Google Cloud

Board of Directors Summary Guide to Cloud Risk Governance

Nick Godfrey, Phil Venables

Office of the CISO

Introduction

This guide is for the Boards of Directors of organizations that are engaging in a new, or substantially increased, adoption of cloud technology perhaps as part of a wider digital transformation of their business. It summarizes the key points that we address in detail in our partner paper Board of Directors Handbook for Cloud Risk Governance.

An Approach to Cloud Risk Governance

The adoption of cloud, at scale, by a large enterprise requires the orchestration of a number of significant activities, including:

- Rethinking how technology is leveraged to achieve strategic outcomes, and changing how software is designed, delivered, managed across the organization to enable those outcomes.
- Refactoring security, controls and risk governance processes to ensure that the organization stays within risk appetite and in compliance with regulation during and following the transformation.
- Implementing new organizational and operating models, enabling a broad and deep skills and capabilities uplift, and fostering the right culture for success.

As such, the organization across all lines of defense, has significant work to do. The board of directors plays a key role in overseeing and supporting management on this journey, and our partner paper is designed to provide a guide to boards in that position. In particular, we provide the top 10 questions to be asked in the boardroom, listed below and expanded on in the partner paper with supplementary points and possible red flags to watch for:

1. How is the use of cloud technology being governed within the organization? Is clear accountability assigned and is there clarity of responsibility in decision making structures?
2. How well does the use of cloud technology align with, and support, the technology and data strategy for the organization, and, ideally, the overarching business strategy, in order that the cloud approach can be tailored to achieve those right outcomes?
3. Is there a clear technical and architectural approach for the use of cloud, that incorporates the controls necessary to ensure that infrastructure and applications are deployed and maintained in a secure state?
4. Has a skills and capabilities assessment been conducted, in order to determine what investments are needed across the organization?
5. How is the organization structure and operating model evolving to both fully leverage cloud, but also to increase the likelihood of a secure and compliant adoption?

6. How are risk and control frameworks being adjusted, with an emphasis on understanding how the organization's risk profile is changing and how the organization is staying within risk appetite?
7. How are independent risk and audit functions adjusting their approach in light of the organization's adoption of cloud?
8. How are regulators and other authorities being engaged, in order to keep them informed and abreast of the organization's strategy and of the plans for the migration of specific business processes and data sets?
9. How is the organization prioritizing resourcing to enable the adoption of cloud, but also to maintain adequate focus on managing existing and legacy technologies?
10. Is the organization consuming and adopting the cloud provider's set of best practices and leveraging the lessons the cloud provider will have learned from their other customers?