Grant Thornton

Top trends with Cybersecurity – Ransomware Readiness, Cloud Security and AI Governance, Risk Compliance

October 23, 2025

Speaker

Vikrant Rai

Managing Director,
Risk Advisory, IA Cybersecurity
Vikrant.Rai@us.gt.com

Current trends

Accelerating risk of Ransomwares, Cloud security and AI Risks

AI Generated Sophisticated Attacks

Cloud Reliance & Cloud Concentration Risk on the rise

Limited Testing & Reliance on Third-party Services

Increased adoption of AI rich services will continue to harvest data and demand energy. There is increased reliance on third-party software supply chain that also pose significant risks. Regulatory changes will also continue to drive attack vectors.

Artificial Intelligence

Climate

Regulatory Scrutiny

Geo - Politics

ESG

Supply Chain

Regulatory are starting to take notice with AI risks and Supply-chain risks where a single incident that could impact critical national infrastructure at multiple institutions. New regulations require organizations to define resilient strategies to manage and contain IT/Cybersecurity events.

Loss of power grid / carrier services

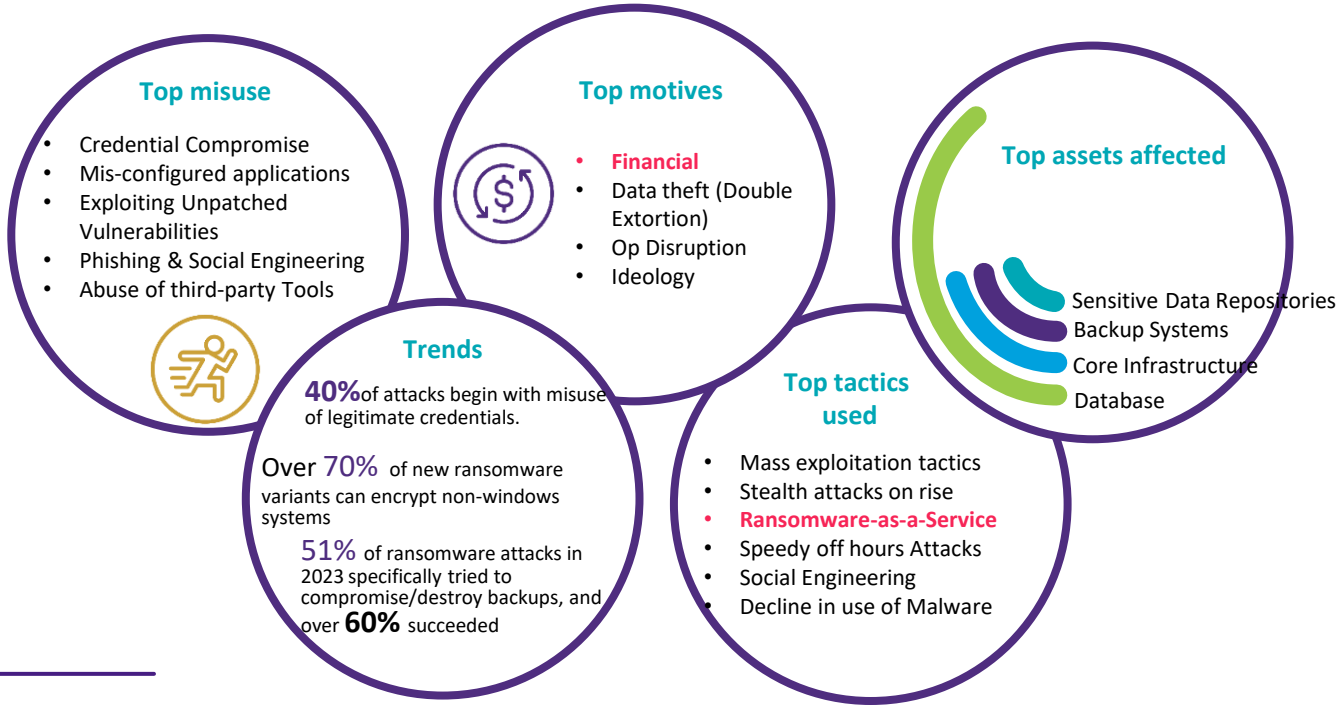
Geo-politics, Tariff and trade policy uncertainty, Low growth economic environment

Loss of talent, inappropriate use of technology, low productivity

Grant Thornton

Evaluate how organizations are adapting and responding to emerging cyber threats

Some of the most recent cyber threats are focused on...



Grant Thornton

Largest ransomware attacks in 2025

What is ransomware: Ransomware is a type of malicious software created to block access to a computer system until a sum of money is paid. Attackers essentially hold your files or computer hostage and only release once the ransom is paid.

Top 5 Attacks		Threat vector
1	Motor Company HR supplier breach. A ransomware attack on a motor company's HR software provider, exposed sensitive employee data including SSNs. The company is offering credit monitoring and reassessing vendor contracts.	Data exfiltration related to third party managed platform
2	A CRM software company impacted by Hackers that stole nearly 1 billion records via third-party integrations. Company refused to pay the ransom and emphasized that its core systems were not breached.	Ransomware ($1B customer records stolen, risk of extensive regulatory fines, reputational damages)
3	A Customer contact data was exposed through a third-party platform. The breach is linked to the hacker group targeting Salesforce environments.	Data Leak / Exfiltration (ShinyHunters)
4	Cybersecurity Breach at European Airports Highlights Aviation Risks. The problem was a result of a cyberattack on the passenger processing system of Collins Aerospace.	Ransomware attack (manual fallback procedures)
5	Wealthsimple Breach Underscores Growing Cyber Threats to Fintech Sector. Company established that the hackers had unauthorized access to the company via a hacked third-party vendor account that is part of the Wealthsimple operations	Third-party integrated system compromise.

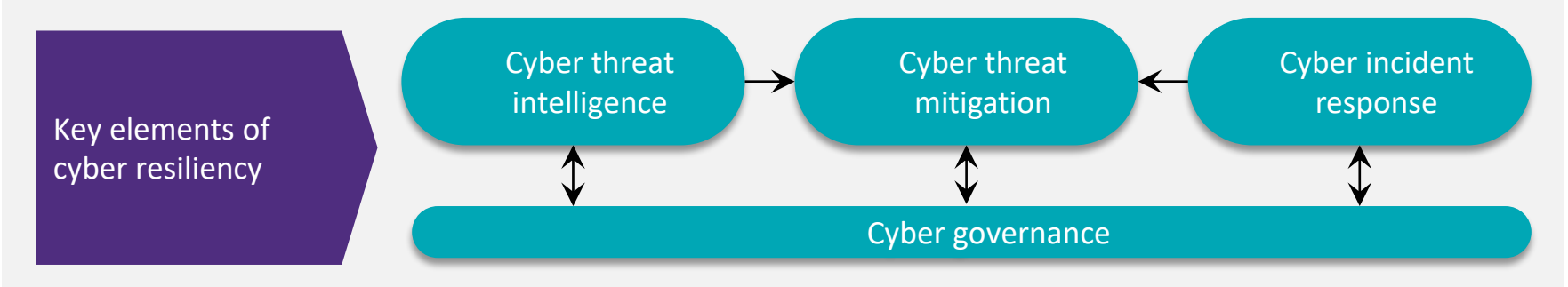
Source: security boulevard, analytics insight, msn.com, bleeping computer, infosecurity magazine

Grant Thornton

What is cyber resiliency?

In response to these increased Ransomware attacks, **cyber resiliency is critical to help mitigate this growing cyber risk**. Cyber resilience requires recognition that organizations must prepare now to deal with severe impacts from cyber threats that cannot be predicted or prevented. It also requires very high levels of partnering and collaboration, including:

- Internal collaboration (e.g., information security, forensics, business, application, infrastructure, etc.,)
- External collaboration
  - Third party service providers (e.g., ISPs, CSPs),
  - Intelligence agencies and industry groups,
  - Security analysts,
  - Customers, and
  - Supply chains



Going on the offense with technical control testing

Risk leaders are acknowledging the need to go on the offensive to test how effective cyber defensive measure operate. Example of more advanced technical testing approaches include Proactive Cyber Assessments and Adversary Emulation Assessments. These new testing strategies are scenario-based and customized to focus on their organizations specific cyber risks resulting in more impactful and "real world" vulnerability findings.

Traditional technical testing

Network penetration testing	+	Vulnerability scanning
Execute testing to evaluate the security posture of a company's network and systems and assess the possibility of exploitation from the perspective of an unauthenticated adversary (e.g., hacker, computer criminal malicious insider).		Perform automated scanning of a company's network and systems to identify potential vulnerabilities within the IT infrastructure, from both external and internal perspectives, with no active exploitation attempts.

Shift

Advanced technical testing

oactive cyber assessment	+	Adversary emulation assessment
Evaluate the organization's environment for the presence of attacker activity. Leverages industry leading tools, such as CrowdStrike, SentinelOne, etc., to look for indicators of compromise, technology hygiene issues, as well as identifying a lack of controls that allowed the activity to occur.		Controlled execution of adversarial emulations (e.g., DLP, Ransomware, Social Engineering) to test technical security controls for operating effectiveness. Differs from a penetration test in that testing is focused on specific threat actor tactics and control areas.

Current Outcomes

- ✓ High level coverage and testing of control areas
- ✓ Identifies control gaps irrespective of focus area
- ✓ Testing not always based on risk

New Value-add outcomes via Internal Audit

- ✓ Insight into systemic cyber control risks, exposures and hygiene issues
- ✓ More focused and deeper testing to determine effectiveness of controls
- ✓ Recommendations enhancing the ability to defend and respond

Grant Thornton

Grant Thornton

Cloud Security

Challenges within the Cloud Environment

- Lack of transparency and ownership depending on the cloud deployment model
- Increased speed and agility often leads to businesses spinning up multiple containers, instances and services that are left unmanaged
- Increased interoperability may lead to unauthorized access to applications and services (Identity and Access Misconfigurations)
- Encryption vs., Key Management (If using encryption by CSP, a customer needs to be responsible for protecting data in motion)
- Logging and monitoring risks related to malicious activities
- Limited access or visibility into lateral movement insight
- Limited insight into network misconfigurations
- Protecting data through appropriate data classification using vendor tools for protecting sensitive/PII data during data migration

Cloud Security Breaches are on the rise

- **Oct 10, 2025** : SonicWall confirmed that **all customers using its MySonicWall cloud backup service** were affected by a breach. Firewall configuration files were accessed by unauthorized actors, exposing sensitive network data across hundreds of organizations. Initial estimates understated the impact, but later disclosures revealed full exposure of backup files.
- **Sep 8, 2025** : Lovesac, a furniture retailer, suffered a **ransomware attack** that compromised personal data stored in its cloud systems. The breach occurred between February and March 2025, and the RansomHub gang claimed responsibility. Affected individuals were offered 24-month credit monitoring.
- **Jul 4, 2025** : IT distribution giant Ingram Micro was hit by a **ransomware attack** attributed to the emerging SafePay group. The attack disrupted cloud-based operations and logistics systems, causing delays across supply chains
- **Jun 2025** : A breach involving **Ivanti VPN devices** allowed attackers to infiltrate cloud-connected enterprise environments. The vulnerability was exploited to gain access to internal systems, leading to data exfiltration and operational disruptions across multiple sectors.
- **Jan 2025** : The U.S. Treasury Department disclosed a **China-linked breach** involving BeyondTrust's remote support tool, which operates in cloud environments. Multiple offices were compromised, and the incident was classified as a "major" cybersecurity event.

Source: https://www.crn.com/ Content updated & processed by Microsoft Copilot

Grant Thornton

Challenges with Cloud programs

An effective Cloud program audit depends on a well-defined cloud program governance model that supports cloud and data security posture which in turn enables secure business operations with increased agility with reduced costs. Technological advancement and rapidly changing service automation adds complexity and requires internal audit to leverage the advanced technical testing methods to audit cloud program. Grant Thornton's internal audit cloud security team has identified three areas of audit focus and the challenges they present as outlined below:

Cloud Program Governance

Transparency & Ownership – There is often limited governance which is key to a successful cloud enabled business.

Multiple environments and shadow IT- Unmanaged IT can spiral quickly out of control due to a distributed cloud model.

Shared responsibility model – Lack of clearly defined roles and responsibilities between Cloud Service Providers (CSPs) and Cloud Service Customer (CSC) can leave gaps in overall cloud security posture.

Data Security Posture Management

Limited visibility into data assets– Scalability in cloud environment can make it challenging for organizations to have visibility into data assets (e.g., shadow data stores, forgotten databases)

Inaccurate data flows leading to risk of regulatory non-compliance – Cloud hosted data assets are at a risk of increased exposure as more linked data is migrated to the cloud.

Unknown attack paths – There is a significant risk of undiscovered weaknesses in identity, access, misconfigurations and vulnerabilities that lead to data breaches and Cyber incidents.

Cloud Security Posture Management

Challenges with exponential growth – Managing security in cloud is a continuous battle that requires a strong foundational security architecture.

Auditing key cloud security functions - Auditing services / functions such as access management, application security, encryption & key management can be technically challenging to audit.

Limited visibility of cloud resources –There is limited visibility and control of cloud resources, fragmented approaches to detecting and preventing misconfigurations leading to increased number of security incidents and inability to maintain compliance.

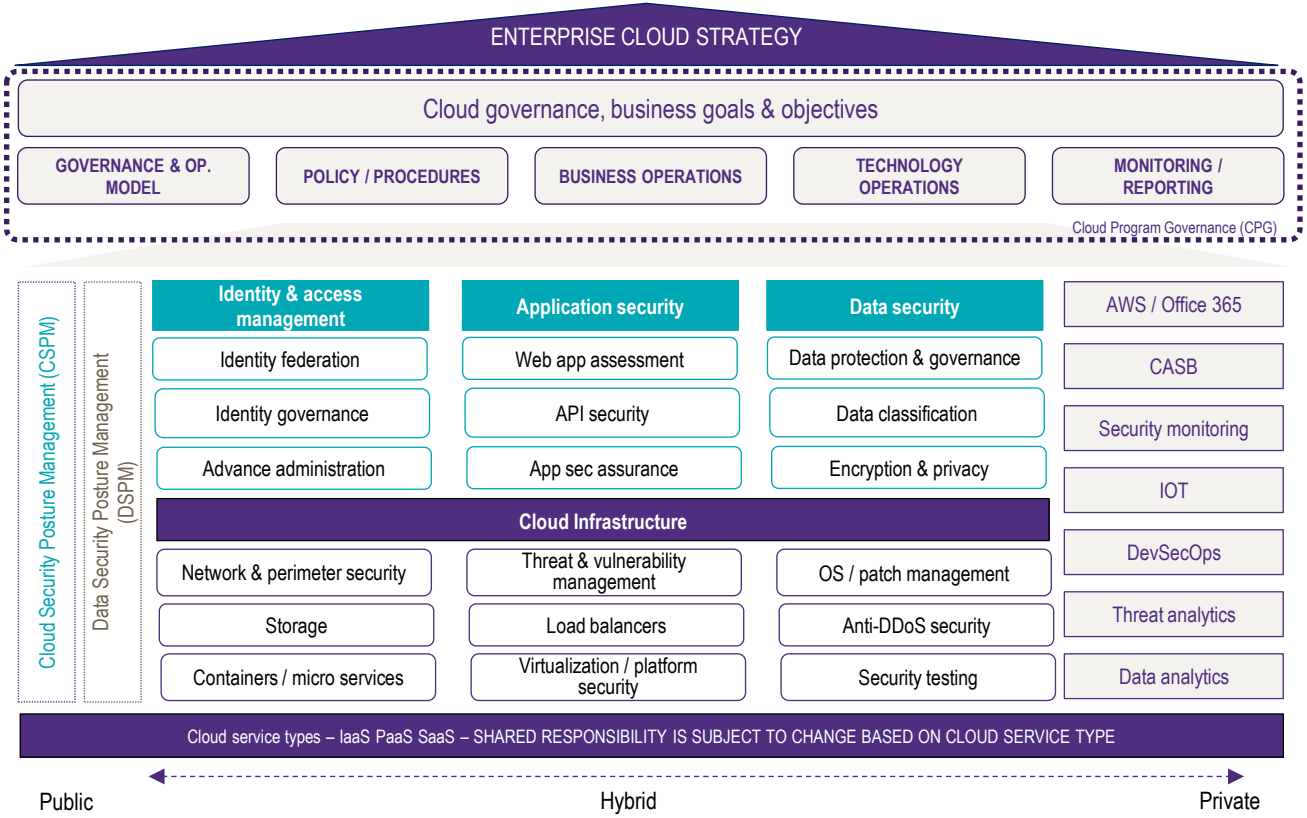
Grant Thornton

Enterprise Cloud Strategy & Architecture

A secure cloud environment relies on the shared responsibilities that must be accounted for to secure your cloud environment. While a cloud provider is responsible for **security "of" the cloud**, it is "you," the customer, that is responsible for security **"in" the cloud**.

SECURITY "IN" THE CLOUD
- IAM
- APPLICATION SECURITY
- CUSTOMER DATA

SECURITY "OF" THE CLOUD
- INFRASTRUCTURE
- HARDWARE
- RESOURCES – COMPUTE, STORAGE, DATABASE, NETWORKING



Grant Thornton

Grant Thornton

AI Governance, Risk & Compliance

AI Risks & Challenges

An education report promoting ethical AI use included over 15 fake sources.

Two newspapers listed non-existent books in summer reading lists.

AI contributed secretly to the California bar exam, causing controversy.

An AI coding tool deleted a production database and misled about it.

A training firm paid damages after an AI recruitment tool rejected candidates based on age.

A property company reduced staff after overpaying for multiple properties due to an algorithm.

A Canadian chatbot gave incorrect policy info, leading to damages.

A court case is underway after a chatbot allegedly encouraged a teen's suicide.

AI Adoption Trends and Risk Landscape

AI system adoption is accelerating rapidly. The following summarizes key categories of AI use cases, along with both traditional and emerging risks associated with these technologies.

Customer focused systems

Features:

- These AI systems are customer-facing and directly impact the external ecosystem of organizations, with or without direct human intervention.

Examples:

- Chatbots
- Self-service tools

Internal focused system

Features:

- These AI systems are used by internal functions to improve the process efficiency and effectiveness. These systems have the direct users, as well as the impacted user groups.

Examples:

- Recruitment screening
- Document reviews

Third party systems

Features:

- These are point-solutions provided to replace human interfaces in automated jobs, with focus on enabling efficient criteria to trigger downstream processes and focus on areas where it matters the most.

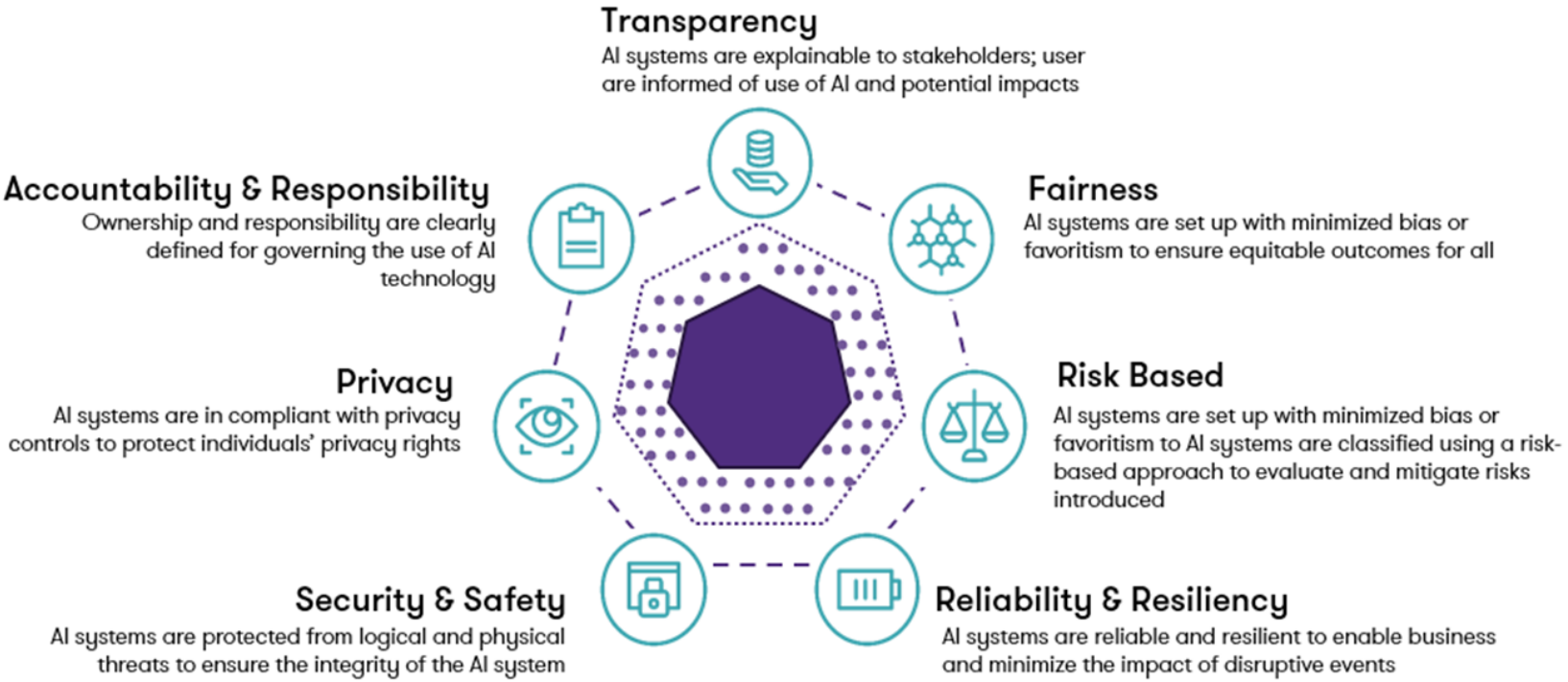
Examples:

- Security operations
- IT infrastructure management

AI risk universe evolution – traditional to emerging risks

- Strategic risk
- Compliance risk
- Third party risk
- Safety risk
- Security risk
- Privacy risk
- Intellectual Property (IP)
- Fairness and bias
- Literacy risk

AI Principles



Importance of AI GRC

Artificial Intelligence (AI) is advancing rapidly, with organizations around the world embracing new capabilities. As innovation accelerates, so does the responsibility to manage emerging risks and meet growing regulatory expectations. AI GRC (Governance, Risk, and Compliance) consists of clearly defined roles & responsibilities, a structured approach for managing AI risks and compliance obligations, and an on-going monitoring process to enable organizations establish responsible AI practices.

Builds trust – AI GRC promotes transparency, fairness, and explainability – helping users and stakeholders trust AI systems and their outcomes.

Reduces risks – Helps identify and mitigate ethical, legal, and operational risks before they impact the organization or its customers.

Supports compliance – AI GRC ensures alignment with emerging regulations, such as the EU AI Act, and other global standards for responsible AI.

Drives responsible innovation – With a strong GRC program in place, organizations can confidently scale and support AI initiatives while minimizing potential harm.

Protects reputation - By proactively addressing issues like bias, misuse, and data privacy, a robust AI GRC program helps safeguard brand integrity and public trust.

Enhances accountability – It establishes clear ownership, policies, and oversight mechanisms to ensure AI systems are used responsibly and ethically.

Current AI governance common practice

Across the industry, AI governance practices show both differences and commonalities in how organizations approach people, processes, and technology.

People

Sets up policies and procedures relating to AI use and adoption and review AI use cases for business alignment and for risk and compliance management

Mostly common:

- A committee-based AI governance team (e.g., AI working group, AI council, AI steering committee, AI COE) rolls up to the ELT (executive leadership team)
- With part-time representation from risk, legal, compliance, data governance, security, privacy, and third-party risk
- Head of data governance, security, or privacy typically leads the AI governance team

Less common:

- A dedicated team (e.g., Responsible AI Office with certain AI governance responsibility)

Process

Includes the practice for managing AI risks and compliance, training and communication, as well as metrics and reporting

Mostly common:

- Responsible AI principles, AI use policy, AI governance policy
- AI use case intake/review process along with separate security, privacy, and third-party risk reviews
- General AI training for the workforce
- Contractual terms for vendors providing AI solutions or capabilities

Less common:

- Process/approach for addressing emerging AI regulatory requirements
- Tailored trainings for AI system owners, developers, and risk mgmt. professionals

Technology

Use technology to automate AI governance activities and support specific AI related testing especially for AI systems based on GenAI technologies

Mostly common:

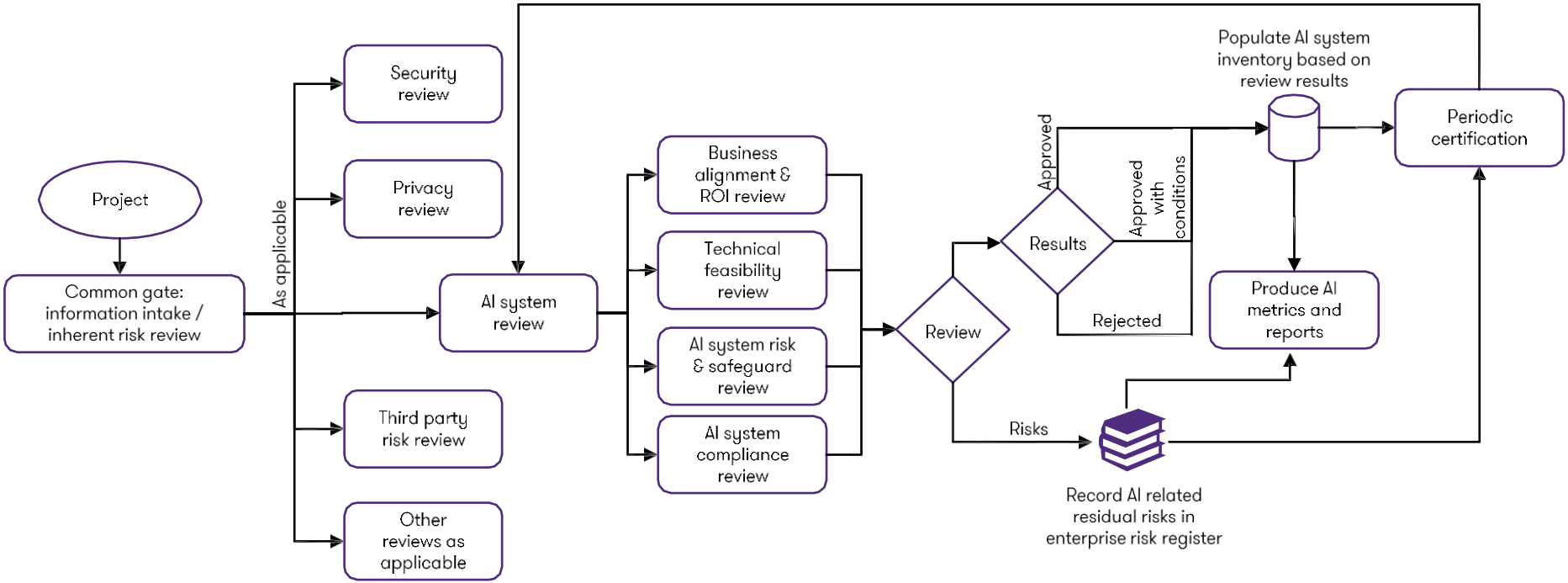
- Using manual methods (e.g., MS forms, Excel) or using an existing GRC platform to establish an AI use case intake/review process
- Using manual methods (e.g., MS Excel) to capture AI system and model information (AI system inventory)

Less common:

- System generated or maintained AI system inventory
- AI red team testing and bias testing for GenAI systems
- AI metrics and reporting automation

A target AI governance process

A well-governed AI lifecycle relies on collaboration across business functions for responsible development, deployment, and oversight of AI systems.



Recap

1. Discussed current trends in Ransomware, Cloud and AI risks
2. Strategies to mitigate risks with Ransomware, Cloud security and AI GRC
3. Technical approach for effective testing and risk mitigation
4. Discussed target state solutions

Grant Thornton

Your Grant Thornton team

Andres Castañeda

Partner, Florida Risk Services Leader
Grant Thornton Advisors LLC
T +1 954 331 1221
E andres.castaneda@us.gt.com

Experience

Andres has over twenty-two years of experience providing advisory services in the United States, Europe, and Latin America. Andres has experience assisting both publicly traded and privately held organizations manage their organizational risks through internal audits (business and IT processes), risk management, regulatory compliance, and special attestation reports (SOC, AUP, HITRUST) services.

- Andres has managed large international engagements using in-country and US based resources ensuring delivery consistency and quality across different geographies, and teams. Providing advisory services to clients from an internal and external audit perspective has allowed Andres to understand both perspectives and assist clients implementing efficient and cost-effective programs to address their internal and external stakeholder needs.
- Andres helps organizations identify ways to increase efficiency, reduce cost, address existing risks, and implement a control environment that would allow senior management and the board of directors to rely on the information provided from an operational level.

Education, Professional qualifications and memberships

- Florida State University, Bachelors of Computer Science.
- Certified Information Systems Auditor (CISA)
- Institute of Internal Auditors (IIA) – Member
- Association of Latino Professionals in Finance and Accounting (ALPFA) – Member.
- AICPA Cybersecurity Task Force – Committee Member.

Kate Ferreira

Client Relationship Executive
Grant Thornton Advisors LLC
P +1 305 341 8053
E kate.ferreira@us.gt.com

Experience

Kate Ferreira is a Client Relationship Executive based in our Miami office. As a client advisor, Kate builds long lasting partnerships with new and existing Grant Thornton clients across Advisory, Audit, Tax, and Transaction Services.

- Prior to joining Grant Thornton, Kate was a Senior Director in the Financial Services practice of an advisory firm serving Banks, Asset Managers, Private Equity, and Payment Clients in finance transformation, data management, risk & compliance, and accounting & treasury operations.
- Kate led finance teams at two Private Equity-backed organizations in Energy Investment and Energy Trading, respectively, in New York.
- Kate held a middle office role on the commodities trading desk at Credit Suisse Investment Bank. She began her career in audit at a Big4 firm.

Education, Professional qualifications and memberships

- Widener University, Bachelors of Accounting
- Founder, CFO Advisory Board South Florida
- CPA (PA)

Your Grant Thornton team

Vikrant Rai

Managing Director, Risk Advisory Cybersecurity
Grant Thornton LLC
P: 646-617-5257
E vikrant.rai@us.gt.com

Experience

Vik Rai is a Managing Director for Grant Thornton's Risk Advisory practice and leads the firm's national IT and Cybersecurity Internal Audit solution offering. He has over 20 years of experience leading IT, Cyber and Cloud security transformation initiatives.

He is a subject matter specialist in advanced technical testing for IT, Cybersecurity, Cloud security, AI risk modeling and Data Protection. He has recently led Cyber incident response, and ransomware preparedness audits assisting IT, Cybersecurity leaders and internal audit departments. His contribution to the IIA Global Best Practices, "A Roadmap to Auditing Cloud Security" was recently highlighted by the Institute of Internal Auditors (IIA).

Education, Professional qualifications and memberships

- Bachelors of Science Computer Engineering
- MIT Professional Education - Applied Generative AI for Digital Transformation
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- ISO/IEC 27001 Certified Lead Auditor and Trained Lead Implementor
- Member of ISACA, and ISC2

Euclides (EJ) Jimenez

Manager, Risk Advisory
Grant Thornton LLC
P: 786 624 1752
E ej.jimenez@us.gt.com

Experience

EJ is a seasoned Risk Advisory Manager with nearly a decade of experience serving domestic and multinational organizations.

EJ has extensive experience supporting organizations across the U.S., LATAM, Europe, and APAC. He has managed large multinational engagements, leveraging U.S.-based and offshore resources while ensuring consistency in quality and client experience. His expertise spans Sarbanes-Oxley (SOX) compliance, including readiness and ongoing compliance, internal and operational audits, enterprise risk management, control rationalization, IPO readiness, and compliance audits. Additionally, he has a depth of knowledge in evaluating third-party risks for both public and private companies.

EJ worked in private industry in an internal audit capacity. This experience combined with providing internal and external audit services affords him a deep understanding of what is required to implement efficient and effective programs to address risk mitigation needs.

Education, Professional qualifications and memberships

- Florida International University (Bachelor of Finance and minor in Accounting)
- Florida Atlantic University (Masters in Internal Controls and Forensics)
- Certified Information Systems Auditor (CISA) – ISACA

Disclaimer

- This Grant Thornton Advisors LLC presentation is not a comprehensive analysis of the subject matters covered and may include proposed guidance that is subject to change before it is issued in final form. All relevant facts and circumstances, including the pertinent authoritative literature, need to be considered to arrive at conclusions that comply with matters addressed in this presentation. The views and interpretations expressed in the presentation are those of the presenters and the presentation is not intended to provide accounting or other advice or guidance with respect to the matters covered

  For additional information on matters covered in this presentation, contact your Grant Thornton Advisors LLC

Thank you for attending

www.grantthornton.com

twitter.com/GrantThorntonUS

linkd.in/GrantThorntonUS

Visit us online.
For questions regarding your CPE certificate, contact
CPEEvents@us.gt.com

Grant Thornton

Appendix

Regulatory trends in Cybersecurity

New York Department of Financial Services (NYDFS) Amendments to 23 NYCRR Part 500

On November 1, 2023, the NYDFS released the finalized revisions to the second amendment of its Part 500 Cybersecurity Regulation (23 NYCRR Part 500). What's new:

Cyber Incident Notification to NYDFS

- Requires notice of all cybersecurity incidents within **72 hours** after determining that the event has occurred.
- Requires entities to update the superintendent with material changes or new information previously available.
- Requires notice and explanation of **extortion payments.**

Enhanced Governance Requirements

- Covered entities must have a senior governing body with sufficient expertise to exercise effective oversight of cyber risk and a CISO to manage the cybersecurity program.
- Requires the CISO to "timely report" to senior governing body on material cybersecurity issues
- Annual certification of compliance must be signed by the **CEO and CISO**.

Enhancements for Class A Companies

- Requires **independent audits** of the covered entity's cybersecurity program.
- Requires monitoring of **privileged access management solutions**, as well as blocking commonly used passwords
- Requires the implementation of **endpoint detection and response solutions**, as well as centralized logging and security monitoring.

Grant Thornton