

Approaches to Cloud Security and Compliance



Summary Results | September 2021

SURVEY SUMMARY

Between April and September 2021, Gatepoint Research invited selected executives to participate in a survey themed *Approaches to Cloud Security and Compliance*.

Candidates from several industries were invited via email and 158 executives have participated to date.

Management levels represented are all senior decision makers: 14% hold the title CxO, 20% are VPs, 20% are directors, and 46% are managers.

100% of responders participated voluntarily; none were engaged using telemarketing.



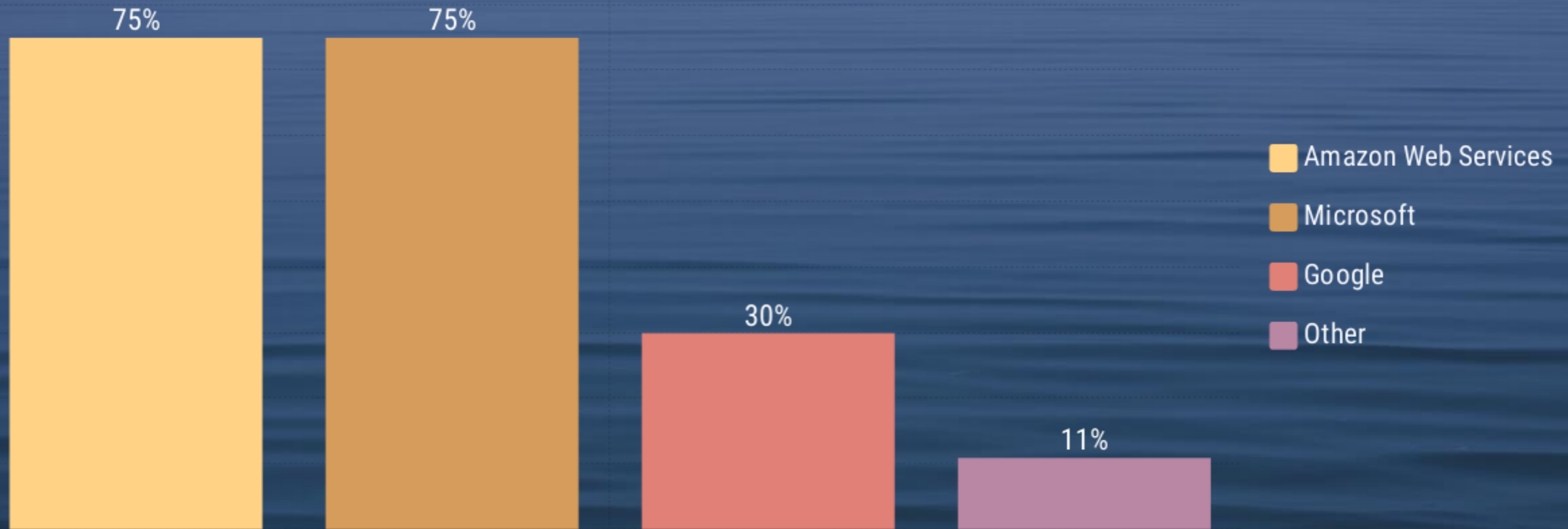
EXECUTIVE OVERVIEW

Companies are under tremendous pressure to protect the data they collect and use. Risks such as sensitive data exposure need to be constantly monitored and mitigated. What are companies doing to ensure they reduce their vulnerabilities?

This survey asks respondents to report:

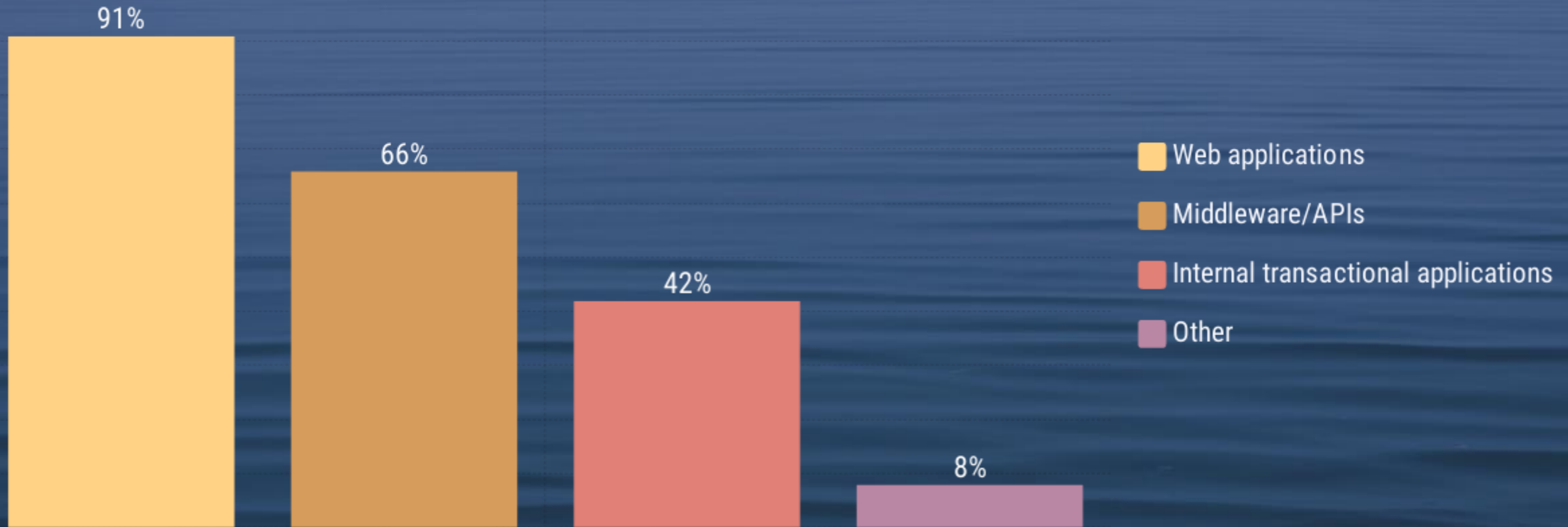
- What apps are they running in the cloud?
- How often do they review their cloud infrastructure for vulnerabilities and/or misconfigurations?
- What challenges do they have maintaining cloud best practices, security, and compliance? What would improve their compliance and security posture?

Which cloud provider(s) do you use today?



The preponderance of respondents, fully three fourths, use AWS and/or Microsoft for cloud services.

What types of applications do you run in the cloud?

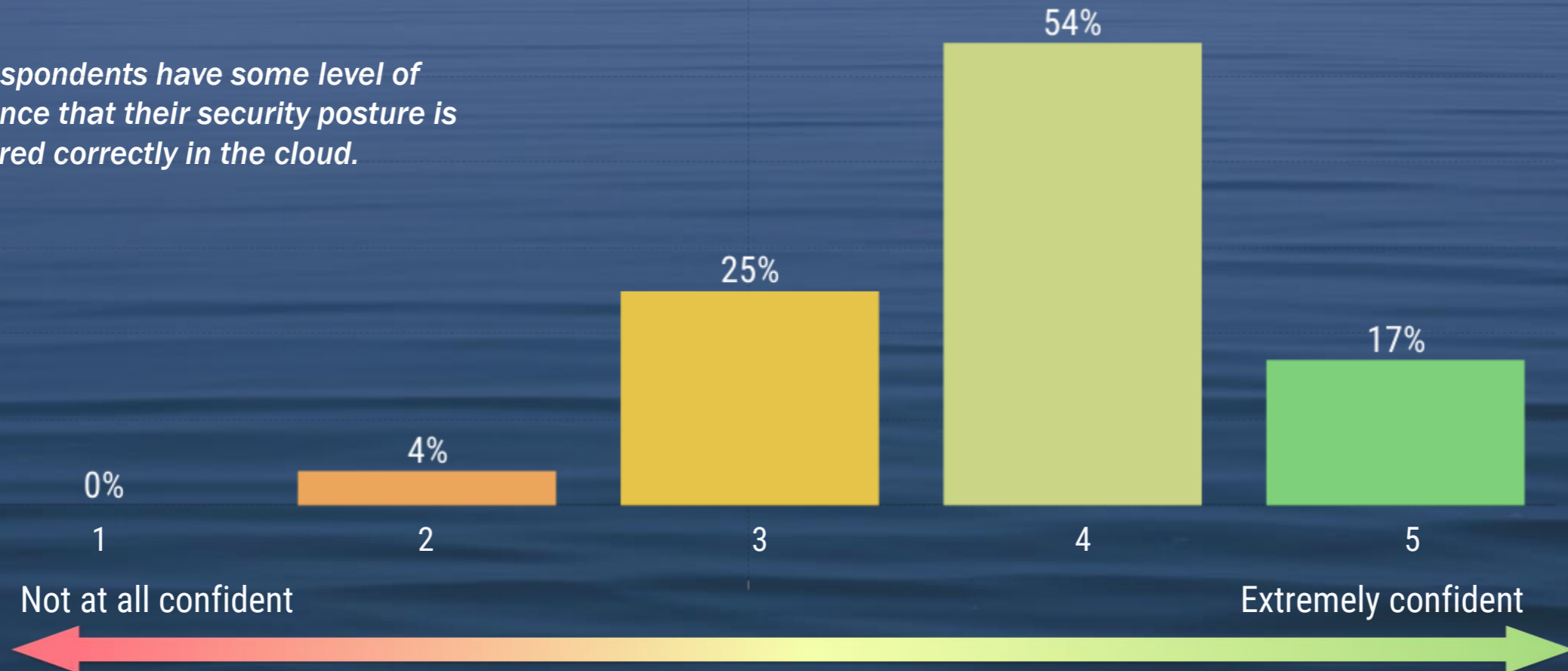


Nearly all (91%) respondents run web apps in the cloud. Two thirds run middleware/APIs, and 42% run their internal transaction apps on their cloud platform.

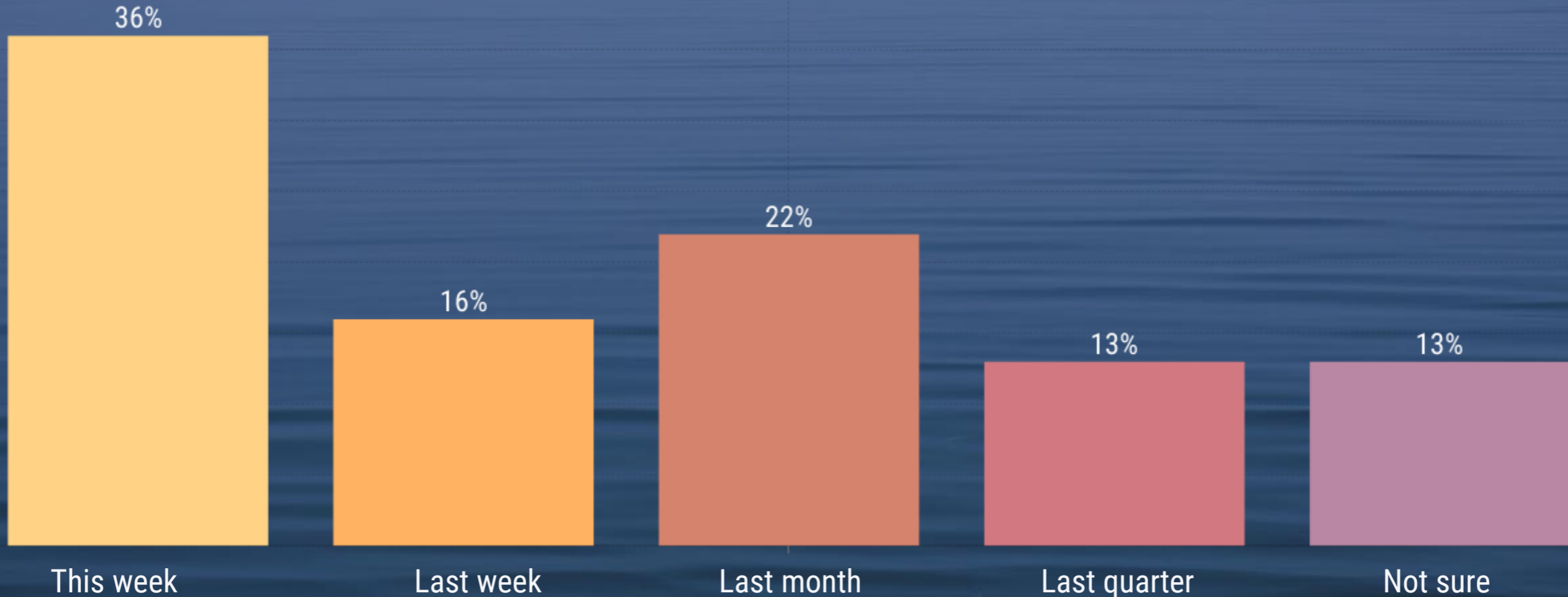
How confident are you that your security posture is configured correctly in the cloud?

(Rate 1 to 5: 1 = not at all confident, 5 = extremely confident)

Most respondents have some level of confidence that their security posture is configured correctly in the cloud.

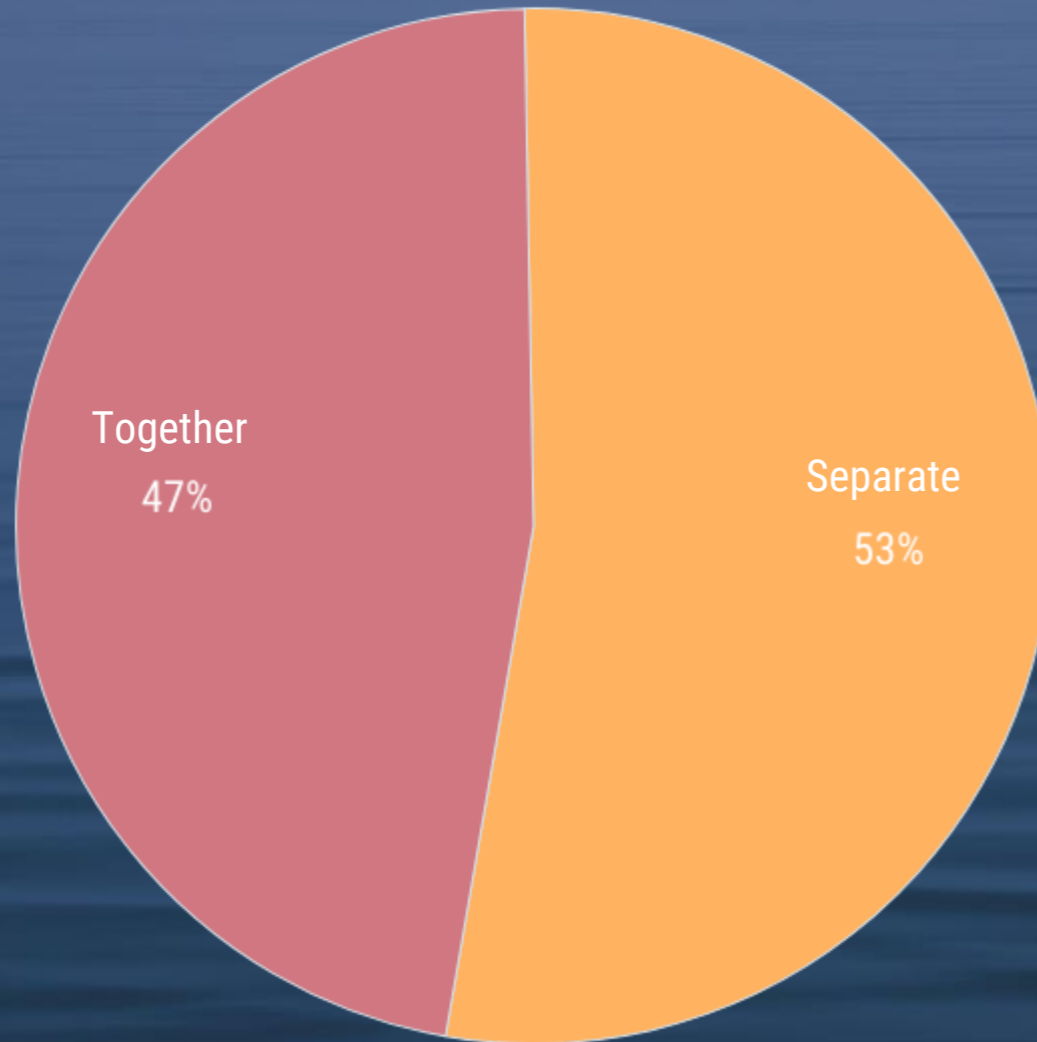


When was the last time you reviewed your cloud infrastructure for vulnerabilities and/or misconfigurations?



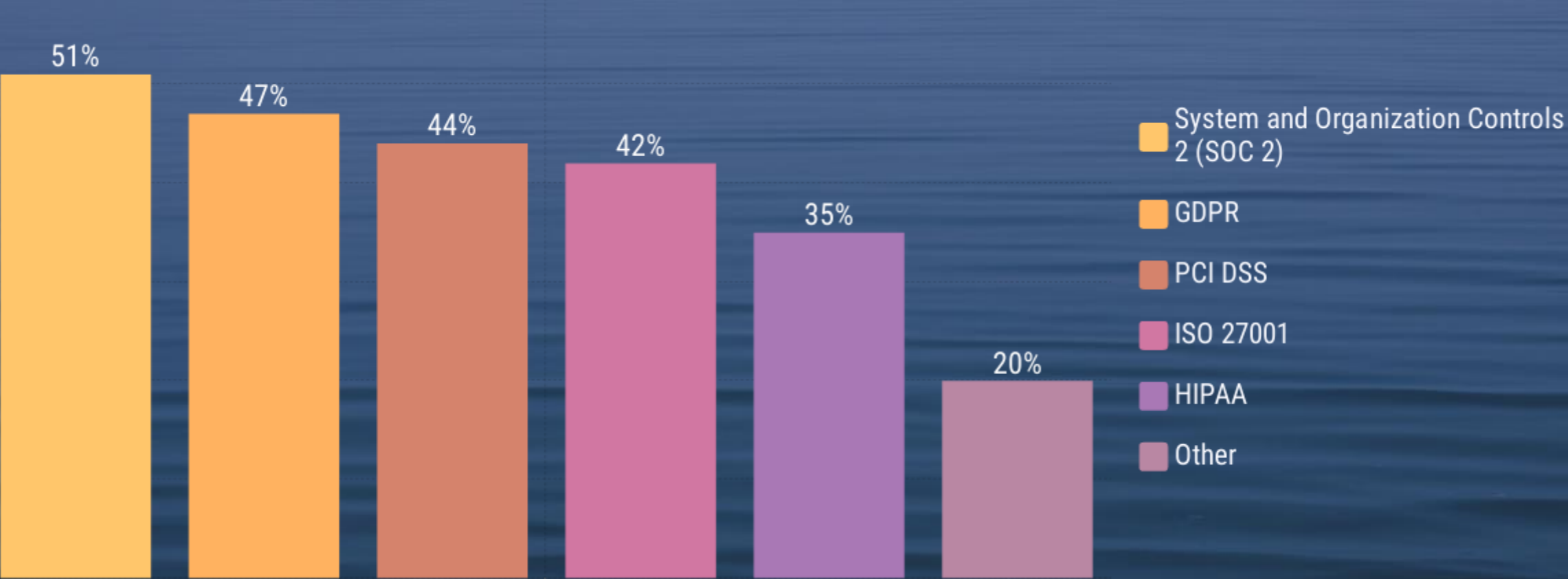
52% of respondents report having reviewed their cloud infrastructure for frailties this week or last. The rest have not performed such a review since the previous month (22%), or quarter (13%).

Are your compliance and threat teams separate or together?



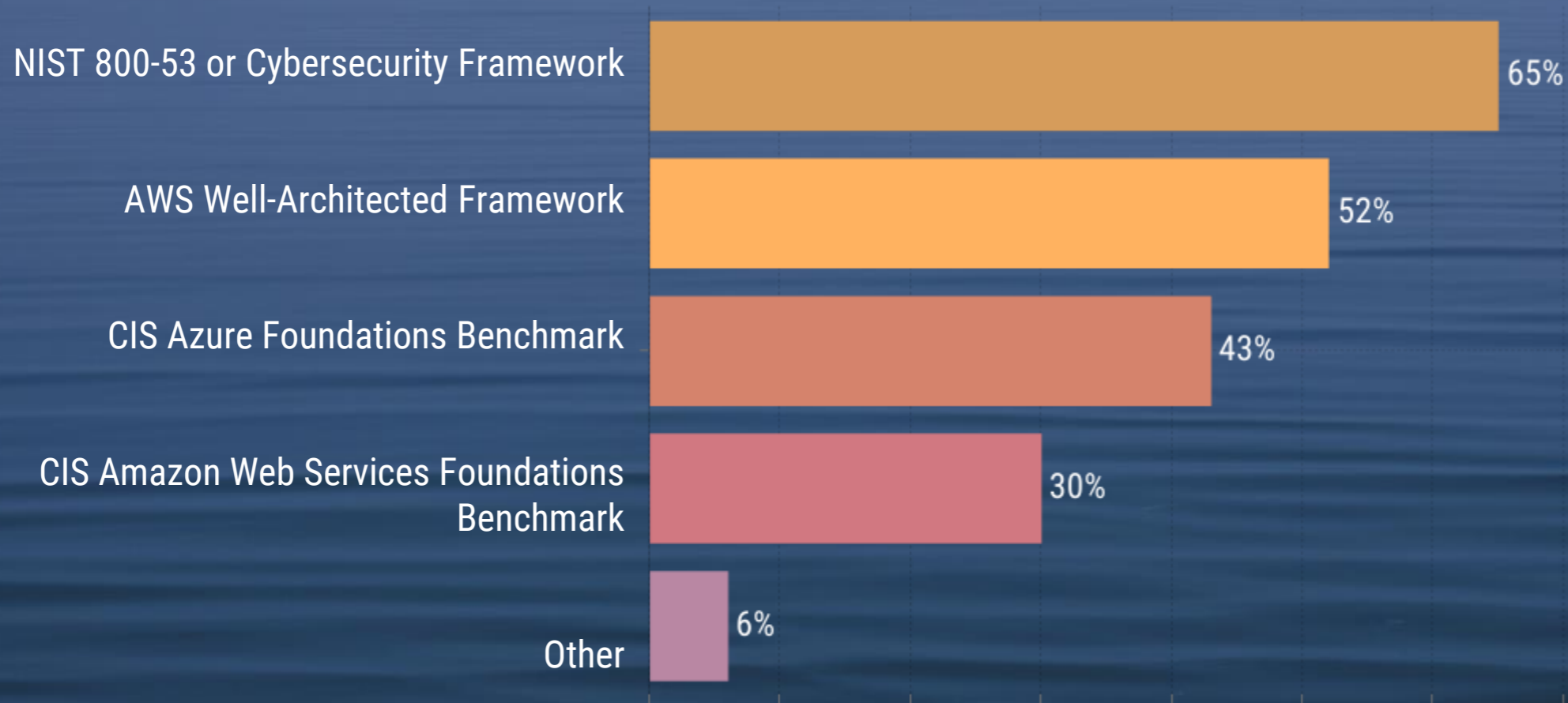
Nearly half of respondents' have a single team to manage compliance and threat, while 53% report the two teams operate separately.

Which compliance standards are relevant to your business?



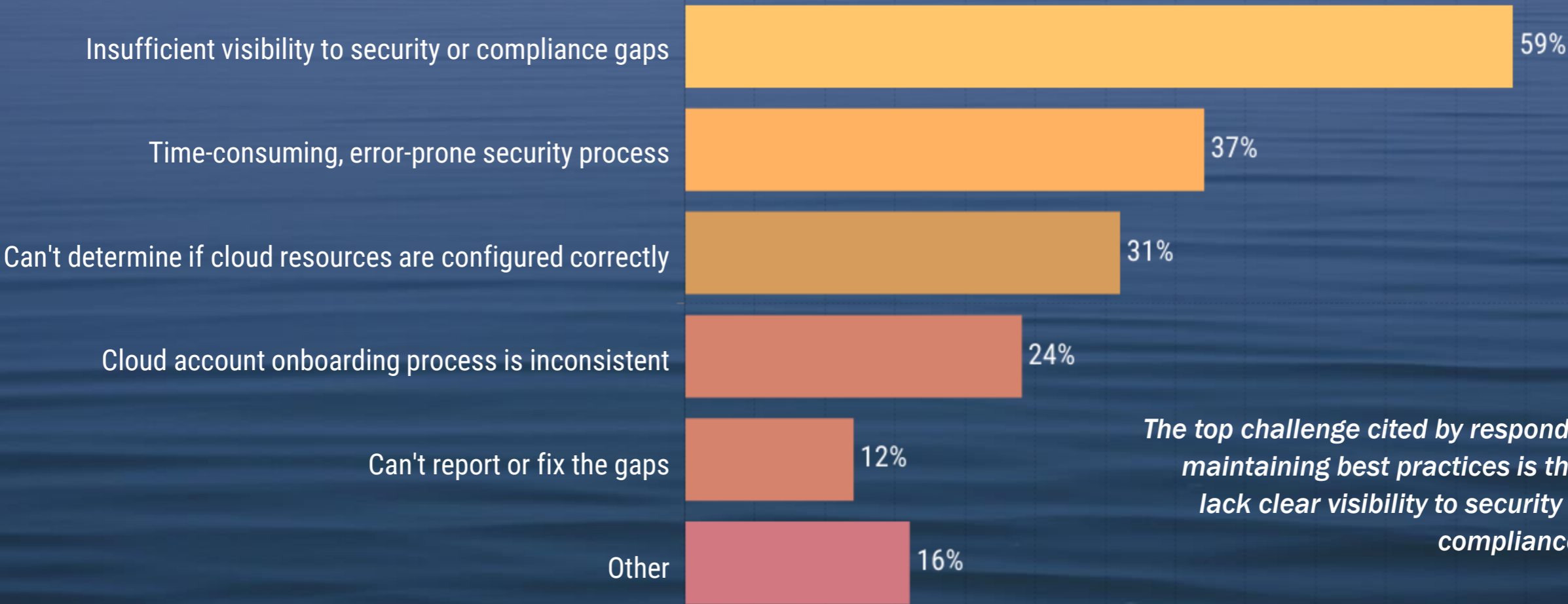
Respondents are responsible for complying with a great many standards, including 51% who comply with SOC 2, 47% complying with GDPR, 44% on PCI DSS, and 42% under ISO 27001. HIPAA is a regulatory standard for 35%.

Which frameworks are important to you?



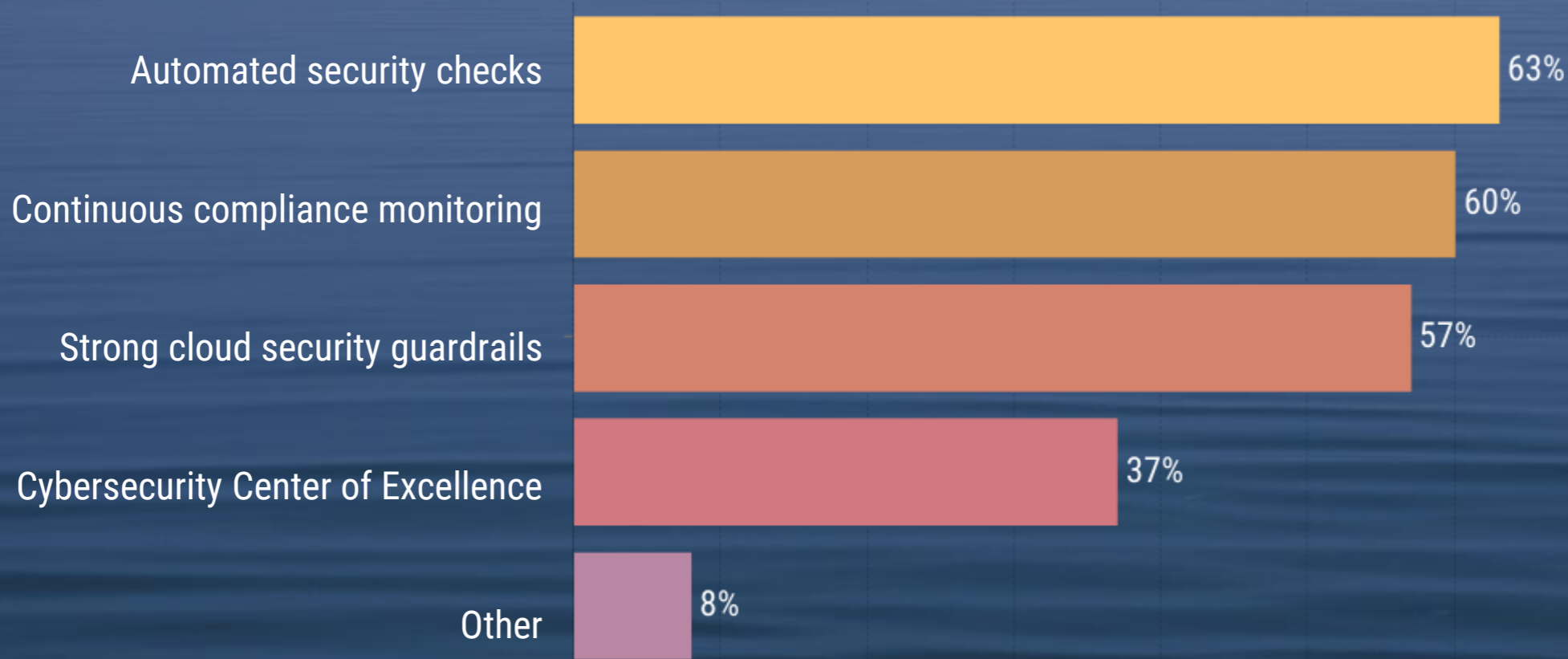
Nearly two thirds of respondents say that they are guided by NIST 800-53 or Cybersecurity Framework in developing their compliance procedures. 52% use AWS Well-Architected Framework, 43% use CIS Azure Foundations Benchmark. Fewest (30%) rely on CIS AWS Foundations Benchmark.

What are some of your challenges maintaining cloud best practices, security, and compliance?



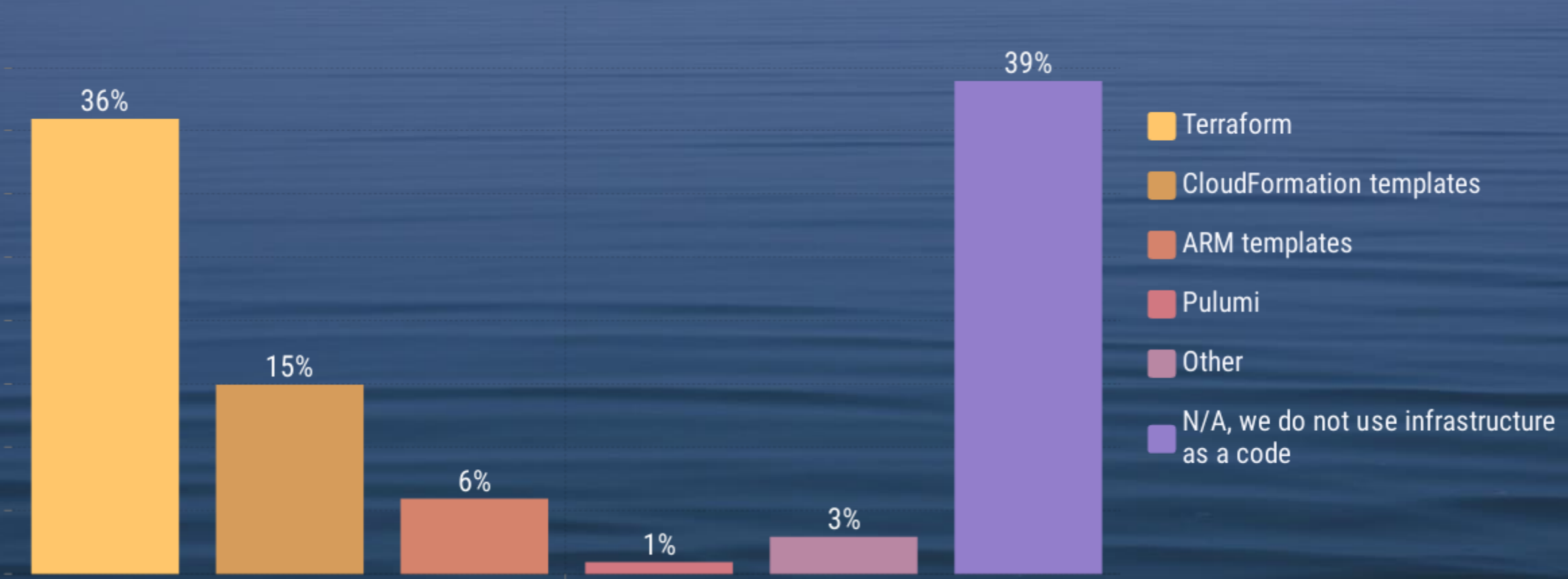
The top challenge cited by respondents to maintaining best practices is that they lack clear visibility to security and/or compliance gaps.

Would any of the following initiatives improve your compliance and security posture?



More than half of those surveyed say three initiatives that would improve their compliance and security posture are: automated security checks (say 63%), continuous compliance monitoring (60%), and strong cloud security guardrails (57%).

Which infrastructure as a code tool do you use to build your infrastructure in the cloud?



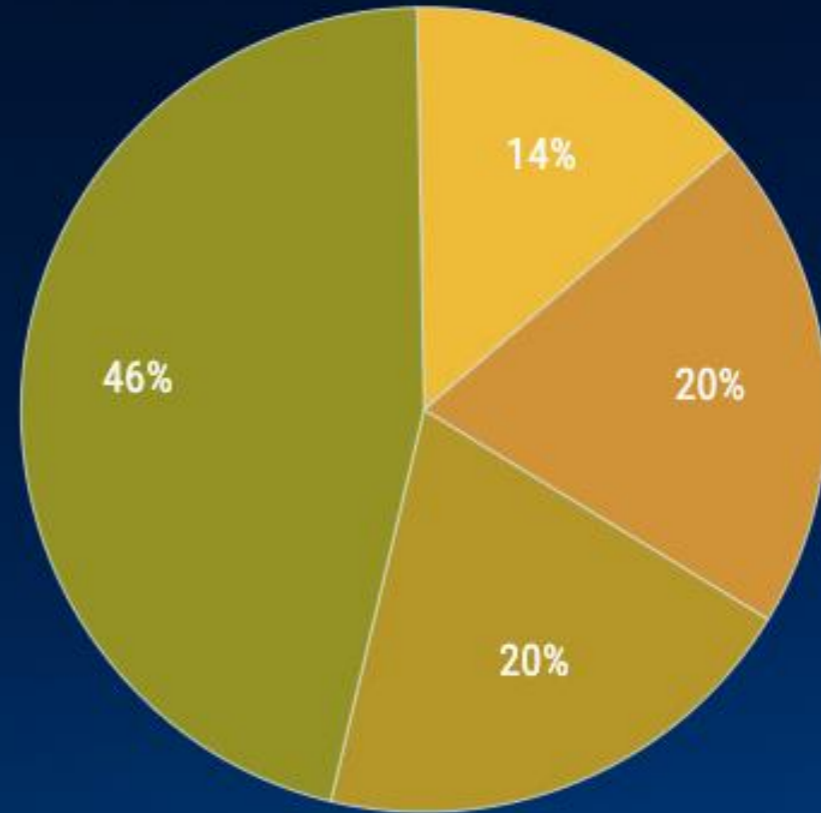
While 61% of respondents use some form of infrastructure as a code tool to build their cloud infrastructure, 39% do not use infrastructure as a code tool at all.

JOB LEVEL



54% of survey respondents hold director or executive level positions in their organization.

- CxO 14%
- VP 20%
- Director 20%
- Manager 46%





Trend Micro offers a continuous assurance tool that provides peace of mind for your cloud infrastructure, delivering support for AWS, Azure, and Google Cloud.

[Learn more at trendmicro.com](https://www.trendmicro.com)