Transformation

Maximising cloud value

The essential role of risk and controls

pwc

PwC's latest EMEA Cloud Business Survey reveals that 'cloud-powered' companies outperform other businesses by a significant margin on key aspects. These include revenue growth, productivity, the ability to respond to cyber threats, and faster recovery from incidents. But what really sets these cloud-powered pioneers apart from the rest?

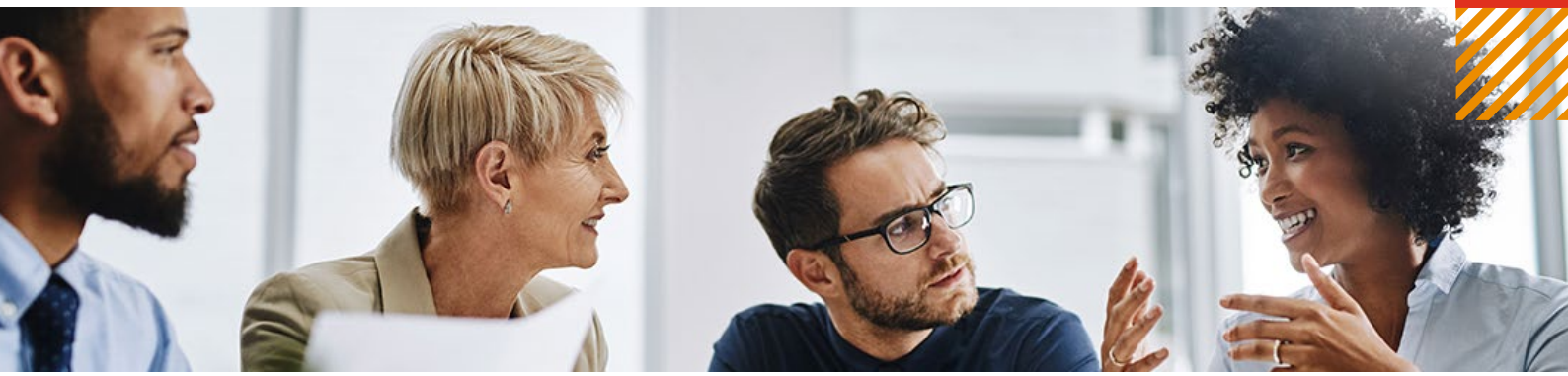
Our analysis shows these pionneers share several distinctive traits. One of the most strinking aspects is that they attach much higher importance than other companies to the **maturity of their cloud governance and internal control framework**.

As a result, these companies are taking a more mature approach to cloud transformation, including involving a wider range of functions across the business; adopting leading practices in cloud controls; forging stronger and closer relationships across all C-suite executives to facilitate collaboration around cloud; and making more effective use of automation and artificial intelligence (AI). These approaches are key to obtain and deliver a higher realisation of sustainable value from cloud technologies.

While the benefits deriving from cloud are evident, the downside of failing to focus sufficiently on cloud risks and controls is equally clear and common. Aside from undermining value creation from cloud, it increases the risks of cybersecurity breaches, business interruption, regulatory violations and budget overruns. Organisations that recognise the need to evolve traditional risk and control frameworks as part of their cloud journey achieve benefits such as a reduction in the time it takes to manage compliance, wider control coverage and improved responsiveness to business demand and change.

To help organisations develop and maintain this focus, we have identified six points that support the existence and the importance of cloud risks and controls being embedded in a control framework. For each point described below, we have developed a set of related actions which can be taken to strengthen cloud governance.

> "An effective cloud control framework is no longer an option… but a crucial tool in the cloud transformation journey to improve governance, data security, operational resilience and business continuity throughout a period of change and uncertainty for an organisation."
>
> **Reggie Kelley**
> Partner, PwC UK



1 Six reasons why cloud-specific risks and controls are required – and related actions for each

1. Mature governance, risk and controls can generate major business benefits

Our research reveals a direct correlation between an organisation's overall cloud maturity and the maturity of its cloud governance. **The vast majority of cloud-powered companies have implemented formal controls to enhance operational efficiency, supported by a common control framework tailored to new cloud services, and have documented their shared responsibilities with their cloud service providers (CSPs).** Crucially, most have also allocated ownership of cloud-related controls for governance, risk and compliance to a single business function with its own dedicated resources.

The business payback from taking these steps is clear and unambiguous. An overwhelming **83% of cloud-powered businesses in EMEA have increased their revenue over the past six to nine months (compared with 67% of other businesses)**, and 89% expect to increase their revenue over the next 12 months (compared with 78% of others). Additionally, 60% have implemented an enterprise-wide transformation, compared with 42% of others.

That said, almost all businesses still have opportunities to make further improvements in adopting leading practices in cloud governance, risk and controls. This is an area that deserves specific focus in cloud to ensure negative consequences are minimised and controlled.

Tellingly, around 1/3 of

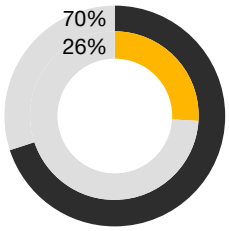
1/3 of cloud-powered companies and

3/4 of non cloud-powered companies have yet to implement cloud-specific controls

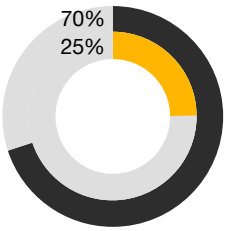
This is an area that deserves specific focus in cloud to ensure negative consequences are minimised and controlled.

Figure 1

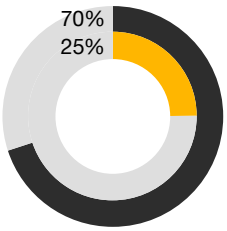
How would you assess the maturity of your organisation's cloud controls across the following areas?



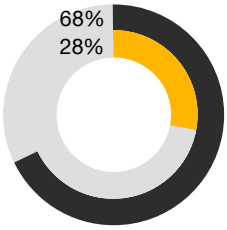
Technically-upskilled resources dedicated to our cloud governance, risk and controls environment.



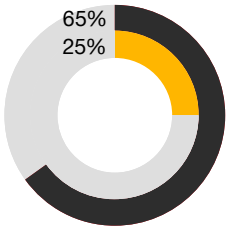
A common controls framework tailored to consider cloud risk and controls.



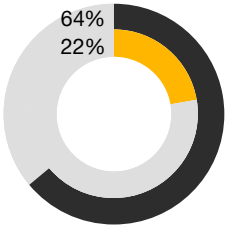
Robust evaluation of shared responsibilities between our organisation and our cloud service providers that is documented.



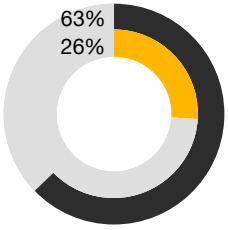
Policies and procedures that are tailored to cloud risk and controls.



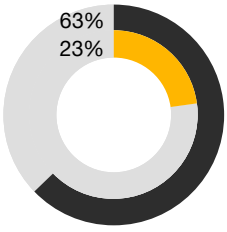
A cloud governance, risk and controls framework that is owned by a single business function.



Formal cloud controls that are separate and distinct from our other compliance and/or controls framework.



Cloud controls designed to optimise workloads (e.g., increased automation, reduced lag in processing), availability and resiliency of workloads.



Cross-functional stakeholder agreement on our cloud governance, risk and controls framework.

Cloud-powered companies Other companies

Source: PwC's EMEA Cloud Business Survey 2023

Key takeaways: as part of implementing mature governance, risk and controls, organisations should…

01 Embrace a shared responsibility model, with accountabilities clearly allocated. CSPs will often manage some, but not all, of the controls (e.g. security, data, resilience and others), required in a cloud environment, depending on the cloud services being subscribed for, such as PaaS, IaaS or SaaS. It is essential that organisations have a good understanding of the responsibilities they share with their CSPs, and translate their own responsibilities into their control strategy and playbooks. Companies should also document the processes and activities outsourced to the CSPs, including contractual arrangements and exit strategies.

02 Implement robust data encryption and security governance procedures to ensure sensitive and/or personal data remain protected, both in transit and at rest. Organisations should also put in place a strong Identity and Access Management (IAM) strategy and access control framework to oversee users' access to the cloud. These provisions and processes may well be different from those already in place for on-premise systems, given that some responsibilities are now shared with the CSPs.

03 Invest in comprehensive employee training to ensure a smooth transition to the cloud, taking into account the resulting changes to processes and workflows.

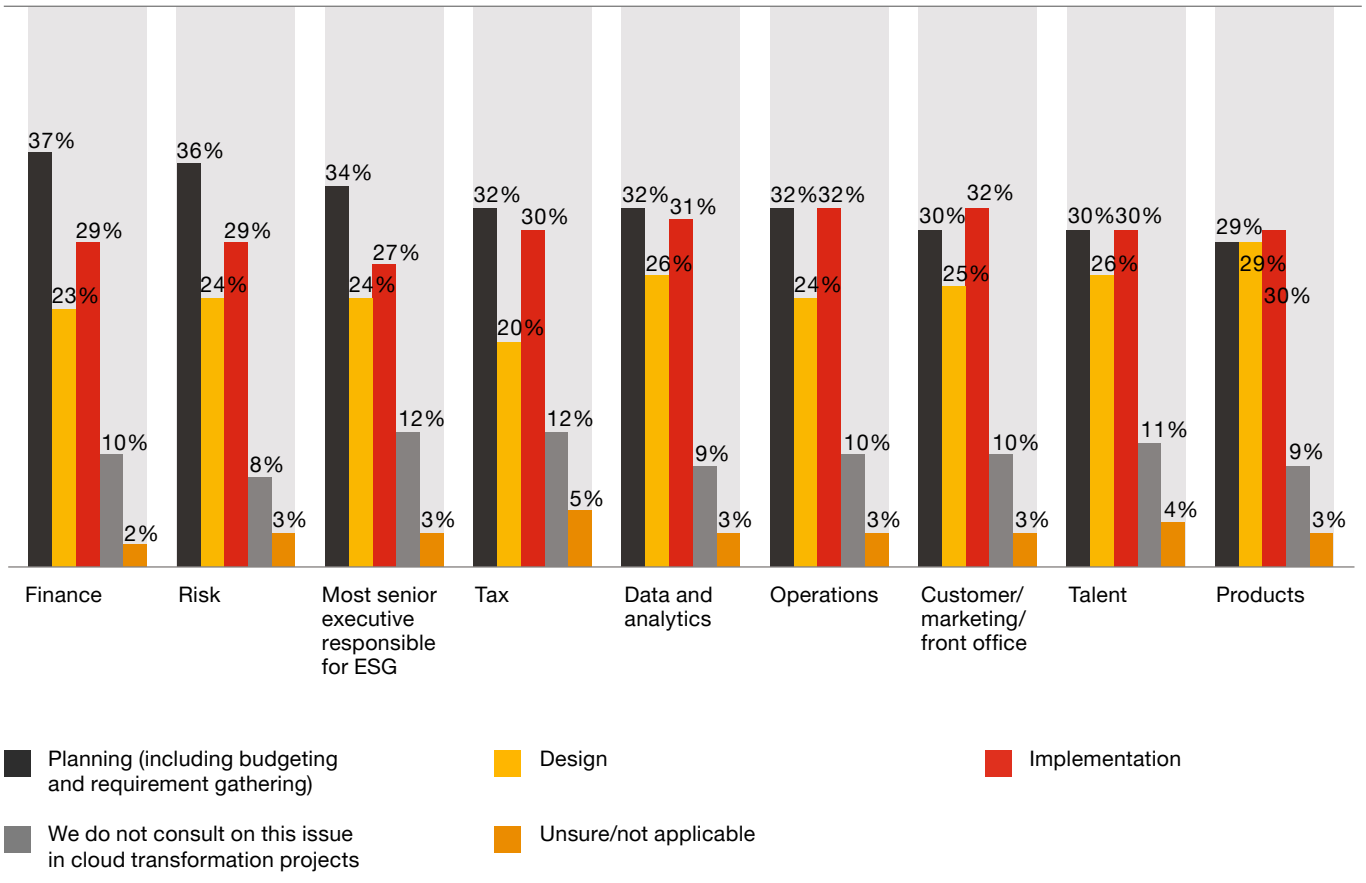
2. Executives must collaborate early to incorporate and address cloud risks

Migrating to cloud is much more than just a technology change. It affects and involves senior leaders and their respective business units or functions across the entire organisation – from Finance to Risk, from Talent to Procurement, and more. To effectively identify all cloud-related risks, it is critical to engage other disciplines and business functions at the earliest point possible. Failing to do this will result in having to 'bolt on' controls later through remediation work that is both labour-intensive and costly, and which may even hamper the development of new applications.

Many organisations still struggle to promote effective collaboration and engagement between technology and business teams. By proactively engaging with management and senior stakeholders at the planning stages of their cloud journey, cloud-powered organisations improve their chances of success. In almost half of the cases, our research shows that companies are currently waiting until the design or implementation phases of their cloud transformation before engaging with leaders from other business areas. As well as delaying cloud-related benefits, this misses an opportunity to co-create flexible cloud solutions with respective controls that can meet differing needs – instead of creating a proliferation of point solutions that need rework to be realigned.

Figure 2

At which stage, if at all, in a cloud transformation project, do you start to collaborate with the leaders or team responsible for each of the following:



Source: PwC's EMEA Cloud Business Survey 2023

Key takeaways: to enable early and successful collaboration around the cloud transformation, organisations should…

01 Create an overall cloud executive leadership steering committee from day one with strong CEO sponsorship. This committee should include representatives from all the relevant functions, with different members taking the lead depending on the nature of the specific risk at hand.

02 Assess cloud readiness and the overall risk profile before beginning your cloud journey and/or before you deploy new workloads. Validating the controls environment for compatibility with the chosen cloud model (public, private, or hybrid) and any industry-specific compliance requirements or regulatory standards that will impact the migration, such as the EU's Digital Operational Resilience Act (DORA) in financial services. This means conducting a readiness assessment against relevant standards and determining what controls will be needed in both the transitional period and the target environment.

03 Ensure that the cloud strategy and plans are aligned with the existing IT architecture, as well as with the organisation's business and technology capabilities and targets. A properly designed control environment will need to take these elements into account, since risks can be present across the whole IT estate and impact business areas across the organisation.

3. Risk and controls become more complex with multi-cloud infrastructures

73% of the companies in our survey are taking a multi-cloud approach to their cloud transformation, with only 25% using one CSP exclusively for all workloads.

This reflects the fact that multi-cloud offers several benefits such as higher flexibility and robustness, by enabling enterprises to choose the right CSP for each workload and select from a wide array of software-as-a-service (SaaS) providers to enable specific business processes.

However, there is also a downside: alongside the benefits, the adoption of multi-cloud introduces higher levels of complexity and risk, requiring organisations to develop a security and controls model that can be applied across different CSPs. Many companies have struggled to create such a model, since each CSP has its own approach to security and governance and uses different security tools, all of which make consistency difficult to achieve.

Key takeaways: to help equip the risk and control framework for a multi-cloud environment, organisations should…

01 Perform an overall assessment of the internal control framework of the chosen CSPs – including aspects such as risk taxonomies, control framework, approach to resilience and continuity management – prior to making (or renewing) any contractual agreement.

02 Adopt strategies to facilitate the monitoring of complex multi-cloud security frameworks through 'single pane of glass" solutions that bring multiple tools together. Defining technology risk in a cloud-agnostic way gives organisations the ability to mandate common controls regardless of vendor or technology stack used. Supplementing these with vendor-specific technology risks gives organisations the detail needed to define specific controls to monitor and manage risk.

03 Move at the speed of the team rather than the speed of the control – replacing legacy controls with automated controls lowers the cost of compliance and improves coverage. Cloud infrastructure is shared and allocated dynamically, requiring new controls and control ownership that can keep pace with modern accelerated software engineering and platform delivery practices. By taking advantage of new cloud workflows, organisations have introduced automated controls for change, release, deployment, configuration, capacity and incident management. Combined, these reduce reliance on manual approaches and free up teams to deliver at speed while demonstrating control.

04 Rigorously address network security and monitoring by implementing cloud-native security solutions that are scalable and adaptable to the dynamic nature of cloud infrastructure. These solutions can provide comprehensive insights into network traffic across both cloud and on-premises environments. A Zero Trust security model and collaboration with CSPs are integral components.

05 Mitigate the risk of vendor lock-in by assessing options from a range of CSPs when procuring new products and/or services. Vendor lock-in can result in a complicated, costly, and operationally challenging transition to other provider(s) and make it more difficult to implement changes to the underlying cloud architecture or landing zone.

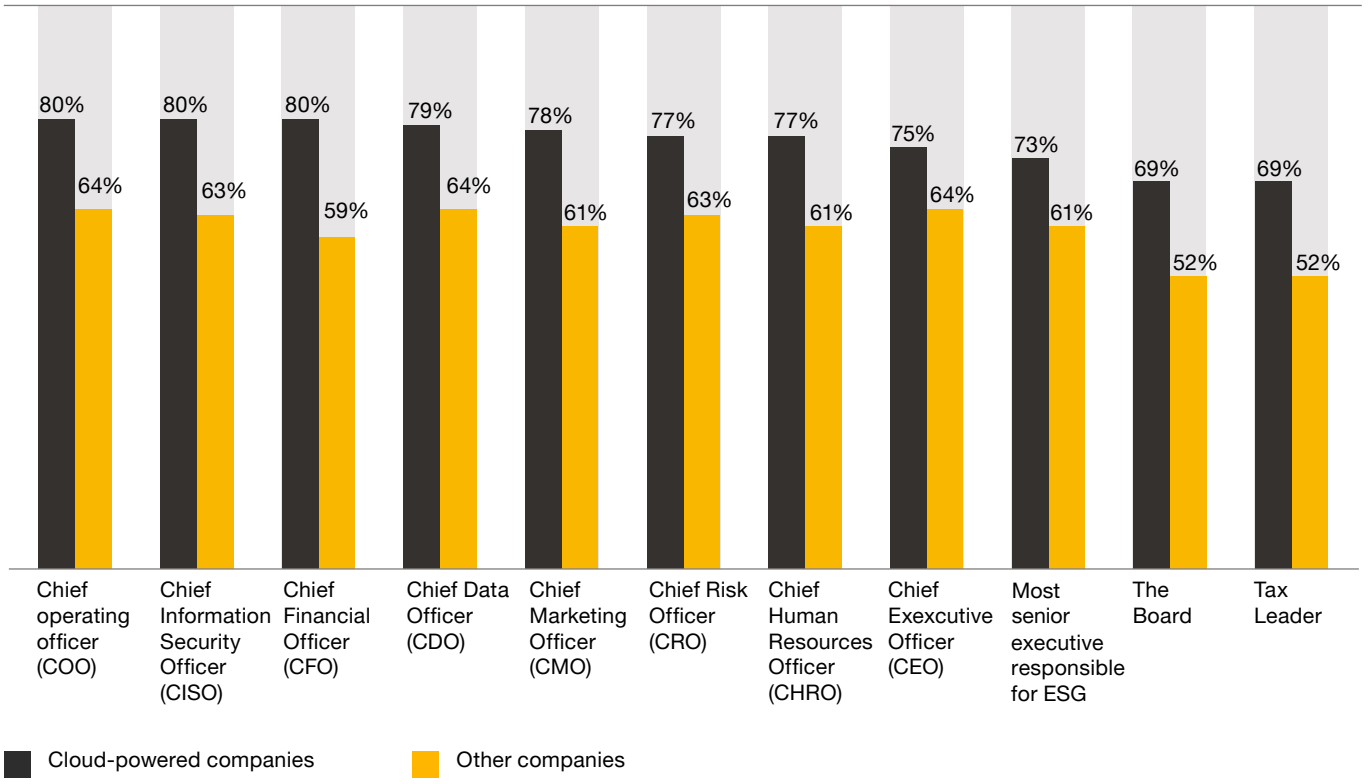
4. Strong relationships between CIOs and risk and security leaders are imperative

Cloud-powered companies tend to have stronger alliances between their C-suite colleagues across both technology and business roles, including risk functions such as 1st and 2nd Line of Defense. These close relationships foster early engagement and facilitate a collaborative approach to leadership and decision-making throughout the cloud transformation journey.

Because risk officers ultimately oversee the effectiveness of the cloud risk and control framework, their involvement is critical from the outset. It is also important to include the 3rd Line of Defense – Internal audit – since the cloud transformation and implemented cloud platforms should form part of the periodic audit-testing reviews.

Figure 3

Which of the following best describes your relationship with each of these executives specifically in relation to achieving your cloud transformation goals?



Source: PwC's EMEA Cloud Business Survey 2023

Key takeaways: to strengthen and optimise relationships across the C-suite, organisations should…

01 Ensure strong support from the Executive Leadership and Board to foster the continuous collaboration required to address cloud risk issues and prevent them from recurring.

02 Make your Chief Information Security Officer (CISO) and Chief Data Officer (CDO) part of the overall Cloud Leadership to help lay the groundwork for security and privacy throughout the cloud infrastructure. Security teams and IT teams should have formal playbooks for working together to secure the cloud.

03 Institute and facilitate regular discussions between between the CIO, CISO, CRO and the different Lines of Defenses.

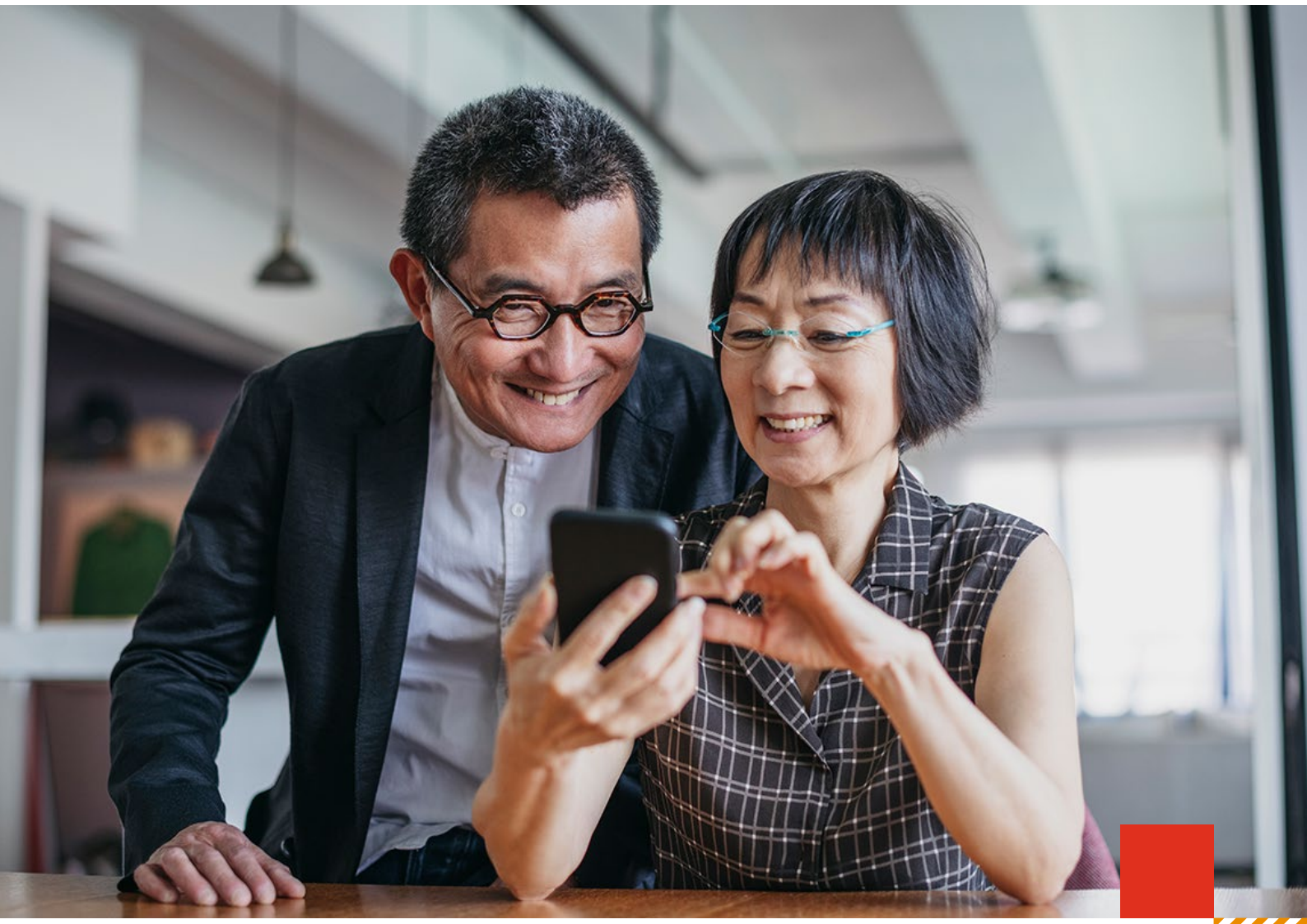
04 Involve the COO/Chief Product Officer and Chief Legal Officer assessing the impact of the cloud transformation on the contractual customer commitment of both the CSP and the organisation.

05 Engage the Executive Leadership in charge of the ESG strategy to ensure they understand and capitalise on the sustainability impacts and opportunities presented by cloud computing.

5. Evolving the cloud approach in line with advancing regulations enables companies to stay ahead of general and industry-specific compliance risks

Regulations around the use of cloud are continually changing – including the complexity of complying with them, in particular when dealing with different regulations across several EMEA countries. As an example, multinational organisations operating in Europe need to consider the different data privacy regulations in force across the 27 EU member states, as well as the General Data Protection Regulation (GDPR), the overarching EU data regulation. Across EMEA, the diversity of regulations is even greater.

There are also industry-specific regulations that companies must comply with. A prime example, already mentioned, is the EU's DORA in financial services, which requires financial institutions to follow specific rules around the protection, detection, containment, recovery and repair capabilities against ICT-related incidents. Regulations like DORA are acting as accelerators for cloud controls and cloud maturity across EMEA – mirroring the effect in the US of regimes like the Federal Risk and Authorization Management Program (FedRAMP) and Health Insurance Portability and Accountability Act (HIPAA).



Key takeaways: to keep pace with data regulation and stay in compliance with industry requirements, organisations should…

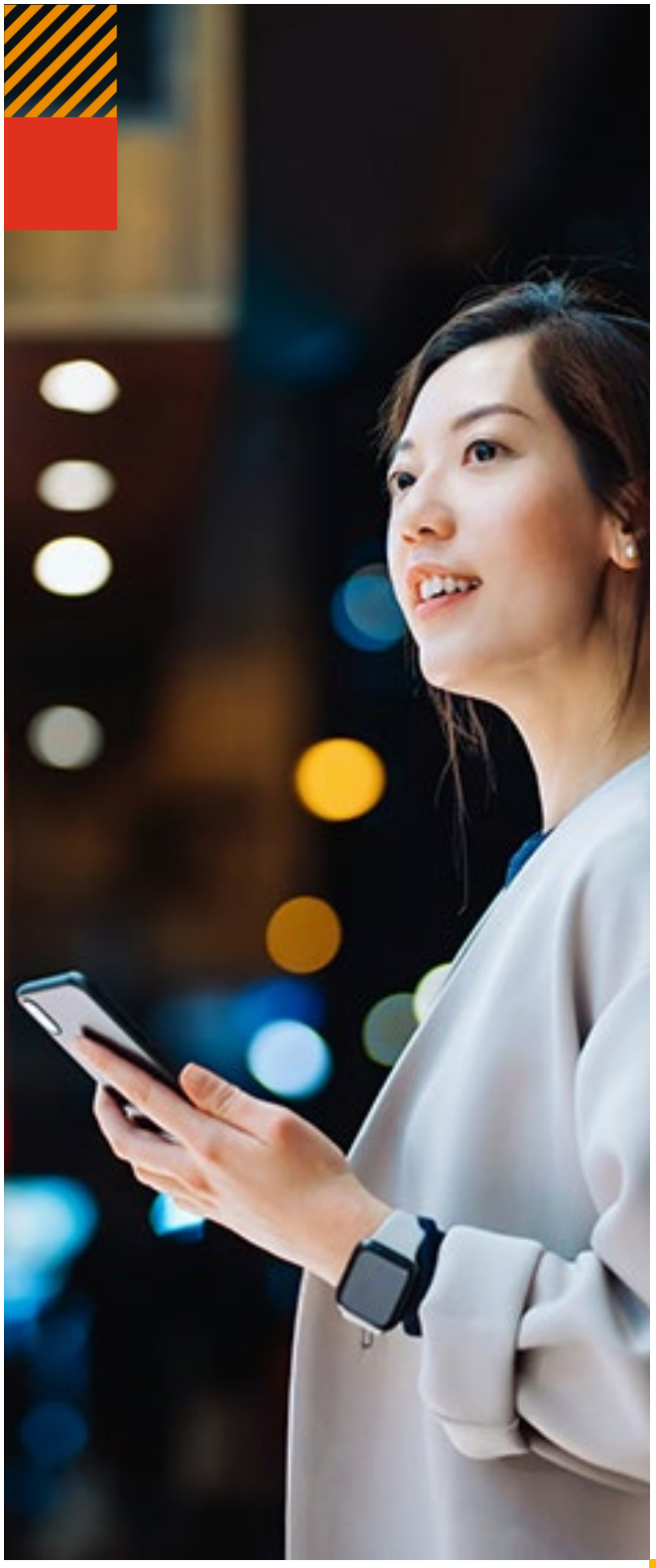
01 Ensure resilience in compliance is maintained with the evolution of regulations, such as DORA incident response and operational resilience program tailored to your cloud environment.

02 Implement a comprehensive testing programme to prove the effectiveness of incident response and operational resilience capability, and implement controls to monitor resilience through both small and major changes.

03 Build and adopt a consistent digital data model, taking into account key compliance issues as well as interfaces, maintenance facilities, and traceability.

04 Define and plan the cloud solutions to adopt ahead of the migration or deploying of new workloads to ensure there is no infringement of local regulations. For example, employee analytics obtained through cloud solutions or people performance measurement based on employees' personal data is not permitted in some territories.

05 Involve the relevant C-suite (i.e. Chief Financial Officer, Chief Compliance Officer, Chief Data Officer) when issues related to regulatory risk arise.



6. Generative AI (GenAI) will drive cloud adoption, but effective integration will necessitate the need for stronger governance

Based on PwC's 27th CEO survey, 70% of respondents said that GenAI will significantly change how their organisation creates, delivers and captures value in the next three years. AI has the potential to enhance productivity within enterprises – however, without data, there is no AI; and without cloud, organisations will struggle to scale AI and unlock value. Clearly, therefore, AI adoption will increase cloud adoption and influence an organisation's cloud strategy. This could lead to the development of a multi-cloud infrastructure for access to the latest models, or rapid migration towards a single cloud provider to reduce cost.

The adoption of AI will create new vulnerabilities and could heighten existing risks in areas such as data, cybersecurity, and technology. These risks range from new threat vectors to uncontrollable cloud expenses associated with operating AI. While cloud-based AI deployment amplifies existing risks like cloud vendor lock-in, there are also new AI components to consider, such as vector databases that may store sensitive data requiring protection. Additionally, AI-specific risks such as 'hallucinations' and the need to comply with new AI regulations like the EU AI Act must be considered, alongside other horizontal and sectoral regulations.

Key takeaways: Unlocking the value from AI requires a strong governance framework

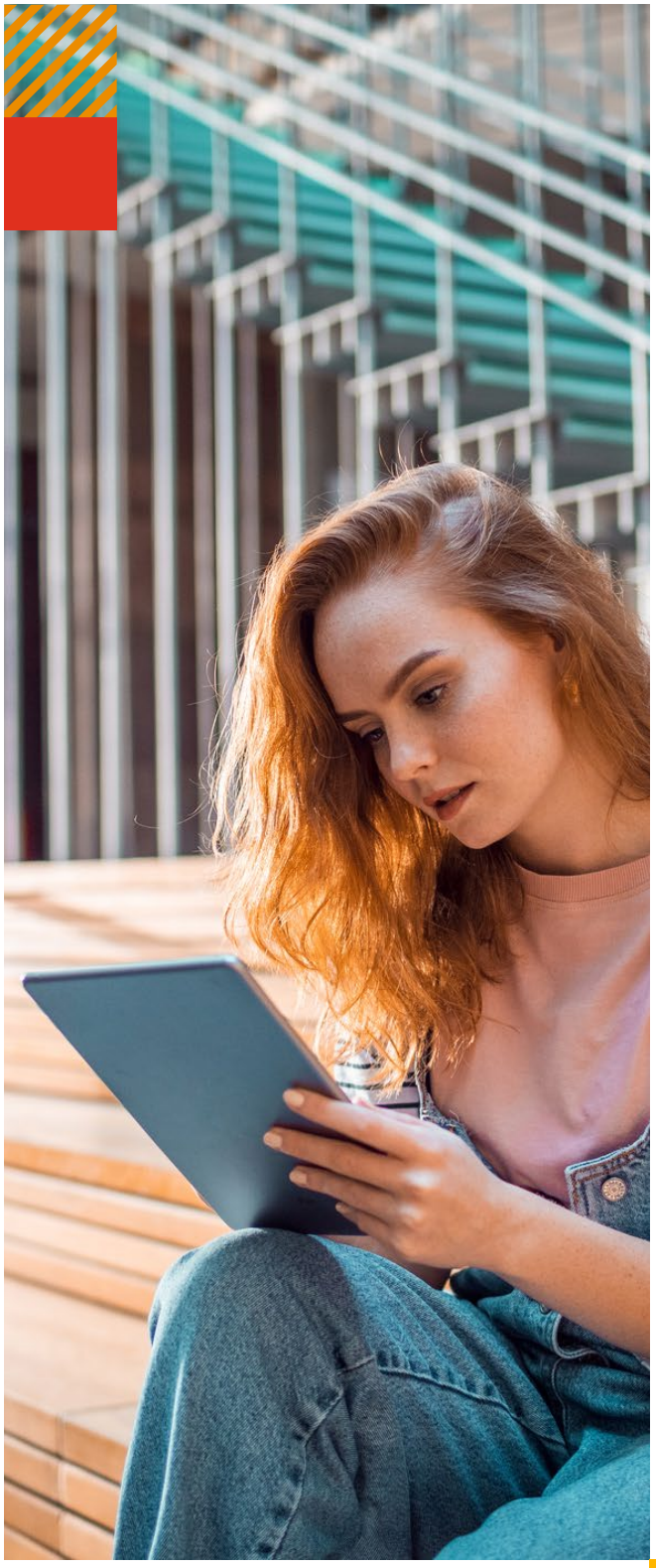
Responsible AI (RAI) is an approach that promotes both risk management and value maximisation in the deployment of AI-based solutions. It involves adopting practices that ensure AI technology is aligned with ethical standards, maximises value, and mitigates risks. This dual focus enables organisations to harness the full potential of AI while being prepared for emerging regulations.

01 Assess the new and heightened risks from adopting and using AI. Alongside your cloud governance framework, integrate and adapt existing controls to protect value from your AI investments.

02 Consider your cloud service providers' ethical and Responsible AI practices, when selecting a third-party cloud-based AI vendor.

03 Implement data and security controls on your GenAI cloud platform.

04 Monitor cloud costs, as these can be exacerbated by the use of AI. Enhance your governance frameworks to effectively manage cloud resources and mitigate the risks of cloud sprawl.



2 Conclusion: your best next step – implement effective controls in your cloud environment

As the experience of cloud-powered companies shows, cloud risks and controls should not be treated as an afterthought to be handled by the technology team only. The organisations which are most advanced in their progression towards cloud maturity are those that adopt a holistic, embedded and integrated approach to risks and controls from day one.

This correlation is no coincidence. Effective cloud controls are the vital enabler of any successful cloud transformation – enhancing governance, data security, operational resilience and business continuity through and beyond the transformation journey. Cloud controls should be embedded within the organisation to support innovation and harness the full potential of cloud technology, while addressing the security and compliance/ regulatory risks that the transformation brings.

> “Cloud risk and controls must be a high-priority focus across the C-suite from day one, addressed through a collaborative, multi-function approach and a clear governance framework, defining the shared responsibilities between the company and the CSPs it uses.”
>
> **Benjamin Zenati**
> Director, PwC France

About the authors

To find out more about how PwC can help you get your cloud risk and controls strategy right, please contact:

Reggie Kelley
Partner
PwC UK

Eleonora Bruni
Director
PwC UK

Benjamin Zenati
Director
Cloud Risk & Regulatory
PwC France

Ivan Frain
Director
Cloud Transformation
PwC France

pwc.com

RITM16921445