Cybersecurity
Action Team

Board of Directors Handbook for Cloud Risk Governance

Nick Godfrey, Phil Venables

Google Cloud

Table of Contents

Introduction

This paper 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.

We aim to offer practical guidance, in the form of questions that can help structure your oversight of, and engagement with, management's approach to adopting cloud, and to ensure that independent risk and audit functions are appropriately equipped to support that process.

To suggest, however, that your organization's adoption of cloud is simply a new series of risks to manage would be wrong. The adoption of cloud is in many cases an increasing imperative for organizations to remain competitive and to fully realize technology, data and overarching business strategies. And, beyond that, the adoption of cloud is a significant opportunity for organizations to reimagine how whole classes of enterprise risk[1] can be better managed, and presents opportunities to tackle risks that previously would have been commercially unrealistic to fully address.

This paper will therefore provide an overview of the key tenets of cloud technology, why it is increasingly important in realizing business strategies, the risk benefits of a well-executed cloud adoption, and our guidance for Boards of Directors in their oversight of that adoption.

[1] Including operational risk, technology risk, compliance risk and strategic risk

Executive Summary

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 this 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 body of the 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?

The What and Why of Cloud

It may be tempting to think of cloud as simply 'someone else's computers' that your organization uses, instead of building and maintaining its own, and in the most primitive sense, the infrastructure that cloud providers build and operate are similar to those hosted in your organization's data centers. However, taking this view would overlook some of the fundamental differences between cloud and on-premise technology, and as such it risks obscuring the opportunities that cloud presents to an organization. Instead, think of cloud as a different way to leverage technology to drive your business strategy: one where your organization uses new technologies and methods of delivering technology, to redesign and redefine relationships with their customers, employees, and partners. At Google Cloud we use the following definition to describe such a digital transformation:

Digital transformation uses modern digital technologies—including all types of public, private, and hybrid cloud platforms—to create or modify business processes, culture, and customer experiences to meet changing business and market dynamics.

Viewed from this perspective, there is an increasing imperative for adopting a cloud-enabled digital transformation in terms of the agility, quality of product and services provided to customers, and relevance in the marketplace (particularly in industries that are prone to disruption by new technology-enabled entrants). As such not adopting cloud could result in strategic disadvantage.

Further, because cloud service providers manage data centers, networks, compute and storage as their core business, they have the capacity and capabilities to manage that infrastructure at huge scale and to extremely high standards, incorporating security capabilities that are uneconomic for companies that build their own infrastructure and data centers. As such, as we will see in the next section, far from being just a new risk to manage, cloud is an opportunity to improve a range of operational risk profiles in your organization and to focus your organization's technology resources (developers and engineers) more on improving business and customer experiences, and less on managing underlying infrastructure.

Cloud as a Means of Managing Risk

Adopting cloud technologies, and adjusting business practices, processes and operating models to fully gain from the advantages of cloud, provides organizations with an opportunity to step change their management of operational risk. For example, the following risks can be addressed and mitigated using cloud in ways that are either technically, organizationally or economically not viable with traditional on-premise technologies.

Cybersecurity

Cloud providers typically have a global scale infrastructure designed to provide security through the entire information processing lifecycle. And the sheer scale of cloud service providers (in terms of personnel, volumes of servers, extent and reach of global networks) means they are able to invest in approaches to security that are beyond[2] the technical and commercial means of most other organizations, simply because the scale drives down the unit cost of that security.

These capabilities include: pervasive, and sometimes by-default (at Google Cloud, we encrypt data at rest by default, with no action needed by the customer[3]), encryption of data; internet-scale capacity to deflect denial of service attacks; feature-rich data loss prevention technologies; the capacity to store unparalleled volumes of security logs and threat intelligence; and sophisticated tooling to manage identity and access to resources. In addition, of course, the cloud provider takes responsibility for the security of data centers, physical servers and network infrastructure, and for the patching of these environments.

[2] https://www.gartner.com/document/code/00350439

[3] https://cloud.google.com/security/encryption/default-encryption

Resilience

Cloud providers operate data centers, with advanced physical security, in locations around the world. This, coupled with the scale of these data centers (the volumes of servers they hold for example), and the abstraction of physical technology from customer applications, means that customers of cloud providers benefit from layers of 'built in' resilience: In effect, the customer is shielded from the effects of component failures (e.g. server hardware failure), data center infrastructure events (such as power failures), all the way up to country-wide events (such as severe weather). Of course, organizations need to architecture their applications to take advantage of these inherent resilience properties.[4]

In addition to this technical resilience, a broader operational resilience can be achieved using a multi-cloud approach. Specifically, by leveraging two or more cloud providers (or an on-premise capability to supplement a single cloud provider - how we define hybrid cloud), organizations can leverage open-source based technologies and management and control planes to build exit strategies to mitigate various scenarios and to meet the requirements of regulators in some industries.[5]

[4] https://cloud.google.com/architecture/scalable-and-resilient-apps

[5] https://cloud.google.com/blog/topics/hybrid-cloud/idc-whitepaper-assesses-multicloud-as-risk-mitigation-strategy

Technology risk

Many organizations are at an inflection point regarding their technology. In the 50 or so years since large organizations started using Mainframes, trillions of dollars has been invested in largely on-premise, self-managed technology. Historically, this meant organizations building their own data centers, global networks, managing hundreds of thousands of servers and PCs, and writing proprietary applications. Enterprises, and their customers now expect to be able to access digitized products and services at any time, through a range of channels. And, as we as a sector have seen, the complexities of achieving this on top of existing technologies can result in significant technical and operational failures.

So there are compelling arguments for a strategic overhaul of the technology used by many organizations. However the costs, and timescales, involved with refactoring existing technologies using the traditional methods of delivering IT (on premise and/or using traditional outsourcing models) are such that it is unlikely to be an achievable strategy for most organizations. In part this is because the traditional models involve the organization managing, as we have discussed, everything from the data center upwards.

By migrating to cloud, organizations can ensure that their technology teams are focussed on delivering high-quality services and experiences to customers, and not on operating foundational technologies, and materially reduce their Technology Risk profile as a consequence. For example:

- Operate above the infrastructure. By migrating to cloud, they no longer have to dedicate resources to managing data centers, physical servers and network equipment, nor do they have to worry about patching or maintaining core operating systems.
- Use cloud to reduce technical debt. Even if a given application is not going to be fully modernized - perhaps it will be demised in the foreseeable future - organizations can reduce the technical debt associated (e.g. unsupported hardware or operating system) with it by migrating it into a container image that runs in the cloud.

Cloud Security and Control Characteristics

The mechanisms used to secure and control cloud technologies can be substantially different to those used for on-premise technologies. Given that, it is important that your organization's control functions re-evaluate relevant key controls: even if the objectives behind existing controls are still valid, the specifics of the control, and the approach to managing it, will often need to evolve in order that the original control objective is still met in a cloud environment. In fact, using cloud native controls instead of relying on existing controls will often produce better outcomes because they are designed with cloud in mind.

Shared fate, not shared responsibility

One of the most substantial differences between cloud service provider technologies and on premise technology is that there is a new party involved in the successful operation of key controls (the cloud service provider). Historically, and typically, this arrangement is defined as a 'shared responsibility' and often depicted as shown here:

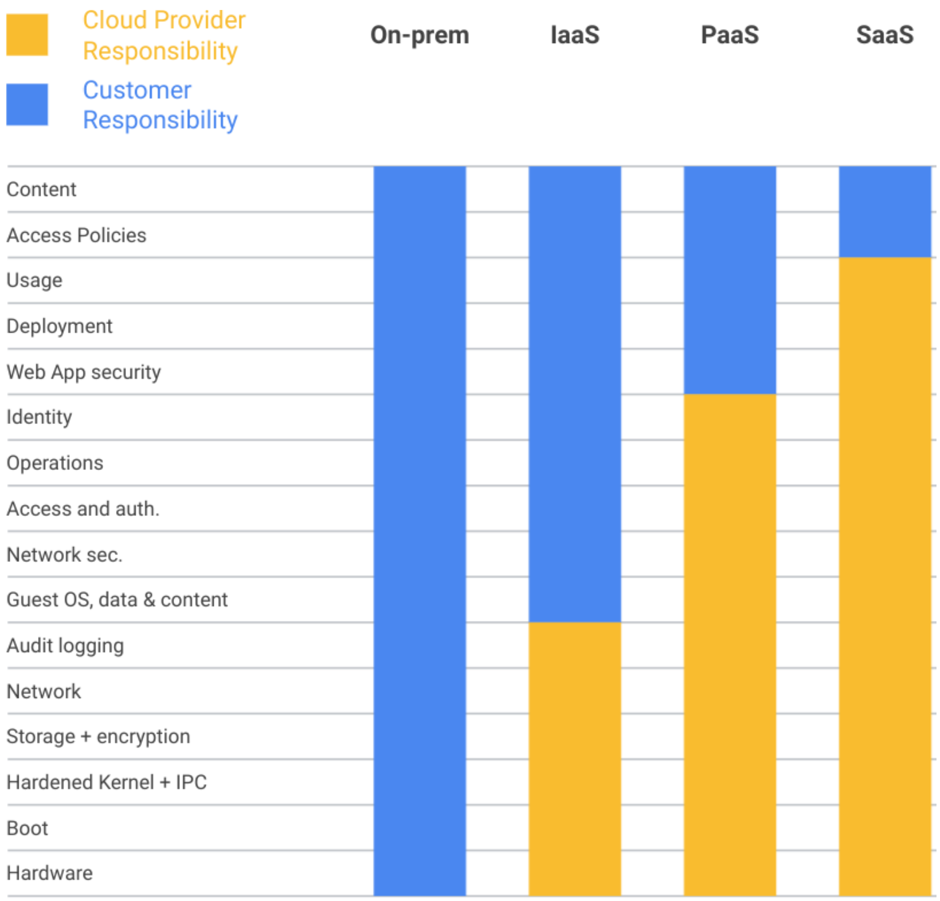


Figure 1. Your responsibilities and your cloud service provider's responsibilities under the cloud shared-responsibility model.

However, getting security right in the cloud can be challenging, and the shared responsibility model implies that customers are responsible for building effective cloud security programs on their own. Specifically, the shared responsibility model for security that has underpinned cloud computing since its earliest days dictates that the cloud provider is responsible for securing the underlying foundation, while the customer is responsible for secure configuration, data protection, access permissions and much more. The result is that enterprises have viewed the cloud as a risk to be managed instead of a platform for managing risk.

Instead, we believe the term 'shared fate' better describes the relationship between Google Cloud and our customers and how in practice the job of securing the cloud requires a partnership. As part of this approach, your technology and security teams will have access to tooling and solutions, provided by Google Cloud, that are designed to simplify the processes of building and maintaining a secure cloud environment. This includes solutions that encapsulate our opinion on how best to implement Google Cloud securely, including landing zones, blueprints and secure by default products.

How control design evolves

In addition to not having direct responsibility for all technology controls, as described above, the nature of the controls your organization does still have responsibility for, evolves. That's because the use of cloud technologies will likely introduce a level of agility, speed and automation that is rarely the case with traditional technologies. Cloud also offers the opportunity to increase the quality, completeness and transparency of controls, and your organization's control owners will be considering the following:

- Cloud native vs existing controls. The nature of cloud technology is such that control approaches that are generally unachievable with on premise technologies, like encryption by default, are now available. Using these cloud native approaches will generally yield better results because they are designed with cloud in mind.

- Embedding policy and controls into code and automation. Cloud technologies can be deployed and managed using code interacting with APIs provided by the cloud provider. And when you manage the cloud in this way, you can integrate your policies and controls directly in the code, making them central to both your company's development process and to any software that your company develops.

- Data-driven control assurance. Leveraging the fact that all cloud technology is declared and discoverable in data, to build data-driven assurance processes that validate that the deployed infrastructure and software is continuously meeting control requirements.

How control ownership evolves

Control owners, often referred to as the first line of defense, such as information security managers, technology managers, and the businesses, will undergo substantial changes in terms of how they fulfill their responsibilities in the cloud world. As we described in our complementary paper, *Risk Governance of Digital Transformation in the Cloud* [6], the following are patterns you may see:

- Operating and organizational models. Many conventional controls associated with the safe operation of IT and changes to business processes leverage central teams of specialists, who will validate or test the work of other teams prior to implementation. This is often the case, for example, with security teams that conduct penetration tests of systems prior to their release. In a cloud world, such models may introduce unwanted delay because of the process handoffs and thus the most effective operating model for certain controls may in fact be where the execution of those controls is federated through the wider organization.
- Increase in control telemetry for better oversight. As control owners move from a model of central ownership of control processes ("confidence through organizational hierarchy"), to one where the control is operated in a far more federated manner, their approach to overseeing the control has to change too. In this model, the control owner focuses on establishing the correct design and implementation of the control, and then on the ongoing assurance of the control's efficacy through observing it in data ("confidence through control observability").

[6] https://services.google.com/fh/files/misc/risk-governance-of-digital-transformation.pdf

Managing control transitions

In the majority of cases the adoption of cloud represents the introduction of a new technology alongside the existing (probably on-premise) environment. And whilst, as we have described above, there is every reason to embrace the new cloud environments with new approaches to control, it is obviously critically important to maintain the existing controls on the on-premise technologies and associated business processes.

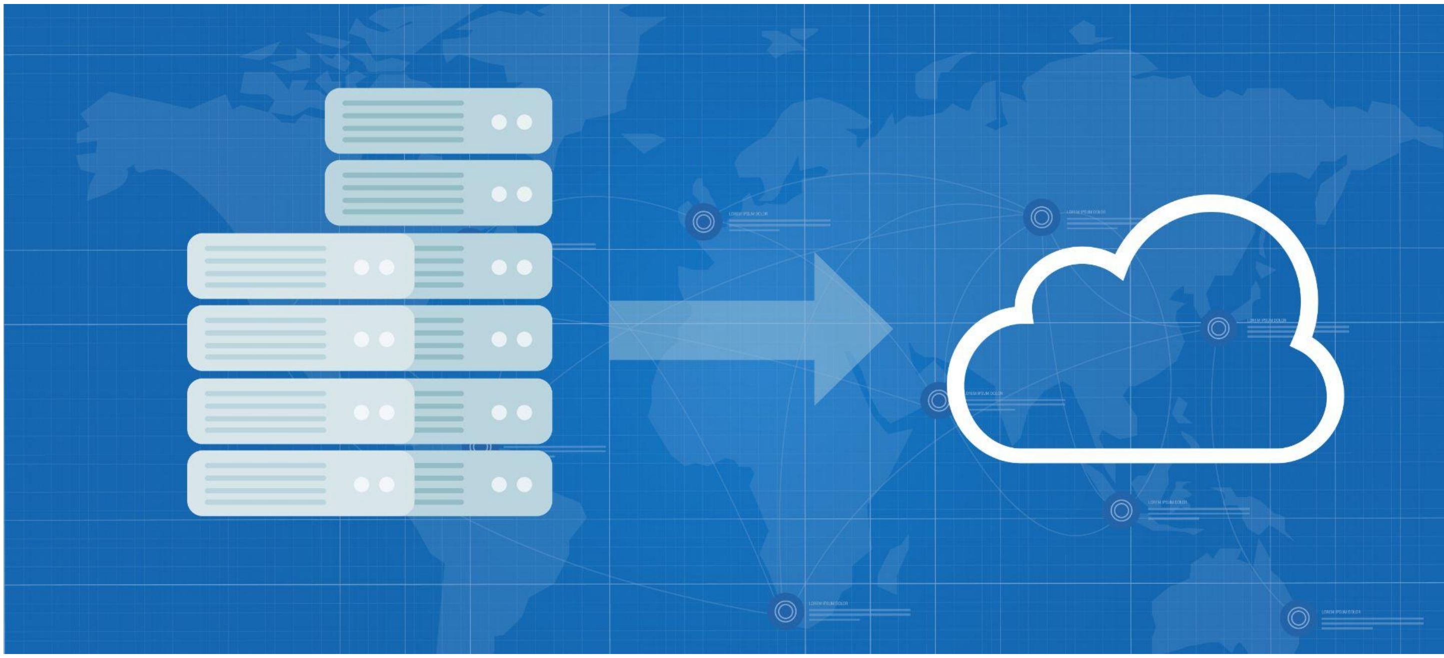
Establishing Cloud Risk Governance

In the preceding section we described some of the common characteristics of cloud security and controls, and how that might cause an adjustment of an organization's control framework. In addition to this specific set of (mostly technical) decisions and activities, it is critical that the organization establishes a comprehensive approach to governing the adoption of cloud: in the same way that controls need to evolve for the effective management of cloud, so does the organization's broader risk and governance apparatus.

The good news is that there is a logical starting point from which to build effective governance for cloud: your organization likely already has sophisticated mechanisms for governing IT, data, systems and other related risks, and in the end (when the majority of IT and data is in the cloud), your cloud governance is in fact your IT, data and systems governance.

Your organization's Independent Risk Management (IRM) function, in partnership with the first line of defense (control owners, IT management, lines of business), and the compliance and audit functions, should ensure that the transformation of those governance structures is consistent with the guidance in this section. The topics covered in this here are described in significantly more detail in our complementary paper, *Risk Governance of Digital Transformation in the Cloud* [7]

[7] https://services.google.com/fh/files/misc/risk-governance-of-digital-transformation.pdf



Adopting a phased approach

A cloud migration that is undertaken without sufficient planning to ensure the technology, security and other teams involved are well-prepared and supported can bring both security and execution risk. However, attempting to define the end state of the various security, control, risk management and governance apparati, too early in the program, will likely be unsuccessful. Instead the IRM function, in partnership with the wider organization, should think of a phased approach by maturing constantly as the work progresses.

In other words, your organization can't reasonably hold back all work until perfect readiness is in place, but similarly you can't reasonably endorse proceeding with no initial planning and governance being in place. We suggest there are four phases, although of course your organization may adopt a different approach to phasing or incrementing its program.

- Set the cornerstones: establishing a common understanding and the key principles that will shape the intent and approach of the organization's transformation over time.
- Manage the initial phases: implementing structures and apparatus that allow the organization to safely conduct initial migrations to the cloud. These may include higher levels of manual checks and formal governance to mitigate the fact that controls may not all be fully matured at this stage.
- Mature and accelerate: adjusting control and governance structures to enable accelerated adoption of cloud, by increasing control rigor and oversight, and right-sizing governance in parallel.
- The new steady state: adapting to broad usage by embedding cloud into all relevant risk programs and governance, and by implementing processes to maintain currency with cloud best practice.

Governance structures

- Program governance. An overall transformation program oversight group/committee and a program office with the relevant executive (business, technology and controls) leadership oversight.

- Risk governance. A forum to ensure that risk management and governance is acting as a check and balance to the program governance and there is sufficient time allocated to fulfill this oversight.

- Project governance. A mechanism to define the approved patterns available to applications teams seeking to deploy into the cloud, and measures to track adherence to these and other requirements. It's important that this is a streamlined process where the only roadblocks are those where teams, for whatever reason, have chosen to step away from the standard approach and tooling.

Skills, organization and culture

At its heart, despite being facilitated by the adoption of different technologies, a digital transformation is fundamentally about people, organizational structures, processes, procedures and "the way in which things are done". Therefore, addressing these aspects as a high priority and as an integral part of the governance process is critical to success. Your organization should be focussed on the following, at least:

- Training and skills development. A comprehensive and sustained training plan tailored for all staff to develop deeper expertise in cloud technologies, but specifically for security and other significant aspects of risk mitigation. There should be provisions made to ensure that a significant portion of the training is on the specific policy and architecture choices the organization has made. This may initially be limited to certain core teams, but over time should be deployed pervasively to all relevant teams, and integrated into core training curricula.

- Organizational models. In addition to changes to formal organizational models, as described preceding sections, your company may wish to adopt more flexible operating constructs, where virtual teams work across boundaries with a focus on the product mission and less on organizational hierarchy and traditional decision making processes. Strategically this is likely to be important, and to help accelerate the overall program. To succeed, management needs to ensure that these teams are empowered and equipped to make decisions quickly and to commit resources, but with the right guardrails to drive discipline in the process.

- Culture. Enabling this broad and deep transformation, including the re-skilling of large parts of the organization, and encouraging an innovative approach, needs to be a key focus area for management, from the top down. Specifically, reflecting the degree of change, and the unease that might create, you should look to ensure management are implementing approaches and leading with behaviors that fosters a culture that is supportive of these new ways of working, and provides physiological safety to give their people confidence to adapt, try new things, positively challenge each other and management, and learn from the inevitable mistakes (which, with the right structures - such as the guardrails we have described - will be of limited consequence to the organization as a whole and so tolerable at that level.)

Adjusting and right-sizing controls

As discussed in earlier sections of this paper, the nature, operation and ownership of controls needs to evolve as part of a cloud transformation. The following, in particular, should be focus areas for the organization.

- Cloud technology and security architecture governance. There should be explicit policies, standards and frameworks for how cloud deployments are undertaken and how they are adhered to. Initially, this may address a subset of the requirements and on the decisions needed to enable initial usage of the cloud in a controlled manner, using the governance described above. Over time, these policies and frameworks can be extended and matured as the organization gains experience if using cloud

- Software development lifecycle maturity. It is hard to take advantage and sustain the security risk mitigation capabilities of the cloud without also progressively modernizing the software development lifecycle. You should expect management to explicitly determine how technology and business units are preparing for that and question if expertise from cloud providers or other external organizations is not being actively used.

The compliance program for cloud

The compliance organization, which in most industries is responsible for ensuring the organization's compliance with internal and external policies, standards, regulations and laws, has a significant role to play in partnership with the risk function and the first line of defense. The exact delineation between an organization's risk and compliance functions will vary from company to company, but, regardless, the overall set of activities remains consistent and the Board should look to the compliance function to fulfill the following:Assessing regulations, standards, and laws that relate to the organization's use of the cloud, including regulations that are specific to the cloud[8].

- Ensuring ongoing compliance with the requirements stemming from regulation by baking them into the policies, standards, frameworks and governance apparatus.

- Engaging with relevant regulators and supervisors, and overseeing the methodology and processes used to notify (or seek approval from) regulators at key junctures.

- Adjusting aspects of the compliance program as the use of cloud matures, including the regulation monitoring and horizon-scanning regime.

[8] https://cloud.google.com/security/compliance

The audit program for cloud

The Internal Audit function plays a critical and independent role to assess and provide assurance that an organization's approach to managing risks and controls, and its governance of those, is effective. As with all other functions described in this paper, Internal Audit is therefore a key component of an organization's safe and secure cloud digital transformation, at all phases. And, as with the other functions, it is likely that some amount of adjustment to the audit program will be warranted. The Board should ensure that the following have been taken into consideration as part of that:

- Assessing and adjusting the audit universe. Does the set of auditable components sufficiently reflect the risks associated with the organization's cloud transformation? Does the audit coverage cycle need to be adjusted to ensure that audits of the cloud transformation are timely and reflective of the broader strategic journey and key milestones?

- Approaches to cloud audits. As we have discussed in this paper, the nature of public cloud technologies is such that management, and the risk function, will adopt approaches to control and risk management that differ to those used to manage much of a traditional technology environment. For similar reasons, the audit function should consider how to adjust certain aspects of the audit process in order to ensure relevancy and completeness, and to take advantage of the different approaches to audit that cloud affords.

- Auditing the cloud service provider. Reflecting that, in all cloud delivery models, the cloud provider maintains significant responsibilities for risks that your organization is ultimately accountable for, such as physical security of the cloud service provider data centers, you should ensure that a comprehensive approach to auditing the provider is implemented.

Communicating with the board

In a wider transformation, or even in a tactical use of cloud services for specific projects it is important to keep the Board of Directors informed, or one of the Board Committees such as Audit or Risk. Technology, security and lines of business should communicate to the Board and the organization's risk and audit functions should provide independent perspectives on the degree of controls and adherence to risk tolerances in the context of those initiatives. That risk tolerance should include a strong perspective on whether there is sufficient funding / resources being allocated to sustain ongoing risk management once new business activities have been launched, projects completed or transitions have taken place.

Board Oversight

In the following section, we outline the top 10 questions that we think would provide the structure for an effective and meaningful discussion on cloud between the Board of Directors and management. The methods through which those questions can be explored, and the underlying topics tested, are the subject of this section.

Additionally, you should consider whether the Board has sufficient expertise on a broad array of technology risks, but specifically related to information and cybersecurity as well as the risks and opportunities of digital transformation in the cloud, and that the composition and remit of the various Board committees is optimized to manage these risks. You may wish to take advantage of opportunities to provide training and educational sessions to the Board, and introduce the use of expert advisors to the Board.

As always, focus on risk

As we've said, cloud computing requires a different approach to managing technology than that typically used to manage on-premise technology, and one that incorporates changes to people, process and technology. Given that, it would be tempting to think that the Board needs to dive into a bottomless pit of technology, complexity, and terminology. But, actually, the best approach is to use the tried and tested methods Boards deploy to oversee complexity and change in their organizations. Whether or not the organization is adopting cloud in a manner that the Board are comfortable with could be summarized as follows:

> "What are the most significant risks to our most critical assets and business services, what controls mitigate those risks and who is continuously assessing whether those controls are in place and effective? What residual risks remain and who at what level of the organization deemed those acceptable with what compensating factors or risk transference? What executive management group regularly monitors the measured outcome of this process?"[9]

The *Top 10* questions that follow provide context-specific ways of probing the key points addressed here, and how to gauge whether the answers to these points are satisfactory and in line with risk appetite as the organization's cloud transformation is executed over time.

[9] https://www.philvenables.com/post/cybersecurity-and-the-board-a-fresh-perspective

Conduct incident reviews and drills

This can align with scenario development, but one of the best means of engagement for Boards is to use cloud-related internal incidents, close-calls or incidents that have occurred at other organizations to run through a learning exercise vs. your organization's controls and use that to stimulate any need for improvement. The latter of these, incidents that have occured at other organizations is a particularly important approach bearing in mind your organization's limited experience of cloud to date, and of course, there are plenty of historical incidents that are in the public domain that can be used to quickly build up this approach.

Test through scenarios

Focus on building a library of scenarios, some of which could be quite severe, and build a narrative around how such scenarios would be prevented, detected, responded to, or recovered from. Use these scenarios as a means to overlay specific metrics and then drive improvements in controls to get those metrics closer to a defined target. A scenario based approach is also an opportunity to do some more plausible "value at risk" form of financial impact analysis using a variety of methodologies. Remember, financially oriented metrics tend to only be meaningful in the context of scenarios. Good scenario selection (vs. your potential risk universe), scenario building and validation are important, but are difficult without the right skilled personnel - so get help.

Top 10 Questions to Ask in the Boardroom

Drawing together the various topics described in this paper, we have identified 10 questions that we believe would help a board of directors in a structured, meaningful discussion with their organization and its approach to cloud. We've included additional points with each, as examples of what a good approach could look like, and potential red flags (🚩) that might indicate all is not well with the program.

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?**

   a. Are program and project governance structures suitably balanced with risk governance structures? For example, for a given cloud use case ("class of workload"), is there a clear mechanism for ensuring that the appropriate controls and governance of that use case are in place?

   > 🚩 The volumes or severity of risk acceptances related to deviation from the agreed controls approach are trending in the wrong direction.

   b. Is the adoption being structured in phases, reflecting that lessons will be learned, and maturity increased following initial adoptions, and are there clear criteria for the transition between phases focused on the balance of control maturity vs governance methods? For example, in early phases you should expect to see a more deliberate and explicit set of approvals for a release, reflecting lower maturity of controls (less automation, more manual checking, for example).

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 ?**

   a. What problem is the use of cloud technology looking to solve, and/or which opportunities is it designed to unlock. For example, is cloud being adopted to facilitate a data center exit strategy, to enable a modernisation of IT, or to enable a wider digital transformation?

   > 🚩 The organization is adopting cloud without a clear articulation of the intended outcomes, or the outcomes are too varied to be collectively achievable.

   b. What is the vendor strategy for cloud adoption (i.e. single, multi cloud, hybrid cloud) and how does that strategy demonstrably satisfy the overarching technology and data strategy, and ensure organization's ability to maintain compliance to regulation and to stay within risk appetite?

c. Is the use of cloud, and the underpinning strategies, also focused on ensuring the organization will benefit from the operational risk benefits that can be achieved with cloud? Cloud is a means to manage risk as much as it is a set of new risks to manage. For example, is the adoption of cloud being considered as a means of addressing security or resilience risks that previously were partially accepted for commercial or practical reasons?

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?**

a. Has the organization's security policy (and other policies) been integrated into the mechanisms used to configure cloud infrastructure, such that it is deployed in a secure by default state? For example, has the organization developed the capabilities and skills necessary to manage 'Infrastructure as Code' so that policies can be embedded and strongly change-managed?

> 🚩 In the later, mature, phases of adoption, the organization is still highly dependent on the use of a console or other mechanisms for manual configuration of the cloud.

b. Are segregations of duties between the cloud infrastructure function and application teams implemented, such that key organizational policies and configurations cannot be undone? For example, are key identity and network policies enforced centrally rather than being dependent on the actions of application teams?

c. Are there well-defined "class of workloads" patterns that provide curated and pre-configured combinations of cloud technologies to development teams that are secure by default? How are new patterns, or changes to patterns, approved?

> 🚩 Significant numbers of applications that use a unique combination of cloud products are being deployed by development teams.

d. How are security and other control checks integrated into the software delivery mechanism (the "CI/CD pipeline"), such that the default and easy path for developers is also the secure path?

> 🚩 High volumes of cases where standard delivery mechanisms are bypassed, indicate development team tooling or experience issues.

e. How are post deployment changes of critical configurations detected, and what response and remedial processes are in place to correct them in a timely manner? For example, does the CISO organization have the capability to independently verify that the 'as deployed' environment is consistent with the intended configurations and policy?

> 🚩 Repeating patterns of configuration deviation indicate a flaw in architecture, deployment or operation models.

4. **Has a skills and capabilities assessment been conducted, in order to determine what investments are needed across the organization?**

a. Did the assessment include key control and risk functions (for example, CISO, risk functions, compliance, audit, legal) in addition to the core technology teams? For example, as described in our risk governance in the cloud paper[10], the independent risk management function will likely need to adjust a range of the core processes and risk oversight methodologies to be effective for cloud.

> 🚩 New and changed roles in control functions are not sufficiently defined to enable a comprehensive skills gap assessment.

b. Is there a structured training program for staff, and is it appropriately tailored to ensure that the organization's principles, approach to cloud, policies and operating models are included in addition to generic cloud provider content?

> 🚩 Training is only being taken by core cloud teams, instead of a structured approach to train all relevant developers, engineers and security specialists.

5. **How is the organization structure and operating model evolving to both fully leverage cloud to benefit customers, partners and employees, but also to increase the likelihood of a secure and compliant adoption?**

a. What adjustments, in particular, are being made in the organizations and operating models associated with implementing and overseeing key controls? For example, how is the CISO and security operating model evolving to enable more "agile" delivery of IT whilst staying within risk appetite, and to provide assurance over key controls in a more dynamic technology environment.

b. How is the IT organization progressively modernizing the software development lifecycle in order that security and risk advantages of cloud can be fully leveraged at sustained? For example, are software developers equipped with the right tooling and processes such that security is baked in? What percentage of the organization's software is continuously built, tested and deployed?

[10] https://services.google.com/fh/files/misc/risk-governance-of-digital-transformation.pdf

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?**

    a. How are existing controls being evaluated for the relevance and efficacy in managing risk in cloud technologies? For example, are the control objectives being used to determine what the appropriate control is, instead of assuming that the existing control is sufficient.

    b. How are risks and impacts being adjusted in the organizational risk maps and how are these being reflected in scenario-based and other forms of risk assessment and oversight? For example, how has the Risk and Control Self Assessment been adjusted to ensure the right focus, to reflect shifts in responsibilities and changes in organizational models?

    c. How are procurement processes generally, and third party risk management practices being updated to ensure relevance to the cloud and alignment with industry best practices? For example, are processes associated with billing reflective of the consumption-based financial model of cloud use, vs other forms of traditional IT?

7. **How are independent risk and audit functions adjusting their approach in light of the organization's adoption of cloud?**

    a. Has the audit universe been adjusted as necessary to reflect the different risk profiles associated with cloud, and the change in the relative inherent risk profile of the organization? Has the approach to auditing the cloud transformation program incorporated the need to be timely in conducting assessments given the iterative approach to maturing controls and governance that we recommend is taken?

    b. What is the approach to auditing the cloud service provider? For example, with what frequency will these be conducted, who will participate to ensure appropriate expertise, and has consideration been given to engaging in pooled audits with peer organizations?

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?**

    a. What feedback is the organization receiving from regulators, and how is that informing our approach to cloud adoption?

    b. How is the organization staying abreast with new and emerging policy makers thinking in respect of cloud computing, and adjusting with that over time?

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?**

    a. Are control functions (like the CISO) sufficiently resourced to be able to adequately maintain both control environments?

    > 🚩 Resourcing levels for key control functions, assuming all other things are equal, are flat.

    b. Are governance mechanisms allocating time and resources appropriately reflecting the continued need for risk management of these existing environments?

    > 🚩 Metrics and other key indicators provided to the Board show a deterioration of key controls on legacy systems

    c. Have clear criteria been established to determine how changes to the resource allocations will be identified and implemented?

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?**

    a. This should include the use of best practices for technical configuration and usage patterns, but should also include deep engagements on non-technical aspects such as organizational models, operating models, process and governance re-factoring. Is the organization implementing a structured methodology to work through these aspects with subject matter experts at the cloud provider?

    b. This should also incorporate the fact that cloud service providers regularly enhance and update their security and compliance features and products, and so be viewed as an ongoing exercise versus a one-time effort.

> 🚩 Updates to the organization's workload patterns, and core security configurations, lag excessively behind the currently available offerings.

Conclusion

We believe that a well-executed migration to cloud based technologies is a real opportunity for organizations to achieve a net reduction in many types of operational risk. And as this paper has outlined, there are significant drivers behind an organization's desire to digitally transform. The Board of Directors play a significant role in overseeing the safe adoption of cloud, and in championing its use to achieve strategic organizational goals. We believe that the following questions, used through the traditional Board lenses of risk, scenario testing and incident reviews, will help ensure that the most important aspects are considered.

01
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?

02
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?

03
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?

04
Has a skills and capabilities assessment been conducted, in order to determine what investments are needed across the organization?

05
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

06
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?

07
How are independent risk and audit functions adjusting their approach in light of the organization's adoption of cloud?

08
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?

09
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?