

CxO Trust Newsletter - May 2022

Organizational Cloud Policy and Risk Review

Vinay Patel, CxO Trust Advisory Council & Finastra CISO

In the rush towards cloud adoption and all the benefits it offers, it can be easy to overlook the basics of cloud governance. Do you have a cloud policy or cloud security policy?

Key Policy Considerations

Organizations should consider the following when drafting a cloud policy:

- Have an executive sponsor. This is essential to enable the policy to be adopted and adhered to.
- Determine who has ultimate authority to authorize what cloud projects get the green light. This is often best accomplished with a steering committee consisting of various senior executives for different functions (eg. CIO, CISO, etc).
- Be prescriptive on the data classification and information types that are approved or not approved for migration to the cloud. Are there data residency requirements to consider?
- If the enterprise is subject to compliance with regulatory or other industry requirements, ensure this is clearly addressed. Explicit and specific mentions of application policies and controls is recommended.

Business Alignment

Ultimately, the cloud policy should strive to support the business desire/demand for cloud consumption while ensuring the security considerations are not left behind. Enterprises should strive to match both IT security requirements and the security capabilities of any cloud implementation to those of the business needs being supported.

Prior to a cloud implementation of any scale, require each project/proposal to develop a risk profile. It does not need to be overly complex. Keep it simple and request information such as data type/classification, criticality of proposed project and business impact, and technical summary and project complexity. Finally, what is the risk tolerance and/or impact due to unauthorized information disclosure or service unavailability?

These should be presented to the steering committee and carefully considered prior to a vote to proceed or defer. This is really a process that you will need to maintain in order to be able to effectively look at the risks of any cloud project. A simple risk review process combined with a decent policy are great initial steps to establishing cloud governance.

In conclusion, whilst a "policy control" and "risk review" may not seem as advanced as other technical measures, it remains fundamental to setting clear organizational expectations and requirements around cloud computing and governing its on-going usage.