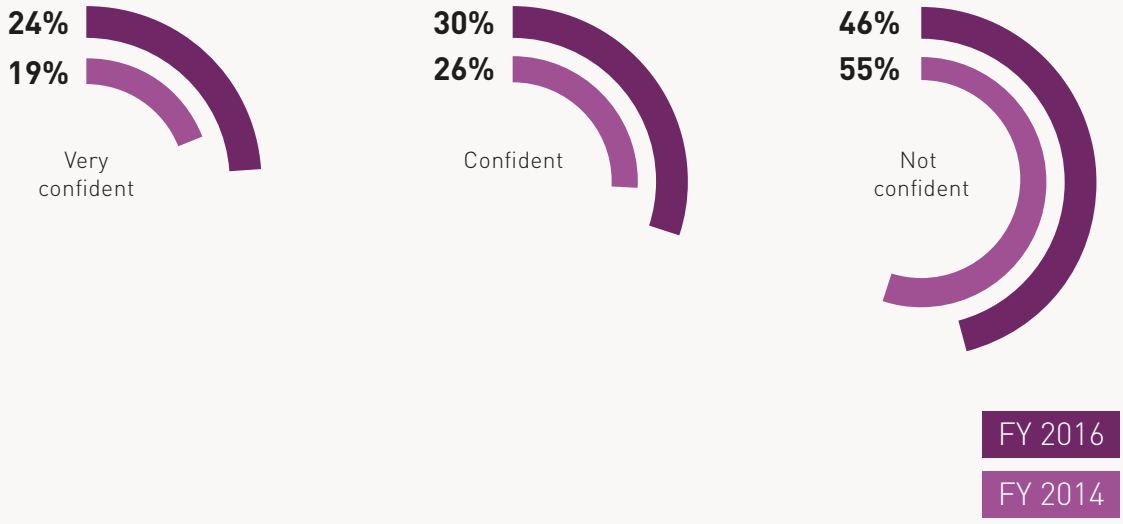


Cloud security is stormy because of Shadow IT

IT does not have control of all corporate data stored in the cloud. An average of 49 percent of cloud services deployed by departments other than corporate IT and an average of 47 percent of corporate data stored in the cloud environment is not managed or controlled by the IT department.

However, on a positive note, confidence in knowing all cloud computing services in use is increasing. According to Figure 5, 54 percent of respondents are either very confident (24 percent) or confident (30 percent) that the IT organization knows all cloud computing applications, platform or infrastructure services in use today. This is an increase from 45 percent of respondents in the previous study.

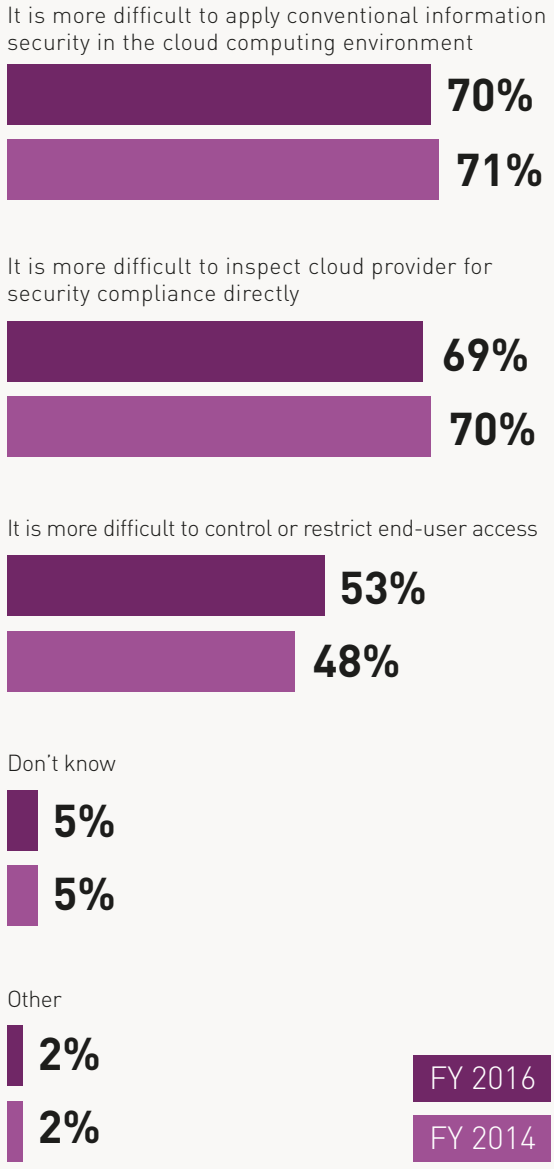
Figure 5. How confident are you that IT knows all cloud computing services in use today?



The difficulty in protecting confidential or sensitive information when using cloud services decreases. In the previous study, 60 percent of respondents said it is more difficult to protect confidential or sensitive information when using cloud services. This year, the percentage has decreased to 54 percent of respondents. However, organizations still face challenges in the protection of confidential information when using cloud services. Figure 6 reveals that the difficulty in controlling or restricting end-user access has increased from 48 percent of respondents in the previous study to 53 percent of respondents. Other reasons why cloud security is a challenge is the difficulty in applying conventional information security in the cloud computing environment (70 percent) and the inability to directly inspect cloud providers for security compliance (69 percent).

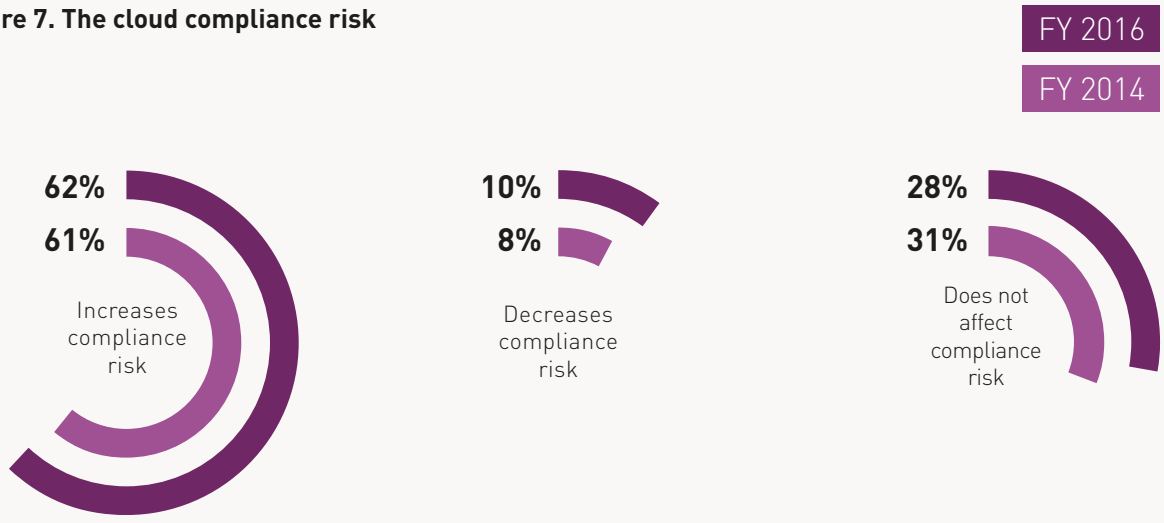
Figure 6. Why cloud security is still difficult to achieve

More than one response permitted



Compliance in the cloud is difficult. Sixty-two percent of respondents say the use of cloud resources increases compliance risk. This can be due to the difficulty in controlling end-user access to sensitive data in the cloud. According to Figure 7, only 28 percent of respondents say the cloud has no effect on the company's ability to comply with privacy and data protection regulations or legal requirements around the globe.

Figure 7. The cloud compliance risk

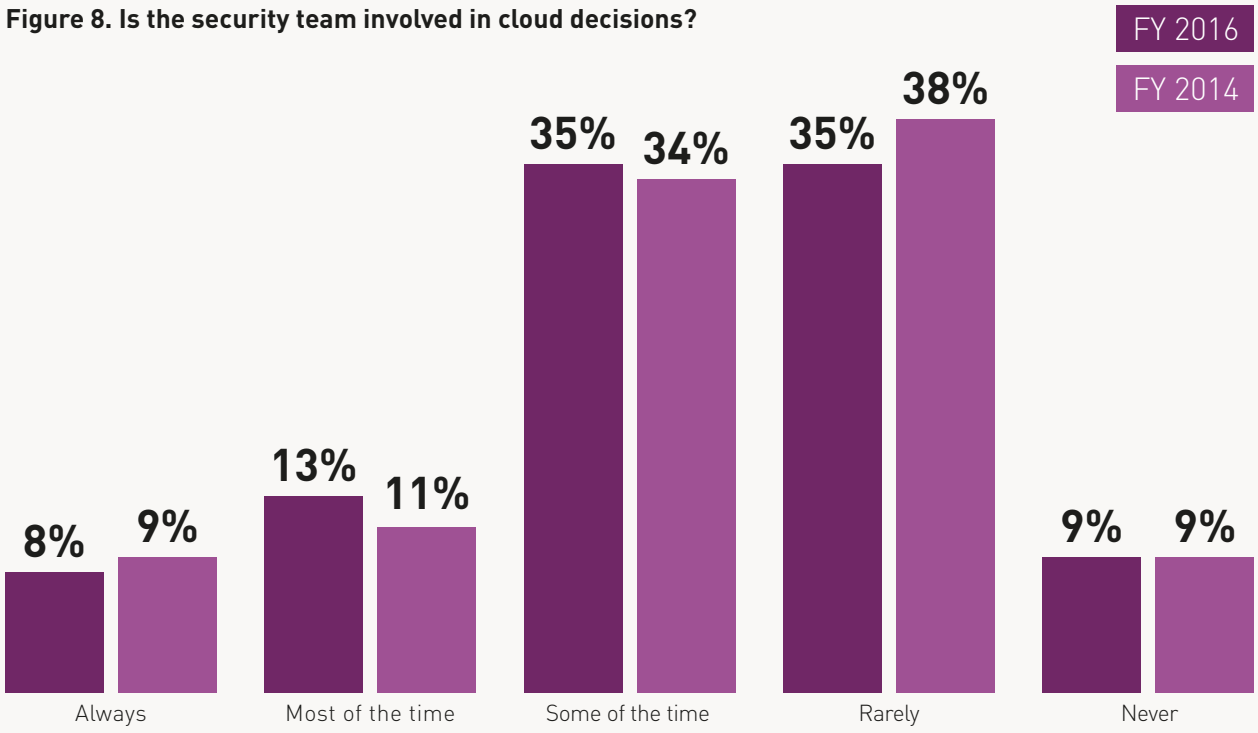


Data security governance practices ignore the security practitioners

Security practitioners are not the decision makers when it comes to the use of cloud resources. According to Figure 8, only 21 percent of respondents say members of the security team are involved in the decision-making process about using certain cloud applications or platforms always (8 percent) or most of the time (13 percent). This is similar to the previous study.

Most organizations still do not have security policies for the cloud. Sixty percent of respondents say their organizations do not have a policy that requires the use of security safeguards such as encryption as a condition to using certain cloud computing applications. However, this is a decrease from 66 percent of respondents in the previous study who said there were no policies.

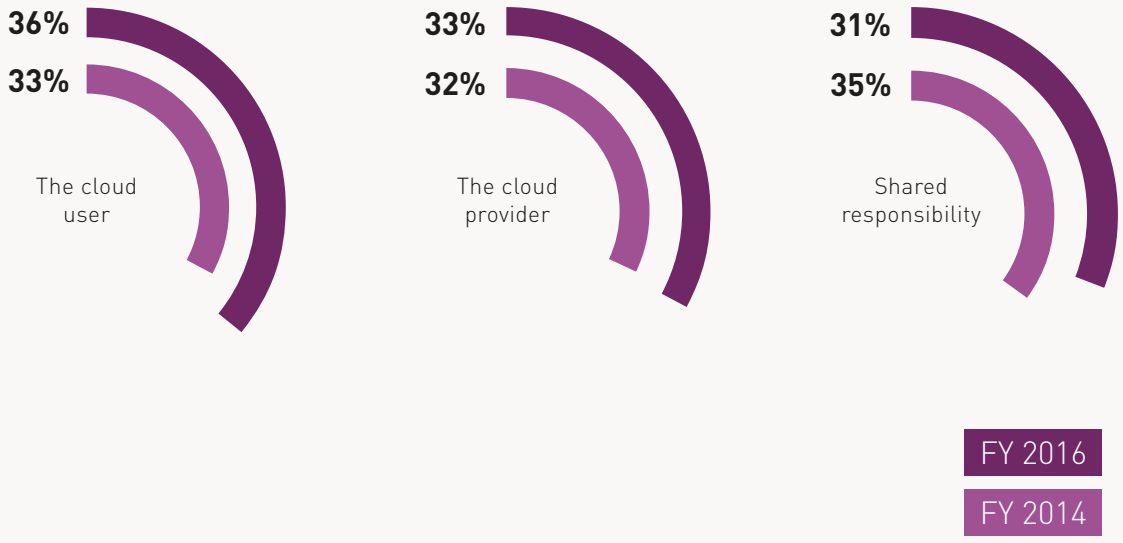
Figure 8. Is the security team involved in cloud decisions?



Responsibility for cloud security is moving to the cloud user.

According to Figure 9, respondents have mixed views on who should be most responsible for protecting sensitive or confidential data in the cloud. Fewer respondents (31 percent of respondents) say it is a shared responsibility and more respondents (36 percent) say the cloud user should be responsible for cloud security.

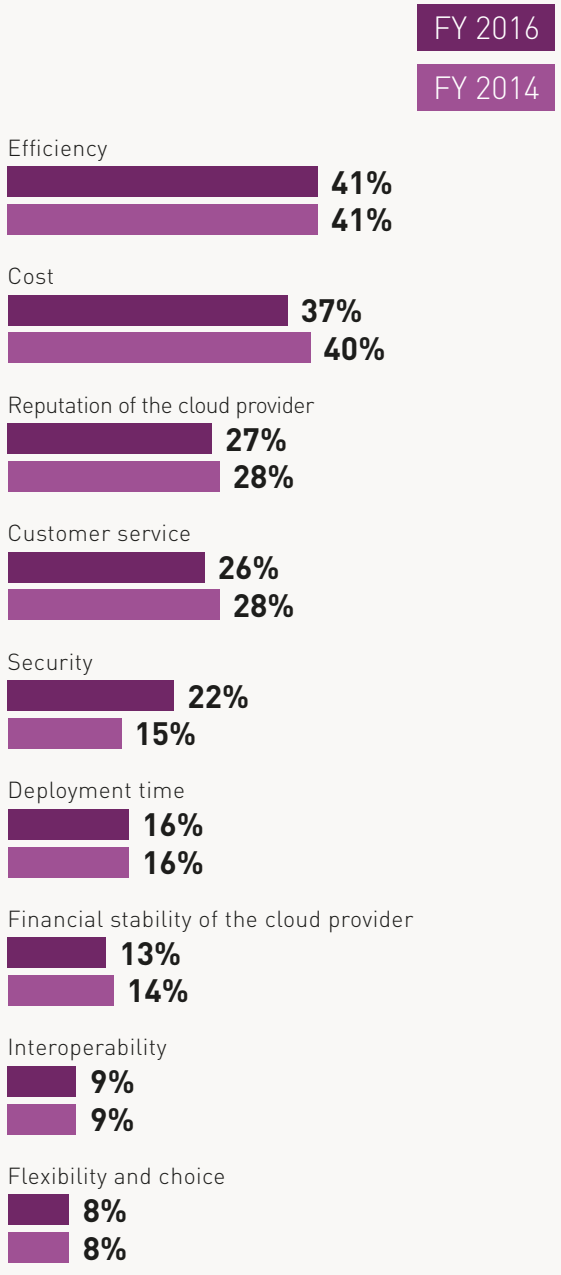
Figure 9. Who is responsible for cloud security?



Efficiency and cost are the most important factors for selecting a cloud provider, not security.

The primary reasons for selecting a particular cloud provider are efficiency (41 percent of respondents) or cost (37 percent), as shown in Figure 10. However, more respondents say security is a consideration when selecting a cloud provider (22 percent vs. 15 percent in the previous study).

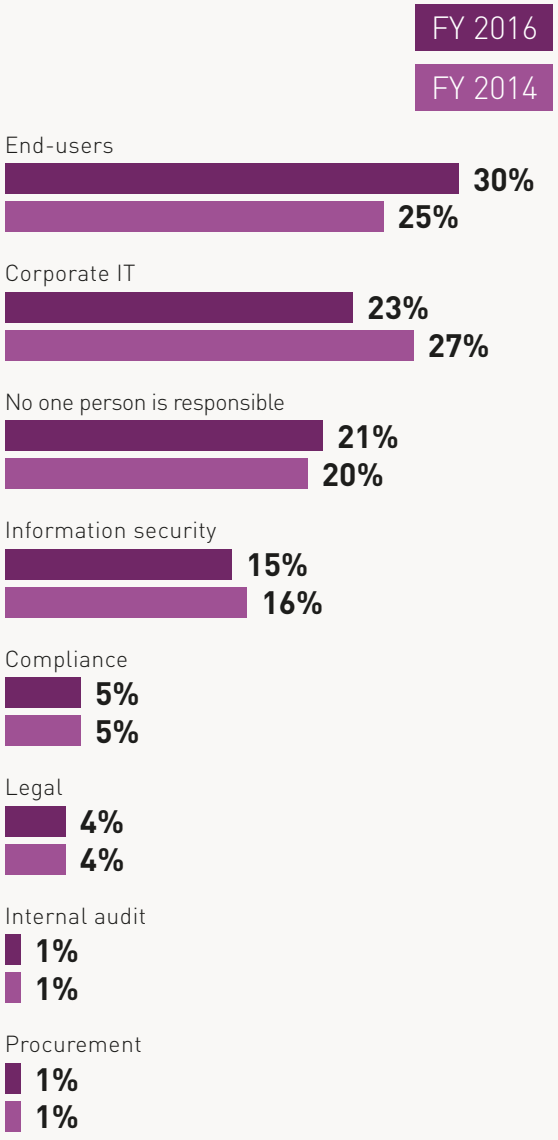
Figure 10. How do you select a cloud provider?
Two responses permitted



Evaluation of cloud providers is shifting to the end-user.

Sixty percent of respondents say their organizations evaluate the security capabilities prior to engagement or deployment. Only 15 percent of respondents say it is the security function that is most responsible for evaluating the cloud provider's security capabilities, as shown in Figure 11. More respondents believe the enduser is responsible for security evaluations (30 percent vs. 25 percent in the previous study), followed by corporate IT.

Figure 11. Who evaluates the cloud provider's security capabilities?



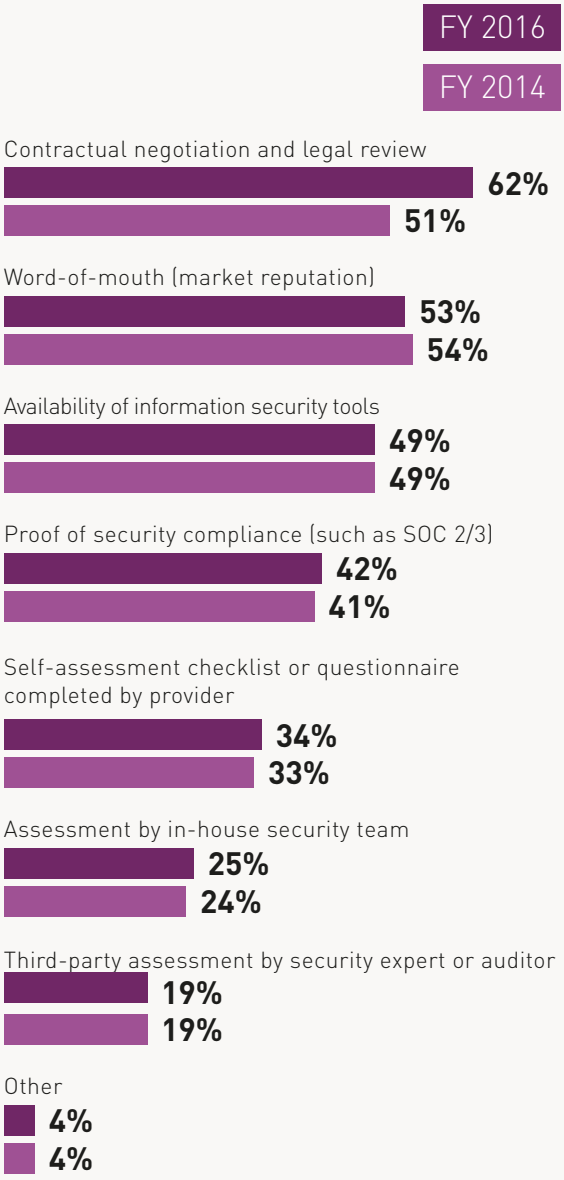
Security evaluations of cloud providers rely increasingly on contractual negotiations and legal reviews.

Figure 12 reveals a significant increase in the use of contractual negotiation and legal reviews to evaluate cloud providers from 51 percent of respondents in the previous study to 62 percent of respondents. Word-of-mouth or market reputation is used to evaluate the provider by 53 percent of respondents, followed by availability of information security tools (49 percent).

Fewer organizations look at proof of security compliance (42 percent), a self-assessment security questionnaire (34 percent) and an assessment by in-house security team (25 percent). Similar to the previous study, only 19 percent of respondents say their organizations conduct a third-party assessment by security expert or auditor.

Figure 12. How cloud providers are evaluated

More than one response permitted

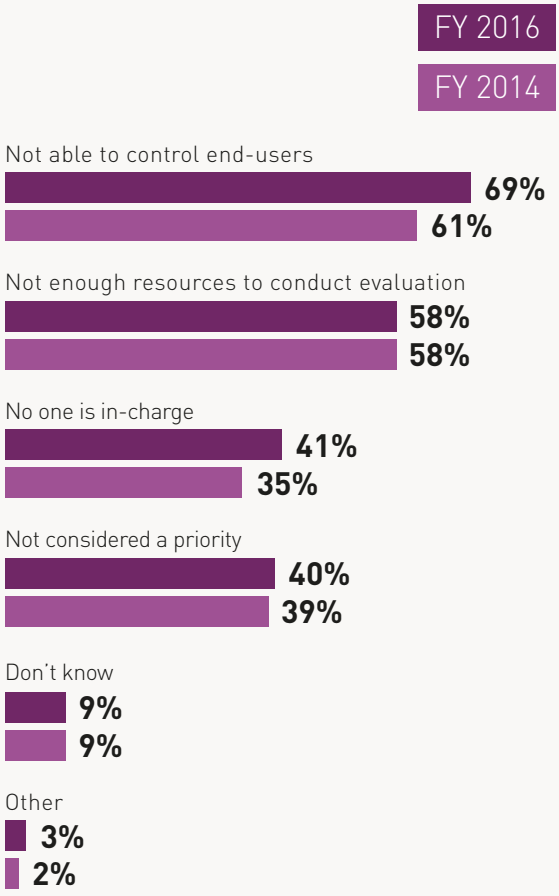


The inability to control end-users is resulting in more cloud resources deployed without evaluation.

As shown in Figure 13, it is the loss of control over end-users that results in cloud resources deployed without security scrutiny. Other reasons are not enough resources to conduct an evaluation (58 percent of respondents) and increasingly no one is in-charge (41 percent vs. 35 percent in the previous study).

Figure 13. Why does your organization permit cloud resources to be deployed without first evaluating for security?

More than one choice permitted

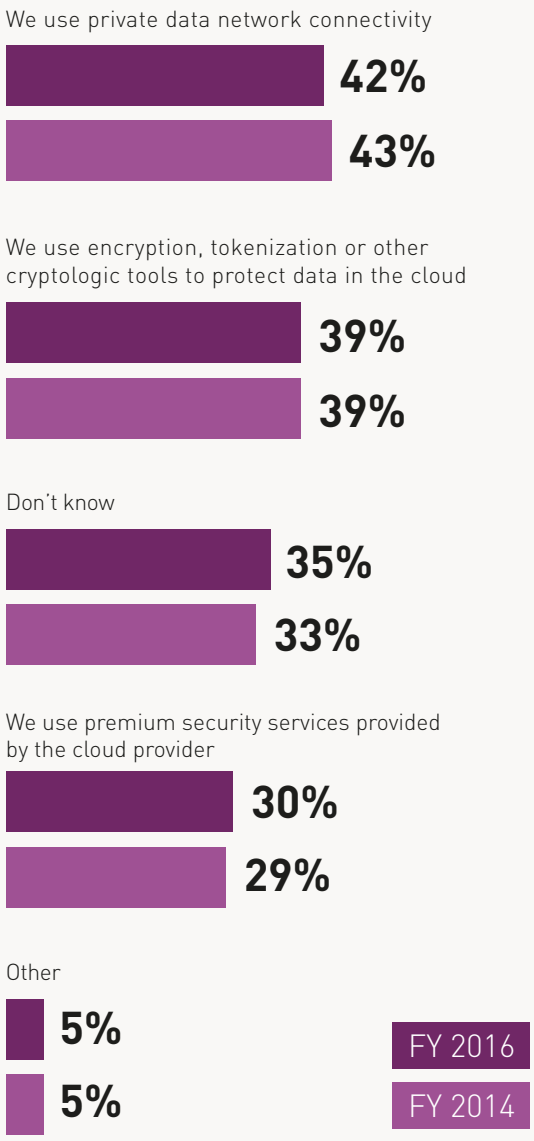


Protection of data in the cloud is important but not practiced

More organizations use private data network connectivity to secure data in the cloud. Similar to the previous study, when asked what security solutions are used to protect data in the cloud, 39 percent of respondents say their organizations use encryption, tokenization or other cryptographic tools, as shown in Figure 14. Most respondents (42 percent) say they use private data network connectivity.

Thirty-five percent of respondents say they don't know what security solutions they use. A possible explanation is that business units and corporate IT are making investments in security without input from IT security.

Figure 14. How data is protected in the cloud
More than one response permitted

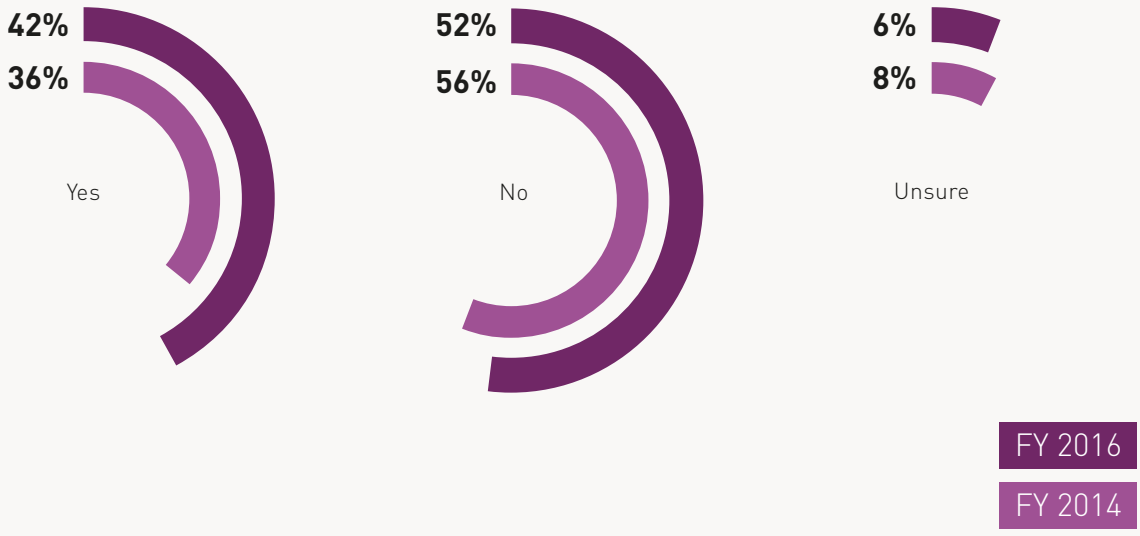


Encryption is increasing in importance.

Seventy-two percent of respondents say the ability to encrypt or tokenize sensitive or confidential data is important and 86 percent say it will become more important over the next two years, an increase from 79 percent of respondents. According to Figure 15, more respondents than in the previous study say their organizations use encryption, tokenization or other cryptographic solutions to secure sensitive or confidential information at rest (36 percent vs. 42 percent of respondents in 2016).

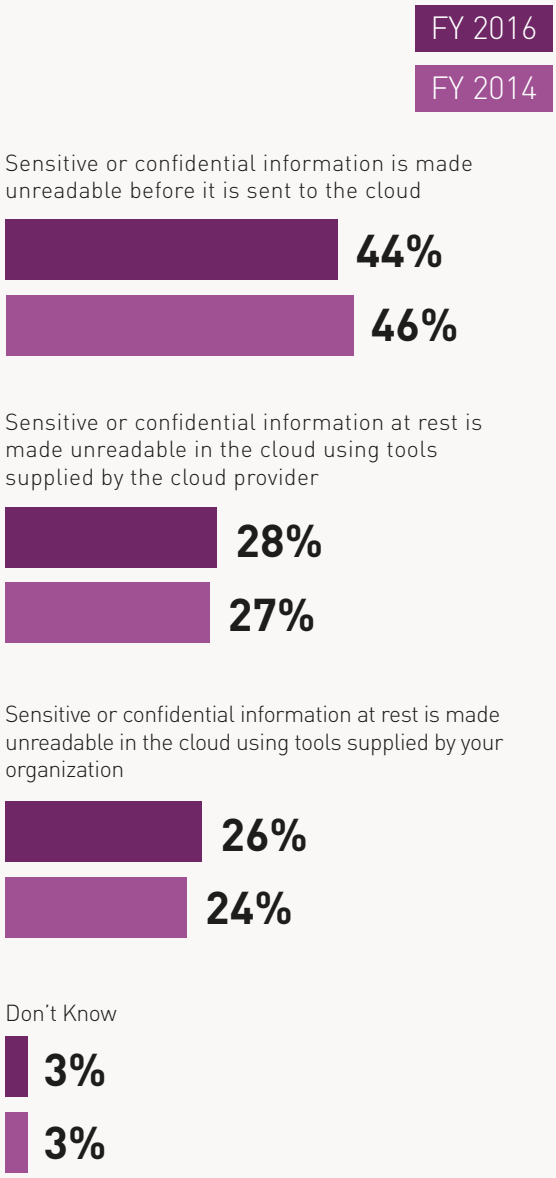
More respondents say encryption is used when it is sent and received by the cloud provider (59 percent). Encryption or tokenization of sensitive or confidential data directly within cloud applications such as SaaS has increased from 28 percent to 34 percent of respondents.

Figure 15. Use of encryption, tokenization or other cryptographic solution to secure data at rest in the cloud



If data at rest is encrypted, as shown in Figure 16, 44 percent say the data is made unreadable before it is sent to the cloud. The remaining respondents say it is made unreadable in the cloud using tools supplied by their organization or the cloud provider (26 percent of respondents and 28 percent of respondents, respectively). These results are similar to the previous study.

Figure 16. How encryption is applied

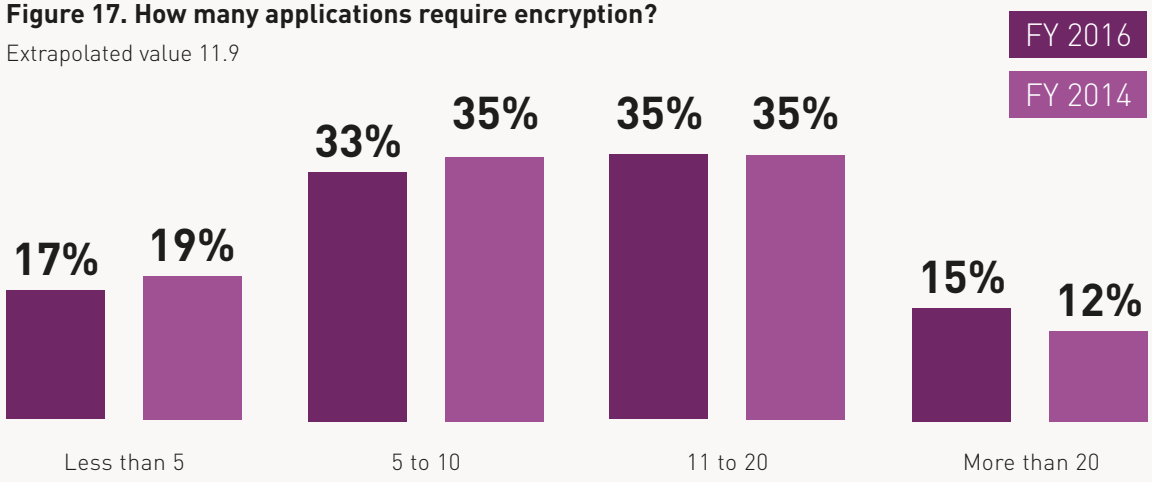


There is a lack of encryption of cloud applications (SaaS).

According to the study, Software as a Service (SaaS) is used more frequently than Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Seventy percent of respondents say they use business applications such as document sharing tools and 54 percent of respondents say they use online backup. However, only 34 percent of respondents say their organization encrypts or tokenizes sensitive or confidential data directly within these applications. According to Figure 17, an average of 11.9 applications requires encryption. This is a slight increase from 11.3 in the previous study.

Figure 17. How many applications require encryption?

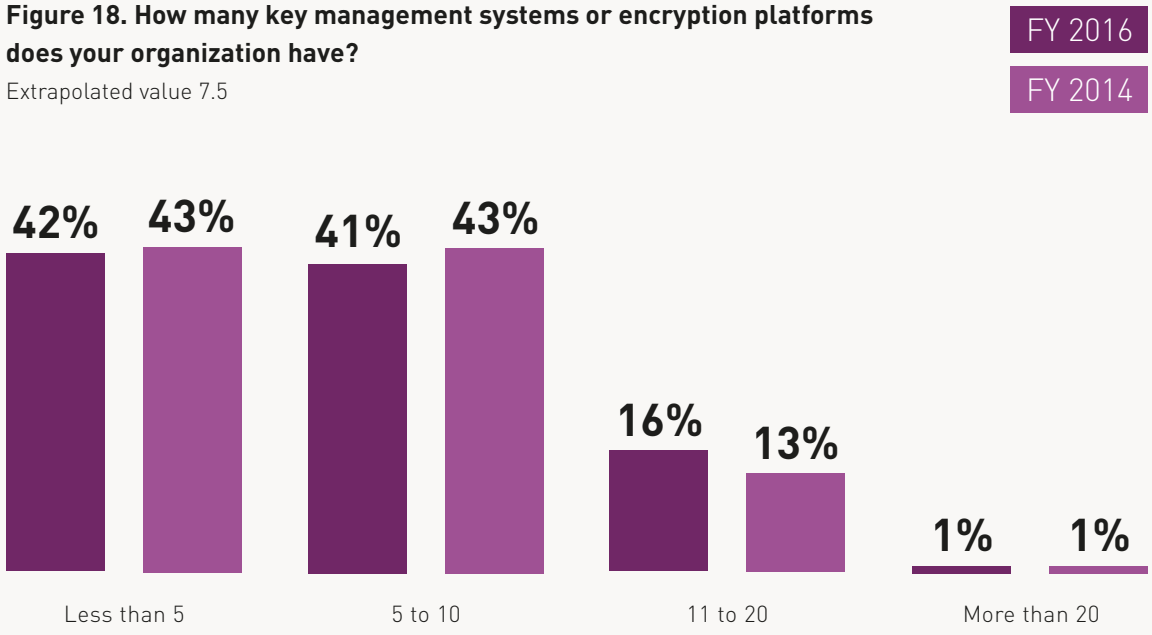
Extrapolated value 11.9



How prevalent is the use of key management systems? Figure 18 reveals that on average organizations have 7.5 key management systems or encryption platforms, a slight increase from 7.2 in the previous study.

Figure 18. How many key management systems or encryption platforms does your organization have?

Extrapolated value 7.5

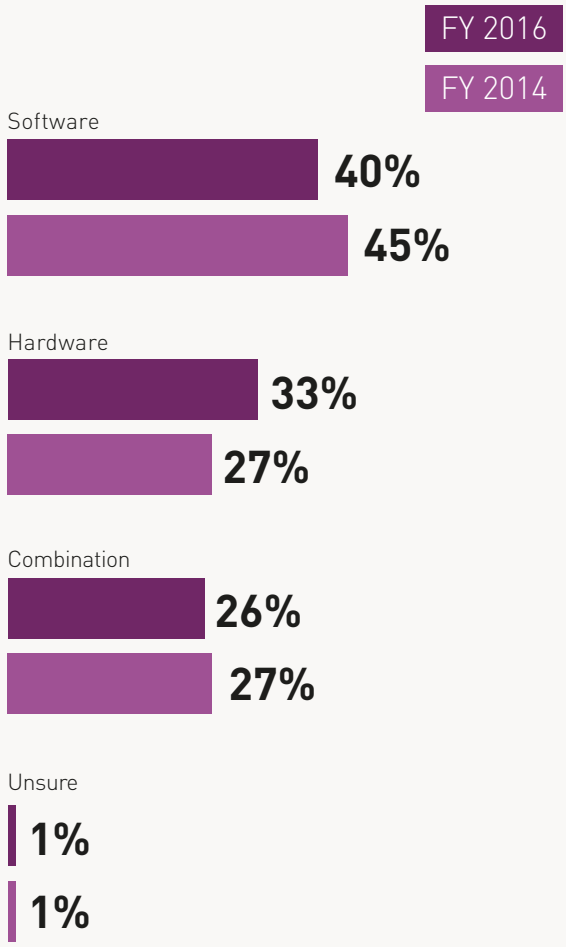


The storage of keys is shifting from software to hardware.

As shown in Figure 19, most encryption keys are still stored in software (40 percent vs. 45 percent in the previous study). However, the storage of keys in hardware increased from 27 percent of respondents in the previous study to 33 percent of respondents.

Fifty-five percent of respondents say their organizations control the encryption keys when data is encrypted in the cloud. Twenty percent say it is the cloud provider and 16 percent say a third party controls the encryption keys (neither the organization nor cloud provider).

Figure 19. Where encryption keys are stored



The cloud complicates identity and access management policies

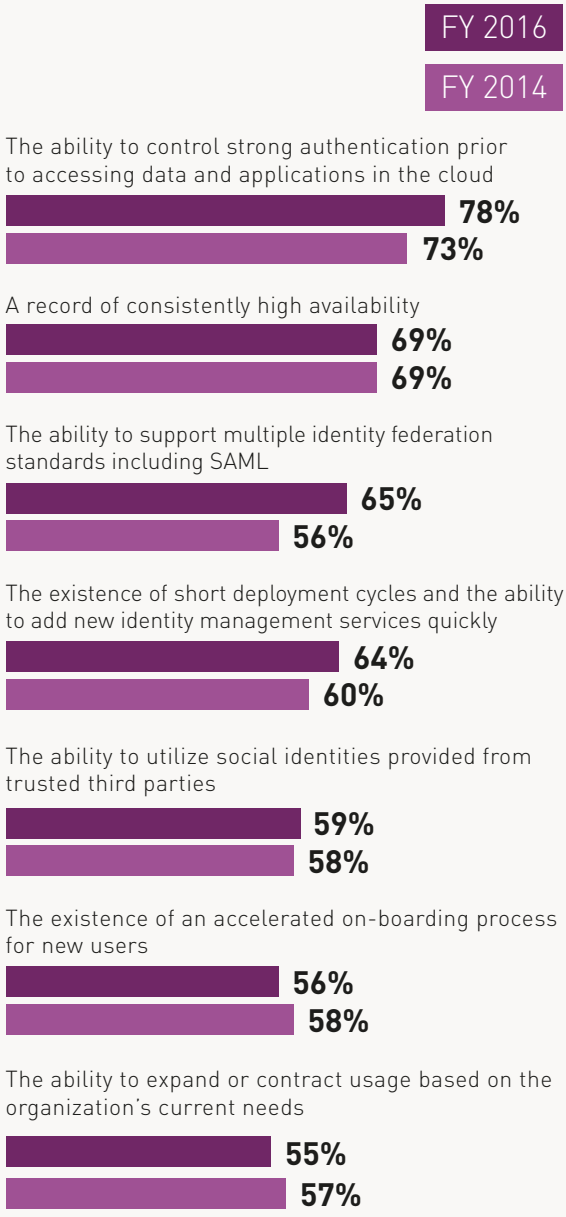
Strong authentication measures continue to be important.

Sixty-seven percent of respondents say the management of user identities is more difficult in the cloud than the onpremises environment. However, organizations are not adopting measures that are easy to implement and could increase cloud security.

The most important features of controlling and securing access to cloud resources are shown in Figure 20. Since 2014, the ability to control strong authentication prior to accessing data and applications in the cloud increased from 73 percent of respondents to 78 percent of respondents. Still, most important is the ability to control strong authentication prior to accessing data and applications in the cloud (78 percent of respondents). A record of consistently high availability is important, according to 69 percent of respondents.

Figure 20. Most important identity and access management features

Essential and very important responses combined

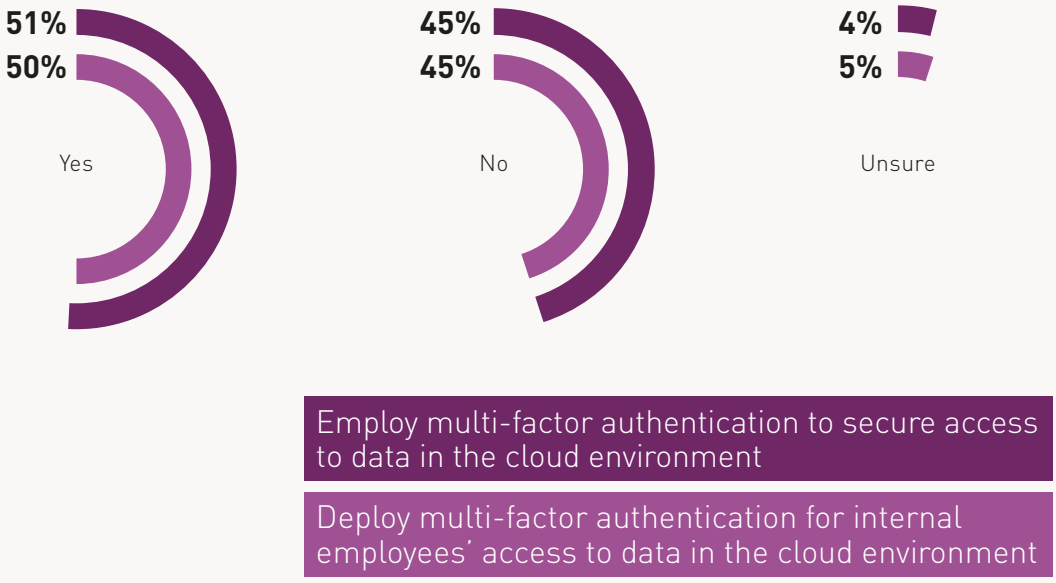


Most organizations permit third-party users to access data in the cloud.

Fifty-eight percent of respondents say their organizations have third-party users accessing their data and information in the cloud. As shown in Figure 21, more than half of respondents (51 percent of respondents) say their organization uses multi-factor authentication to secure access to data in the cloud environment.

About the same percentage of respondents (50 percent) say their organizations use multi-factor authentication for employees' access to the cloud. When asked the percent of cloud applications that have user-enabled access controls, the average is only 18 percent.

Figure 21. Use of multi-factor authentication for third-party access



Country differences

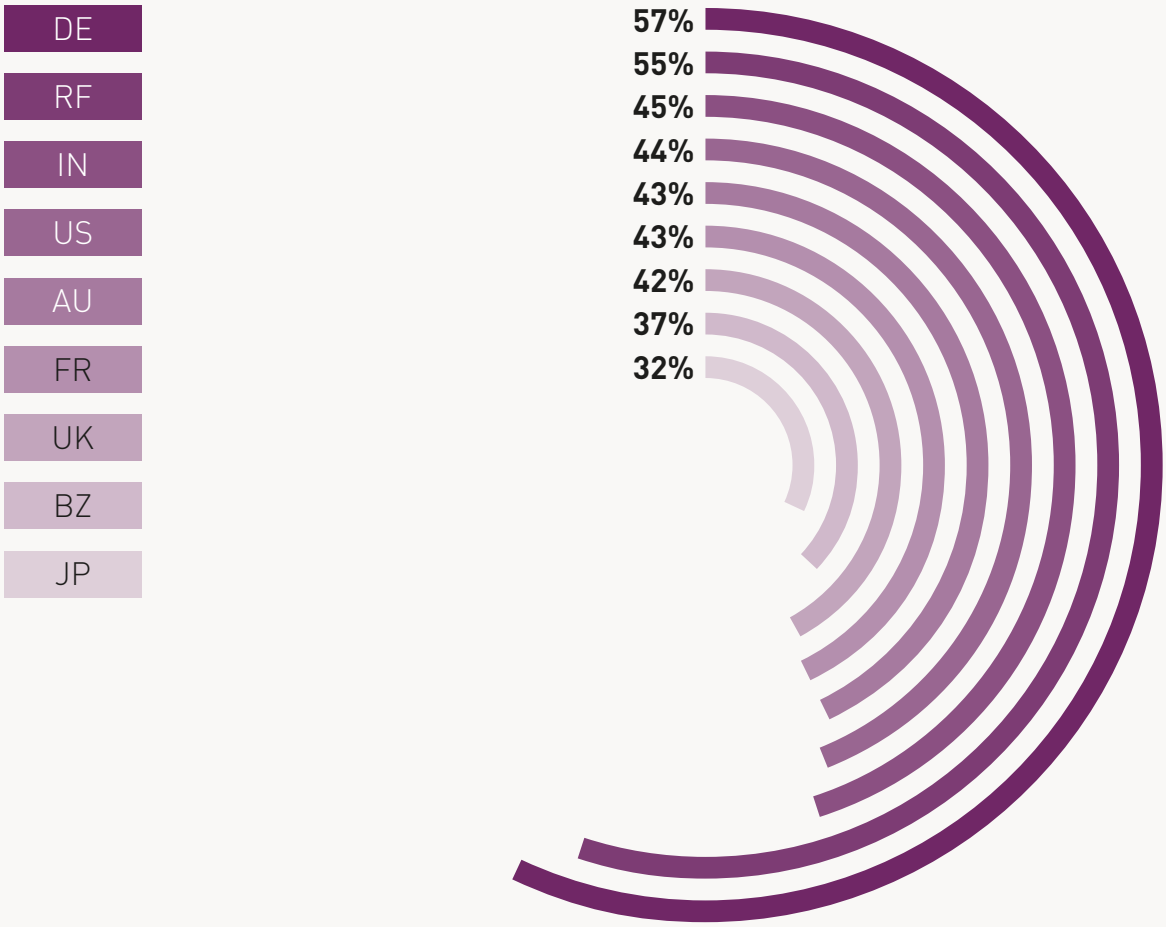
In this section, we analyze the differences among the following countries included in this research: United States (US), United Kingdom (UK), Australia (AU), Germany (DE), France (FR), Japan (JP), Russian Federation (RF), India (IN) and Brazil (BZ). As shown, German organizations seem to be the most proactive in securing sensitive and confidential information in the cloud, managing the complexity of privacy and data protection regulations in the cloud environment, and ensuring security polices for the cloud are in place.

Third party data sharing practices are most strict, according to respondents, in German and Russian organizations.

As shown in Figure 22, 57 percent of German respondents and 55 percent of Russian respondents agree that their organizations are careful when sharing sensitive and confidential information with third parties. Only 37 percent of respondents in Brazil and 32 percent of Japanese respondents agree their organizations are careful when sharing sensitive information.

Figure 22. My organization is careful about sharing confidential or sensitive information with third parties such as business partners, contractors and providers in the cloud environment

Strongly agree and agree responses combined

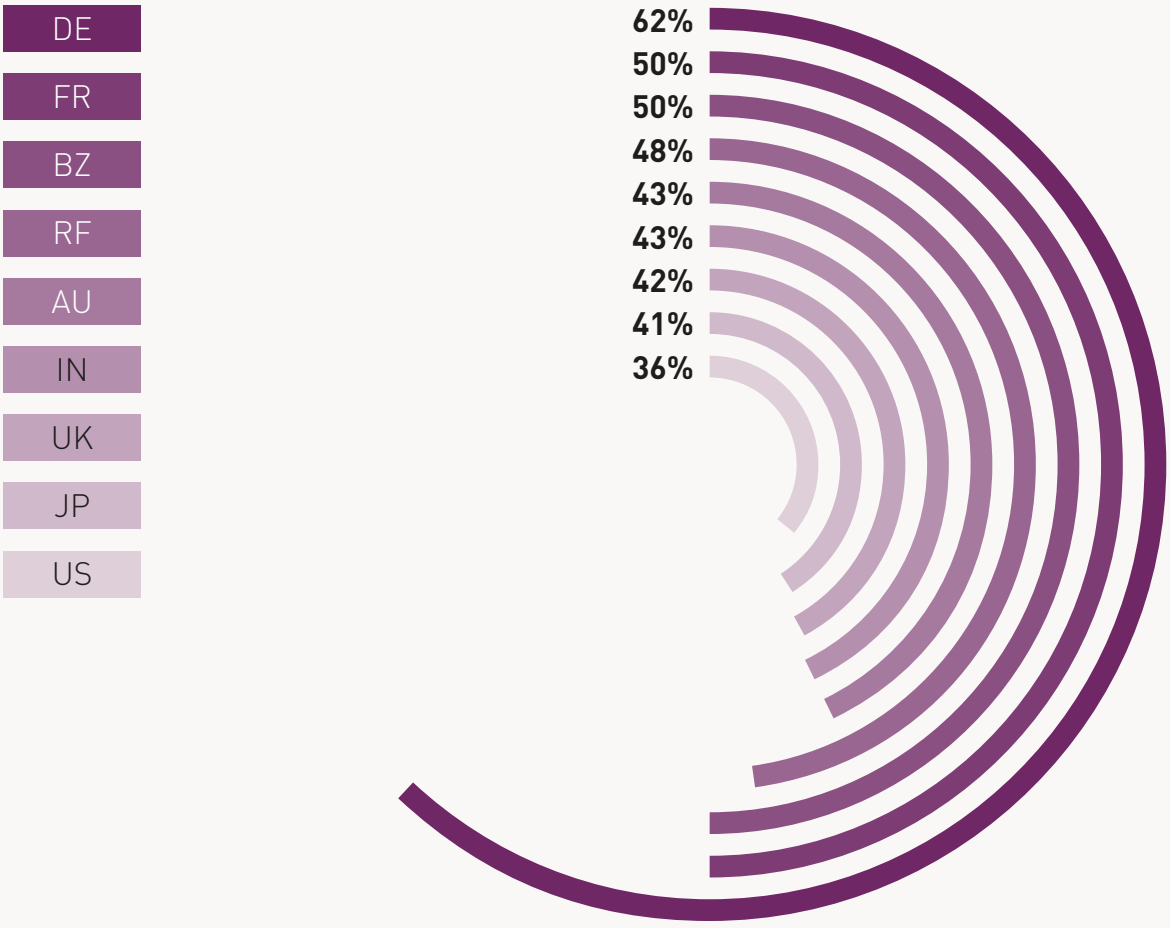


German organizations are most proactive in managing compliance with regulations.

Sixtytwo percent of respondents in Germany agree their organizations are most proactive in managing compliance with privacy and data protection regulations in the cloud environment. Only 36 percent of US respondents say their organizations are proactive in making sure the handling of sensitive and confidential information is in compliance, as shown in Figure 23.

Figure 23. My organization is proactive in managing compliance with privacy and data protection regulations in the cloud environment

Strongly agree and agree responses combined

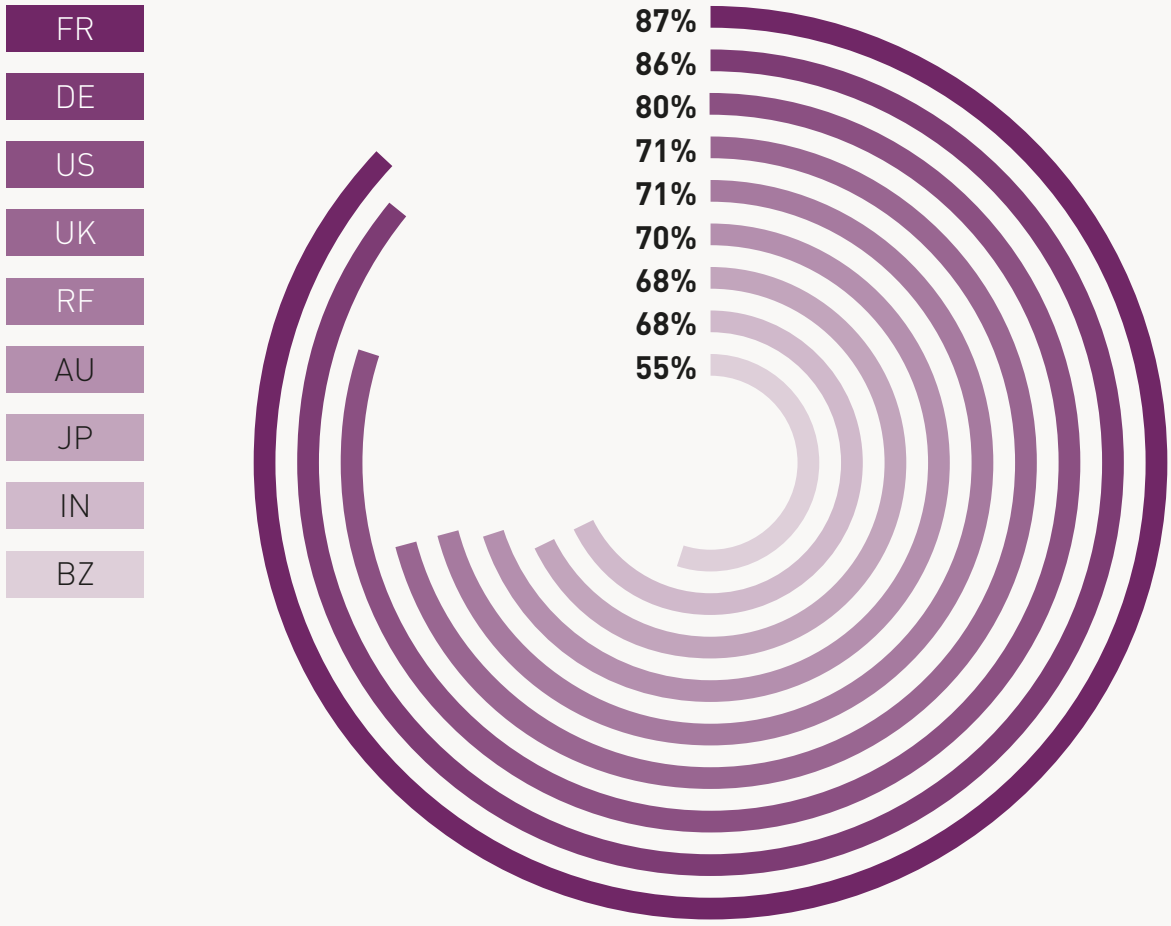


Most global respondents believe it is a challenge to manage privacy and data protection regulations in the cloud.

According to Figure 24, respondents in France, Germany and the US (87 percent, 86 percent and 80 percent, respectively) believe it is more complicated to manage privacy and data protection regulations in a cloud environment than in on-premises.

Figure 24. It is more complex to manage privacy and data protection regulations in a cloud environment than in on-premise networks within my organization.

Strongly agree and agree responses combined

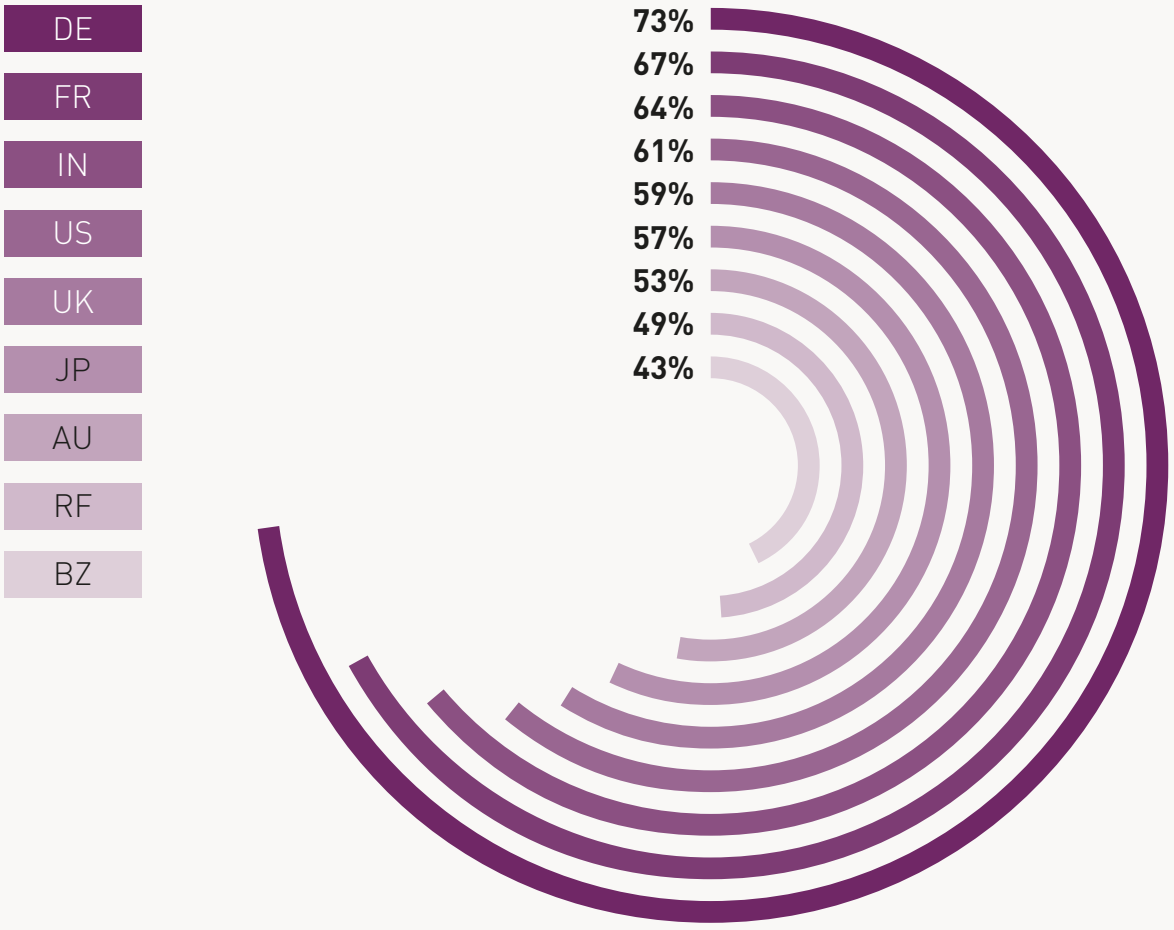


Germany and France are most likely to evaluate the security capabilities of cloud providers.

As shown in Figure 25, 73 percent of German respondents and 67 percent of French respondents say their organizations evaluate the security capabilities of cloud providers. Only 49 percent of Russian respondents and 43 percent of Brazilian respondents say their organizations evaluate cloud providers prior to deployment or engagement.

Figure 25. Are cloud providers evaluated for security capabilities prior to engagement or deployment within your organization?

Yes responses

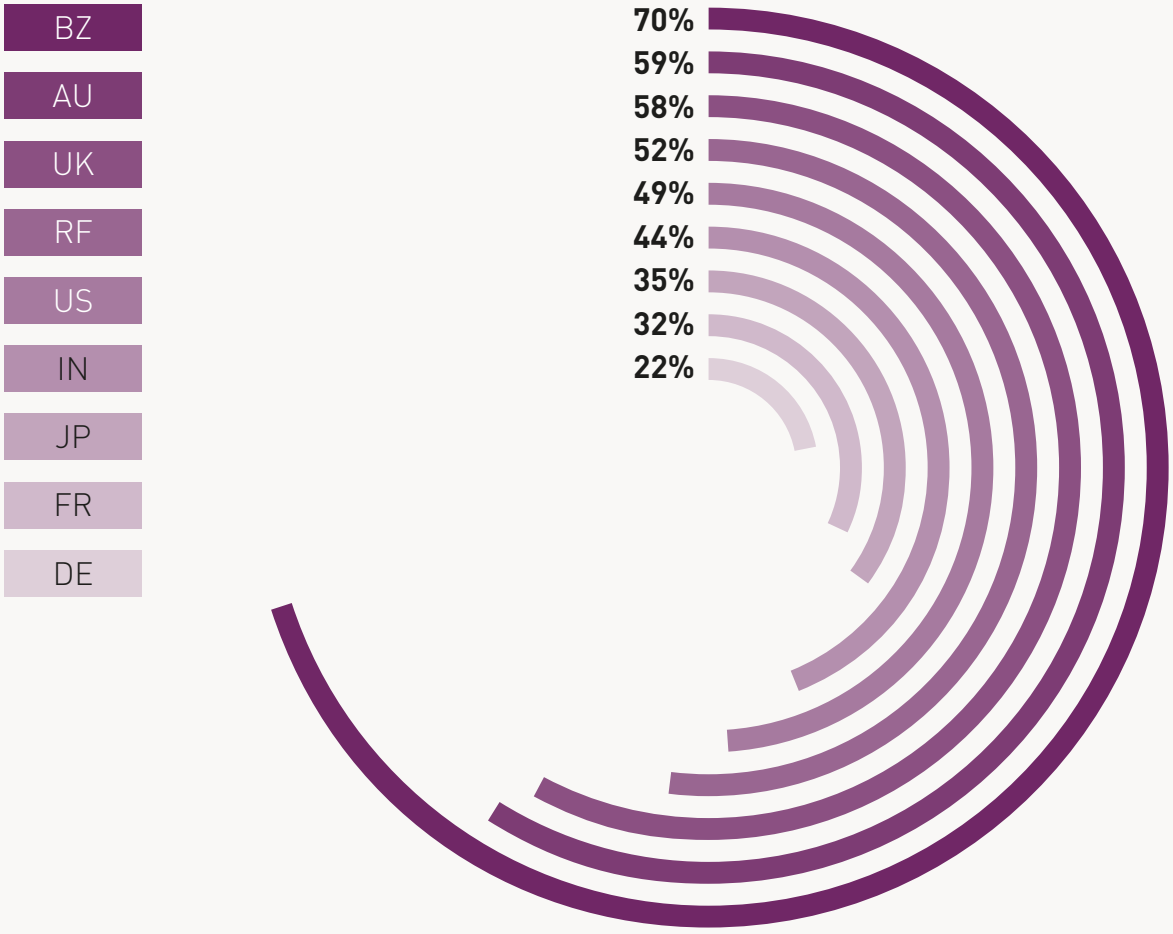


How confident are respondents that they know all cloud computing applications, platform or infrastructure services in use in their organizations?

Seventy percent of respondents in Brazil are not confident that their organizations have visibility into the use of cloud computing applications, platform or infrastructure services. Germany is the most confident (only 22 percent of respondents say they are not confident), as revealed in Figure 26.

Figure 26. Are you confident your IT organization knows all cloud computing applications, platform or infrastructure services in use today?

Not confident responses

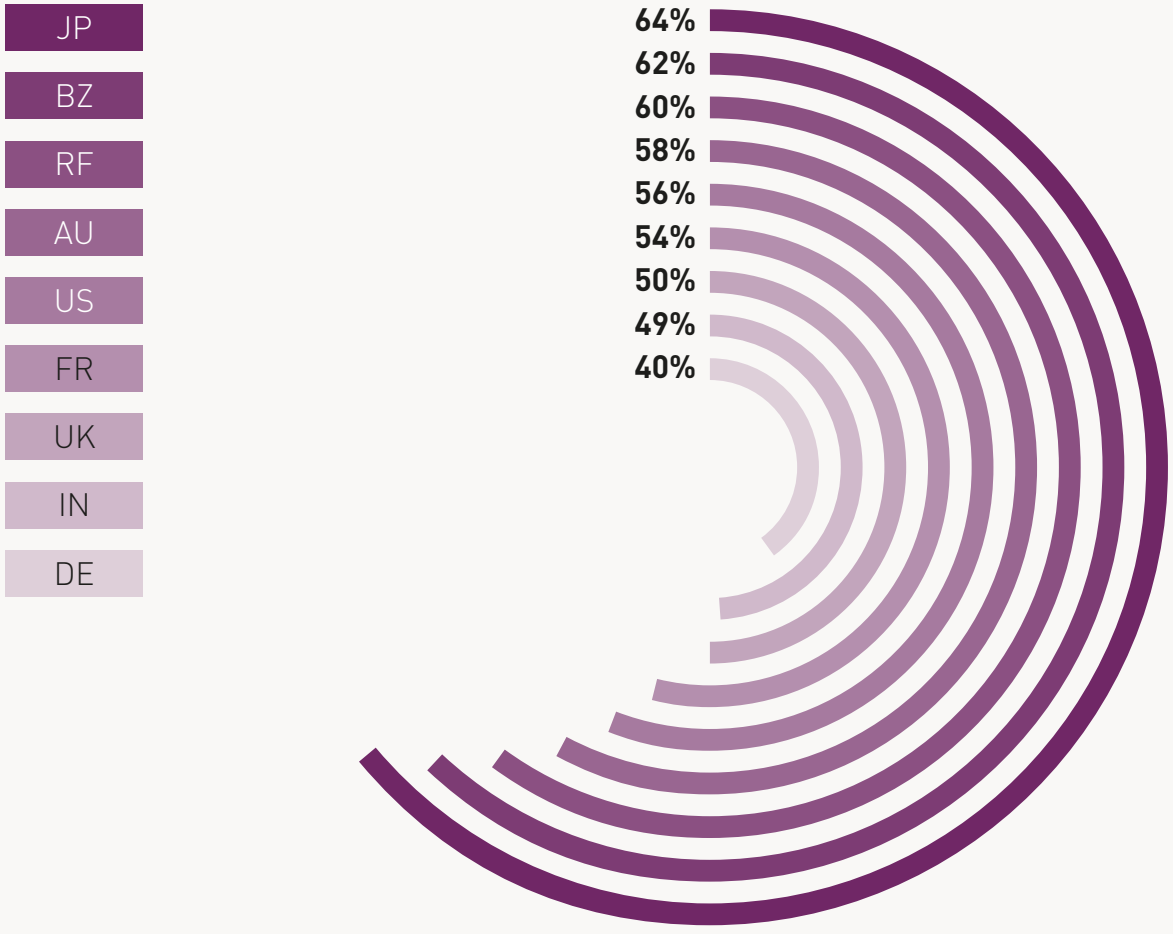


Cloud services are considered to make the protection of confidential or sensitive information difficult.

As shown in Figure 27, 64 percent of respondents in Japan believe it is more difficult to protect confidential or sensitive information. Respondents in Germany and India are least likely to think it is difficult.

Figure 27. Do cloud services make it more difficult to protect confidential or sensitive information?

Yes responses

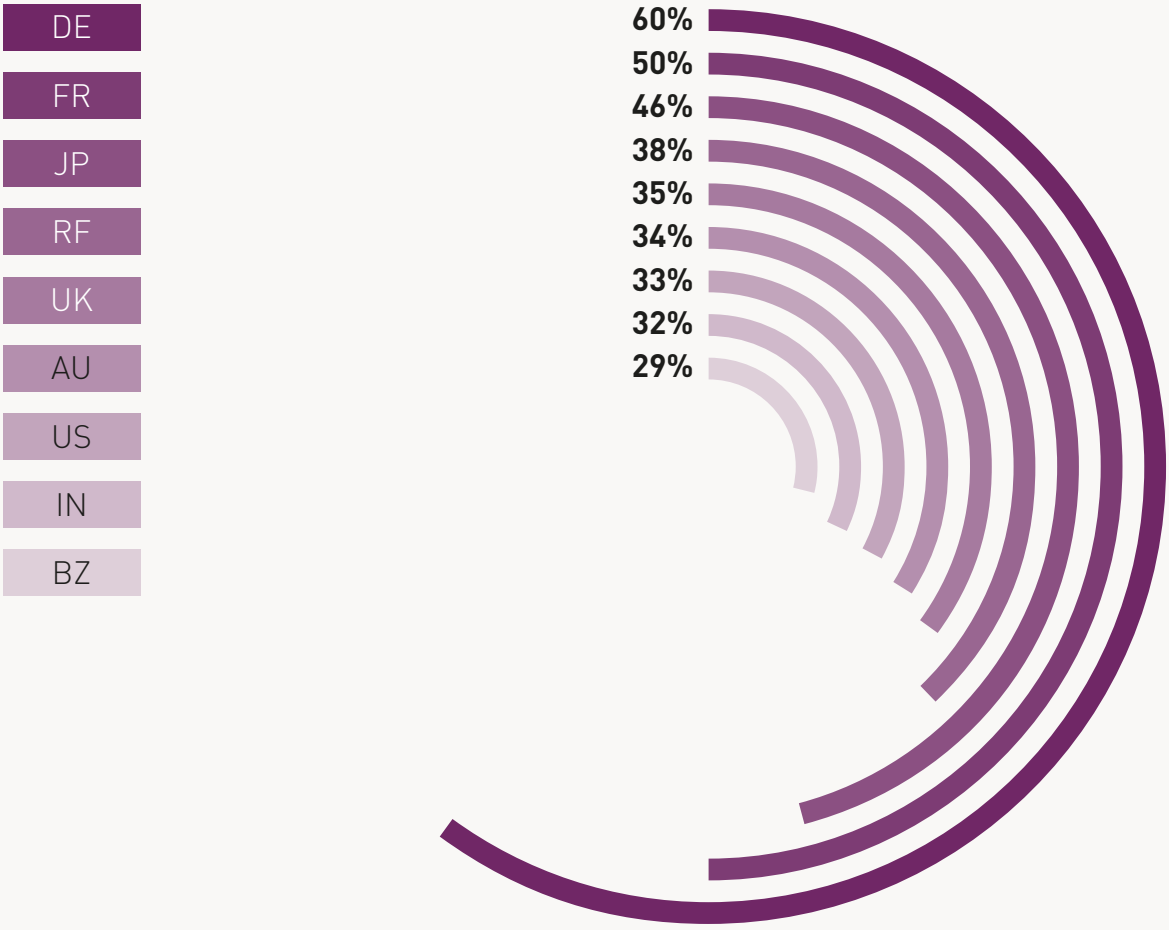


Security policies are most likely to exist in Germany and France.

Sixty percent of German respondents say their organizations have a policy that requires the use of security safeguards such as encryption as a condition to using certain cloud computing applications, according to Figure 28. In contrast, only 33 percent of respondents in the US, 32 percent of respondents in India and 29 percent of respondents in Brazil say their organizations have such policies in place.

Figure 28. Does your organization have a policy that requires the use of security safeguards as a condition to using certain cloud computing applications?

Yes responses

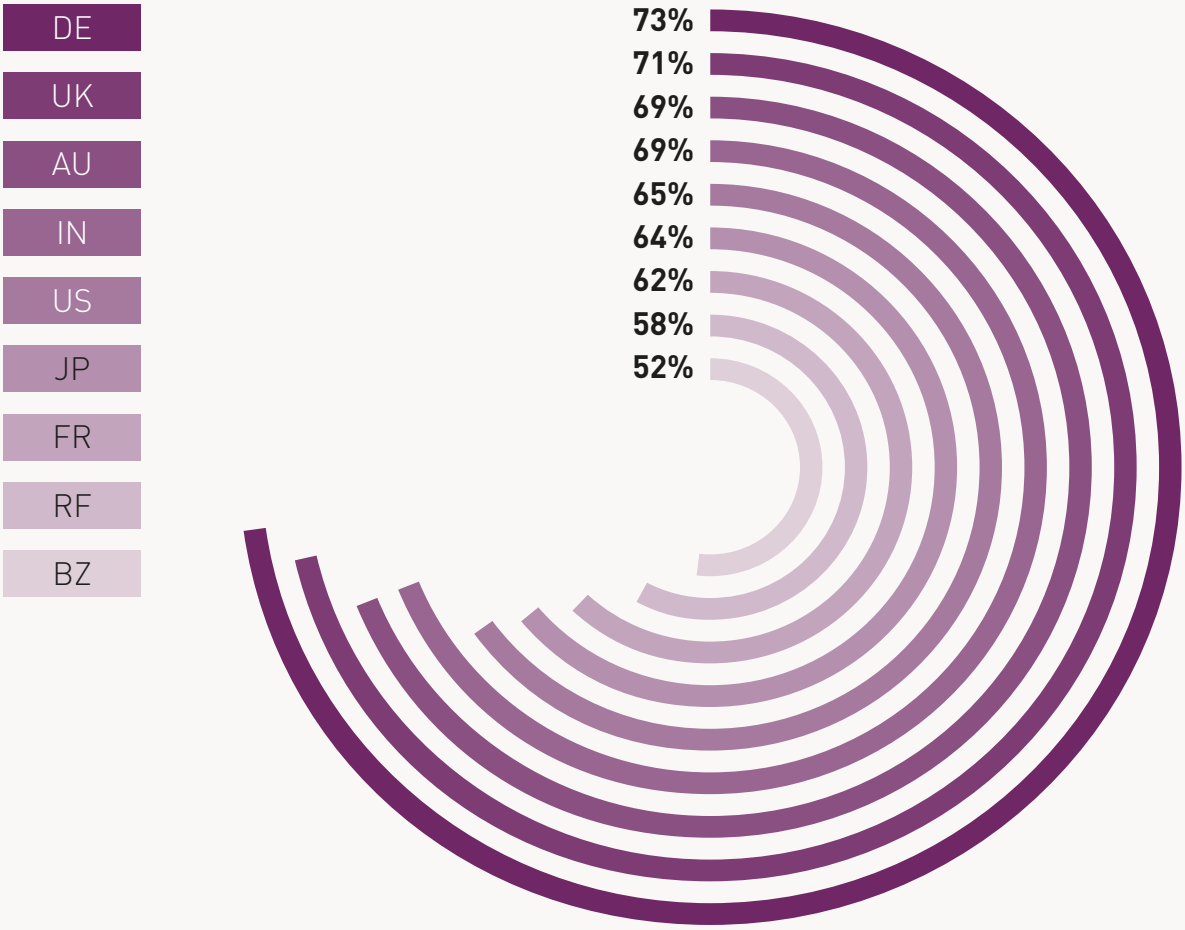


Strong authentication measures are important globally.

Germany and UK are most likely to believe the ability to support federations including SAML are essential or very important (73 percent and 71 percent of respondents, respectively). The least likely to think this ability is important are Brazil and Russia (52 percent and 58 percent of respondents, respectively).

Figure 29. How important is the ability to support multiple identity federation standards, including SAML, to control and secure access to cloud resources?

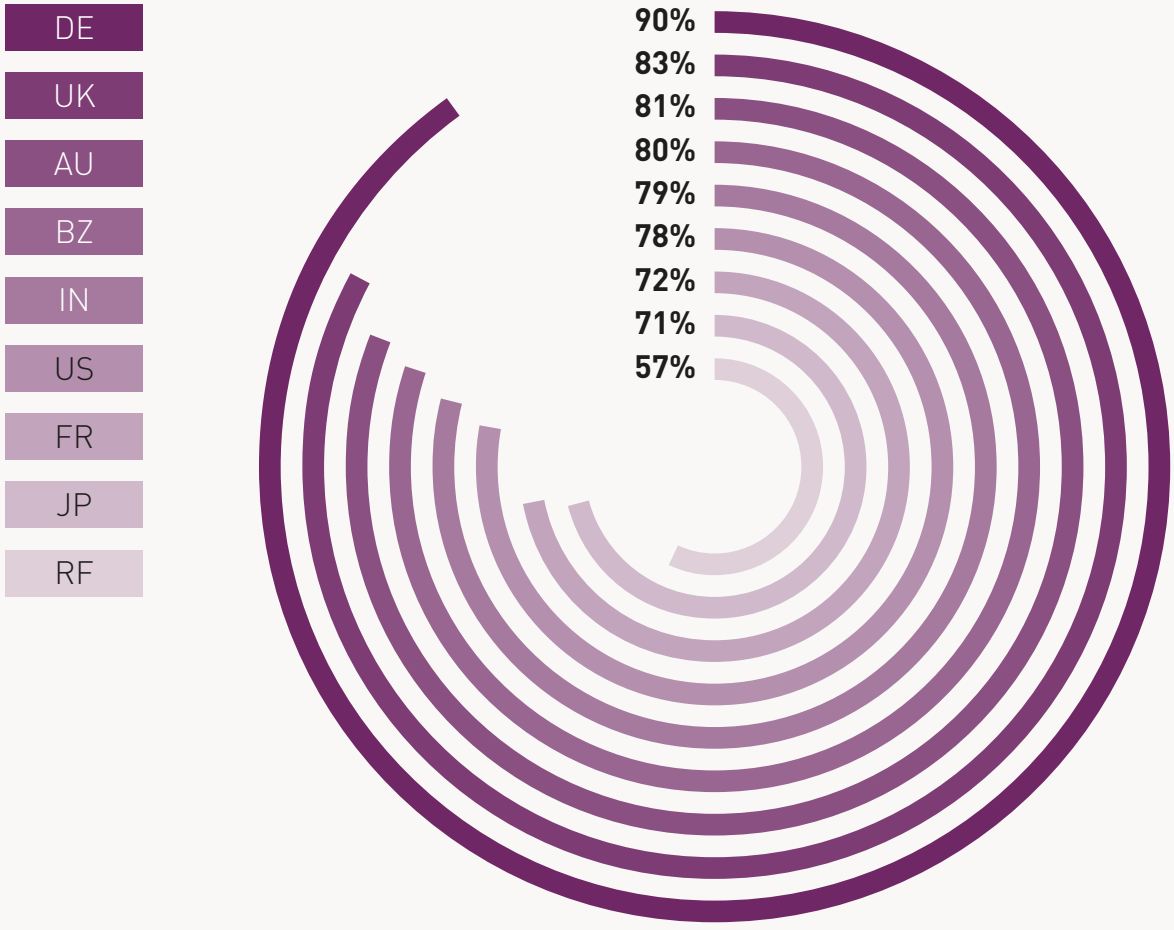
Essential and very important ratings combined



As shown in Figure 30, respondents in Germany and the UK (90 percent and 83 percent of respondents, respectively) believe the ability to control strong authentication prior to accessing data and applications in the cloud is essential or very important. Fifty-seven percent of respondents in Russia are least likely to believe that such an ability is critical.

Figure 30. How important is the ability to control strong authentication prior to accessing data and applications in the cloud to control and secure access to cloud resources?

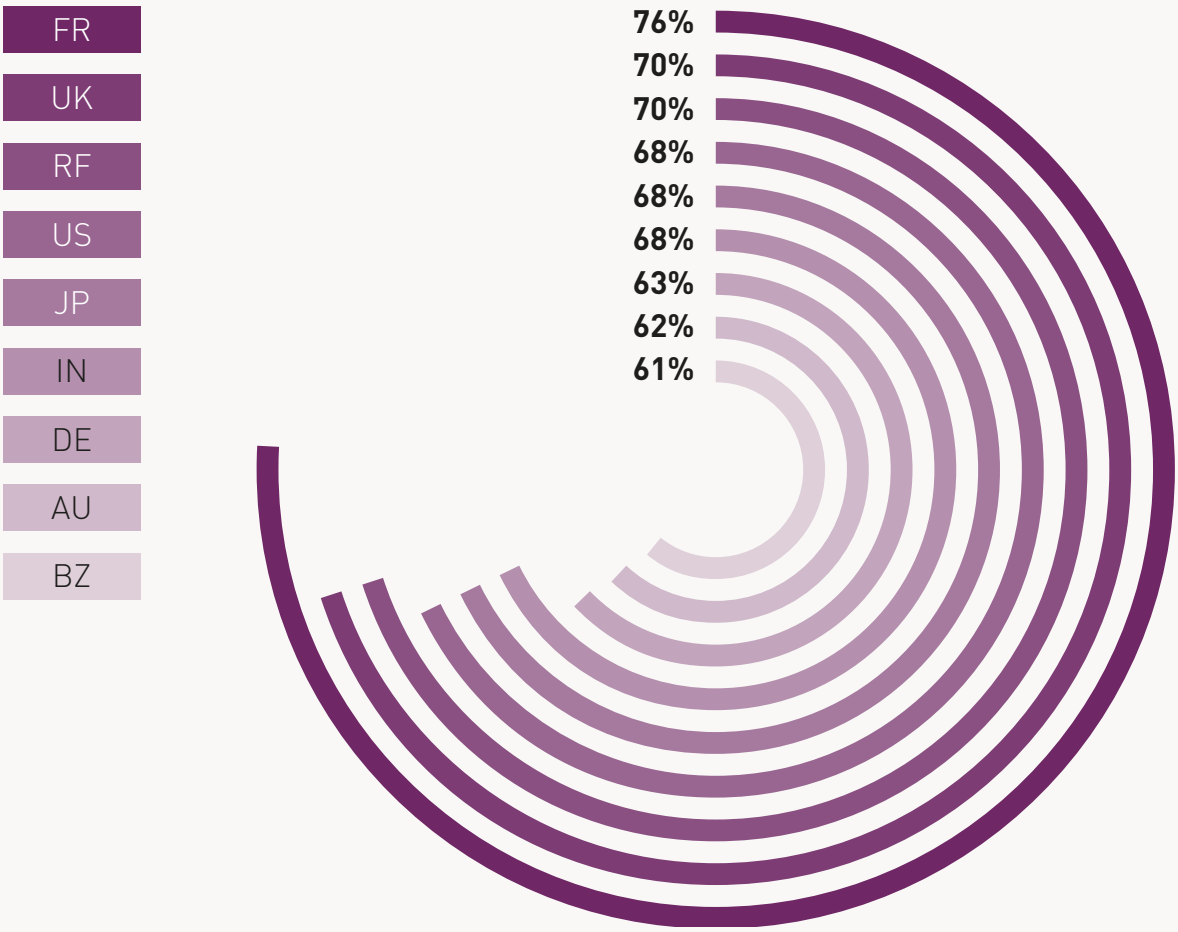
Essential and very important ratings combined



Respondents in France, the UK and Russia (76 percent, 70 percent and 70 percent of respondents, respectively) are more likely to agree that the management of user identities is more difficult in the cloud than the on-premises environment

Figure 31. The management of user identities is more difficult in the cloud than the on-premises environment

Strongly agree and agree responses combined



Part 3. Recommendations on improving cloud governance

The findings reveal that global organizations have challenges when securing data in the cloud due to the lack of critical governance and security practices in place. The following are steps that will lead to a more secure cloud environment.

- Confirm if the cloud provider or cloud user is most accountable and responsible for cloud security. If it is the cloud provider, involve IT security in vetting and evaluating its security practices. If the organization assumes responsibility, make sure there are clearly defined roles for the business functions using cloud services. Again, including IT security in establishing security policies and procedures is important.
- Increase visibility into the use of cloud applications, platforms and infrastructure to reduce the Shadow IT risk.
- Protect data at risk in the cloud. According to respondents, payment and customer information are some of the data types most often stored in the cloud and are also considered most at risk.
- Business cloud applications such as document sharing are growing in popularity. However, policies about the secure use of these applications are not being communicated. Organizations should make employees aware of the risks with specialized training about not circumventing security policies when using SaaS applications.
- Organizations need to consider the adoption of encryption, tokenization or other cryptographic solutions to secure sensitive data transferred and stored in the cloud.
- Improve compliance with data security and privacy regulations with the use of encryption and identity and access management solutions such as multi-factor authentication.
- Even if the cloud provider has overall responsibility for data stewardship, companies should look to maintain control over their encryption keys for ultimate protection.
- Companies should store their encryption keys in hardware to ensure their keys are secured and stored separately from the encrypted data they are protecting, which is often what happens with software key storage.
- Given the wide variety of cloud-based services being used, companies should consider "bring your own encryption" solutions that enable them to encrypt data and store keys centrally across multiple cloud environments.
- With the increasing use of encryption, companies will need solutions that enable them to
- centralize key management across multiple encryption platforms in order to ensure better
- control and security of their encryption keys.

Part 4. Methods

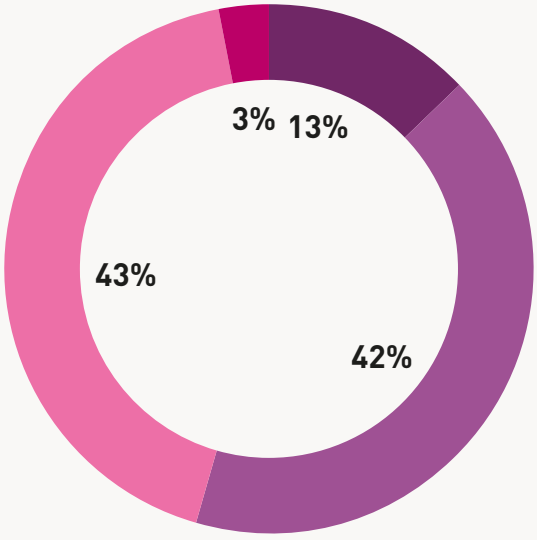
A sampling frame of 99,453 experienced IT and IT security practitioners located in the United States, United Kingdom, Australia, Germany, France, Japan, Russian Federation, India and Brazil who are familiar and involved in their company's use of both public and private cloud resources were selected as participants in the research. Table 1 shows 3,859 total returns. Screening and reliability checks required the removal of 383 surveys. Our final sample consisted of 3,476 surveys or a 3.5 percent response.

Table 1. Sample response	US	UK	AU	DE	FR	JP	RF	IN	BZ	TOTAL
Sampling frame	16554	11401	6788	11881	10600	11340	6900	12009	11980	99453
Total returns	665	457	261	501	345	452	268	512	398	3859
Rejected or screened surveys	76	33	21	30	43	30	67	47	36	383
Final sample	589	424	240	471	302	422	201	465	362	3476

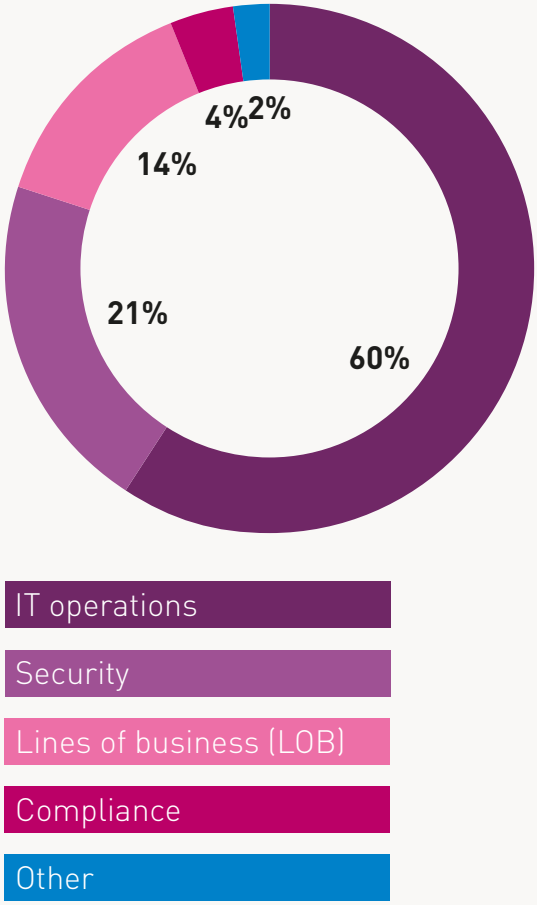
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 55 percent of respondents are at or above the supervisory levels.

As shown in Pie Chart 2, 60 percent of respondents reported their functional area as IT operations, 21 percent reported security and 14 percent report lines of business (LOB).

Pie Chart 1. Current position within the organization

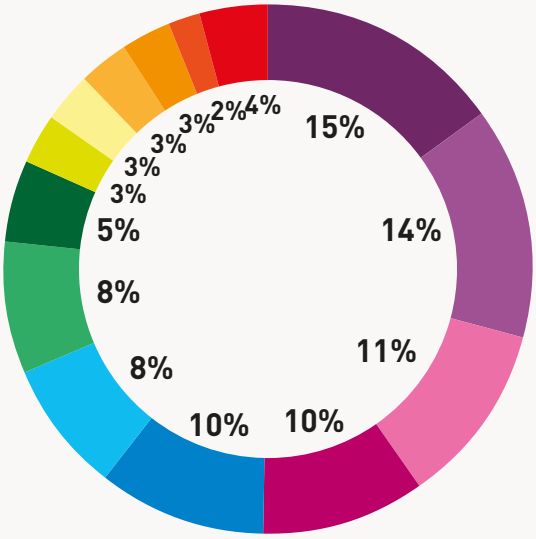


Pie Chart 2. Functional area within the organization



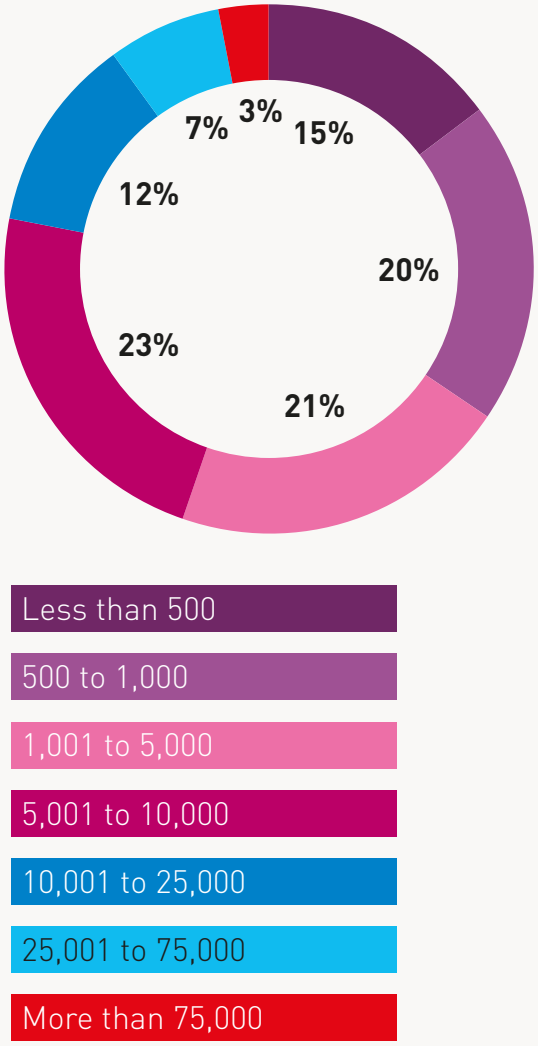
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (15 percent) as the largest segment, followed by public sector (14 percent) and industrial organizations (11 percent).

Pie Chart 3. Primary industry focus



As shown in Pie Chart 4, 65 percent of respondents are from organizations with a global headcount of more than 1,000 employees

Pie Chart 4. Global employee headcount



Part 5. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.