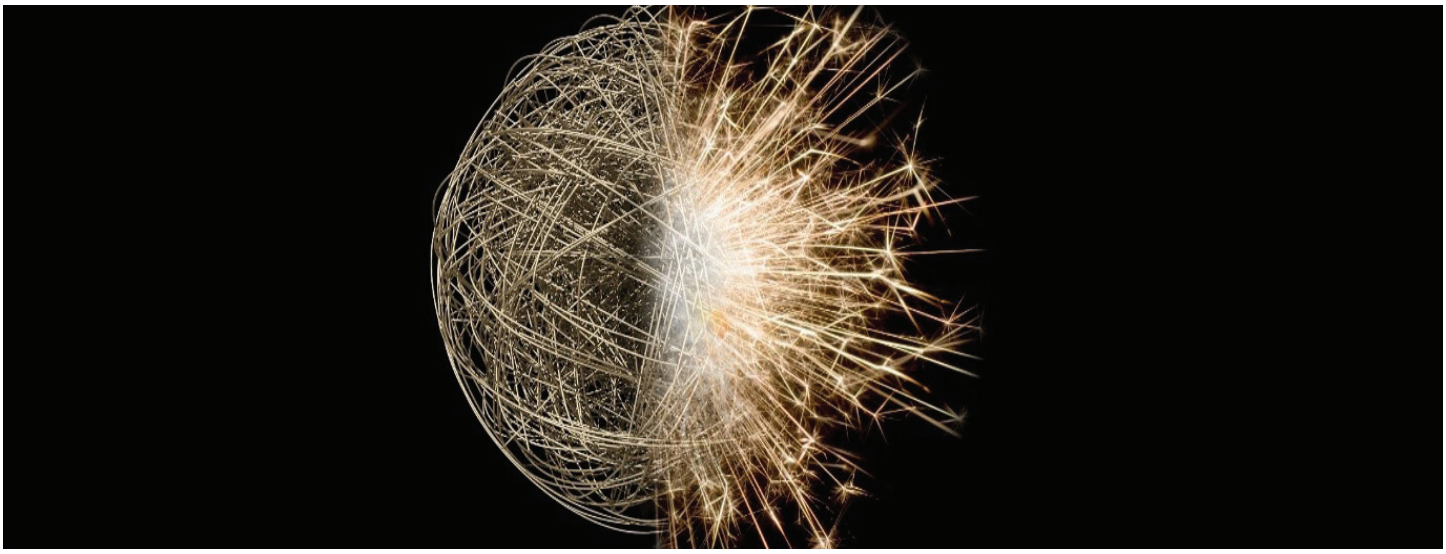


# Achieving cyber governance risk & compliance in the cloud

## A closer look at Amazon Web Services

When transitioning or implementing workloads into the cloud, often the top-most concern of an organization is to manage cyber risks and effectively demonstrate compliance. Not complying with regulatory requirements, or not having a strategy to effectively manage cyber risks, can clearly lead to negative implications on businesses, and the way they operate.

A good cyber governance, risk, and compliance (GRC) program is fundamental to securing the "crown jewels" (business critical assets) of an organization as it provides a broad approach to manage cyber risks and enable organizations to proactively meet their security and compliance objectives. As organizations look toward increasing adoption of cloud, they should also consider extending the cyber GRC program to address cloud services and gain greater visibility into exposure to related cyber risks.

Amazon Web Services (AWS) provides a suite of services that can be leveraged for securing workloads and automating compliance activities on AWS cloud. By selecting and appropriately configuring a combination of AWS services that are relevant to the business, security teams can efficiently deploy security controls for people, processes, and technology to effectively demonstrate compliance with regulatory and governance requirements.

### Cyber GRC within the cloud is as important as on-premesis

The achievements of a cyber GRC program do not just depend on deploying AWS native services, but more on the way the cloud strategy is built to manage risks beyond the boundaries. In a nutshell, the strategy should cover:

- Identification and inventory of your cloud assets and relevant security and compliance requirements
- Identification and inventory of data and relevant security and compliance requirements
- Implementation of security controls (access controls, guardrails, firewall, patching, anti-malware, etc.) on cloud components
- Continuous monitoring and automation of security and compliance requirements
- Continual improvement of processes and services

Cloud's inherent ability to provide a high degree of transparency, when combined with AWS's suite of security services, can provide significant value without compromising on cyber security. It is important to note, however, that it is not a matter of leveraging the services, but configuring and leveraging them the most effective way. For more information visit our published AWS whitepapers.[1]

As organizations are experiencing the journey of digital transformation, cyber is moving in multiple dimensions across multiple disciplines, and more importantly – the cloud. Therefore, organizations should consider Deloitte's "Cyber Everywhere" strategy as a foundational element in their strategy and leverage cloud GRC capabilities to drive a more agile and efficient risk and compliance management program.

1. https://www2.deloitte.com/us/en/pages/risk/articles/cyber-risk-aws-security-capabilities.html

# A challenge

Organizations often have several independent cloud initiatives operating simultaneously across the businesses. Lack of a standardized and well-defined cloud GRC program affects the organization's security posture, and overall maturity in terms of ability to fully and efficiently meet compliance and regulatory requirements.

AWS offers numerous services with associated security use cases, that are critical to the overall security program. Some of the common questions that organizations ask about AWS services include:

- By default, does AWS support our compliance with Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Federal Risk and Authorization Management Program (FedRAMP), etc.?
- How can AWS help in enforcing policies and achieving compliance?
- Can AWS services assist in performing security assessment of the cloud environment?
- How can AWS assist in monitoring compliance status?
- How can I automate my compliance?
- How does my organization's compliance policy need to be changed to embrace the cloud?

## Success of a cloud GRC program depends on a holistic strategy, not just tools.

As organizations build new services on AWS, customer controls are needed to achieve a compliant and secure integrated cloud platform. The Deloitte cyber risk methodology incorporates a broad approach and enables organizations to comply with applicable regulatory requirements and more effectively achieve GRC in the cloud. Specifically, Deloitte has developed a cloud GRC program based on industry leading practices, which enables organizations to incorporate AWS controls into their governance frameworks for managing overall security, risk, and compliance.

Our cloud GRC program capabilities include security and governance, risk management, and compliance and regulatory reporting.

Figure 1. Factors to be considered when aligning security capabilities to cloud strategy

# Pillars of Cloud Cyber GRC

**An effective cyber GRC approach is based on three integrated and inter-related pillars -- governance, risk management, and compliance**

## Governance

Governance enables organizations to understand current risks and regulatory landscape and align the cyber strategy with desired objectives. An effective governance strategy ultimately supports an efficient and secure information technology (IT) environment.

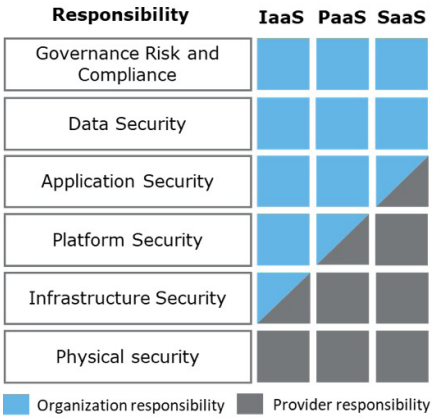
Identifying and **managing IT resources** is the first step in effective governance. Tagging cloud resources and managing an accurate inventory of IT resources and optimizing the resources is solely the responsibility of the organization.

**Securing IT resources** is one of the cornerstones of the governance program. While the cloud service provider (CSP) is responsible for security "of" the cloud, and the organization is responsible for security "in" the cloud, making cloud security a shared responsibility.

**IT performance management** and monitoring has become a strategically important part of the governance program due to the increasing complexity of applications in the cloud and their interdependencies.

As cloud services are inherently designed to provide high performance, organizations are responsible to prevent, detect, and correct IT issues that may impact performance and/or security.

Organizations can benefit by establishing a cloud governance body with empowered members, clear goals and vision, roles and responsibilities, and reporting structure.

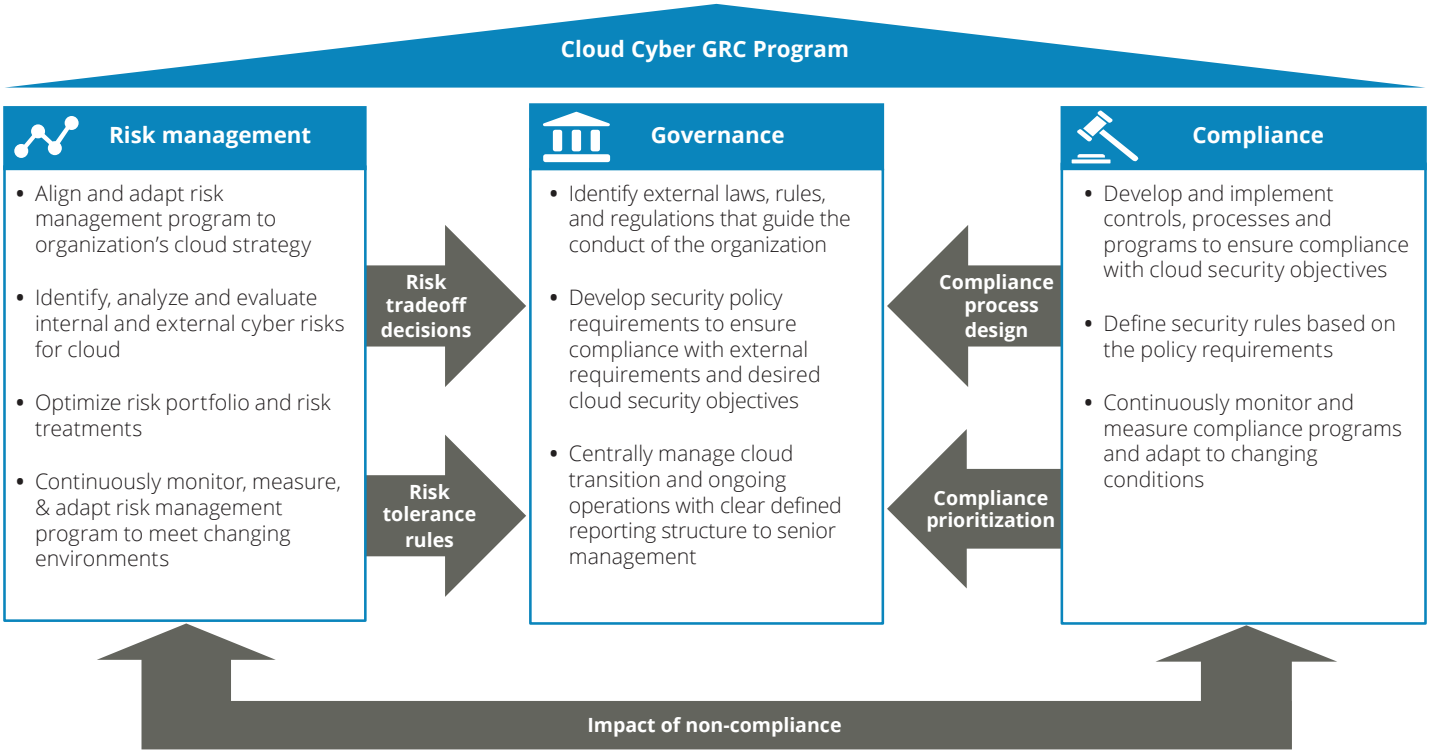



IaaS – Infrastructure as a Service

PaaS – Platform as a Service

SaaS – Software as a Service

The cloud governance body enables organizations to centrally manage and effectively oversee the transition of business to cloud.



## Risk Management

Organizations deploying their applications/ data/ infrastructure in the cloud should identify associated threats and vulnerabilities to not only mitigate risks, but also to spot opportunities to improve performance of the services in the cloud. As a result, risk assessments, vulnerability scans, penetration testing, and other risk monitoring activities need to be regularly performed on the cloud environment for effectively managing the risks. The risks and challenges in cloud adoption are identified, including:

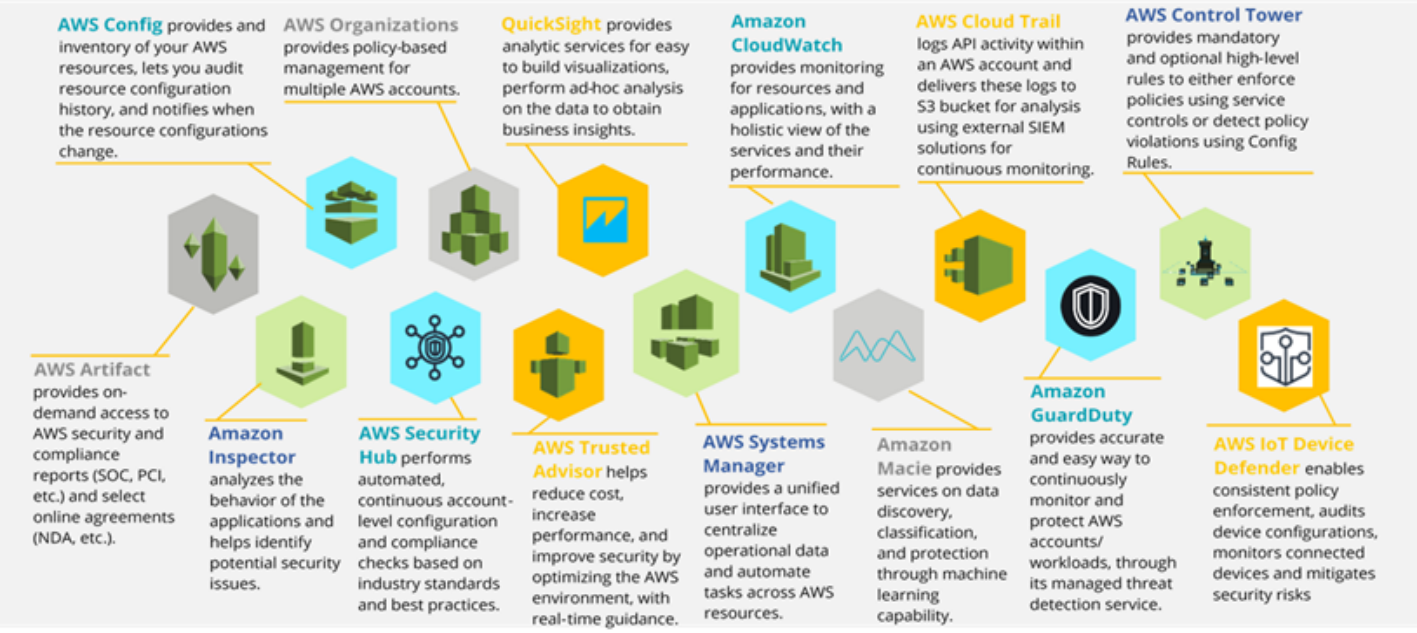
- Identification of various infrastructure components and architecture that need to be transitioned to cloud
- Identification of crown jewels, defining the migration profile, and determination of scope, schedule, and resources for risk treatment
- Identification and adoption of new technology such as cloud-based functions (Example: AWS Lambda) that may have to be recoded, critical data that may be better suited for storage and transmission on one platform as compared to another, etc.
- Migration of databases, applications, user roles, groups and permissions may lead to challenges such as cloud platform incompatibility, code changes, architecture changes, etc., which should be identified and planned for before cloud transition is implemented
- Identification of the monitoring requirements that are required to capture insights such as application performance, user actions, etc.

## Compliance

Organizations embracing cloud should first understand their compliance objectives required to effectively support business operations and then carefully choose the desired services that help meet those objectives by primarily focusing on the cyber responsibilities, as they may vary depending on various factors such as the services used, the way the services are integrated into IT environment, applicable laws and regulations, etc.

Cloud service providers are responsible for providing customers with information regarding the policies, processes, and controls established in the cloud environment through white papers, reports, certifications, and other third-party attestations.

The AWS suite of services can help organizations bolster their cloud posture across the cloud cyber GRC pillars. Together, Deloitte and AWS can offer services that help clients simultaneously reap the benefits of cloud services and improve their overall security posture.




API – Application Programming Interface
S3 – Simple Storage Service
SIEM – Security Information and Event Management
SOC – Secure Operations Center
NDA – Non-Disclosure Agreement

# Achieving GRC in the cloud using the Deloitte methodology

Moving IT infrastructure to AWS requires a model of shared responsibility between organizations and AWS. In this shared model, AWS is responsible for security of the cloud and organizations are responsible for security in the cloud. In order to achieve security in the cloud, organizations can leverage AWS native services for managing assets, risks, controls, policies, and for performing assessments or choose to complement the native services with a third-party provided service.

Deloitte has developed a methodology to help organizations speed up adoption of AWS, automate GRC in the cloud, and build a sustainable cloud risk management program.

The activities involved in the Deloitte GRC methodology leverage tools and frameworks created by Deloitte, coupled with AWS services, that help address specific use cases to enhance operational efficiency.

GRC aims to increase the effectiveness of controls in AWS, while helping to meet business, regulatory, and compliance requirements.

**Cloud GRC – Adoption of AWS**

| Assess cloud security risk | Cloud migration planning | Automate governance and compliance | Evaluate and integrate AWS controls | Continuous monitoring |
|---|---|---|---|---|
| Identify specific risk areas and assess current maturity by identifying gaps and create a roadmap for secure cloud as an integrated part of the cloud strategy | Devise a strategy to provide near zero-downtime application migration to the cloud environment with minimal disruption in user productivity | Develop an automated solution for governance and compliance to reduce the cost, time, and effort to deploy applications in AWS while reducing risk and simplifying the architecture | Assess if the controls "in" the cloud are operating effectively and pre-defined security requirements and AWS leading practices have been implemented | Identify risk and compliance issues by effectively tracking and monitoring system activity |

### 1. Assess cloud security risk

The very first activity in an efficient cloud GRC program setup is to assess the current state maturity of the capabilities deployed on cloud, with respect to leading practices, industry standards, and regulations such as federal financial institutions examination council (FFIEC), PCI-DSS, HIPAA, etc.

- Identify cloud cyber risks and provide specific recommendations to remediate the gaps
- Identify applicable threat actors and threat vectors for the overall cloud transition and for specific applications/data that are planned to be transitioned into the cloud
- Prioritize gaps and create roadmap for secure cloud as an integrated part of your cloud strategy

### 2. Cloud migration planning

Utilize a demonstrated and reliable approach to provide zero-downtime application migration by conducting a migration readiness assessment (MRA), executing migration readiness planning (MRP), and establishing a migration execution factory (MEF). This approach can support a hot/hot-phased deployment of applications to the cloud environment with minimal disruption in user productivity in the following phases:

- MRA: The enterprise application portfolio is analyzed to assess cloud suitability, leading landing zone, and migration path
- MRP: Migration portfolios are created and a pilot phase is executed to migrate select applications into the cloud, thereby establishing a landing zone
- MEF: The applications identified are grouped into migration waves and then executed using standard processes and tools
- Multi-Speed IT Transformation: Adopting multi-speed IT through a structured program helps organizations provide IT services at different speeds to the end users

### 3. Automate governance and compliance

Automating security tasks on AWS reduces human configuration errors and gives organizations more time to focus on other work critical to the business.

- AWS Trusted Advisor provides real-time guidance to help provision an organization's resources to reduce cost, increase performance, and improve security by optimizing the AWS environment
- AWS CloudFormation and AWS OpsWorks play a vital role in the initial security configuration of services, such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Load Balancing Service (ELB), and Amazon Elastic Block Store (Amazon EBS) or applications and can demonstrate a "known good state" at the point of deployment for use in compliance scenarios
- AWS Config and AWS Inspector can be leveraged to perform automated compliance checks and assessments to take a defined action in response to changes in the environment, such as isolating resources, enriching events with additional data, or restoring configuration to a known-good state
- AWS CloudFormation templates automate and enforce the baseline standards for security and compliance
- AWS Organizations use service control policies (SCPs) to centrally manage access, compliance, and security and share resources across the AWS accounts

Compliance-related information obtained from the reports provided by AWS are reviewed to understand the current IT environment and to assess and check if any additional security controls are required to meet the organization's cyber objectives. The compliance-related information is also used to establish cyber risk governance objectives for visibility, onboarding, and management of cloud assets.

### 4. Evaluate and integrate AWS controls

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, and other third-party attestations.

Deloitte can help by conducting a technical security and compliance assessments against pre-defined security requirements and AWS leading practices to identify non-compliant workloads, security posture, and configuration gaps in the client environment. The accreditation and approval plan for automated deployments include:

- The existing security requirements related to networking, continuous monitoring, access control, and auditing
- The current tools for security analysis, scanning, and monitoring
- The hardening requirements for deployed operating systems, and the need for pre-hardened custom images
- The processes and methods used to compare both architecture templates and deployed configurations

Additionally, during an incident, containing the event and returning to a known good state are important elements of an incident response plan.

- Amazon EBS snapshots with the AWS CloudFormation templates can efficiently help organizations to efficiently recover to a known good state and protect themselves from ransomware attacks such as 'NotPetya' and 'WannaCry'
- AWS Lambda and AWS CloudWatch, together, can be leveraged to create event-driven architecture that create triggers to automatically remediate an event such as enabling of services that were disabled during an incident

### 5. Continuous monitoring

AWS provides a suite of tools designed to address many of the organization's needs on the monitoring, assessment, and compliance spectrum. The challenge for many organizations is to integrate such tools natively into existing security operations toolkits. Our approach to monitoring cloud environments involves enabling those AWS native logging, monitoring, and response services along with other third-party security solutions to fulfill cloud security requirements with visibility into the AWS configuration:

- AWS Config can be leveraged for detailed tracking and notification whenever a resource in an AWS account is created, modified, or deleted
- Amazon CloudWatch is used to centralize application logs, where the agent is configured to send application log data directly to CloudWatch. Metric filters can then be used to track certain events and activity at the operating system (OS) and application levels
- AWS CloudTrail service logs API activity within an AWS account and delivers these logs to an Amazon S3 bucket for analysis using AWS Security Hub or other third-party SIEM solutions

## Devote more resources to your business goals

By implementing a standardized and well-defined cloud GRC program with an established cloud governance body, organizations are able to effectively manage cloud applications and cloud migration. Additionally, automated solutions for GRC can reduce the cost, time, and effort required to deploy applications in AWS, while also reducing the risk and simplifying architectural design. With automation, AWS can actively monitor legal and security requirements every time the system is changed, rather than relying on a periodic system review.

As a result, organizations can scale and adapt to changing business requirements, while leadership can trust the cloud GRC program, knowing that the security controls can be monitored and reviewed on the go.

## Cyber is about security enablement, not guarding the gates. Deploy the security controls that give freedom to create value.

# The strength of Deloitte / AWS relationship

aws partner network

**Premier**
Consulting Partner

- Security Competency
- Government Competency
- Financial Services Competency
- Public Sector Partner
- MSP Partner
- Machine Learning partner

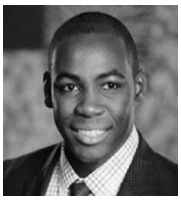
Our relationship brings together Deloitte's leadership in cyber and enterprise risk management with the **security-enabled cloud infrastructure of AWS.** In 2006, AWS began offering IT infrastructure services to businesses in the form of web services—now commonly known as cloud computing. Today AWS provides 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 an **AWS Premier Consulting 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**

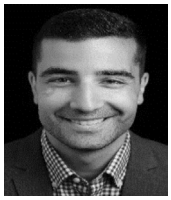
**Aaron Brown**
**Partner, Cyber Risk Services**
Deloitte & Touche LLP
AWS Alliance Leader
aaronbrown@deloitte.com



**Temi Adebambo**
**Senior Manager, Cyber Risk Services**
Deloitte & Touche LLP
Cloud Security Architect
tadebambo@deloitte.com

**Sasikumar Parupalli**
**Manager, Cyber Risk Services**
Deloitte & Touche LLP
sparupalli@deloitte.com

**Amazon Web Services**



**Piyum Zonooz**
**Global Partner Solution Architect**
pzonooz@amazon.com

**Josh Hammer**
**Global Partner Solution Architect**
johammer@amazon.com


# Contributor


**Suraj Thotalu**
**Senior Consultant, Cyber Risk Services**
Deloitte & Touche LLP
suthotalu@deloitte.com