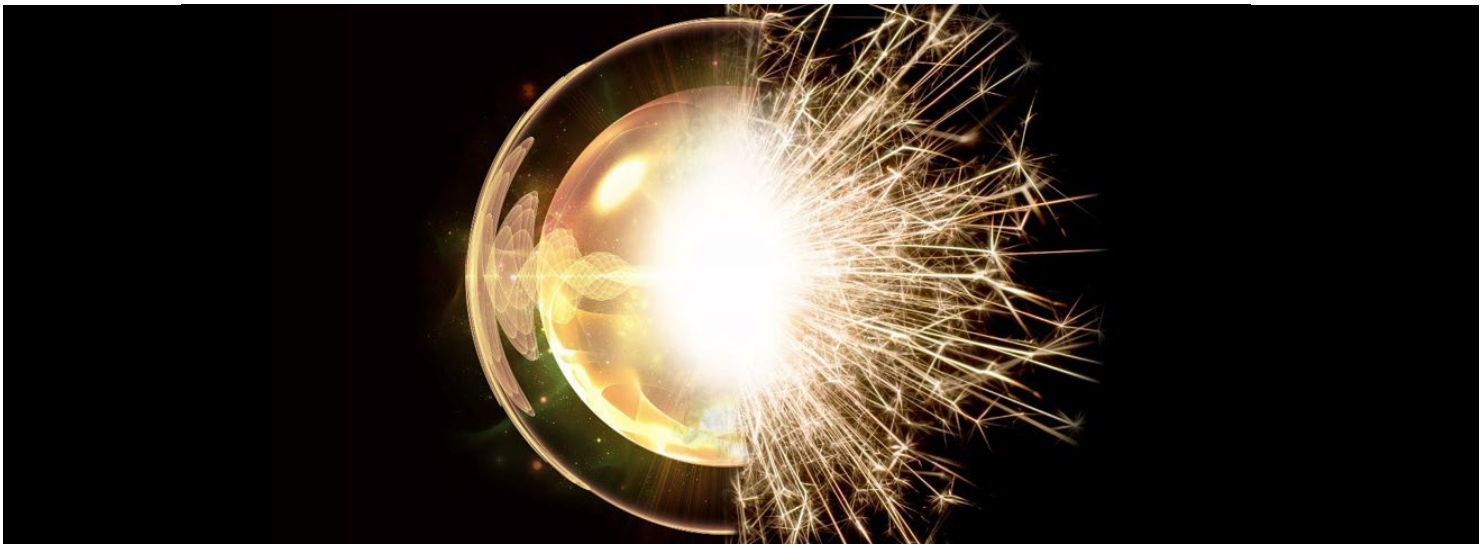
Deloitte.



Remove barriers to accelerate AWS adoption

Manage cyber risks related to customer-control responsibilities

Cyber risk capabilities for AWS

Amazon Web Services (AWS) provides innovative services that include a broad set of public cloud capabilities. AWS's scalability, elasticity, flexibility, and business benefits are driving adoption at a rapid pace across many industries and sectors as a major cloud technology enabler for digital transformation. As organizations adopt cloud to transform their businesses, cyber risk management should also be transformed.

A strategy that leverages Deloitte's Secure.Vigilant.Resilient.™ framework, coupled with the native services built in AWS, can help enterprises move to the cloud with confidence that cyber risks are being addressed.

Like each major technology shift over the years, cloud has both enabled business innovation and introduced new capabilities for enterprises to master, as well as cyber risks to manage. Not only are new capabilities introduced, but many existing capabilities are performed differently in the cloud.

For example, patching the source VM configuration and deploying the updated image with automation is the leading practice rather than patching in place. Adopting AWS requires an enterprise to be accountable for the customer control responsibilities related to AWS services. These responsibilities vary and have different implications depending on the specific services used.

There are a variety of enhanced security capabilities introduced by cloud innovation that should be integrated as part of the security roadmap. The traditional enforcement and perimeter-based approaches for IT security are no longer enough. CISOs have the opportunity to show that they are business enablers by enhancing their existing security capabilities and integrating with the AWS cloud. For example, their strategic roadmap should include capabilities tailored to an organization's risk appetite, control responsibilities, and specific cloud use cases for AWS.

Capabilities can include native AWS security features such as Macie, Trusted Advisor, and GuardDuty to name a few.

In-house security technology can be extended and integrated with AWS to leverage existing investments such as the enterprise identity and access management capability. Also, there are new cloud security services from the AWS Marketplace that are specifically built as cloud-aware services that can be taken advantage of. Given the switch from client/server to application programming interface (API)-based technologies and serverless computing, the tools and techniques used to address cyber risk should be updated. Automating security controls across DevSecOps, Continuous Integration and Continuous Delivery (CI/CD), and orchestration capabilities will be a necessity if the security organization is going to keep pace as the enterprise scales out cloud usage.

> "Through 2022, at least 95% of cloud security failures will be the customer's fault." [1]

[1] "Is the Cloud Secure?", Gartner, Inc., March 27, 2018, https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

Is cyber risk really any different in the cloud?

Understanding the shared responsibility model

The same fundamental cyber risks exist in the cloud, but responsibility has shifted. If you run your own data center, then you are responsible for the integrity of the software for the virtualization layer and underlying infrastructure. With the move to the cloud, this responsibility is delegated and now rests with AWS. Conversely, if you use an Application Service Provider (ASP), and you move applications to the cloud, the responsibility for patching and monitoring the applications will remain with you.

Deloitte's Shared Responsibility Model for cloud services defines the security control responsibilities between the enterprise and cloud provider. The model helps clarify the responsibility of AWS for the inherited control domains related to Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

Security *of* the cloud

AWS is responsible for the reliability, security, and compliance of the services that make up the AWS cloud. Some of the responsibilities include the integrity of the software for the virtualization layer and underlying infrastructure. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.[2]

Security *in* the cloud

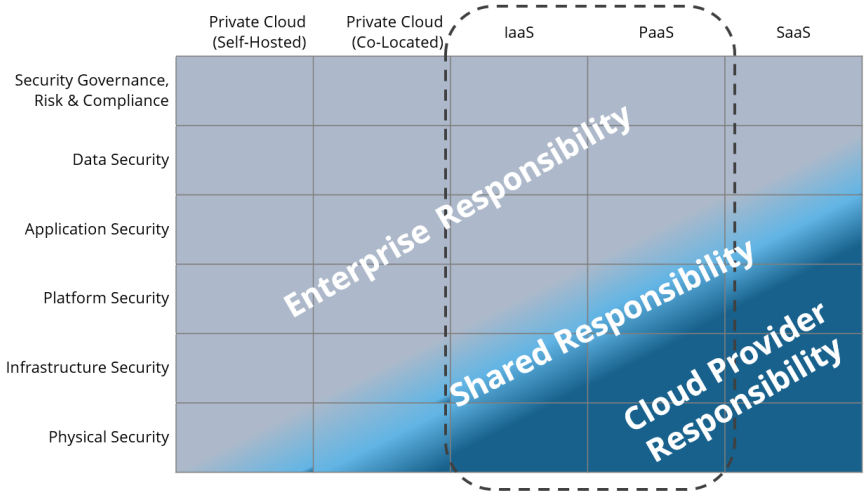
The enterprise is expected to understand the appropriate configuration of AWS services and virtual components they deploy to AWS. Therefore, the enterprise should implement controls to secure their own AWS cloud environment depending on their selection of AWS cloud services. For example, if a customer deploys an Amazon Elastics Compute Cloud (Amazon EC2) instance, they are responsible for the management of the guest operating system, application software or utilities installed, and the configuration of the AWS features such as security groups related to each instance.

The enterprise also should consider the sensitivity of the data placed in the cloud and their regulatory environment in determining their responsibility for cyber risk.

As an example, there are decisions that the enterprise should consider related to what encryption and key management model for AWS is acceptable according to their security policy and regulatory requirements. AWS offers several key management approaches, but the enterprise should decide and implement their preferred option.

What AWS is doing

To maintain security, comply with regulatory requirements, and fulfill committed responsibilities, AWS maintains a series of assurance programs across multiple industries and jurisdictions to inform and support AWS customers. These assurance programs provide analysis and reporting on compliance with laws and regulations for AWS services. Additionally, AWS Artifact provides on-demand access to AWS security and compliance reports as well as specific online agreements.



Deloitte's shared responsibility model for cloud services

[2] "Shared Responsibility Model", AWS, https://aws.amazon.com/compliance/shared-responsibility-model/

Reports available in AWS Artifact include Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, certifications from accreditation bodies across jurisdictions, and reporting on compliance with regulations that compares the implementation and operating effectiveness of AWS security controls.

A baseline for managing risks associated with customer responsibilities

From strategy to implementation, Deloitte is a leader in helping clients address challenges as they embrace cloud, mobile, social, and analytics technologies. Deloitte created the Secure.Vigilant.Resilient framework, which enables the full spectrum of cyber risk capabilities and tools, that when coupled with AWS native services provide preventative, detective, and corrective controls. With security and architecture in mind, Deloitte aligned to the AWS cloud adoption framework, by incorporating leading practices from industry-specific security and compliance practices, and leveraging Deloitte's extensive cyber risk experience. It focuses on delivering end-to- end cloud cyber risk capabilities and incorporates considerations for privacy, security, monitoring, incident response, and governance for integrating the AWS cloud across the enterprise. There are seven cyber risk domains in Deloitte's AWS Cyber Risk Management framework.

The Secure pillar of Deloitte's Secure.Vigilant.Resilient framework provides capabilities including data loss prevention, device hardening, identity and access management (IAM), and network and infrastructure security.

At the core of the Secure pillar is the first domain, **Network and Infrastructure security,** encompassing the virtual infrastructure with a focus on protecting network traffic, hardening endpoints and protecting services using AWS Shield and Web Application Firewall (WAF). The second domain, **IAM**, is another core part of the Secure pillar. IAM is designed to help address different cloud requirements for authentication, authorization, access governance, and accountability. Specific elements include multi-factor authentication, privileged access management, and access certification.

A fundamental requirement of a commercial-grade cloud platform is a security design that incorporates multiple layers of protection to help withstand potential cyberattacks. Multiple technical security controls are embedded to harden and protect AWS native services within the integrated platform. The third domain of the Secure pillar is **Data Protection**, which covers controls recommended for protecting data at rest, in transit, and in use. Core elements are encryption, key, and certificate management using AWS Key Management Service (KMS), CloudHSM, and AWS Certificate Manager (ACM).

Deloitte's Vigilant pillar includes the integration of event sources across on-premises and AWS sources to enable security teams with contextual information that can identify, detect, and respond more effectively to security threats. The fourth domain, **Logging and Monitoring**, involves techniques for detecting security events, collating a multitude of log sources, and integrating with a Security Information and Event Monitoring (SIEM) to monitor the AWS cloud to enable the enterprise to identify where critical data assets live, who accesses them, and how they are used.

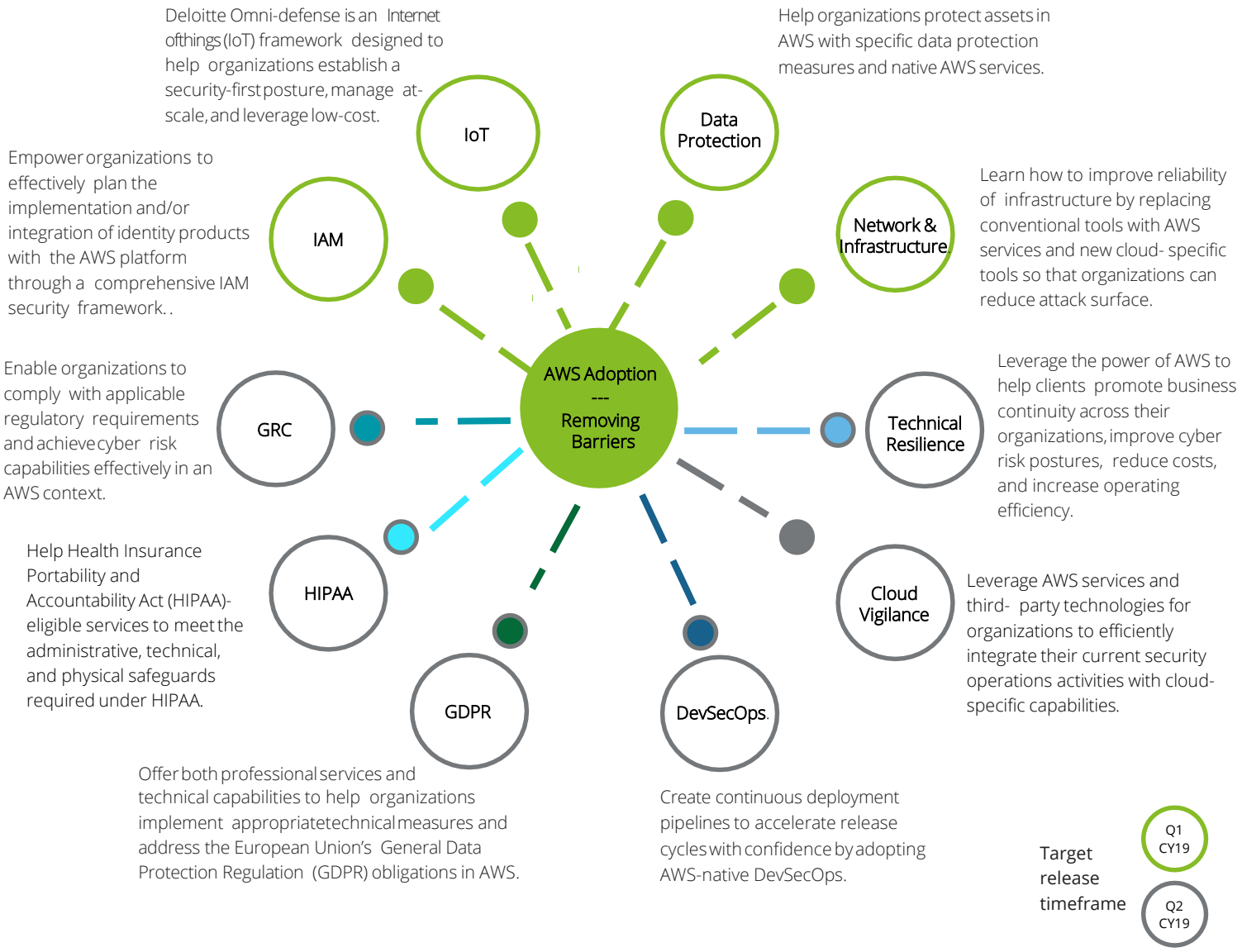
Creating a mature Vigilant capability includes extending security monitoring to a virtualized cloud infrastructure, managing ephemeral assets, and integrating threat intelligence. It also requires AWS-aware alerts leveraging a variety of services such as CloudTrail, Amazon CloudWatch, AWS Lambda, Amazon GuardDuty and a SIEM.

The fifth domain, Resilient, is its own pillar including elastic designs for "always on" capabilities, new models for contingency planning, recovery, and resilience. As cloud computing becomes a more integral part of core business operations, there is necessity to reduce downtime due to disruptions from minutes to seconds. AWS provides accessible features such as scalable, on-demand APIs that allow companies to cost-effectively create redundant infrastructure and backups with low latency to reduce disruption. Other design concepts and tools are cross-region replication of virtual instances, multi-availability zone deployments, and data archiving services like Amazon Glacier.

The sixth domain, **DevSecOps**, encompasses secure configuration, vigilant security monitoring, and resilient deployment designs. The concepts are brought together to achieve business goals with secure software. DevSecOps leverages the agility of the cloud to automate security and fuse it into the DevOps process. This replaces the traditional waterfall gates of software development with its manual approvals. Done correctly, DevSecOps can increase agility and application enhancement velocity.

Deloitte's AWS Cyber Risk framework provides for security capabilities and leading practices. To define and manage the cyber risk requirements specific to your enterprise, the seventh aspect, **Governance, Risk, and Compliance** (GRC), provides guidance for establishing governance, policy, standards, processes, technology, and reporting to achieve enterprise goals.

Index of Deloitte / AWS Whitepapers on Cyber Risk



Deloitte and AWS

Going deeper into Deloitte's AWS capabilities

As one of the largest cyber risk professional services practices of its kind, Deloitte is sharing some lessons learned based on our experience of helping clients with their cloud transformations. With capabilities across the wide spectrum of cyber risk domains, Deloitte combines this breadth of experience with deep knowledge of AWS native services to assist clients in addressing their portion of the customer responsibility model. This experience with clients across many industries has been captured in whitepapers on individual topics derived from the Secure.Vigilant.Resilient. framework. Three of the papers discuss industry-specific requirements related to the topics of GRC, IoT, HIPAA, and General Data Protection Regulation (GDPR). There are six additional papers that provide information on enhancements needed for security capabilities: Network and Infrastructure, IAM, Data Protection, DevSecOps, Cloud Vigilance, and Technical Resilience. Refer to the figure above ("Index of Deloitte / AWS Whitepapers on Cyber Risk") for additional details for each paper.

Deloitte's cyber risk services

For several decades, Deloitte's Cyber Risk Services group has worked with organizations across many industries. As a designated AWS Premier Consulting Partner with the Security Competency in Security Engineering, we offer services that are built upon our demonstrated delivery methodology for AWS and we leverage our deep technical experience, industry and regulatory knowledge, vendor ecosystems, and our access to a large global network of experienced professionals. We help clients across the cyber risk spectrum. On one end of the spectrum, developing a comprehensive strategy for an organization beginning their cloud journey to better understand and address of their responsibilities as an AWS customer, and on the other end, implementing a very specific capability or a particular security tool. We leverage our breadth of capability across cyber risk domains, and our depth of knowledge of AWS, to tailor an approach to help clients secure their AWS environments and enabling the acceleration of workload deployments and ultimately, business outcomes.

Strategy and Scoping

Establish controls and responsibilities specific for the cloud to address governance model and technology gaps that can support risk reduction efforts

Baseline security requirements; identify and prioritize gaps to create the prioritized roadmap for cyber risk enhancements as an integrated part of your AWS strategy

Implementation

Leveraging Deloitte templates, baseline a reference security architecture and repeatable design patterns with a set of security and sprint plans

Build, test and deploy a security architecture with integrated controls; Deploy and document updated processes

Optimize and scale security with a support model to baseline and sustain operation of security services

Providing value at the intersection of risk, regulation, and AWS

- We are an APN Premier Consulting Partner and an AWS Security Competency Partner (Launch Partner)
- We have a dedicated Cloud Cyber Risk practice and relationships with AWS cloud security vendors
- Our cyber risk professionals have experience with design and implementation of secure AWS environments using DevSecOps
- Our services are built on AWS technologies, leveraging pre- built integrations that our clients can leverage to shorten time-to-value
- We have developed standard architecture patterns that enable a cloud-aware, end-to-end AWS security monitoring solution
- Our rich experience across a range of industry sectors guides focus on the regulations, standards, and cyberthreats that are likely to impact your business
- We have approximately 3,100+ cyber risk professionals in the US
- Part of a global team of 21,000 risk management and cyber risk professionals across the Deloitte Touche Tohmatsu Limited network of member firms

The strength of the Deloitte / AWS relationship

Our relationship brings together Deloitte's extensive industry experience in cyber and enterprise risk management with **the security-enabled cloud infrastructure of AWS**. In 2006, AWS began offering IT infrastructure services to businesses in the form of web services—now commonly known as cloud computing. Today AWS provides a highly **reliable, secure, scalable, low-cost** infrastructure that powers hundreds of thousands of businesses in 190 countries around the world, with **over a million active** customers spread across many industries and geographies.

Deloitte can help organizations adopt AWS securely and establish a security-first cloud strategy. Deloitte is a leading information technology and advisory company. Deloitte is an **APN Premier Consulting Partner and an AWS Security Competency Partner (Launch Partner)** and was one of the first eight organizations globally to achieve the **Security Competency** as a launch partner. Deloitte's vast experience in Cyber Risk, combined with its extensive experience with AWS and Cloud technologies, enable us to provide **end-to-end** security solutions.

Authors

Deloitte & Touche LLP

Aaron Brown
Partner, Cyber Risk Services
AWS Alliance Leader
aaronbrown@deloitte.com

Mark Campbell
Senior Manager, Cyber Risk Services
Cloud Security Architect & AWS Alliance Manager
markcampbell@deloitte.com

Ravi Dhaval
Manager, Cyber Risk Services
Cloud & IoT Security Architect
rdhaval@deloitte.com