Evolving with GRC

An anecdote of Cybersecurity's Impact on GRC

November 8th, 2024
ISC2 East Bay Fall Conference
@Las Positas Livermore, CA

Chandra Sekhar Dash
Ushur Inc., California, USA

ISC2 CHAPTER | EAST BAY

My Bio

Chandra Sekhar Dash

https://www.linkedin.com/in/chandra-sekhar-dash/

Cyber Security and IT professional with 20+ years of experience spanning Cyber Security Operations, IT/OT Security, Cloud Security, and Governance, Risk, & Compliance (GRC).

Work Experience

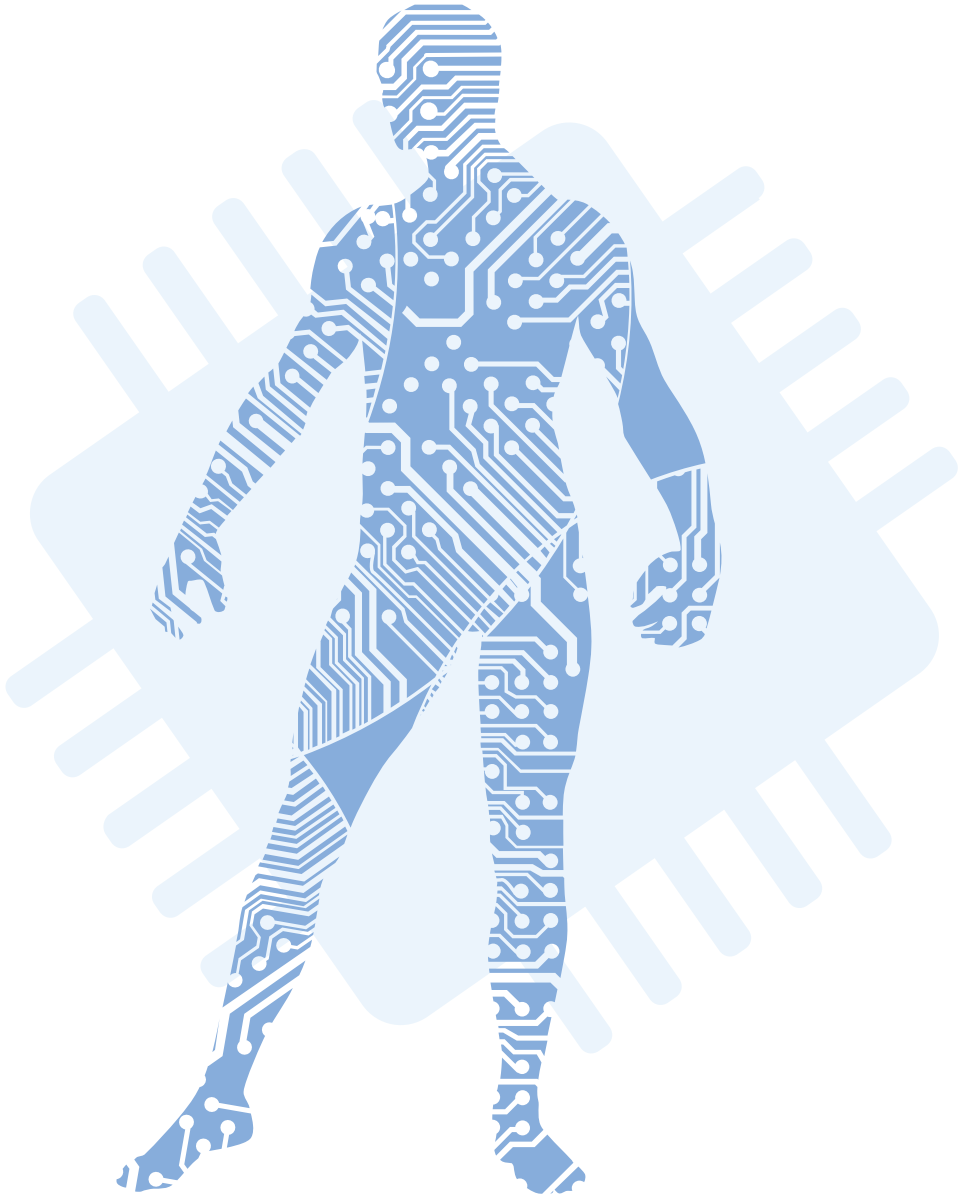
Senior Director – GRC and SecOps
Ushur Inc., California, USA

Skills

Cybersecurity Expert | Researcher | Cloud Security | Risk Management | IT/OT Security | Cyber & Strategic Risk Consulting | Data Privacy | Data Governance | Artificial Intelligence | AI Governance | AI Safety | Quantum Computing | Compliance Management | Cryptography | Assessments | Audits |

Outline

- **Key Trends of GRC Evolution**
- **Building a Resilient GRC Program Amidst Cybersecurity Challenges**
- **The Evolution of GRC**
- **GRC: The Ultimate Superhero Team**
- **GRC: An Organization Perspective**
- **GRC: Learning Through Examples**
- **From Compliance to Cybersecurity: Our Adaptation Journey in GRC**
- **Q & A**

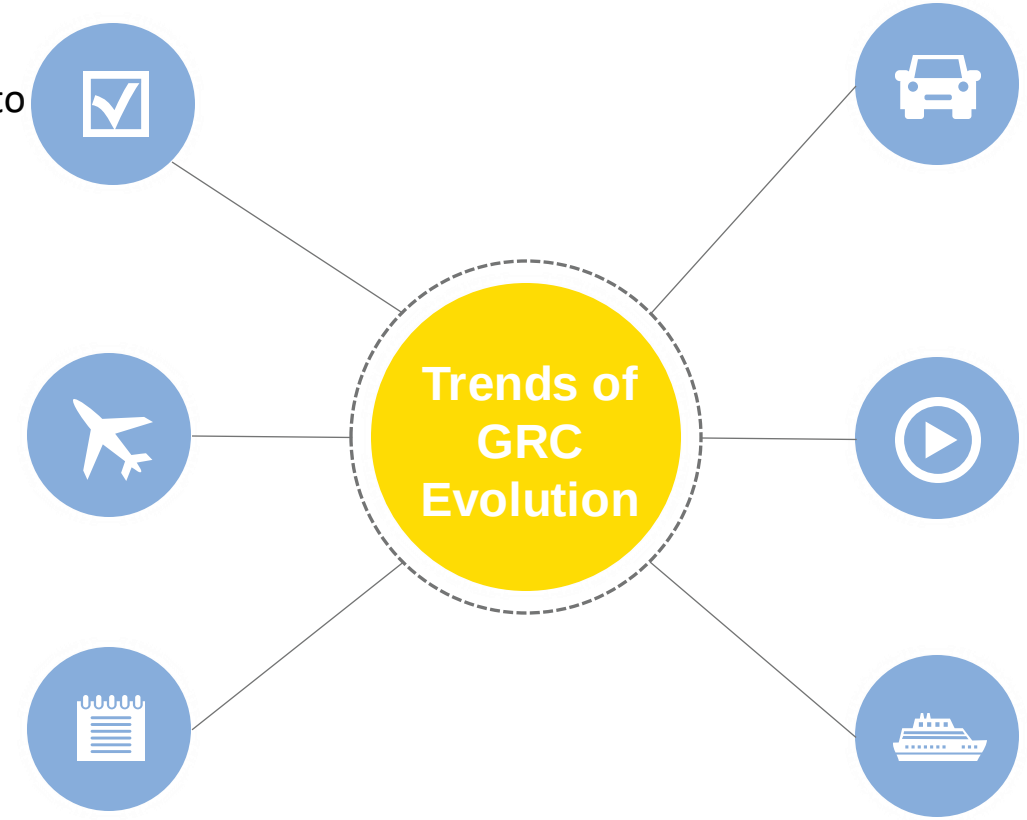


Key Trends of GRC Evolution

Strategic Alignment
Shift from a "check-the-box" mentality to viewing GRC as a strategic asset

User-Centric Design
Development of more intuitive, configurable interfaces to engage all levels of the organization

Proactive Approach
Moving from reactive compliance to proactive risk management and opportunity identification



Increasing Integration
From siloed approaches to integrated, enterprise-wide systems

Technological Advancement
Progression from manual processes to sophisticated, AI-driven solutions

Expanded Scope
Evolution from narrow financial compliance to comprehensive risk and governance management

Source: inmorphis, grc2020, edgefi

Building a Resilient GRC Program Amidst Cybersecurity Challenges

Ongoing

Current Stage

Timeline

Stage 4

Continuous improvement

Manage and continually refine the GRC program through strategic improvements aligned with shifts in the cyber threat landscape and evolving business objectives.

Stage 3

Stabilize the GRC in Ushur environment

Enhance scalability and develop skills, process efficiencies, and automation to bolster ongoing cybersecurity capabilities and ensure consistent performance management and oversight.

Stage 2

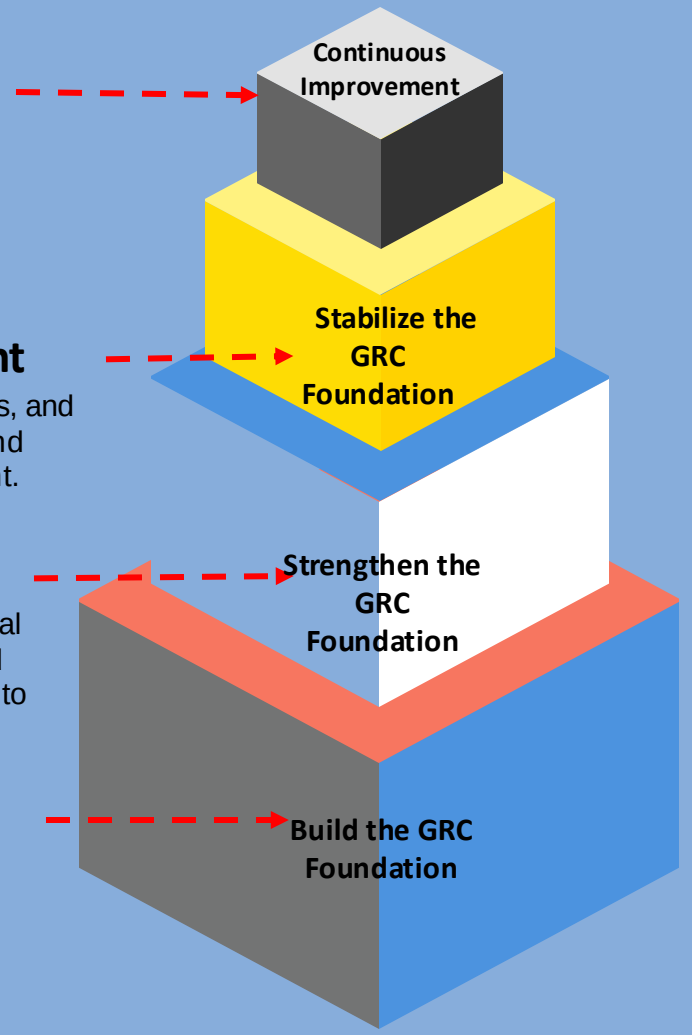
Strengthen the GRC Foundation

Identify control gaps and assemble a team of skilled internal and external resources to implement tools, processes, and standards, ensuring due diligence across the organization to enhance the GRC foundation.

Stage 1

Build the GRC Foundation

Establish the fundamentals by developing strategies, policies, standards, procedures, and controls to form the foundation of GRC.

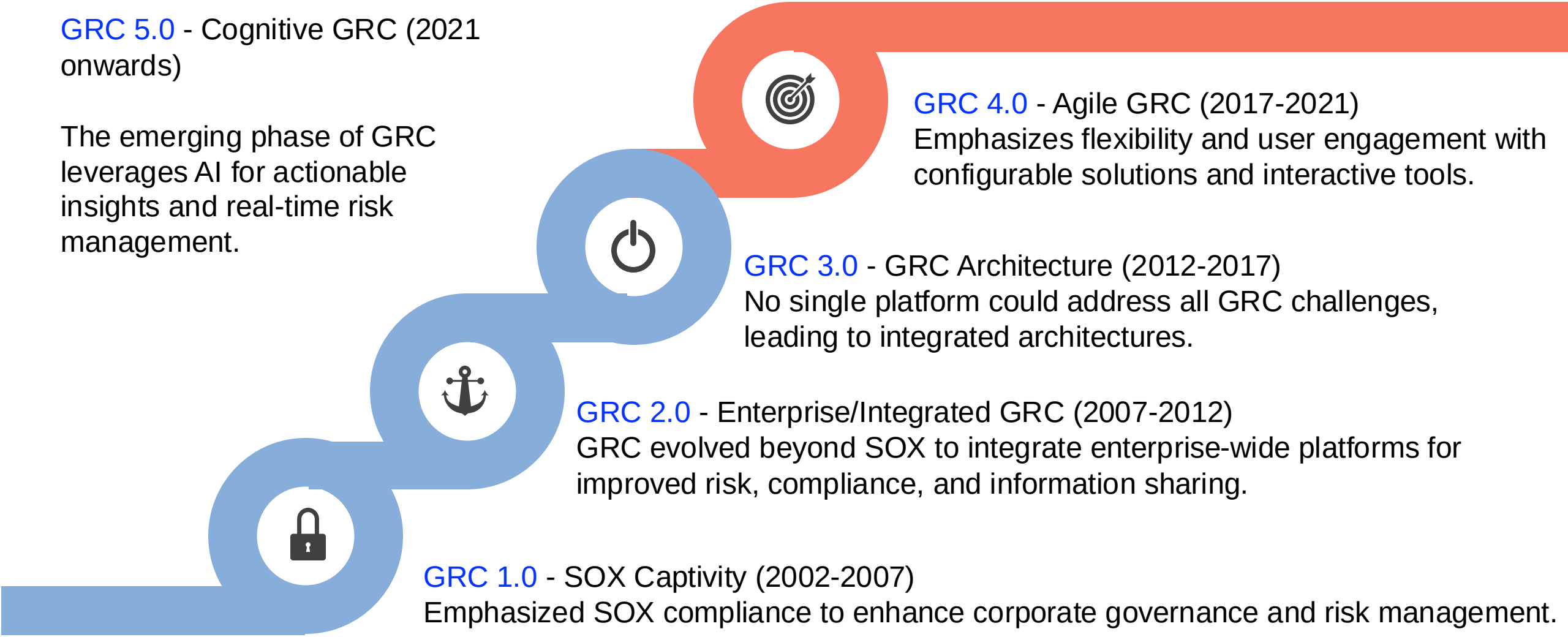


Security maturity increases over time

The Evolution of GRC

GRC 5.0 - Cognitive GRC (2021 onwards)

The emerging phase of GRC leverages AI for actionable insights and real-time risk management.



GRC 4.0 - Agile GRC (2017-2021)
Emphasizes flexibility and user engagement with configurable solutions and interactive tools.

GRC 3.0 - GRC Architecture (2012-2017)
No single platform could address all GRC challenges, leading to integrated architectures.

GRC 2.0 - Enterprise/Integrated GRC (2007-2012)
GRC evolved beyond SOX to integrate enterprise-wide platforms for improved risk, compliance, and information sharing.

GRC 1.0 - SOX Captivity (2002-2007)
Emphasized SOX compliance to enhance corporate governance and risk management.

Source: inmorphis, grc2020

GRC: The Ultimate Superhero Team

Governance: The wise sage, ensuring everyone knows the rules—like a wizard with a thick spellbook of policies.

Risk Management: The cautious sidekick, always saying, “Watch out for that falling piano!” Assessing dangers from rogue spreadsheets to cyber villains.

Compliance: The strict but lovable enforcer, like the school principal checking uniforms. Ensuring the organization walks the walk when it comes to laws and regulations.

Together, they fight chaos and confusion, helping the organization thrive while having a good laugh!

GRC: An Organization Perspective

Governance	Risk	Compliance
Mgmt. and Oversight	Risk Management	Compliance Adherence
Framework of policies, processes and structures	Risk domains, strategy and appetite	Adherence to Law, Regulatory and organization policies and procedures
Organization Strategy	Risk operational processes & measurement	Audit, Assessment and Security Testing
Roles and Responsibilities	Coordinated risk assurance	Assurance: Certifications and Attestation of Compliance SOC2, HITRUST, ISO 27001, PCIDSS, CCPA, GDPR, TCPA etc.
Accountability and Transparency	Monitoring & Control	

Note:
SOC2 – Service Organization Control 2
HITRUST - Health Information Trust Alliance
HIPAA - Health Insurance Portability and Accountability Act)
PCIDSS- The Payment Card Industry Data Security Standard

Question-1

Take your 2003 iPad and write at least 3 consequences on society if there were no governance or established laws to maintain order?

Introduction to Governance

Imagin a world without law, rules, regulations and policies.

Enron Scandal 2001[1]

One of the most infamous corporate governance failures was the Enron scandal in 2001

Wells Fargo Account Fraud Scandal[2]

From 2002-2016, Wells Fargo employees created millions of fraudulent accounts without customer consent

Source: 1,2- Wikipedia,

Question-2

Take your 2003 iPad and write at least 3 consequences if no one though about wildfire risk in California?

Introduction to Risk Management

Imagine no one thought about wildfire risk in California.

CrowdStrike Incident 2024

If someone could have assessed the potential risk of the CrowdStrike patch, the company could have avoided the turmoil it is going through.

Impact of Wildfire Risk on Supply Chain Resilience

A supply chain includes “the entire process of making and selling commercial goods, including every stage from the supply of materials and the manufacture of the goods through to their distribution and sale.

- **Supply Chain Interruptions**
  - Affects critical manufacturing and distribution hubs, delaying production and delivery.
- **Inventory Management**
  - Need for protective measures against fire damage, including relocating stock.
- **Labor Shortages**
  - Employees may evacuate or be unable to work due to hazardous conditions, impacting workforce availability.
- **Insurance and Risk Management**
  - Increased wildfire risks lead to higher insurance premiums and necessitate updated risk strategies.
- **Market Demand and Prices**
  - Wildfires can shift consumer demand, increasing need for specific products.

Conclusion:

- Proactive planning and collaboration are essential for mitigating supply chain risks.

Source: A definitive guide. (supplychaindigital.com)

Impact of CrowdStrike Incident on SBOM

A Software Bill of Materials (SBOM) is a list of all the components, libraries, and modules that make up a piece of software, including their supply chain relationships. SBOMs are a key part of software security and supply chain risk management.

- ❑ **Increased Awareness of Vulnerabilities**
- ❑ **Demand for Transparency**
- ❑ **Regulatory Implications**
- ❑ **Enhanced Risk Management**
- ❑ **Collaboration Across Stakeholders**
- ❑ **Strengthened Incident Response**

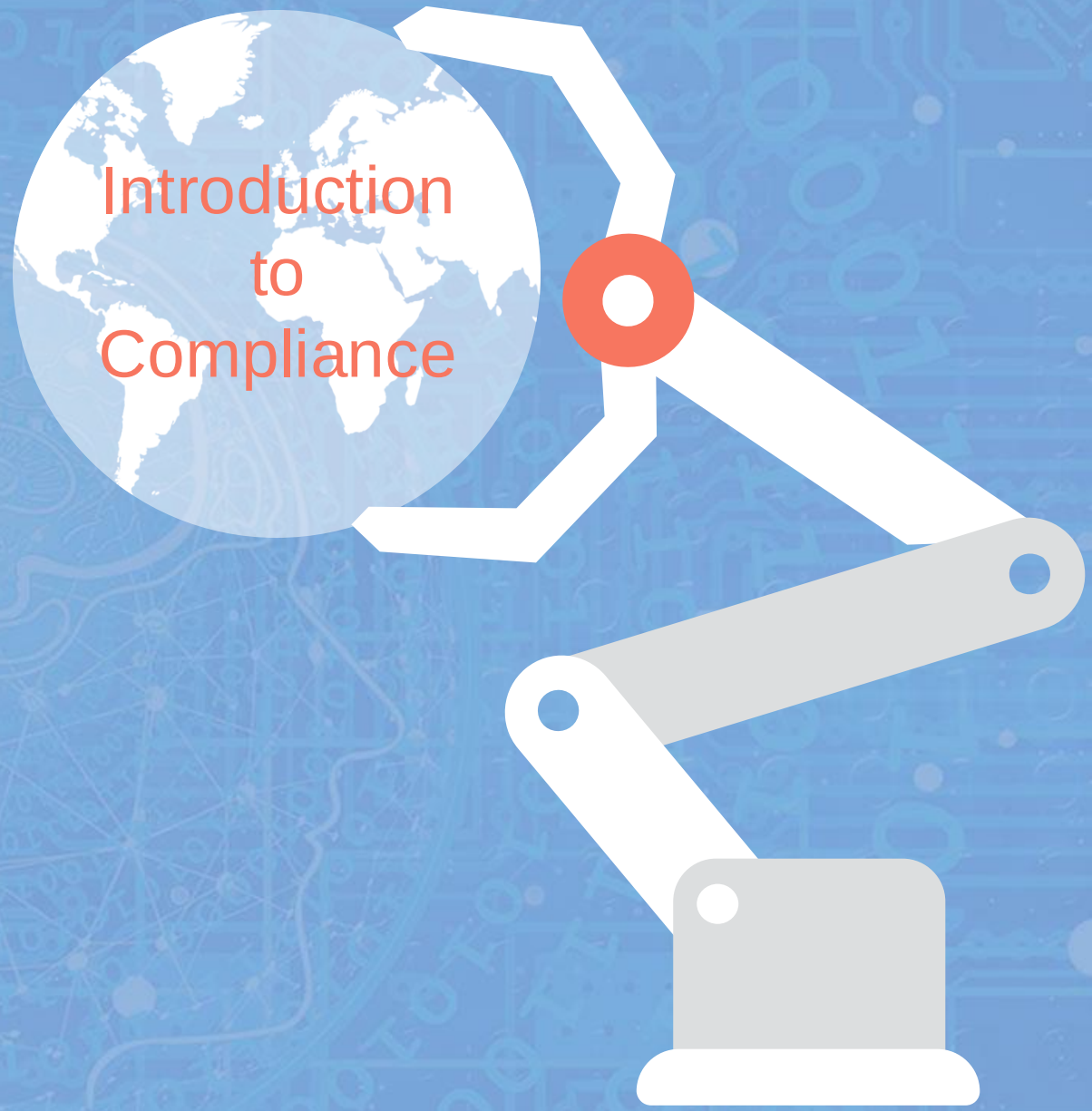
Conclusion:
The CrowdStrike incident highlights the crucial role of SBOMs in improving cybersecurity and ensuring resilient software supply chains.

Source: CrowdStrike. (2021). *REQUEST FOR COMMENT RESPONSE Software Bill of Materials Elements a*
Considerations. https://www.ntia.gov/sites/default/files/publications/crowdstrike_-_2021.06.17_0.pdf

Question-3

Take your 2003 iPad and write at least 3 consequences if your credit card information is available to all in internet?

Think of scenarios where your credit card information or health records are available to all in internet.



TRW/Sears credit card breach[1]

The leading credit union TRW/Sears credit card breach of 1984 stands out as a major credit card breach that occurred before the establishment of PCI DSS compliance in 2004.

Source: 1- Investopedia

From Compliance to Cybersecurity: Our Journey in GRC

2002-2009
GRC=Compliance

GRC was focused primarily on compliance

Our roles and responsibilities in ensuring regulatory adherence

2010-2019
Cybercrime on rise, Cyberlaws Regulatory expansion

Recognition of the importance of cyberlaws

79% of countries had enacted cybercrime legislation, with Europe leading at a 93% adoption rate

2020 -2023
Strategic Integration

A "check-the-box" to Strategic Compliance

approach to a more strategic and holistic GRC framework

2023-2024
AI, GenAI- Cybersecurity Challenge

AI Safety, Responsible AI

The rapid pace of AI development outstripped the regulatory landscape, leaving many organizations in uncharted territory.

Future

AI and GenAI Integration in GRC. Regulatory changes ahead !!!

The integration of AI and GenAI into GRC processes is expected to revolutionize the field. The regulatory environment is expected to become more complex and stringent.

Source: ISACA


Q & A
Thank You