10 Questions

Cloud Champions should ask for **Strong Cloud Governance**

The migration to the cloud is occurring faster than ever in an era of widespread remote work and increased need for speed and agility in conducting business. As enterprises move away from on-premise servers and embrace cloud computing and SaaS applications, enterprise cloud champions must account for the resulting risks and compliance hurdles. Here are 10 cloud questions that should be addressed for effective cloud governance.

CSA cloud security alliance®

ISACA®

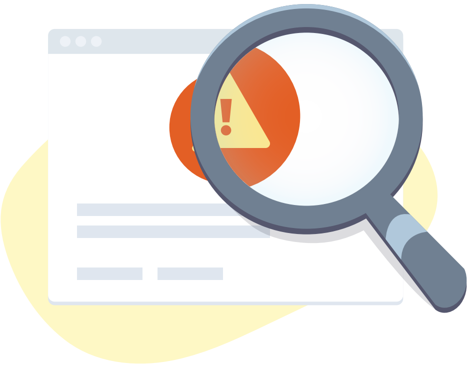
1 How can we accelerate our Move to the cloud?

Enterprises should consider going beyond the usual budgetary investments: if the management team had more resources, what could they accomplish? It might be better to invest more initially and move faster.

2 What percentage of our Business-critical applications are Currently running on the cloud?

After being told X percentage of apps are running on the cloud, a logical follow-up question for cloud champions is whether there are plans to make that total 100%. If not, why? If so, when will the last server be turned off?

CCAK™
Certificate of Cloud Auditing Knowledge
A Cloud Security Alliance® and ISACA® Credential



3

Have we done a risk assessment related to our present and future use of cloud?

Any major transition done on an aggressive timeframe poses new risks. There should be a way for management to show the board that cloud-related risks have been assessed and the appropriate mitigations have been put in place. It is also important to call out which risks, if any, exceed the organization's risk appetite.

4

Did we include a third-party supplier risk assessment in our cloud risk assessment?

Many organizations have not done so, and the recent high-profile hack involving SolarWinds surely has caught the attention of many enterprise leaders. Third-party supplier risk needs to be specifically accounted for as part of the risk assessment. Organizations can automatically assess third-party risk by using tools that block, report and warn about such risks in the CI/CD pipeline.

5

What are the key cost considerations?

In many cases, there is a cost hump organizations have to get through as they continue to operate data centers while transitioning to the cloud. Application by application, though, those servers can be turned off as cloud adoption expands. In the long haul, cloud adoption can often provide organizations with significant cost savings.

CCAK™
Certificate of Cloud Auditing Knowledge
A Cloud Security Alliance® and ISACA® Credential

6

How else are we measuring value versus risk with cloud adoption?

On the other end of the spectrum from risk is the value that organizations derive from leveraging the cloud. Management should be prepared to convey to enterprise leaders how the value comes into play by moving to the cloud at whatever level is intended, going beyond cost savings – for example, how much faster new applications can be built and how much more resilient the organization can become.

7

Have we implemented devsecops to develop and deploy cloud applications?

Migration to cloud without DevSecOps doesn't make sense. DevSecOps is the way to successfully implement cloud applications from the standpoints of both security and quality. For organizations on this path, cloud champions should ask what percentage of our CI/CD pipeline is fully automated? Does it include automated unit tests, third-party risks, integration tests, security tests, security checks and audit artifacts, and can security leaders show a simple chart reflecting the DevSecOps capability progress over time?

8

What sensitive data do we store in the cloud, and is that data subject to regulation?

Given high-impact data privacy and data governance regulations such as GDPR, PCI and HIPAA, organizations have to make sure that if they are storing data in cloud, they are taking the necessary steps to be compliant, or substantial penalties can result. Cloud champions will want to ensure their organization's cloud strategies account for the evolving regulatory landscape. Consider using encryption, obfuscation, microsharding and other techniques to address privacy needs.

9 Do we have knowledgeable cloud practitioners in place?

Any major transition done on an aggressive timeframe poses new risks. There should be a way for management to show the board that cloud-related risks have been assessed and the appropriate mitigations have been put in place. It is also important to call out which risks, if any, exceed the organization's risk appetite.

10 Have we had an independent cloud audit?

If enterprise leaders are only hearing from internal staff, they likely will not have the level of confidence needed regarding their organization's cloud procedures and implementations. Independent reviews are critical, and cloud audits performed by credentialed auditors will typically surface significant security and/or compliance shortcomings. Pentests can provide an additional, useful crosscheck, but they typically are not as thorough as an audit.

CCAK™

Certificate of Cloud Auditing Knowledge
A Cloud Security Alliance® and ISACA® Credential

Cloud auditing can give organizations a big picture understanding of thetype of cloud services and deployment strategy that would best benefit the business. The new Certificate of Cloud Auditing Knowledge, a Cloud Security Alliance and ISACA credential, prepares IT professionals to address the unique challenges of auditing the cloud, ensuring the right controls for confidentiality, integrity and accessibility, and mitigating risks and costs of audit management and non-compliance.

For more information on CCAK, visit www.cloudsecurityalliance.org/education/ccak/.