Google Cloud

# Risk Governance of Digital Transformation in the Cloud

A Guide for Chief Risk Officers, Chief Compliance Officers and Heads of Internal Audit

Office of the CISO

# Table of contents



***Disclaimer:*** *The content contained herein is correct as of April 2021, and represents the status quo as of the time it was written. Google Cloud's security policies and systems may change going forward, as we continually improve protection for our customers.*

# Introduction

This paper is for Chief Risk Officers, Chief Compliance Officers, Heads of Internal Audit and their teams, embedded risk functions and governance committees. This guidance is important not only for those organizations that are embarking on the use of cloud computing, perhaps in support of a broader digital transformation of the organization, but also for those who are looking to sustain and expand their use of cloud computing.

Ensuring the safe adoption of cloud computing is becoming an increasing priority for these functions, reflecting the significant benefits that an organization can accrue from a digital transformation in terms of agility, quality of product and services provided to customers, and relevance in the marketplace.

And, whilst it is true that a safe adoption of cloud computing requires an adjustment to the risk, compliance and audit practices, we shouldn't assume that the use of cloud computing simply means there is more risk to manage or that it will result in a net increase in risk. Adopting cloud computing technologies and services presents the organization with substantial opportunities to address many forms of operational risk in new, innovative and more substantial ways. Done right, adopting cloud can improve your organization's operational risk and resilience profile[1]. And in fact, not adopting cloud services could result in strategic disadvantage, both in terms of digital innovation, and by being unable to access security and resilience capabilities that are increasingly uneconomic in on-premise approaches.

Adopting cloud computing technologies and services presents the organization with substantial opportunities to address many forms of operational risk in new, innovative and more substantial ways.

This paper, then, aims to help you achieve those benefits, by guiding you through the transformational activities that will be taking place within your organization, and what in turn those mean for your functions and their own transformations and how to best position your risk, compliance and audit programs for success in the cloud.

[1] https://services.google.com/fh/files/misc/google_cloud_operational_resilience_fin_serv.pdf

# Executive Summary

This paper is structured to describe the nature of a cloud-based digital transformation and the different considerations and approaches that will be required across the three lines of defense[2] to enable such a transformation whilst keeping your organization secure and protected. There are many detailed considerations for each of the functions involved in a successful transformation, however we suggest that the following principles, adopted in four core phases, should be your guide and reference when navigating the journey.

***Set the cornerstones: establish a common understanding and the key principles that will shape the intent and approach of the organization's transformation over time.***

1. **Build a common understanding.** A successful digital transformation requires the orchestration of organizational, cultural, technical and procedural changes. A common and shared understanding of terminology and approaches provides a reference model for those involved in planning and executing across all lines of defense.

2. **Think long term, but act iteratively.** Mature your risk and control approach as you go. Delaying your digital transformation to build "perfection" from day 1 is unlikely to be practical but also can be ill-advised from a risk perspective as engagement and maturing through learning will yield a better process in the long run.

3. **Prioritize organizational readiness.** Ensure that assessing and enhancing capabilities and skills, and implementing the right organizational structures and operating models are prioritized. Initially this may take the form of dedicated teams, but longer term will require a more holistic approach.

4. **Implement dedicated, but integrated, governance.** Establish an overall transformation program oversight approach (e.g., council or committee) and a program office with the relevant leadership oversight. Ensure your technology, operational and security risk governance is acting as a check and balance to the program governance.

***Manage the initial phases: implement structures and apparatus that allow the organization to safely conduct initial migrations to the cloud.***

5. **Define initial minimum security and configuration standards.** Make sure security and other configuration standards, and principles, are developed and updated in light of new work. There

[2] The Three Lines of Defense in Effective Risk Management and Control, Institute of Internal Auditors, 2013

should be a clear definition of the minimum standards that apply to given classes of workload (based on criticality of data or business service) during the initial phases.

6. **Define initial risk and compliance oversight.** Establish initial risk monitoring frameworks and constantly iterate based on experience and learning - these should include specific metrics and associated thresholds or limits. Leverage independent expertise and testing to validate designs and projects, particularly in initial phases.

7. **Communicate with boards and regulators.** The first line of defense should proactively demonstrate to the board of directors, and separately to regulators, that the organization has the appropriate risk management in place. Risk, compliance and audit functions should provide an independent perspective on the degree of controls and adherence to risk tolerances.

8. **Training and skills development.** Make sure that the organization has a comprehensive training plan tailored for all staff to develop deeper expertise in cloud technologies, to ensure the safe future transition of responsibility and execution from small dedicated teams to the wider organization.

***Mature and accelerate: adjust control and governance structures to enable accelerated adoption of cloud, by increasing control rigor and oversight, and right-sizing governance in parallel.***

9. **Develop comprehensive security and configuration standards.** Require that there are explicit policies, standards and frameworks for how cloud deployments are to be undertaken and how such standards are to be adhered to. This should enable 'classes of workloads' to be developed and deployed, rather than just single projects.

10. **Modernize IT delivery.** Determine how technology and business units are preparing to progressively modernize the software development life cycle in order to take advantage of, and sustain, the security risk mitigation capabilities of the cloud. Embed the security and configuration standards into the life cycle and its tooling.

11. **Mainstream risk oversight.** Update risk and control taxonomies (risks, controls, impacts) to reflect the organization's maturing use of the cloud. Adjust oversight processes, such as Risk and Control Self Assessment, in particular to take account of changed responsibility and accountability models, including those of the cloud provider.

12. **Extend continuous control monitoring.** When deploying technology in the cloud more of your controls can be expressed as code or otherwise systematized. Leverage this property of cloud to continuously monitor key controls, to assure the controls remain deployed, active where expected and performing in line with stated objectives.

***The new steady state: adapt to broad usage by embedding cloud into all relevant risk programs and governance, and by implementing processes to maintain currency with cloud best practice.***

13. **Interconnect cloud with other risk programs.** Oversee adjustments in connected risk programs, for example in third-party risk assessment and resilience programs, to reflect the use of cloud by the organization to deliver technology, but also to take advantage of reduced risk and increased transparency in cloud services.

14. **Drive continuous improvement cycles.** Measure the organization's ability to continuously improve. Are controls continuously monitored, leveraging the systematic technology and security controls of cloud? Are architectures periodically enhanced, to enable controls that were previously deemed unworkable? Are new cloud provider features being used?

15. **Stay current with cloud best practices, and constantly revalidate assumptions.** Adjust regulatory and standards monitoring regimes in order to identify and respond to changes to external cloud requirements and best practices. Amend scenario planning processes designed to examine tail risks in light of these, and as your organization's use of cloud evolves.

16. **Manage legacy in parallel.** Ensure that the risk and governance apparatus continues to focus appropriately on existing technology, and that decision making regarding maintenance, upgrades and other day-to-day management is consistent with the ongoing safe operation of legacy systems.

# Digital Transformation Decoded

It's a commonly used term, and has become particularly prominent over the past few years, but what are the key components of a digital transformation, how do they relate to the use of cloud technologies, and why are so many organizations pursuing this?

## Definition of digital transformation

Digital transformation is when an organization takes advantage of new technologies to redesign and redefine relationships with their customers, employees, and partners. Digital transformation for business covers everything from modernizing applications and creating new business models to building new products and services for customers. At Google Cloud we use the following definition:

> *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*.[3]

However it is defined, it is important to realize that digital transformation drives how an organization operates, optimizes internal resources, and delivers value to customers.

## Benefits of a digital transformation

Digital transformation is what propels businesses and industries forward. Organizations of all sizes—from startups to global enterprises—choose digital transformation not only to make scaled improvements, but also to drive significant change and fully embrace the digital age. It requires a strong commitment from both businesses and IT teams, as well as a willingness to support the resulting changes.

The journey to digital transformation includes the following benefits:

- Flexible technology to build, deploy, and manage applications more quickly in the cloud
- Experimentation to embrace new ideas and gain new insights on customer demands
- Measurement of experimentation results with data analysis to guide decision-making
- Collaboration across organizational boundaries with tools for quick knowledge sharing
- Customer focus and data analysis to deliver greater value to customers
- Agility to scale and accelerate without hesitation to succeed in the digital age
- An opportunity to reduce operational risk and increase operational resilience[4]

---

[3] https://cloud.google.com/learn/what-is-digital-transformation
[4] https://services.google.com/fh/files/misc/google_cloud_operational_resilience_fin_serv.pdf

# How a Digital Transformation is Executed

A successful transformation will involve changes to many parts of the organization. In order to understand how those changes affect the approach to controls, risk oversight, compliance to regulation, and audit, it's useful to understand not only *how* they will change, but also *why* those changes will be implemented.

As we will see, the common theme behind the changes that are made is that the traditional life cycle of understanding customers' needs, designing business product and services to meet them, and delivering IT and applications to support those products and services, is too cumbersome to keep up with the pace at which customer expectations change in the modern world. Improving the speed and responsiveness of that life cycle is key to how an organization changes to effect a digital transformation.

## Business product and service delivery

In order to respond to the expectations of customers, and market sentiment, it is increasingly critical to adopt business processes that are as agile as the changes in the outside world. Conventional models of product or service development, including fully-specified and detailed requirements that are tested with deep market research, long lead-time IT delivery of the new technology and applications that support that new product or service, and big-bang launches to the market, are increasingly likely to result in that product or service arriving too late. That's simply because in the background the expectations of customers had shifted prior to launch. In sectors where technically able digital-native entrants are active this is increasingly the case.

To address this, businesses that execute a digital transformation will often seek to use a far more iterative approach to the delivery of products and services: the fast creation of a minimum viable product with which to test the market, the sophisticated use of data to measure the effectiveness of the approach on an ongoing basis, and the quick iteration of the product using that feedback loop. This speed and agility allows for more timely adjustments to respond to customer sentiment, and it also means that the cost of failure from a misstep or idea that didn't pan out as expected, is significantly reduced compared to the cost of failure associated with traditional means of delivering new products.

To achieve that agility, and to unlock that innovation, businesses will increasingly adopt more flexible organizational constructs, where virtual teams work across organizational boundaries with a focus on the product mission and less on organizational hierarchy and traditional decision making processes. To succeed, these teams need to be empowered and equipped to make decisions quickly and to commit resources, but with the right guardrails to drive discipline in the process. To that end, one of the most important things to recognize is that a digital transformation requires significant commitment to addressing the people aspects, including fostering a culture that is supportive of this new way of working.

## Technology delivery and change

One of the key organizations that will work in the virtualized way described above is the IT team. In digital businesses, the ability to translate the business's desire for increasingly iterative product development is clearly highly dependent on the delivery of IT being able to keep pace with that.

To achieve this pace, most IT organizations will adopt the following practices, as further described in our first paper in this series "A CISO's Guide to Cloud Security Transformation"[5]:

- **Use of cloud technologies.** Adopting a cloud-led IT strategy is a key enabler in the wider execution of a digital transformation. It allows IT teams to focus on delivering value-adding functionality to business applications, instead of managing data centers, networks and physical servers. It also provides a greatly enhanced ability to provision, and scale, the infrastructure technologies (such as virtual servers) that underpin the applications. Servers can be provisioned, and storage added, at the click of a button (or the execution of script) rather than the days or weeks lead time often associated with provisioning on-premise technology.

- **Accelerated application delivery.** Developing and deploying in the cloud can significantly reduce the time between releases, often creating a continuous, iterative release cycle. The shift to this development process, whether it's called Agile, DevOps or something else is possible in part due to the ability to better lifecycle manage the creation, testing and deployment of software into the environment, by building automated mechanisms to manage and control that process and dedicated, cloud-based, test environments that ensure that changes to production environments are successful and safe.

The speed of change to the technology environment that emerges by adopting these practices could be viewed as a significant risk when viewed through the lens of traditional IT change management and security practices. However, as we will explore in the following sections, cloud technologies offer the opportunity to radically enhance the approach to IT control management, by reducing the amount of human and manual interaction, embedding organizational IT and security policy into the automation that manages the environment, and leveraging the declarative nature of cloud to perform high-fidelity controls assurance at scale and with velocity.

[5] https://services.google.com/fh/files/misc/ciso-guide-to-security-transformation.pdf

# How the Control Environment Evolves for Cloud

Just as the approach to business product and service delivery and IT management will change in a cloud transformation, so must the approach to managing the associated operational risks and their mitigating 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.

## Designing effective controls in a cloud world

An effective control, for any type of technology or business process, is highly contextualized to that specific technology or process: the properties of the control tend to reflect the properties of the technology or process that it is designed for. Manual business processes tend to be overseen by largely manual controls that are often retrospective in nature, for example.

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.

Given that, it is important to think about what makes an effective control in a cloud world, where there is a level of agility, speed and automation that is rarely the case with traditional technologies. Additionally, you no longer have responsibility for all of the controls associated with managing technology (although clearly you retain overall accountability). When designing controls for the cloud world consider the following:

- **Cloud native versus existing controls.** The nature of cloud technology is such that control approaches that are generally unachievable with on premise technologies, like encryption by default and zero-trust architectures are now available. Using these cloud native approaches will generally yield better results because they are designed with cloud in mind. And, in many cases, seeking to overlay native controls with existing legacy controls (like firewall devices) will create a complex and incoherent control environment that may in fact create more fragility.

- **Embedding policy and controls into code and automation.** When servers, racks, and data centers are managed for you in the cloud, your code becomes your infrastructure. And when you deploy infrastructure as code, 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. Remember though, that not all controls will work this way, and so you should still ensure that controls that cannot be embedded are otherwise sufficiently managed.

- **Data-driven control assurance.** Leverage 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. These changes are a necessity when you consider the ways in which control environments have to change in order to both adopt cloud safely, and to fully leverage the benefits of cloud, as described in the preceding sections. The following, in particular, are patterns of change that 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 undermine some of the benefits of a digital transformation. As we discuss in our CISO transformation paper, 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”). Of course, the correct design and implementation of the control should ensure that the telemetry emitted can be trusted.

## 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. To achieve the right focus, consider the following:

- What is the balance of resourcing between the functions focused on cloud, and those focused on maintaining the existing infrastructure?
- Are the mechanisms used to govern each appropriately sized and robust, or is the newness of cloud commanding all of the attention?
- Are employees not directly involved in the cloud migration kept informed, and are they clear about their future roles and responsibilities so that they remain motivated?
- Does the cloud migration strategy identify the milestones where the relative investment priorities of cloud versus on premise resourcing should be re-examined?

# The Risk Program for Cloud

In the preceding section we outlined ways in which the control environment, and control owners in the first line of defense, could change in order to best manage the risks of using cloud, and to do so in a way that also ensures the organization can fully benefit from the opportunities it creates.

This section, and the subsequent sections for Chief Compliance Officers and Heads of Internal Audit, explores the consequences of those changes on the methods and practices they can take to discharge their responsibilities, and to leverage useful features of cloud-based technologies when doing so.

Every industry/sector has different constructs for the second line of defense, or independent risk management (IRM). In some industries such as financial services it is a standard practice to have an independent risk management organization under a Chief Risk Officer reporting to the board of directors. Other industries, particularly large organizations, have an Enterprise Risk Management team that fulfills this role, reporting to the board, CEO, CFO or other senior role. In all of these cases the role of that team is the same, to ensure that the organization's operations are conducted within acceptable risk tolerances or risk appetite.

As an organization digitally transforms itself, the IRM function needs to adapt to manage risks to ensure appropriate caution and safety in such transformation. However, it also needs to create the environment to permit increased business agility and innovation to avoid significant strategic risk. Faster adoption can also contribute to other risk mitigation as cloud services can also improve both security and resilience.

There are a number of areas to focus on which will be covered in the following sections, which address:

- Making sure the wider organization has the right capabilities (skills and resources) to effect a risk-managed cloud transformation - this includes the IRM function itself

- Adapting the risk management apparatus to the new reality, including governance, frameworks and monitoring

- Establishing continuous risk monitoring to ensure that in a faster moving environment risk tolerances are sustained and risk frameworks are sufficiency adaptive.

## Assessing organizational readiness

A cloud migration can result in significant risk reduction, from security improvements to increased operational resilience. Additionally, the wider business benefits that stem from the broader digital transformation can have significant business unit specific risk reduction as other controls are improved or made more pervasive.

However, 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. The key steps for the IRM function here are to assess and improve upon this level of readiness, often by maturing constantly as the work progresses. In other words, you 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. Such steps include:

- **Program governance.** Establish an overall transformation program oversight group/committee and a program office with the relevant executive (business, technology and controls) leadership oversight. For example, as part of the overall governance of the use of cloud, your organization might build a cloud center of excellence[6].

- **Risk governance.** Ensure your risk management governance is acting as a check and balance to the Program Governance and there is sufficient time allocated to fulfill this oversight. Note: for your early stage deployments and migrations consider a more explicit "Go, Flight"[7] approach where control teams need to *explicitly declare ready* as opposed to assuming silence means ready. Over time, positive confirmation of readiness can be reverted back to a more exception driven approach.

- **Project governance.** Each project will need to be well managed and under the control of the Program Governance framework and its approval process. 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. A project's secure path should be the fast path by default.

- **Training and skills development.** Make sure that the organization has 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.

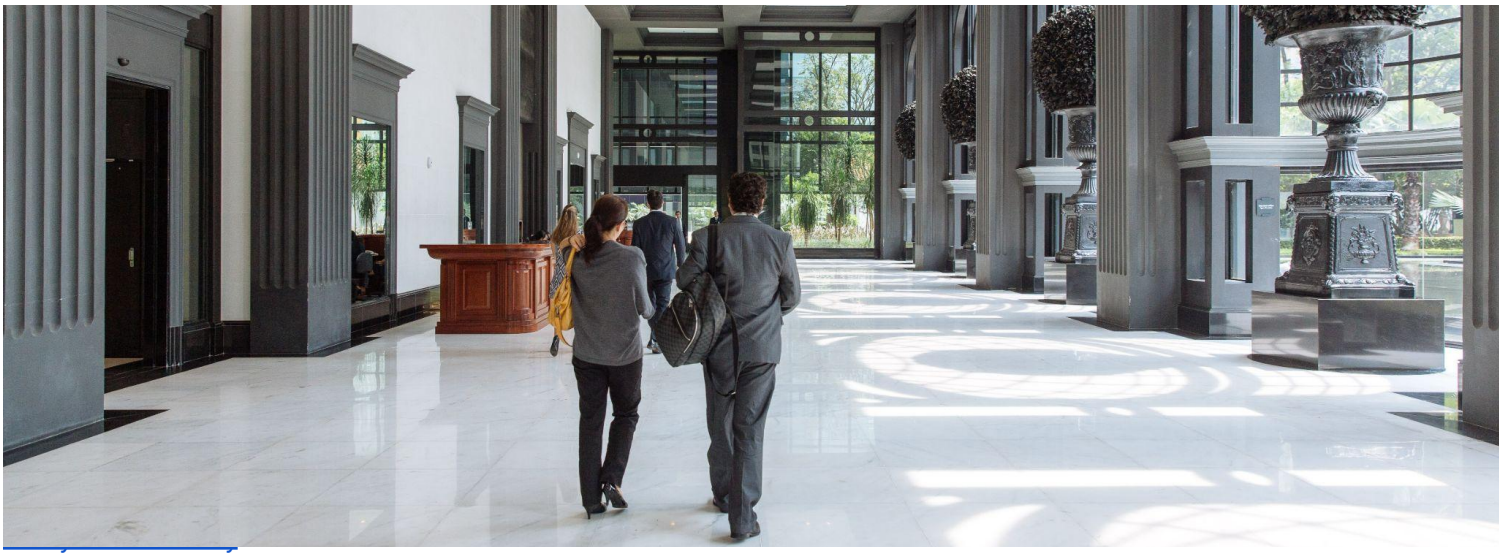
- **Cloud technology and security architecture governance.** Require that there are explicit policies, standards and frameworks for how cloud deployments are to be undertaken and how they are to be adhered to. Initially, this may address a subset of the requirements and on the decisions

[6] https://services.google.com/fh/files/misc/cloud_center_of_excellence.pdf
[7] https://history.nasa.gov/afj/ap11fj/01launch.html

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 in using cloud.

> *The IRM function should get a satisfactory answer to at least these four questions, and recognize that these questions will need to be periodically re-asked, and answered in detail, as the transformation evolves:*
>
> - *"Do our control standards sufficiently mitigate our anticipated risks?"*
> - *"Does our deployment conform to those standards?"*
> - *How quickly are we adopting new security features that the cloud provider enables or releases?*
> - *"What, if any, cloud provider or other industry standard security recommendations and secure defaults have been relaxed and why?"*

- **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. The IRM function should 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. As part of this, ensure that the organization is considering the security of its software supply chain[8].
- **Test or retest existing processes.** Examine current processes built for the on-premise environment and determine what adjustments are planned, including: incident detection and response, inventory and asset discovery, security penetration testing, independent security reviews, and validate the teams or providers for these processes have evidenced skills and experience in cloud environments.



## Enhancing skills and capabilities in the IRM function

As well as ensuring the wider organization has the right skills to get the most out of digital transformation and cloud transition, in a risk managed way, it is also important that the IRM function itself has the necessary skills to provide oversight and independent challenge.

Each organization, of course, is best positioned to determine the specific mix of skills it needs in each function. However, there may be challenges if an IRM function attempts to staff and sustain people with engineering skills that are exact peers with their technology colleagues. It is not only difficult to attract engineering professionals into non-engineering roles but even if they were hired it would be hard to sustain the right depth of activity needed for them to maintain those skills - this will result in churn.

Rather, a better approach is often to have people that have a reasonable depth of understanding of modern technology environments, in particular cloud, coupled with security and technology risk management experience. These people, who may well have been technology leaders in prior roles, will be able to define the right risk frameworks, oversight approaches and ask sufficiently challenging, but informed, questions that can exercise the first line teams. These roles, or team, can be periodically augmented with more in-depth skills either by rotating in first line staff or, more likely, engaging specialist consultants for targeted reviews.

## 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 IRM function should provide an independent perspective 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.

Additionally, the IRM function should ensure the board has developed a reasonable degree of 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. This might range from organizing educational briefings for the board, advising on board composition so as to ensure the right skills and experience mix at the board level as well as making available trusted external advisors that the board can use directly to augment their expertise.

## Establishing and aligning risk frameworks and tolerances

Having assessed and prepared the organization for transformation and transition, including the IRM function itself, it is important to establish new or adjust existing risk frameworks and tolerances. These should be in line with the new ways in which business, technology and security will be managed. There are many drivers for this, ranging from the increased rate of business and technology change, the changing nature of digitized business processes through to the new security and resilience mitigants.

First, consider which risks need to be reexamined in the context of cloud which will include at least the following:

- **Cybersecurity.** Continuously adjusting key controls, people, processes and technology to prevent, detect and react to external threats and malicious insiders.
- **Pandemics.** Sustaining business operations in scenarios where people cannot, or will not, work in close proximity to colleagues and customers.
- **Environmental and infrastructure.** Designing and locating facilities to mitigate the effects of localised weather and infrastructure events, and to be resilient to physical attacks.
- **Geopolitical.** Understanding and managing risks associated with geographic and political boundaries between intragroup and third-party dependencies.
- **Third-party risk.** Managing supply chain risk, and in particular of critical outsourced functions by addressing vendor lock in, survivability and portability.
- **Technology risk.** Designing and operating technology services to provide the required levels of availability, capacity, performance, quality and functionality.

Second, look at the points in your IRM or wider business/technology risk process that might need to be adjusted, or at least reviewed to ensure they are still valid in the new context:

- Update risk and control taxonomies where new risk types, causal factors, impacts, control objectives or specific control implementations may need to be added or adjusted.
- Update Risk and Control Self-Assessment content and processes, in particular to take account of adjusted responsibility and accountability between lines of business, technology, security and the cloud provider. Re-imagine traditional technology controls so that they can be undertaken in more rigorous, continuous and broadly scoped ways.
- Realign audit and control certifications to source components of the certifications (for example, SOC1 / SOC2) from the cloud provider.

- Depending on the industry, adjust and add to scenario planning processes, stress tests and calculation of loss-absorbing retained capital.
- Be prepared to take advantage of adjustments (increased coverage and possibly lower premiums) in cybersecurity and other insurance coverage[9] that may result from the improved security and resilience of cloud services.

- Oversee and chart adjustments in connected risk programs, as listed above, for example what needs to change in third-party risk assessment and resilience programs to take advantage of the reduced risk and increased transparency in cloud services.

Finally, look to establish more continuous and formal monitoring of risks and controls in a highly digital environment supported by cloud services. There are many things you *need* to be doing because of the increased pace of change but, more importantly, there are now many things that you *can* be doing more frequently because of the nature of the new environment. These include:

- More widely scoped and frequent continuous control monitoring. For example, more of your controls can be expressed as code or otherwise systematized and therefore such controls can be continuously monitored. With this you can assure the controls remain deployed, active where expected and performing in line with stated objectives.

- Establish more frequent incident reviews and close-call analyses not just from your own environment but by sourcing information about incidents and close-calls from other organizations and your cloud provider(s). Lessons learned can be more easily and quickly applied in the cloud and so you will want to do more introspection.

## Steady state risk management

As your organization matures in its digital transformation and use of the cloud then you should continue to mature the steady state risk management approach. Some key elements to consider as part of this are:

- Establish criteria for default risk approvals of migrations if business units and their technology teams show how they are conforming to prescribed policies, standards and required configurations. This may include establishing different levels of control (stringency) applicable to different classifications of data or business service.

- Reexamine what parts of your vendor ecosystem should be brought into the same degree of oversight and control standardization that may have been previously delivered by Software-as-a-Service (SaaS) and commissioned directly by business units or technology teams without following this risk process.

[9] https://cloud.google.com/risk-protection-program

- Determine what further adjustments might be needed on insurance coverage - to potentially reduce premiums because of the more standardized control environment.

- Enhance continuous testing processes to take a more aggressive simulation based approach to validate your organization's means of detecting control or security incidents. For example, by establishing non-critical production controls or configurations that can be disabled to test the timeliness of the automated detection processes.

- Focus more intently on insider risks and the "blast radius" of trusted insiders going bad or being coerced into dangerous actions.

> *Ask the following question of technology and security leadership.*
>
> *"How many individuals could unilaterally change the environment such that they could remove or adjust controls and how quickly could their actions be discovered and dealt with if they were unauthorized?"*

- Similarly, conduct scenario analyses of ever more extreme but still plausible scenarios to identify opportunities to reduce risk and reduce the potential impact of tail risks. For example, the economics and scale of cloud means that more capabilities are available at lower unit cost. What risk you might have accepted in the past because of the excessive cost of mitigations can now be cost-effectively mitigated.

- Establish an approach of taking and applying more frequent updates to products and services. This is not just patching and updating software but rather it is also important to take the new security and control features that cloud providers are constantly innovating around.

- Develop more stringent operational risk metrics that encode the health of the configuration management process as opposed to more conventional (but also important) metrics, for example:

    - The lag time between new cloud provider security features being available and those being used in your environment.

    - Percentage of vulnerabilities or other issues that are recurrent issues, meaning that there is an unaddressed root cause going unaddressed.

# 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 IRM 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. As with the IRM function, there is a need to engage early and then adjust processes over time. The following sections explore these areas:

- Assessing regulations, standards, and laws (*regulations* from here, for brevity) that relate to the organization's use of the cloud, including regulations that are specific to cloud.
- 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.

## Assessing applicable regulations, standards and laws

Many of the regulations applicable to an organization using the cloud are no different to those that are already relevant to that organization, but they may require a nuanced application in the context of cloud. Additionally, there are a growing number of regulations that are specific to the use of cloud. The following types are typically relevant to, and will need to be reconsidered in light of, your organization's use of cloud, in addition to any that are specific to it:

- Outsourcing/Third-Party Risk Management
- Resilience
- Information Security
- Information and Communication Technology (ICT) Risk Management
- Privacy and Data Protection

Further, in highly regulated industries, various additional regulations may come into play depending on the nature of the workloads or data that are being considered for migration to the cloud. For example, financial services requirements for the recording of certain voice calls, retention of e-communications, and methods for storing certain types of transaction records. Ensure that the cloud provider is able to demonstrate their conformance with the laws, regulations and standards that are applicable to your organization's use of the cloud, such that you can in turn remain compliant. Often these will be available as documented mappings that demonstrate how the cloud provider meets the requirements of the sections that are relevant to their obligations under the shared responsibility model.

## Aligning policy and governance

In addition to ensuring the cloud provider's conformance with applicable regulations, there will also be implications that will need to be incorporated into the organization's overall approach to using cloud. Partner with the cloud project and governance functions to ensure a joined up understanding of these, in particular in respect of the parameters they represent when determining how to use cloud in a manner that is compliant. Examples of this may include:

- Location of data and the implications of privacy or data protection regulation that is applicable to that data
- The levels of materiality of the business function and associated data that will be moved to the cloud and the levels of encryption and other controls that are applied to each

Partner with the first line and the IRM function to embed these parameters into the organization's policies, standards and frameworks (as described in the Risk Program section), and into the cloud governance structures such that project and 'class of workload' proposals explicitly address their conformance with them.

## Communicating with regulators

It is important to make sure that regulatory expectations are met in both steady state operations as well as in program and specific project oversight for transformation and cloud transition activities. Your regulators, or other external stakeholders with authority over some or all of your operations, will likely need to be kept informed as you progress. For example, your regulators will likely want to understand the scope of the relationship between your organization and the cloud service provider, the outcomes from your risk assessments, and the nature of the business processes and associated data that will be hosted in the cloud[10].

IRM functions should partner with lines of business, technology and security teams as well as Compliance and Legal functions to develop the right approaches and cadence for keeping regulators informed. Many of the materials available from cloud providers such as regulatory conformance statements, certifications and control mappings are designed to assist with this.

## Adjusting regulatory monitoring regimes

Consider how to adjust your law and regulation monitoring regime to ensure that regulations that pertain to your organization's use of the cloud are identified early and incorporated into your existing compliance and/or risk management program. Regulations, standards and policymaker attitudes towards cloud, and associated domains such as operational resilience, cyber security, sovereignty, operational resilience and outsourcing are constantly evolving and we can expect that to continue for some time given the relative newness of cloud. As such, staying on top of emerging themes, and assessing the potential impact to

[10] https://services.google.com/fh/files/misc/googlecloud_regulatory_notification_support_qrg.pdf

your organization, and the way your organization engages with policymakers on such themes is important.

# 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.

## Assessing and adjusting the audit universe

The range of risks inherent in adopting public cloud technologies is broad, reflecting that cloud is a form of technology with all of the associated risks, in addition to a significant outsourcing exercise. And, as we have discussed, skills, capabilities, organizational structures, operating models and governance approaches are foundationally critical. This is not to say that adopting cloud necessarily increases risk: as we said previously, a well-executed adoption of cloud is an opportunity to reduce risk overall. However it is important to ensure the appropriate risks are identified and assessed as part of any cloud audit. In particular, consider the following two dimensions:

- Does the set of auditable components sufficiently reflect the risks associated with the organization's cloud transformation? Do certain components need to be more highly prioritized or explicitly assessed instead of covered via other approaches in light of the increased complexity, relatively lower maturity and relative pace of change vs traditional technology delivery and outsourcing models? Consult with external standards for cloud security, risk and compliance, some of which include guidance specifically for auditors. And, as with other parts of the organization, ensure the audit team receives appropriate training and skills updates to cover cloud technologies and operating models.

- 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. For example, this paper describes the journey in four core phases: your organization may take a similar approach: integrating an audit plan into that will ensure audits are focused on the right thing, at the right time, and provide confidence to management and the board at key junctures.

## Considerations during 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.

- **Setting a clear scope for each audit.** As we have discussed, a wide-scale cloud-based digital transformation will touch many parts of the organization, and include a broad range of risks to consider. As such, conducting a single "cloud audit" is likely to be unwieldy and complex, and risks taking so long to complete that the organization will have moved on substantially by the time it is published. As such, consider how to break down the cloud transformation audit approach into a number of discrete items.

  *Audit functions could scope their cloud audits by considering which question they are looking to answer. We think there are, broadly, three such questions:*

  - *Is the organization set up for success? The definition of success naturally will depend on where the organization is on the journey, but regardless this audit considers whether the foundational elements of governance, strategy, organization, skills and capabilities have been appropriately implemented for the phase of the journey that the organization is in.*

  - *Is the organization designing and delivering the right technical solutions? Herewe assess whether the teams that are designing the core architectures, infrastructure models, and capabilities for development teams to leverage doing so in a manner that is consistent with policies and standards, and such that development teams will have appropriate guardrails in place.*

  - *Are specific projects being delivered safely? This audit assesses whether the lifecycle of a specific project to migrate an application or workload to the cloud met the organization's policies, standards and best practices, and whether the outcome is a secure, resilient and otherwise compliant application.*

- **Sampling in an ephemeral cloud environment.** For certain cloud audit scopes, the approach to sampling will need to consider the dynamic nature of cloud technology as against traditional on premise technologies. For example, compute resources may be automatically created to respond to increased business volumes and subsequently automatically demised when that activity peak has passed. More than offsetting this challenge, however, is the fact that cloud offers a different approach to audit sampling due to its declarative and discoverable nature. In some situations, instead of using small samples, the audit function may be able to use data analytics to perform a far broader assessment of the environment.

## 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.

The basis of this starts with forming a clear understanding of the shared responsibility model, and in particular the boundaries of responsibility between your organization and the cloud service provider. The cloud shared-responsibility model assigns responsibility as follows:

- Your cloud service provider is responsible for managing the risks and controls of the underlying cloud infrastructure, including hardware and networks.

- Your organization is responsible for managing the risks and controls of its environment in the cloud, such as securing your data and managing your applications.

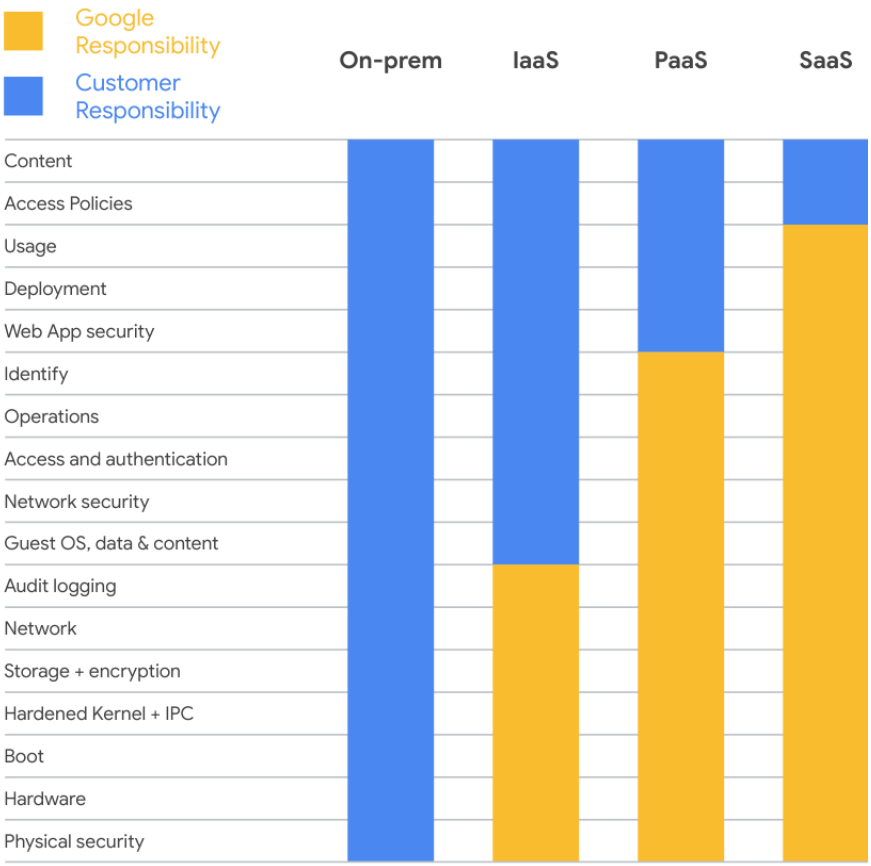



Figure 1. Your responsibilities and your cloud service provider's responsibilities under the cloud shared-responsibility model.

As shown in Figure 1, many responsibilities depend on whether you adopt an Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) architecture.

When structuring the audit approach, consider the following, and incorporate any ongoing due diligence or continuous assessment regime your organization is otherwise conducting to oversee the cloud provider:

- **Scoping control domains.** Each organization will have its own definition or set of control domains against which it conducts audits, usually these being aligned with one or more of the external best practice approaches. Typically these will include the following domains and you should consider how to focus activities within these that are most relevant:
    - Business continuity and operational resilience
    - Risk Governance and Audit
    - Third-Party Risk Management
    - Information Security
    - Incident Management
    - Compliance with Regulation and Standards

- **Independent audits and certifications.** Most cloud service providers will maintain certifications and have various other independent audits conducted: you should ensure that you have access to these certifications and other reports in order to inform your own audit and findings.

- **Conducting pooled audits.** In some industries, such as Financial Services, it is increasingly the case that similar organizations are working together to conduct pooled audits, an approach that regulators are increasingly positive about. There are benefits to all parties involved: the organizations may be able to conduct a more thorough audit and leverage specialist skill sets across their organizations; share and adopt learnings from prior audits conducted by the organizations; and the cloud service providers are able to provide high quality support for audits in a more efficient manner than if each organization conducted an audit independently.

## Communicating with the board

As outlined in previous sections, with any use of cloud services it is important to keep the board of directors informed, and likely specifically the Audit Committee of the board of directors. The audit committee will in particular look to understand how well positioned the internal audit function is in its ability to provide an opinion on management's use of cloud services. This could include considerations regarding the audit plan, and whether the function is adequately resourced with the right skills. It is also likely that due to the relatively fast moving nature, and newness of cloud transformations, that the committee will look for more frequent updates on audit status and on the remediation of any findings by management.

# Conclusion and Key Takeaways

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. Chief Risk Officers, Chief Compliance Officers, Heads of Internal Audits and their teams and embedded risk functions have a critical role to play in that process. And to achieve those outcomes, we advocate that the following principles can help you safely navigate a cloud transformation:

*Level the playing field: establish a common understanding and the key principles that will shape the intent and approach of the organization's transformation over time.*

1. Build a common understanding.
2. Think long term, but act iteratively.
3. Prioritize organizational readiness.
4. Implement dedicated, but integrated, governance.

*Manage the initial phases: implement structures and apparatus that allow the organization to safely conduct initial migrations to the cloud.*

5. Define initial minimum security and configuration standards.
6. Define initial risk and compliance oversight.
7. Communicate with boards and regulators.
8. Training and skills development.

*Mature and accelerate: adjust control and governance structures to enable accelerated adoption of cloud, by increasing control rigour and oversight, and right-sizing governance in parallel.*

9. Develop comprehensive security and configuration standards.
10. Modernize IT delivery.
11. Mainstream risk oversight.
12. Extend continuous control monitoring.

*The new steady state: adapt to broad usage by embedding cloud into all relevant risk programs and governance, and by implementing processes to maintain currency with cloud best practice.*

13. Interconnect cloud with other risk programs.
14. Drive continuous improvement cycles.
15. Stay current with cloud best practices, and constantly revalidate assumptions.
16. Manage legacy in parallel.