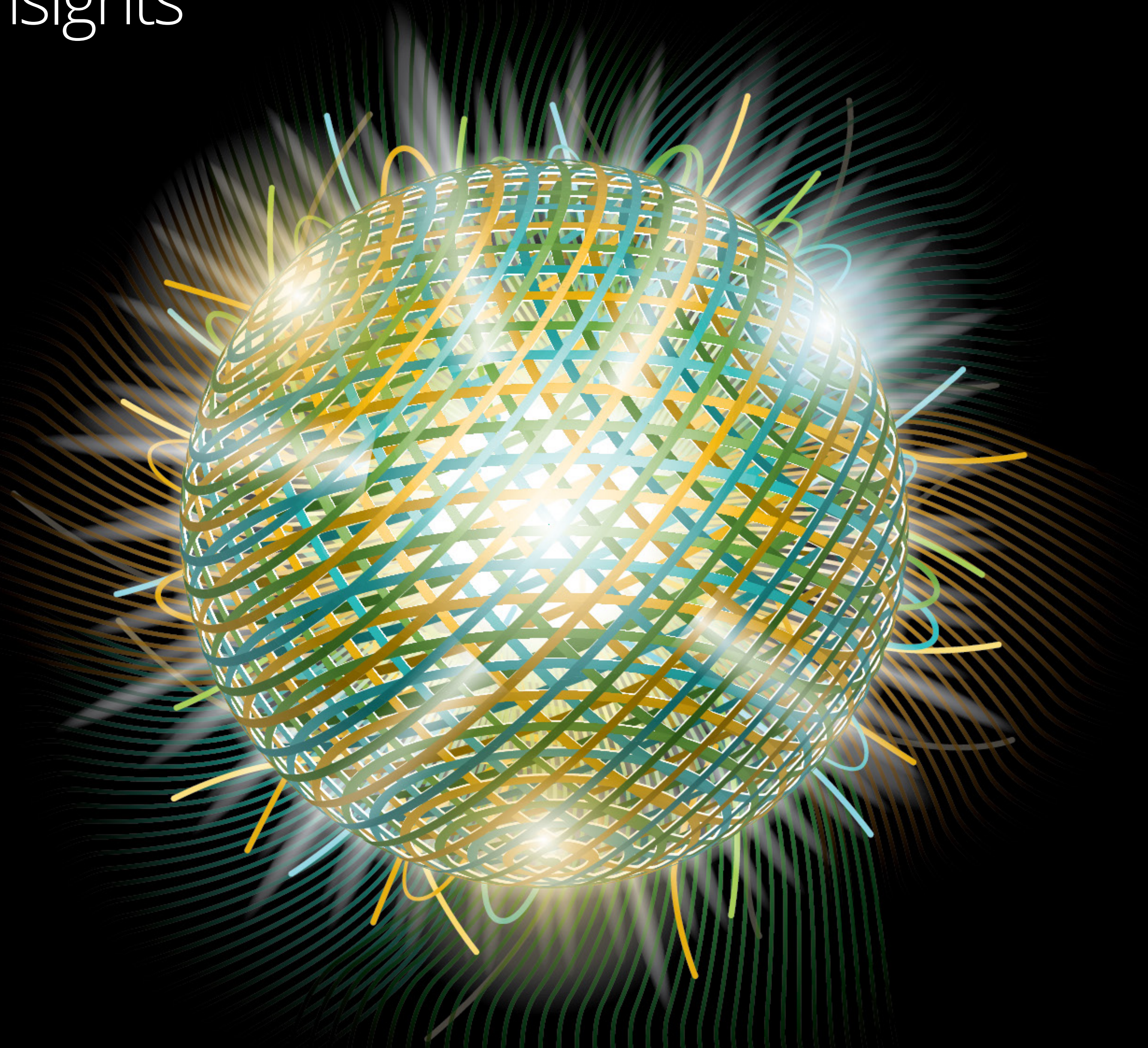
Deloitte.
Insights

A report from the
Deloitte Center for Integrated Research



An integrated cyber approach to your cloud migration strategy

Why cloud migration programs should consider a cyber-forward cloud strategy

About the Deloitte Center for Integrated Research

Deloitte's Center for Integrated Research focuses on developing fresh perspectives on critical business issues that cut across industries and functions, from the rapid change of emerging technologies to the consistent factor of human behavior. We look at transformative topics in new ways, delivering new thinking in a variety of formats, such as research articles, short videos, in-person workshops, and online courses.

Connect

To learn more about the vision of the Center for Integrated Research, its solutions,
thought leadership, and events, please visit www.deloitte.com/us/cir.

Deloitte Cloud Consulting Services

Cloud is more than a place, a journey, or a technology. It's an opportunity to reimagine everything. It is the power to transform. It is a catalyst for continuous reinvention—and the pathway to help organizations confidently discover their possible and make it actual. Cloud is your pathway to possible. To learn more, visit Deloitte.com.

Contents

Introduction

INCREASINGLY, GLOBAL ORGANIZATIONS are migrating from legacy on-premise infrastructure to the cloud in order to achieve greater business agility and resilience with a modern IT approach. Yet too often, cloud migration and cybersecurity are considered separately, with different teams focused on different phases of what could be a shared process. With cybercrime estimated to cost US$6 trillion annually by the end of this year,[1] cloud migration raises the cybersecurity stakes. At the same time, despite the benefits—and even though "security and data protection" is a number one or two top driver for cloud migration[2]—investment in integrated cloud cyber technology strategies is often lacking. Deloitte & Touche LLP's 2019 Future of Cyber survey found that 90% of responding organizations spent 10% or less of their cyber budget on cloud migration, software-as-a-service (SaaS), analytics, and machine learning.[3]

Indeed, many organizations are moving fast to migrate to the cloud without paying enough attention upfront to security.

This points to an opportunity for cybersecurity modernization that drives business and technology resilience—wherein cyber can become the *differentiator* to provide consumer trust. An integrated cloud cyber strategy enables organizations to use security in their transformation in a way that promotes greater consumer trust, especially in today's digital age.

Achieving this combined approach often requires bringing together cloud and security specialists with shared goals, and a modernization program that balances agility with security and consumer trust requirements.

For organizations looking to enhance business and technology resilience, increase security, and cultivate trust during their cloud migration, a conscious decision to embrace cloud "security by design" can be essential. By pursuing security by design, organizations can benefit from:

- incorporating leading-edge, innovative approaches such as intelligent threat detection
- balancing needs of speed while reducing risk related to technology, insider threats, and the supply chain
- supporting developers and engineers while enabling the business with DevSecOps
- establishing a cyber-forward approach that reinforces business objectives such as security and trust

This article asserts the importance of taking a conscious approach to "security by design" (focused on mission-critical business applications) to guide greater collaboration between cloud and cyber teams and to drive greater agility, security, and trust.

Based on our research, which combines primary data analysis, secondary research, and internal interviews with nine Deloitte executives versed in cloud and cyber strategies, we've detailed specific considerations for organizations embarking on the cloud migration journey.

WHY IT MATTERS: AN INTEGRATED CLOUD CYBER APPROACH CAN HELP BUILD BUSINESS AND TECHNOLOGY RESILIENCE

Deloitte Global's fourth annual readiness report survey data, based on responses from 2,260 C-level executives and senior public sector leaders,[4] found that organizations with more mature cloud and cyber technology strategies tend to be more resilient than respondents overall as well as those with only advanced cloud or advanced cyber strategies. Those with a mature cloud and cyber strategy scored the highest when answering questions related to how well their organization is doing using advanced technologies to "become more resilient and agile" (75% versus 53% overall) and "to predict future trends, risks, and threats" (70% versus 49% overall). While a cloud or cyber strategy advances resilience about equally when combined, cloud and cyber are a force multiplier equating to two times resilience/agility compared to organizations with no cloud or cyber strategy (see endnote 5 for detailed analysis methodology).[5] See Appendix: Integrated cloud cyber strategies drive greater business and technology resilience.

Security by design: Specific considerations

Ultimately, the cloud and cyber teams should come together managed by a modernization and migration Center of Excellence (CoE) leader (often the digital transformation leader) and enabled by cross-teaming, cross-skilling, and a shared operating model. Once in place, the operating model can be used to guide greater collaboration, coordination, and implementation across controls, and risk management and compliance practices in a way that builds in security at the IT infrastructure layer while promoting the business (and ultimately) the customer experience.

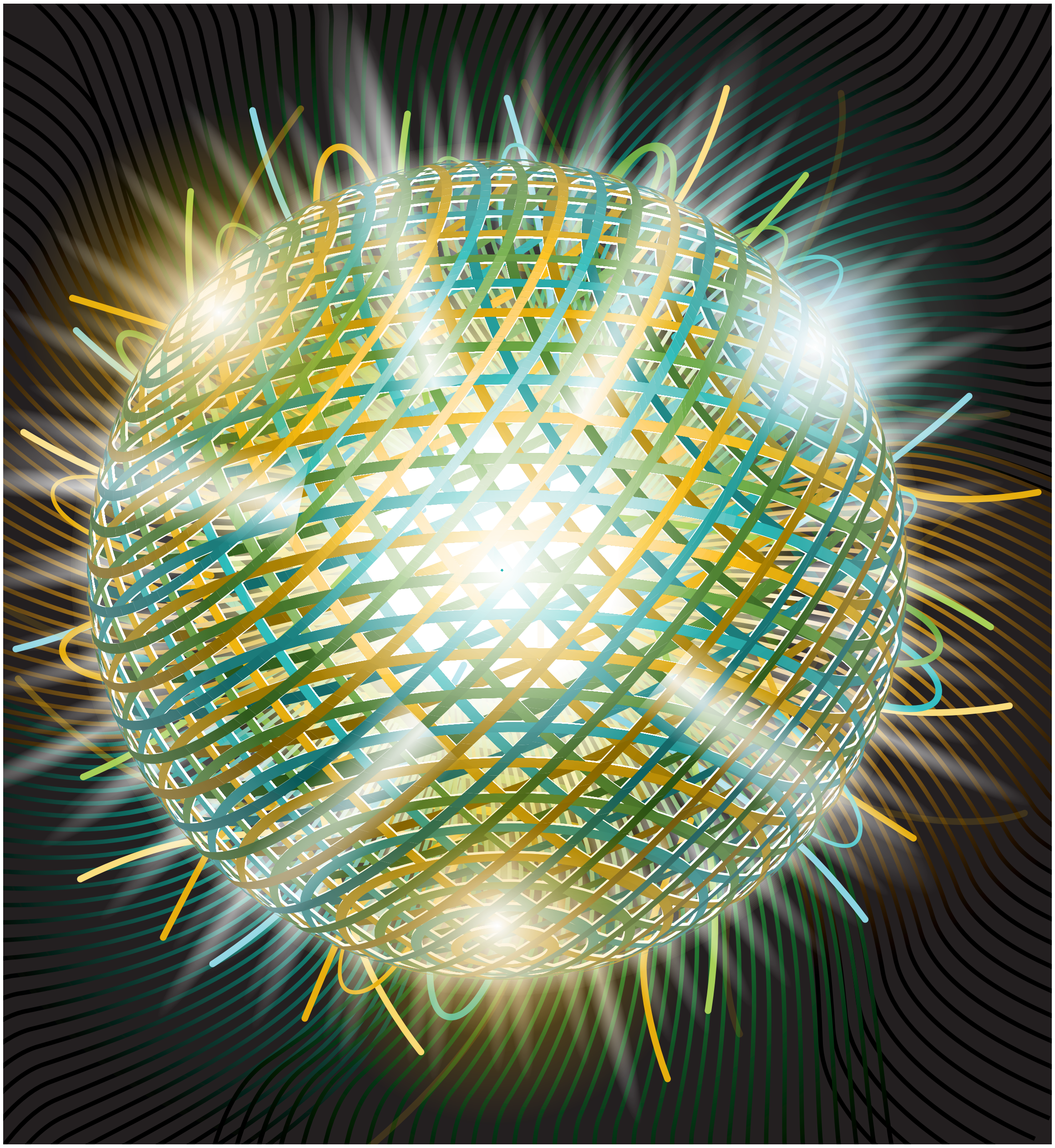
This integrated team may need to collaborate around:

- **Initiating the modernization and migration program.** This cannot be envisioned in a silo without understanding broader business objectives, and it includes assessing business continuity issues, service-level upgrades, and potential customer impact. It also means understanding the important assets of the organization and protecting them with a cyber-centric strategy. For example, with a major retailer this could be data on product sales and customer preferences.

- **Understanding innovative new cloud security technologies and approaches.** Leaders should embrace a new operating model that brings together the cloud and cyber teams, taking into consideration the various aspects of modernization including talent operating model, DevSecOps, microservices, and more. The operating model can consider new offerings, implementations, and capabilities from the solution providers (such as cloud native access points) and cybersecurity leading practices (for example, National Institute of Standards and Technology's cybersecurity framework).

- **Determining the enterprise security requirements upfront.** It can be critical to make sure requirements are frictionless and baked into the development process, rather than bolted on. Select a platform with the applicable security layers based on enterprise requirements such as risk and regulation. For example, one cloud provider may have more mature, customized industry solutions for the Health Insurance Portability and Accountability Act (HIPAA), which aims to modernize the flow of health care information, versus another cloud provider, or might share data quarterly instead of affecting monthly compliance reporting.

- **Identifying who may likely do the work with a shared services model and cloud cyber team structure.** Develop conscientious cloud security inclusive of identity access, application-level security, network security, platform security, infrastructure security, and even code-level security. Ideally, this process should understand cloud provider service-level agreements and tap into relevant controls, risk strategies, and regulatory compliance leading practices. Organizations, for example, can set up a CoE with internal cloud and cyber team members as well as external cloud and managed service providers.



A new cloud modernization operating model for cloud security by design

IN MANY ORGANIZATIONS, cyber entities are siloed from the rest of the organization, often with minimal and/or incomplete transparency, which can impede trust. As companies migrate to the cloud, this issue will likely grow—and perhaps the migration itself become more difficult.

This makes security by design by an integrated team more critical. Indeed, evidence suggests this is already happening. Our interviews reveal that the biggest cloud-security shift has been a move away from developers handling security toward a more collaborative model across the technology C-suite. As recently as five years ago, a chief information officer (CIO) could oversee and fund cloud-migration projects, without security involved until the end. Today, there is more coordination among the chief security officer (CSO), chief information security officer (CISO), and CIO,[6] and this collaboration should trickle down into the modernization and migration CoE, allowing ownership to shift clearly across shared operating and responsibility models, from pre-contracting and across the development process.

This conscious, integrated approach can be used to help guide baseline analysis and security requirements during *discovery and cloud vendor selection*; to determine the *shared responsibility model* across the integrated CoE team with the cloud vendor; to set up *guardrails within the IT infrastructure* itself; and to *manage DevSecOps processes* with the applicable mix of talent and technology in place.

Discovery and cloud vendor selection

Pre-contracting, many cloud vendors expect a minimum baseline of analysis and security configurations that are handled by the client. These differ for each cloud vendor. Cloud teams can benefit from their cyber colleagues' perspectives to better address these areas during contracting. Post-contracting and during implementation, a joint cloud-cyber team approach can accelerate the team's ability to understand, assess, and reconfigure the cloud environment. It can also better position and prepare the CIO/CISO to perform the required third-party cloud vendor analysis risk assessments on business operations sustainability. This activity can even be written in the contract as ongoing annual activity for business continuity to avoid a "vendor lock-in" situation.

Additionally, in an ever-evolving cyberthreat landscape, cloud vendors could have insight into new cloud security product developments and implementation considerations and innovations to factor in to the operating model. In 2020, for example,

- The US Air Force created the first accredited cloud-native access point enabling the organization to connect to the cloud directly without a shared access point.[7]

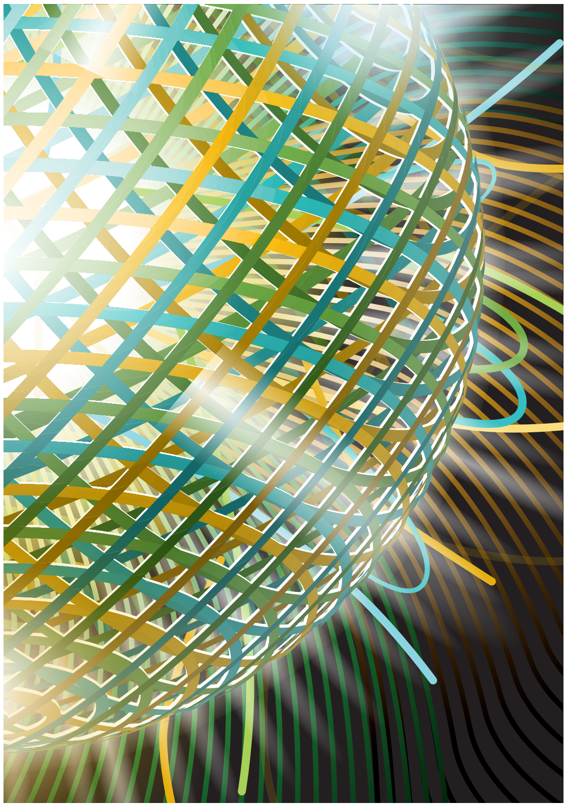
- One hyperscaler introduced confidential computing, which allows organizations to keep data encrypted in memory.[8]
- Organizations used "business process as a service" to scrub confidential or personally identifiable data.

Furthermore, better awareness of compliance **reporting requirements when negotiating cloud provider contracts** can help to determine that the data will be shared at the frequency required for reporting. To that end, a government organization was looking to report patching data to demonstrate continuous compliance, but data reporting at the frequency needed was not part of the cloud service-level agreement (SLA). To address the issue, it was able to pull source code data and integrate it into a manual reporting process. However, this could potentially have been a smoother process if addressed at the time of contracting.[9] To avoid challenges like this, assess these reporting needs and adjust SLAs or determine alternative reporting solutions.

The shared responsibility model

According to one industry study, 66% of surveyed executives report using cloud providers for baseline security; 73% believe public cloud providers are mainly responsible for securing SaaS solutions; and 42% believe they are responsible for securing infrastructure-as-a-service (IaaS) solutions.[10] Yet, while an organization might lean on the cloud provider for secure data centers and infrastructure, a shared responsibility model gets an organization only so far. It's still the organization's responsibility to secure the data and applications in the cloud. An integrated cloud cyber team enables clearer demarcation of where the organization's responsibility ends and the cloud vendor's begins (and vice versa) and guides on how to approach ongoing monitoring.

Unlike in an on-premise environment, with cloud, physical infrastructure is rented, and shared operating models may vary based on several contributing factors. For example, 40% of US states are operating in a federated model where the CISO oversees enterprise policy and agencies lead shared services; 10% of US states have a decentralized model where the CIO advises individual state agencies on policy.[11] Such has been the case in the New York City Cyber Command Initiative, where the project's deputy CISO and the agency's head of threat management adopted cloud technology to access security data from a government network-connected device in the city.[12]



CLOUD SECURITY INNOVATIONS ON THE RISE?

The threat landscape is continuously evolving with malicious actors employing new cyberattack tactics drawing on cryptocurrency mining and ransomware malware,[13] cyber artificial intelligence (AI) strategies that propagate data poisoning, generative adversarial network attacks, and bot manipulation.[14] Staying one step ahead of these attacks will require keeping up to date on the latest cloud cyber innovations. Our analysis of US patents applied for and granted between 2018 and 2020 shows that:

- Over half have focused on core cloud security technology with an emphasis on data encryption, authentication, tokens, control and storage modules, and more.
- There is a growing focus on organizations exploring the use of various advanced technologies such as AI/machine learning (ML), big data, and blockchain to improve cloud security.
- Apart from technological patents, organizations are focused on process engineering related to deployment, monitoring, programming, and provisioning.

While there were approximately 1,500 patents related to cloud security in 2018 and 2019, that number dropped to 500 last year, presumably due to the pandemic.[15] Thus, integrated teams with a solid backbone—operating model, processes, and controls—could be even more critical.

All information on cloud security patents is sourced from Derwent World Patents Index via Quid (https://quid.com). The purpose of the analysis is to identify general themes in cloud security. Deloitte did not review any individual patents in preparing this analysis.

Guardrails within the IT infrastructure

With security central to the vendor selection and responsibility model creation, the security team now has a strong vantage point to embed security into the cloud migration process by setting up base guardrails and minimum configurations to protect deployment before migration activities begin. For example, workload protection and secure landing zones can create a standard configuration template that is scalable and sustainable for rapid deployment of future applications without the need for reengineering. Given the cloud methodology is meant for Agile and DevOps, an organization without secure DevOps could be undertaking a significant amount of risk, and it could be an additional component to managing development during the migration process.

Manage DevSecOps processes with the desired mix in place

DevSecOps enables organizations to embed security into their workflow rather than as a bolt-on to development.[16] This allows developers and security professionals to have the shared goals of secure configurations continuously monitored, remediated, and managed for cybersecurity that drives creation of agile, resilient solutions. One insurance company, for example, migrated hundreds of applications to the cloud. DevSecOps enabled the cloud engineering team to better plan the architecture of the environment and build the cloud infrastructure to enable a secure migration. These processes can be further complemented by security automation and orchestration tools to implement structured workflows, automate security tasks, and prevent and detect threats.

- **Skills/talent.** Legacy technologies use virtual appliances such as those from firewall vendors to secure systems, whereas cloud technologies require understanding of security configurations. The shift requires a new talent operating model that moves work away from a develop, implement, and deploy framework, followed by security. Shift-left means security is involved upfront to provide baselines and configurations and set up architecture before go-live, reducing the need to be involved afterward. This leads to a very different talent operating and integration model.
- **Microservices.** As organizations look to modernize legacy applications to create more agile point-to-point services, cloud microservices operating models should consider vendor limitations and vendor portability/interoperability issues. Organizations can consider an agnostic middleware layer or microservices deployment model that helps the client resolve issues such as multi-cloud, as well as issues across enterprise systems.

DevSecOps enabled the cloud engineering team to better plan the architecture of the environment and build the cloud infrastructure to enable a secure migration.

The cloud security controls framework

ACROSS THE C-LEVEL, the move from on-premise to cloud typically requires a security mindset shift—from managing physical infrastructure to monitoring access across a “stateless distributed environment.” Importantly, the controls framework should address *network, platform, and infrastructure; user and data security; and core application security*.

Network, platform, and infrastructure

“Security by design” enables cloud developers and security teams to build guardrails into the infrastructure itself, establishing agile and secure processes. Therefore, before developers gain access to the cloud environment, the CIO and team should consider the leading approach to secure the network. It might be to embed guardrails into the cloud platform itself with “security by design” IT infrastructure, or to put in place restrictive “security by design” IT processes (e.g., authorized users responsible for reviewing infrastructure and source code before pushing to production). Industry-leading practices are moving away from perimeter-based security toward zero-trust network security architectures,[17] which enable more modular developer environments, as well as micro segmentation to allow for varying levels of infrastructure access and controls across the network, identity access, and applications.

As an example of the infrastructure approach, one asset management organization moved from private to public cloud and embedded hundreds of controls into the cloud platform at the code level before giving developers administrative access. These controls served as guardrails, resulting in the successful creation of a safe and compliant development environment. [18]

Alternatively, taking the process approach, another financial services organization removed or highly restricted developer keys to shift access and processes for code deployment. This prompted a major cultural shift for developers who previously had been able to push application changes live more autonomously; the privilege was now restricted to a small group. To reinforce the new protocol, the organization monitored for behaviors that deviated from the new controls process; in particular, one common scenario of developers now unauthorized to push live updates using a virtual machine to bypass the privilege-access management tooling, thereby potentially creating an exposed port. To address this risk, the organization implemented a security orchestration automation and response solution, enabling the company to collect security operations data; built a business case to detect security configuration changes; and orchestrated a custom workflow resolution for reviewing them. This gave the firm required visibility for proactive network monitoring and the ability to close open ports.

User and data security

Cloud migration often requires a new approach to identity. While previously physical credentials (e.g., building access) were acceptable authorization, in a distributed system that can be accessed anywhere, user-level access credentials and key management may be required. Identity access management protocols can be fed into a modularized identity platform with user-level access requirements.[19] A focus on data protection, privacy, resilience, and regulations can guide data access rights and user privileges. Executives should plan on balancing legal minimum requirements for encryption against too much encryption, which may slow down applications.[20]

Core application security

Before moving data or workloads to the cloud, the cloud and cyber teams should determine that the following minimum controls are in place:

- **Workload protection**—set base guardrails and minimum configurations to protect deployment. For instance, an organization may have preset templates for function-based or container-based applications.
- **Secure landing zone**—establish a secure environment covering account structures, security rules, and other foundational services, based on the operating model. For example, many organizations establish a public subnet and a private subnet as a public-facing landing zone versus a private virtual network for corporate users.
- **Secure by design/DevSecOps**—follow security by design and DevSecOps principles as discussed with the operating model recommendations.
- **Segmentation and zero trust**—employ network segmentation and zero-trust protocols. For example, the organization can restrict full administrative access to the application to only the senior-most developers with stricter security credentials and training, using containers for tiered access segmentation.
- **Attack surface management**—manage the vulnerability landscape with tailored services to enhance vulnerability and attack surface programs. Organizations can focus on identifying and assessing cloud assets through their life cycle and across different architecture layers. As an example, smart factories can think through data flows across cloud and edge tiers to determine security is in place across the ecosystem.

Risk management considerations for the cloud cyber program

CLOUD MIGRATION CAN reduce certain infrastructure security risks managed on-premise, with encryption, logging, private networking, monitoring, DDoS protection, automated patches, and other elements built into the cloud environment. However, many migrated systems and applications were not designed to operate online. To avoid disappointment on this front, before the cloud migration begins, organizations can conduct a cyber risk maturity assessment[21] to understand specific **technology**, **regulatory**, and **insider and supply chain risks** as well as recommended remediations.[22]

Technology risk

While some of these may be new territory for a cloud migration team, organizations face a number of potential technology risks to mitigate as part of their cloud cyber programs where an integrated cloud cyber team can help create a more secure, agile, and trustworthy outcome (figure 1).

Understanding technology risks can be critical—and potentially surprising for organizations that believe their systems to be well protected. One financial institution, for example, conducted a routine scan that found its technology stack had more than 100,000 built-in vulnerabilities, posing a high-security threat and requiring immediate remediation at the application, database, middleware, and code levels. This risk, in part, prompted the cloud migration and is an example of the legacy on-premise platform and applications risk noted in figure 1.[23] Had the cloud migration team opted to lift and shift the infrastructure without an understanding of these vulnerabilities first, the organization could have shifted certain risks to the cloud.

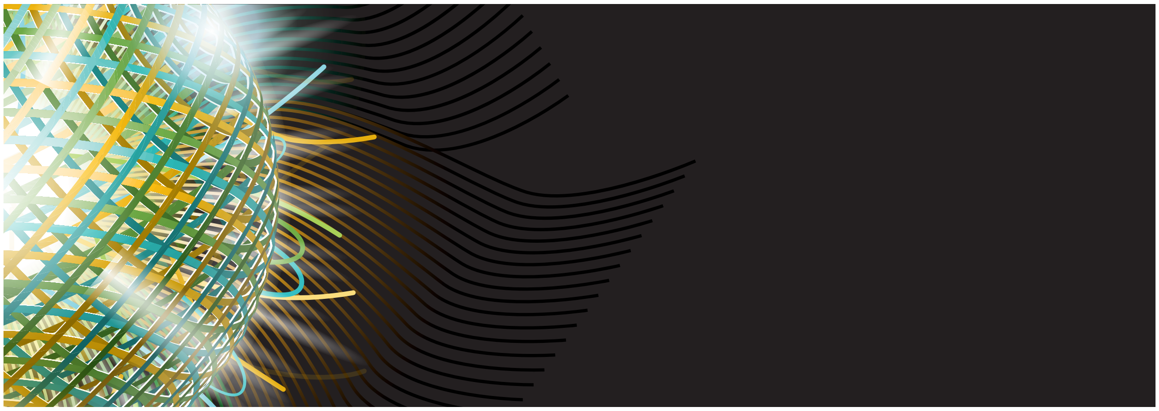


FIGURE 1

Four types of technology risk to consider and how to mitigate them

Technology risk	Manifestation of risk	Mitigation activity
Legacy on-premise platforms and applications	May *seem secure* due to higher control and physical proximity, but may be challenged to keep up with modern security standards or harbor known vulnerabilities.	Scan for vulnerabilities across the operating system, data centers, applications, middleware, and more.
Technology talent gap	Existing technology talent skillsets ranging from outdated coding languages, such as COBOL vs. Python, to functions like server management may not "migrate" to a cloud security team.	Reallocate existing talent to align with new parallel functions; reskill members of the workforce to achieve relevant coding experience (Python, Java) and to become certified in the required cloud vendor platform, inclusive of its security functions to manage talent risk.
Business continuity and disaster recovery	Legacy systems were not built with modern business continuity and disaster recovery plans in mind.	Consider using the cloud migration as an opportunity to update the business continuity and disaster recovery plan and to purchase additional cloud capacity for disaster recovery failover as part of a modern disaster recovery plan.
Misconfiguration risk	Can create an entry point for malicious actors.[a] According to one industry-based study on globally reported data breaches from January 2018 to December 2019, cloud misconfigurations resulted in 196 data breaches, with more than 33 billion records being exposed, and at an estimated cost of nearly US$5 trillion.[b] This misconfiguration risk cuts across cloud storage, database, and other services.[c]	Implement compliance-monitoring solutions to search for new configurations such as an unauthorized, open port that could expose the network to risk.

Notes: [a]Accurics, *State of DevSecOps report for summer 2020*, August 4, 2020; [b]DivvyCloud, *2020 Cloud misconfiguration report*, February 2020; [c]Ibid.
Source: Deloitte analysis.

In another example, a consumer goods organization running an outdated operating system had its data center taken over by ransomware when a software patch in the development environment went into production. Legacy security vulnerabilities that may have been somewhat protected by firewalls or perimeter security became exposed when moved to the cloud and weren't remediated. Had the organization had better orchestration across the cloud and cyber teams, with proper controls in place, this type of incident—which can significantly erode consumer trust—might have been avoided.

Managing technology risk requires a balance of understanding the existing and future technology at its core—a strength of the cloud migration team—and advising on how to desirably mitigate the vulnerabilities with a security approach rooted in leading practices across the four risk categories before the migration occurs and even before the cloud vendor is selected.

Regulatory risk

When assessing their cloud vendor and before migrating data or workloads, organizations should bring together cloud and cybersecurity teams to consider four essential regulatory compliance requirements that will likely impact downstream data workflows and system configuration, including global and regional data governance regulations, industry-based frameworks, and broader technology standards, as well as US government-specific regulations (figure 2).

A large global multinational organization doing work in the public and private sectors may have to contend with a larger number of data and technology regulations, while a smaller organization may still need to consider some combination of data, industry-specific, and regional regulations while devising its cloud data strategy and subsequent risk controls. However, even "smaller organizations" can still be subject to broader regulations across borders due to globalization of data.

A regulatory risk requirement review performed by a collaborative cloud and cyber team can enhance understanding of existing data frameworks, relevant risks, and required technology specifications to improve cloud vendor selection, SLA negotiations, and contracting.

Insider and supply chain risk

Finally, a cloud cyber risk program should consider *insider threats* and the organization's *supply chain* as specific threat vectors to balance security and trust inside and outside the organization and to avoid potential data leaks and spillage. Where the cloud migration activity could collide with insider risk is through sharing credentialed access or creating an open network access point. Cloud access security brokers that monitor for data loss and enforce controls across a multi-cloud environment are on the rise. They can help organizations to better manage internal threats[24] and monitor for data loss prevention, which about 75% of organizations indicate to be an important element of cloud security.[25]

Managing cyber risk requires organizations to look inward and outward at different insider risks and potential points of vulnerability across their supply chains. This can be achieved by an integrated cloud and cyber team, with visibility and transparency, communication, and collaboration and execution of an integrated compliance program (and tooling) across the supply chain. For more on this topic, see Deloitte Consulting LLP's *Looking beyond the horizon: Preparing today's supply chains to thrive in uncertainty*.

FIGURE 2

Four examples of regulatory risk categories to consider for the cloud cyber program

Regulatory risk category	Description	Example
Global and regional data governance regulations	Government data protection and privacy regulations require a data governance framework that addresses data ownership, data retention, breach response and coordination, need for a multi-country cloud strategy, etc.[a] Many regions or countries have their own data protection laws, creating the need for regulatory harmonization, especially for companies that have business or consumers across states and regions.	**General Data Protection Regulation (GDPR) in the European Union** has global implications as it requires a global understanding of data across the enterprise.[b] **North America and Latin America:** California Consumer Privacy Act, Canadian Privacy Laws, and Brazil, to name just a few. **Asia:** Thailand's Personal Data Protection Act as well as others for Australia, Japan, Hong Kong, Malaysia, Singapore, and a number of other countries in the region.
Industry-based framework examples	Certain industries, such as health care and insurance, banking and finance, education, and telecom, have specific laws and frameworks that regulate data governance policies and create additional complexity.	In the United States: • **Health care and insurance:** HIPAA • **Banking and finance:** Sarbanes–Oxley Act, Gramm-Leach-Bliley Act, Payment Card Industry Data Security Standard (PCI DSS) • **Education:** Family Educational Rights and Privacy Act (FERPA) • **Telecom, media, and entertainment:** Video Privacy Protection Act, Motion Picture Association of America (MPAA)
Broader technology standards	Cybersecurity standards protect the cyber environment—users, networks, devices, software, processes, applications, services, systems, etc.	**The National Institute of Standards and Technology (NIST) cybersecurity framework** is a leading technology standards framework for commercial organizations in the United States. Its five functional elements include: Identify, Protect, Detect, Respond, and Recover.[c] While designed from a traditional infrastructure perspective, the core principles can be extended for cloud deployments. **CIS benchmarks** that provide product configuration guidelines across vender solutions.
US government-specific frameworks	There are additional requirements for government agencies to use modern cloud technologies while determining the security and protection of federal information.[d] Cloud solution providers need to ensure compliance with these requirements to serve federal agencies.[e] Some frameworks place additional restrictions, such as on export data being shared outside of the US, requiring additional data segmentation and security controls.	**Cybersecurity Maturity Model Certification (CMMC)** **The US Federal Information Security Management Act and the Federal Information Security Modernization Act** focus on standards and guidelines to modernize federal security practices and the cyber risk supply chain. **The US Federal Risk and Authorization Management Program** enables government agencies to use modern cloud technologies, while ensuring the security and protection of federal information.[d] **International Traffic in Arms Regulations (ITAR)** **Defense Federal Acquisition Regulation Supplement (DFARS)** related to processing, storing, and transmitting covered defense information, and others.

Notes: [a]Alex Tolsma, "GDPR and the impact on cloud computing," Deloitte, accessed January 7, 2021;[b]Klaus Julisch and Florian Widmer, "GDPR and the impact on cloud computing," Deloitte, accessed January 7, 2021;[c]National Institute of Standards and Technology, "Cybersecurity Framework," accessed January 7, 2021;[d]US General Services Administration, "FedRAMP," accessed January 7, 2021;[e]Josh Fruhlinger, "What is FedRAMP? How cloud providers get authorized to work with the US government," CSO, April 8, 2018.
Source: Deloitte analysis.

Cloud program scenarios

FINALLY, THE TYPE of cloud program itself will impact the operating model and subsequent program. The following graphic details four common cloud program scenarios and high-, medium-, and low-complexity considerations for the integrated cloud and cyber team (figure 3).

FIGURE 3

Cloud program scenarios: Risk, control, and compliance considerations

	Risk	Control	Compliance
DATA CENTER MIGRATION—LIFT AND SHIFT	**Low complexity** Hyperscalers accredited with essential compliance certifications data, standards, industry, regional, etc.	**Low complexity** Unmatched investment from providers in cloud data center security	**Low complexity** Vendors have had considerable regulatory compliance validation rigor
APPLICATION MIGRATION—LIFT AND SHIFT	**High complexity** Improper cloud configuration is a top security threat, along with organizational and regulatory risks that require data and governance planning	**Medium complexity** Over-reliance on built-in security technology features requires more coordination of broader security controls and requirements	**Low complexity** Mature compliance automation and monitoring market with innovation in multicloud security orchestration
CLOUD NATIVE DEVELOPMENT—SHIFT AND ADOPT	**Low complexity** Refactoring/redeployment of applications	**Medium complexity** Embedding cybersecurity into new products, services and channels is a concern,* though organizations gain code-level interoperability of java-based systems	**Medium complexity** Organizations should embrace security by design principles for cloud native development
ON-PREMISE/CLOUD MIGRATION/CLOUD NATIVE COMBINATION	**High complexity** Large threat surface area across complex, heterogeneous infrastructure requiring coordination across cloud cyber teams	**High complexity** Variety of control mechanisms needed across on-premise and multicloud infrastructure layers from ownership model to information flow across the enterprise	**Medium complexity** A broader range of applicable compliance requirements requiring more automation for auto remediation and anomalous activity detection

Note: * Julie Bernard and Mark Nicholson, *Reshaping the cybersecurity landscape,* Deloitte Insights, July 24, 2020.
Source: Deloitte analysis.

Conclusion: Getting started

CLOUD DEVELOPERS CAN'T be expected to become security specialists overnight, or to stay on top of the evolving threat landscape. They can, however, embrace working on integrated cloud and cyber teams that bring target operating model, shift-left mentality, microservices, risk, control, and compliance experience to bear during integral points in the cloud migration life cycle and with "security by design" principles. For these teams, here are a few parting thoughts to consider that can help guide the cloud modernization and migration journey, bolster business and technology resilience, enhance security, and reinforce customer trust:

- **Develop a modernization operating model that brings together innovative new approaches and technologies.** Include new talent models, DevSecOps, and microservices and consider precontracting responsibilities and breakdown of roles and responsibilities across a shared responsibility model. A cloud provider's investment in security may be better than your security at present.

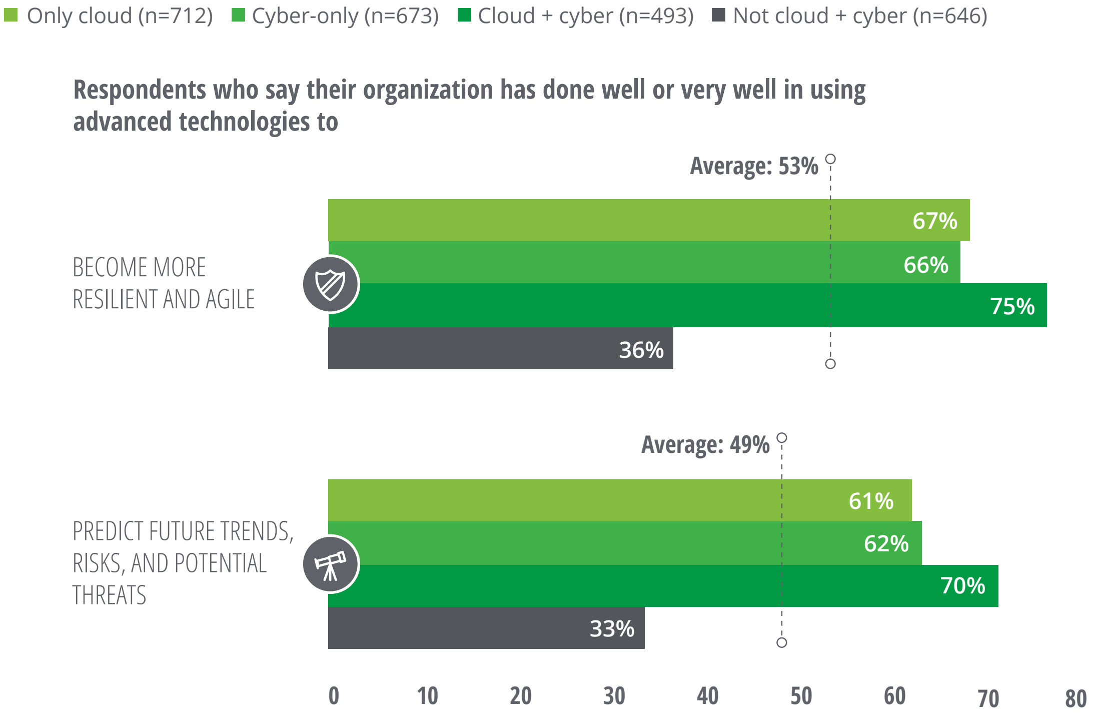
- **Develop a controls framework that allows you to lever up with a more integrated cloud and cyber approach.** The process of migration provides an opportunity and necessity to rethink security models, tools, and capabilities. The cloud controls framework should start with an understanding of the data requirements and encompass user/identity level, network/infrastructure/application, and core application controls. Organizations can conduct a risk assessment across their technology, regulatory, and cyber environment; implement the appropriate controls to fill gaps and remediate those risks; and migrate workloads to secure cloud landing zones.

- **Manage compliance with innovative approaches.** There continues to be new and innovative processes and approaches available to automate and ease the burden of modern compliance monitoring. Stay informed of the latest tools and processes.

By bringing together each of these components through a cloud migration CoE that includes an integrated team of cross-skilled cloud and cyber professionals, organizations can be better positioned to address the need for a broad "life cycle" to prioritize security risk levels and mitigate those risks with the proper governance, risk management, and compliance across these security components. Ultimately, the cloud migration provides an opportunity for not just greater business and technology resilience but also potentially improved security and enhanced consumer trust.

Appendix: Integrated cloud cyber strategies drive greater business and technology resilience

Integrated cloud cyber strategies drive greater business and technology resilience



Respondents who say their organization has done well or very well in using advanced technologies to

Notes: Mature cloud-only strategies were determined based on those who answered “Well” or “Very Well” to the question, “How well do you think your organization has done (or is doing) in transitioning business systems to the cloud to support remote working (e.g., collaboration tools, VPN, data centers, servers, etc.) in July through September 2020?”

Mature cyber-only strategies were determined based on those who answered “Well” or “Very Well” to the question, “How well do you think your organization has done (or is doing) in managing evolving cybersecurity threat detection, remediation, and prevention in July through September 2020?”

And cloud + cyber were determined by combining those who responded “Well” or “Very Well” to both of these questions.

Source: Deloitte analysis of 2021 Resilience study data.

Endnotes

1. Steve Morgan, “Cybercrime to cost the world $10.5 trillion annually by 2025,” *Cybercrime Magazine*, November 13, 2020.
2. Karthik Ramachandran and David Linthicum, “Why organizations are moving to the cloud,” Deloitte Insights, March 5, 2020.
3. Deloitte, *The future of cyber survey 2019*, 2019.
4. Analysis of data from a survey of 2,260 C-level executives and senior public-sector leaders from 21 countries, conducted by KS&R Inc. in July, August, and September 2020, for the Deloitte Global 2021 Resilience study, *Building the resilient organization: 2021 Deloitte Global resilience report*.
5. Those with mature cloud programs are understood as those who responded “Well” or “Very Well” when asked how well their organization has done or is doing in “Transitioning business systems to the cloud to support remote working (e.g., collaboration tools, VPN, data centers, servers, etc.),” and for those with a mature cyber program, those who responded “Well” or “Very Well” when asked how well their organization has done or is doing in “Managing evolving cybersecurity threat detection, remediation, and prevention” *during the period of July–September 2020*.
6. Deloitte experience.
7. Jason Miller, “Air Force’s game-changing approach to cloud accreditation,” *Federal News Network*, July 30, 2020.
8. Sunil Potti and Eyal Manor, “Expanding Google Cloud’s Confidential Computing portfolio,” Google Cloud blog, September 8, 2020.
9. Deloitte experience.
10. *Help Net Security*, “Top security risks for companies to address as cloud migration accelerates,” June 11, 2020.
11. NASCIO and Deloitte, *States at risk: The cybersecurity imperative in uncertain times*, Deloitte Insights, October 14, 2020.
12. Ryan Johnston, “Remote work marked ‘culmination’ of NYC Cyber Command’s cloud initiatives, agency heads said,” *StateScoop*, October 7, 2020.
13. Alicia Hope, “Almost all cyber attacks on cloud servers involve cryptocurrency mining, a new study found,” *CPO Magazine*, September 25, 2020.
14. Veronica Combs, “3 ways criminals use artificial intelligence in cybersecurity attacks,” *Tech Republic*, October 7, 2020.
15. Deloitte analysis of patent data from 2018–2020 for targeted keywords focused on cloud and cybersecurity.
16. Vikram Kunchala et al., “DevSecOps and the cyber imperative,” Deloitte Insights, January 16, 2019.
17. Christina Brodzik, Kristi Lamar, and Anjali Shaikh, *Tech Trends 2021*, Deloitte Insights, 2021.
18. Deloitte experience.
19. David Linthicum et al., “The future of cloud-enabled work infrastructure,” Deloitte Insights, September 23, 2020.
20. David Linthicum, “Three cloud security problems that you can solve today,” Deloitte On Cloud Blog, September 20, 2018.

21. Roland Labuhn, "Trend 7: Modernizing core technologies" from *Tracking the trends 2020*, Deloitte Insights, February 3, 2020.

22. Aaron Brown et al., *Achieving cyber governance risk & compliance in the cloud*, Deloitte, 2019.

23. Deloitte experience.

24. Itir Clarke, "What is CASB (Cloud Access Security Broker)?" ProofPoint, June 20, 2019.

25. Cloud Security Alliance, *The cloud balancing act for IT: Between promise and peril*, January 2016.

Acknowledgments

The authors would like to thank **Douglas Bourgeois**, **Aaron Brown**, **Mark Campbell**, **Mike Kavis**, **Timothy Li**, **Ryan Lindeman**, **Lauren Nalu**, and **Tony Witherspoon** for their insight. A special thanks to **David Linthicum**, **Natasha Buckley**, **Monika Mahto**, **Lisa Beauchamp**, **Purnima Roy**, **Jayee Hegde**, **Bhadra Gordon**, **Kavita Saini**, **Aparna Prusty**, and **Kimberly Donohue** for their perspective and support.

About the authors

Deborah Golden | debgolden@deloitte.com

Deborah Golden is a principal at Deloitte & Touche LLP and the US Cyber & Strategic Risk leader for Deloitte Risk & Financial Advisory. With 25 years of cross-industry experience, she currently leads one of Deloitte's largest growth initiatives, positioning cyber for strategic differentiation by converging business, technology, and cyber to provide solutions beyond the technology organization as business continues to operate in a "Cyber Everywhere" world. She primarily helps commercial organizations and government agencies navigate multifaceted cyber problems and transform business or mission strategies and operations. She received a bachelor's degree in finance at Virginia Tech and a master's degree in information technology at George Washington University.

Vikram Kunchala | vkunchala@deloitte.com

Vikram Kunchala, a principal at Deloitte & Touche LLP, is the Consumer industry leader for the Cyber & Strategic Risk practice of Deloitte Risk & Financial Advisory. He also serves as the Cyber Cloud leader for the Cyber Risk Services practice of Deloitte Risk & Financial Advisory. He has more than 20 years of experience in design and implementation of cybersecurity solutions and cyber risk management programs. His areas of specialty include application security, cloud security, identity and access management, and cyber threat and vulnerability management. He has extensive experience helping technical and business organizations achieve strategic and tactical objectives.

Amod Bavare | abavare@deloitte.com

Amod Bavare is a principal of the Cloud Engineering division at Deloitte Consulting LLP and leads Deloitte's global cloud migration and modernization market efforts across all industries and sectors. Bavare has more than 25 years of IT industry experience. He specializes in renovating architecture and migrating complex enterprise applications to the cloud, essentially helping to create value by modernizing clients' legacy systems. He is on the board of the Indo-American Chamber of Commerce of Greater Houston and serves as the local office lead for United Way annual donations campaign for Deloitte Consulting.

Bhavin Barot | bbarot@deloitte.com

Bhavin Barot is a principal in Deloitte Advisory's Cyber practice with more than 20 years of experience in helping clients enhance their cyber program, meet security standards, and maintain continuous compliance. His focus is on application security, business process controls, and information technology controls design and implementation. He has led numerous strategic project initiatives encompassing IT security and risk management strategy, governance, cybersecurity, identity management, technology and organizational resiliency, and service management, in addition to several large global risk and security transformation projects.

Ritesh Bagayat | rbagayat@deloitte.com

Ritesh Bagayat is a senior manager in Deloitte & Touche's Cyber Risk Services practice. He has over 14 years of experience in design and implementation of cybersecurity and regulatory compliance solutions. His areas of expertise include application modernization, cloud security, identity management, application security, process controls, and regulatory compliance. He has extensive experience in architecting, designing, and implementing security solutions for large-scale enterprise digital transformations.

Diana Kearns-Manolatos | dkearnsmanolatos@deloitte.com

Diana Kearns-Manolatos is a senior manager in the Deloitte Center for Integrated Research where she analyzes market shifts and emerging trends across industries. Her research focuses on integrated technology strategies and the cloud. She also supports the Deloitte MIT Sloan Management Review Future of the Workforce Big Ideas research initiative and has more than 15 years of award-winning marketing communications expertise to align insights with business strategy. She speaks on technology and women in leadership and holds a bachelor's and master's degrees from Fordham University.

Jay Parekh | jparekh@deloitte.com

Jay Parekh is a senior analyst with the Deloitte Center for Integrated Research. He has more than six years of experience in research and analysis focused on emerging technologies and digital innovations related to cloud computing, augmented and virtual reality, the Internet of Things, and other advanced technologies. He also focuses on developing Deloitte's perspectives on cross-industry topics such as climate change and sustainability. He specializes in applying quantitative and qualitative research techniques to enable data-driven insights.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Rob Masse
Partner | Risk Advisory | National Leader, Cloud Security | Deloitte Canada
+1 514 393 7003 | rmasse@deloitte.ca

Robert is a Partner and the National Leader for Cloud Security in Deloitte Canada's Risk Advisory practice.

Jean-Francois Allard
Partner | Risk Advisory | National Leader, Crisis and Resilience | Deloitte Canada
+1 514 393 7147 | jeallard@deloitte.ca

Jean-Francois is a Partner and the National Leader for Crisis and Resilience in Deloitte Canada's Risk Advisory practice.

Aaron Fleming
Director | Risk Advisory | Cloud Security | Deloitte Canada
+1 416 521 4632 | aafleming@deloitte.ca

Aaron is a Director for Cloud Security in Deloitte Canada's Risk Advisory practice.

Naresh Kurada
Director | Risk Advisory | Cloud Security | Deloitte Canada
+1 416 956 9194 | nkurada@deloitte.ca

Naresh is a Director for Cloud Security in Deloitte Canada's Risk Advisory practice.

Vikram Kunchala
Principal | Cyber Cloud leader | Consumer Cyber & Strategic Risk industry leader | Deloitte & Touche LLP
+1 713 982 2807 | vkunchala@deloitte.com

Vikram is the Cyber Cloud leader for the Cyber Risk Services practice of Deloitte Risk & Financial Advisory.

Bhavin Barot
Principal | Advisory Cyber | Deloitte Consulting LLP
+1 313 396 3472 | bbarot@deloitte.com

Bhavin Barot is a principal in Deloitte Advisory's Cyber practice with more than 20 years of experience in helping clients enhance their cyber program, meet security standards, and maintain continuous compliance.

Amod Bavare
Principal | Global Cloud Migration leader | Deloitte Consulting LLP
+1 713 982 3040 | abavare@deloitte.com

Amod Bavare is a principal of Cloud Engineering at Deloitte Consulting LLP and leads Deloitte's global cloud migration and modernization market efforts across all industries and sectors.

Deloitte Center for Integrated Research

Diana M. Kearns-Manolatos
Senior manager | Subject Matter Specialist | Deloitte Services LP
+1 212 436 3301 | dkearnsmanolatos@deloitte.com

Diana M. Kearns-Manolatos is a senior manager with the Deloitte Center for Integrated Research focused on integrated technology transformation and the cloud.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Kavita Saini, Aparna Prusty, and Nairita Gangopadhyay
Creative: Nagaraju Mangala, Sanaa Saifi, and Victoria Lee
Promotion: Alexandra Kawecki
Cover artwork: Daniel Hertzberg

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.