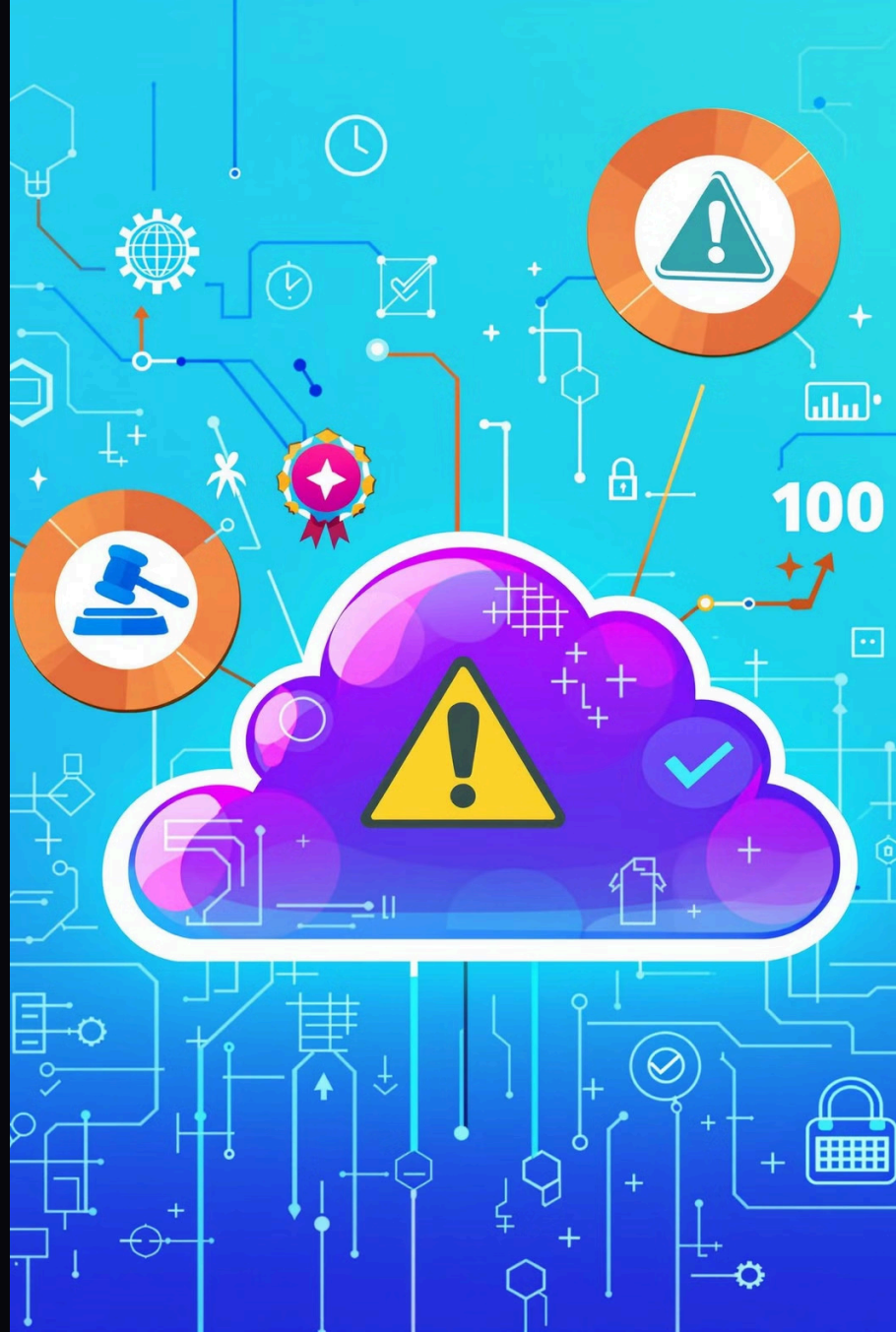
GRC in the Cloud: Building a Secure Future

Developing a GRC Mindset for Cloud Environments and the importance of GRC in the Cloud.

STUDY GRC

Network Learn Contribute



About the Presenter



Chris Whitlock

President of Study GRC and Director of Community at Simply Cyber



Daily Live Streams

Empowering and Fostering Community in the space.



Experience

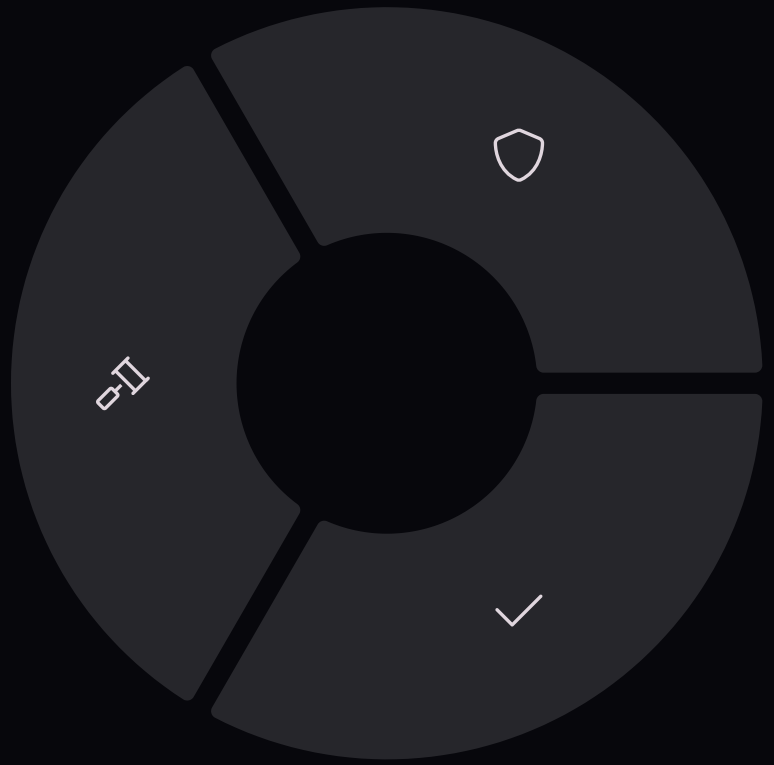
Existing pursuit since Nov. 2023 and many years of hobby IT.

What is GRC?

Governance

Structures defining control and operation of cloud resources

- Resource provisioning and access policies
- Accountability frameworks
- Decision-making hierarchies



Risk

Identifying and mitigating cloud-specific threats

- Data exposure risks
- Service availability concerns
- Third-party vendor dependencies

Compliance

Meeting relevant regulatory requirements

- Industry standards
- Regional regulations
- Certification and auditing



Why GRC Matters in the Cloud

Unique Challenges

Misconfigurations, unauthorized access, and data breaches pose constant threats.

80% of companies faced an increase in cloud incident.

Dynamic Nature

Rapidly scaling resources demand continuous oversight. Cloud environments change daily.

Regulatory Complexity

Navigating GDPR, HIPAA, and industry-specific regulations requires expertise.

[50+ Cloud Security Statistics in 2025]

Benefits of GRC in the Cloud



Enhanced Security

Proactive threat mitigation reduces breach probability. Comprehensive protection across assets.



Cost Savings

Avoid regulatory fines and operational disruptions. Prevent expensive security incidents.



Stakeholder Trust

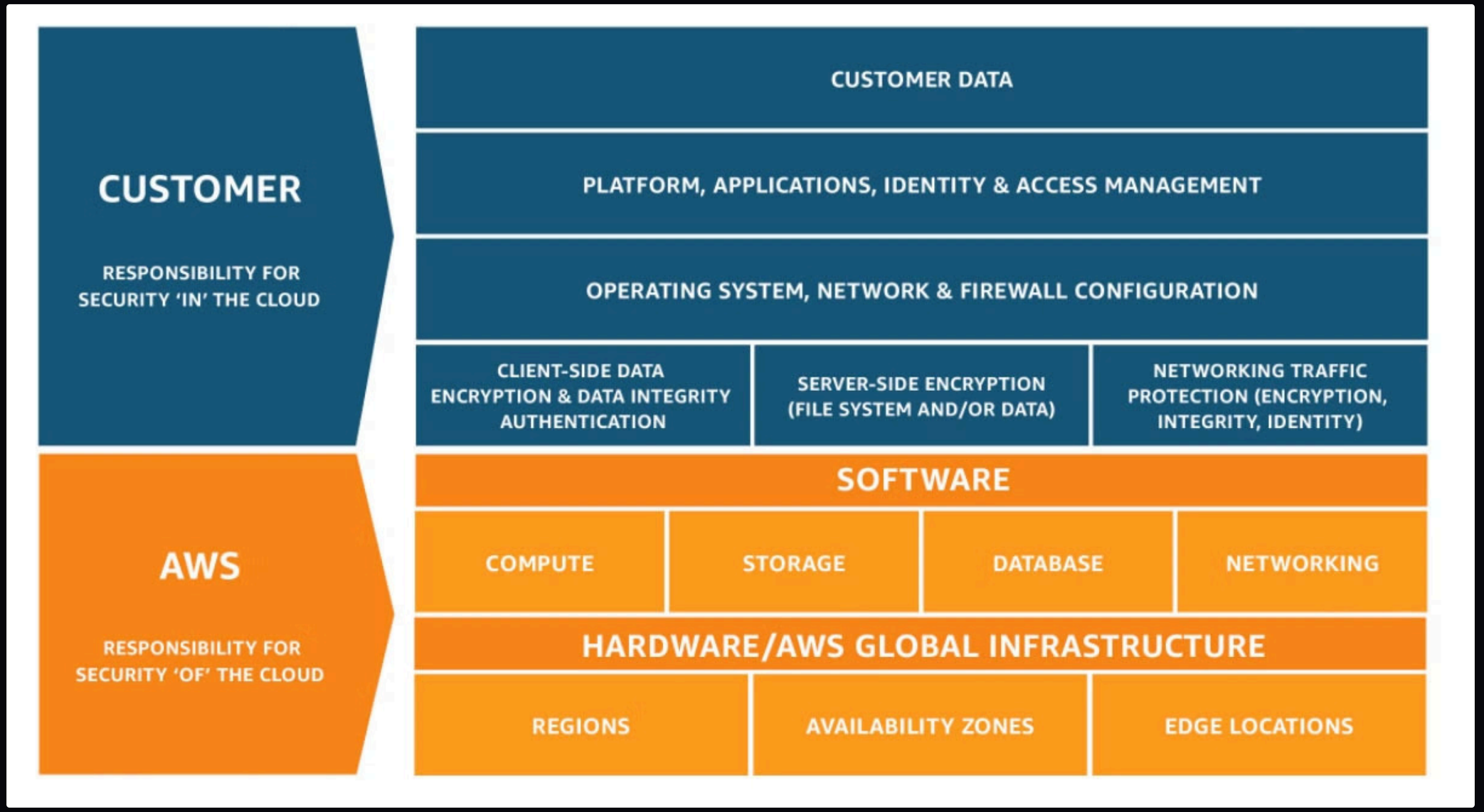
Build confidence in data protection practices. Meet customer expectations for security.



Operational Efficiency

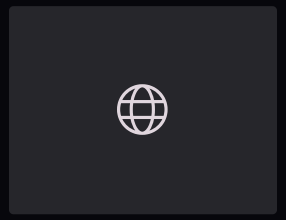
Streamline processes via automation. Reduce manual compliance tasks significantly.

The Shared Responsibility Model



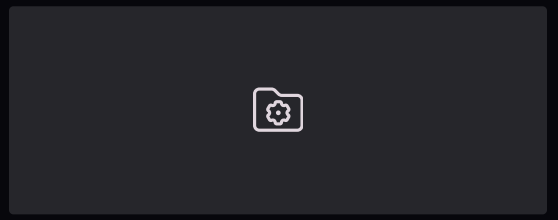
View this image and more information at: **https://aws.amazon.com/compliance/shared-responsibility-model/**

Key Challenges in Cloud GRC



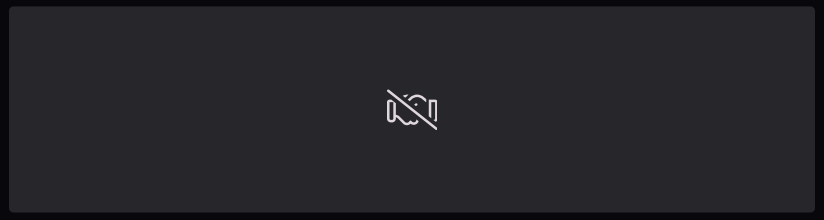
Data Sovereignty

Ensuring data complies with regional laws like GDPR



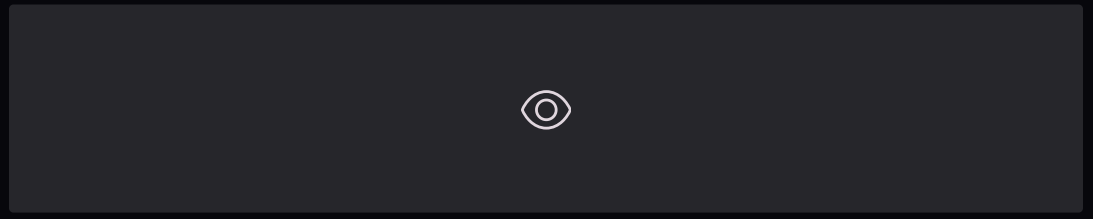
Dynamic Infrastructure

Tracking rapid resource changes from auto-scaling



3rd Party Management

Verifying third-party compliance, collaboration



Visibility

Identifying hidden misconfigurations and security gaps



Major Regulations

Regulation	Region	Focus
GDPR	European Union	Personal data protection
HIPAA	United States	Health data security
PCI DSS	Global	Payment card security
CCPA/State Laws	United States	Consumer privacy rights

Staying Updated with Regulations

Subscribe

Follow regulatory newsletters from CSA, ISACA, and NIST

Automate

Implement tools like AWS Config and Azure Policy

Designate

Establish a regulatory watch team with clear responsibilities

Schedule

Set regular review cycles for compliance requirements





The Cost of Inaction

$4.45M

Average Breach Cost

Per incidents

287

Days

Average time to identify and contain a breach

???

Customer Loss

Customers leave, reputation loss after major breaches

Beyond direct costs, reputational damage and operational disruption can devastate organizations for years.

Starting Your GRC Program - Overview

Assess

Evaluate current capabilities and cloud assets

Identify

Map applicable regulations and standards

Choose

Select appropriate cloud providers and tools

Govern

Implement access controls and policies

Manage Risk

Develop strategies to address threats

Monitor

Continuously track compliance and security



Best Practices for Cloud GRC

Automate

Use tools to automate compliance checks. Reduce human error. Save valuable time.

Continuous Compliance

Monitor constantly, not just at audit time. Adapt to regulatory changes quickly.

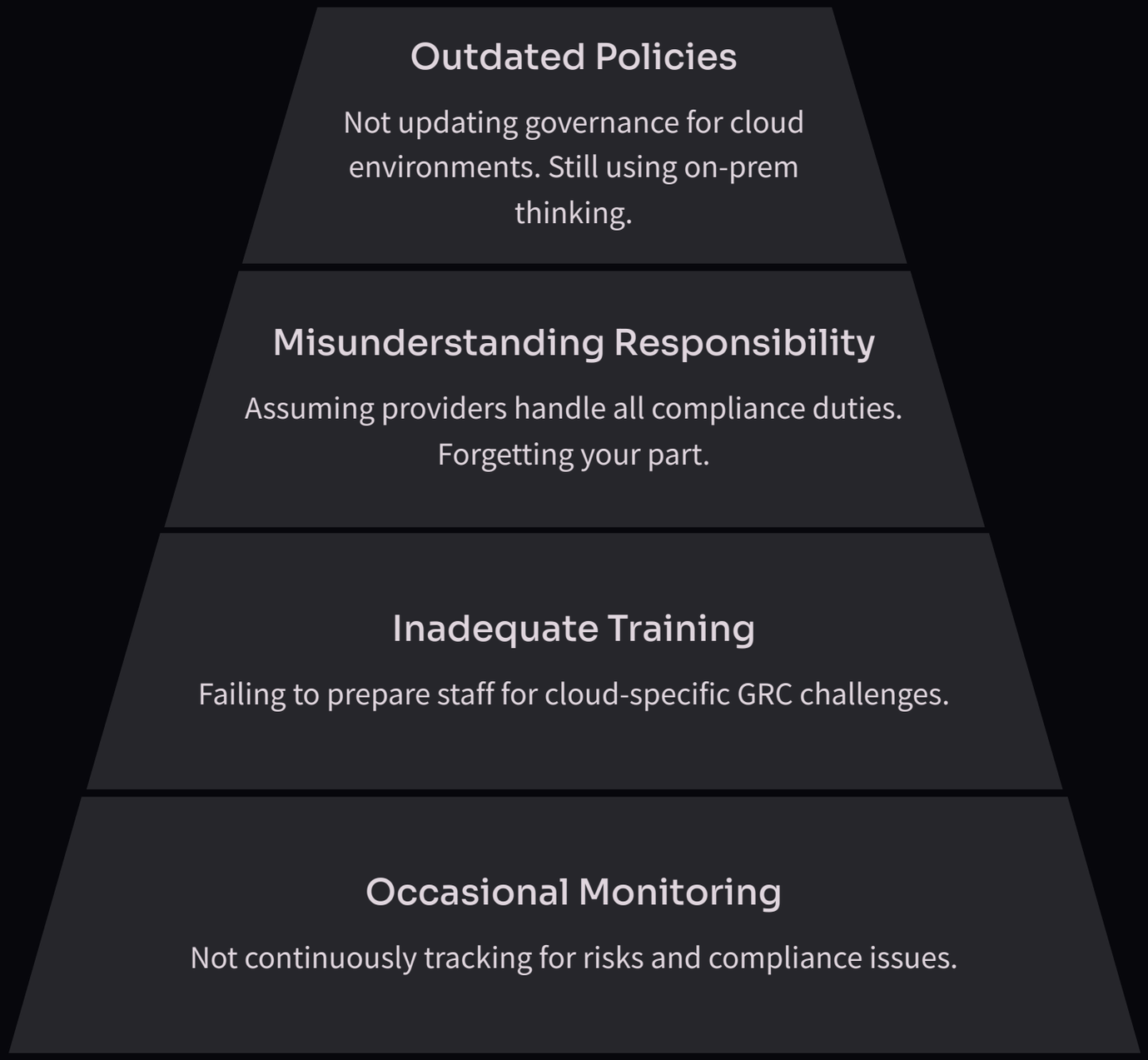
Train Employees

Foster a GRC-aware culture. Educate on security responsibilities.

Document Thoroughly

Maintain policies and evidence. Be audit-ready at all times.

Common Mistakes to Avoid



Future Trends in Cloud GRC

AI-Driven Security

Machine learning for predictive threat detection and automated response

RegTech

Real-time compliance automation and regulatory intelligence

3 Integrated Risk Management

Holistic approaches connecting all security and compliance efforts

Quantum-Safe Security

Cryptography resistant to quantum computing threats



Next Steps



Join Study GRC

Connect for ongoing support and learning



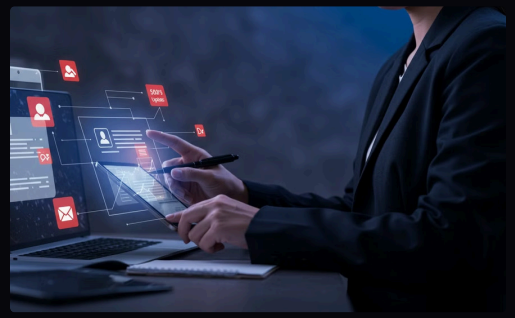
Assess Your Assets

Inventory cloud resources this week



Enforce MFA

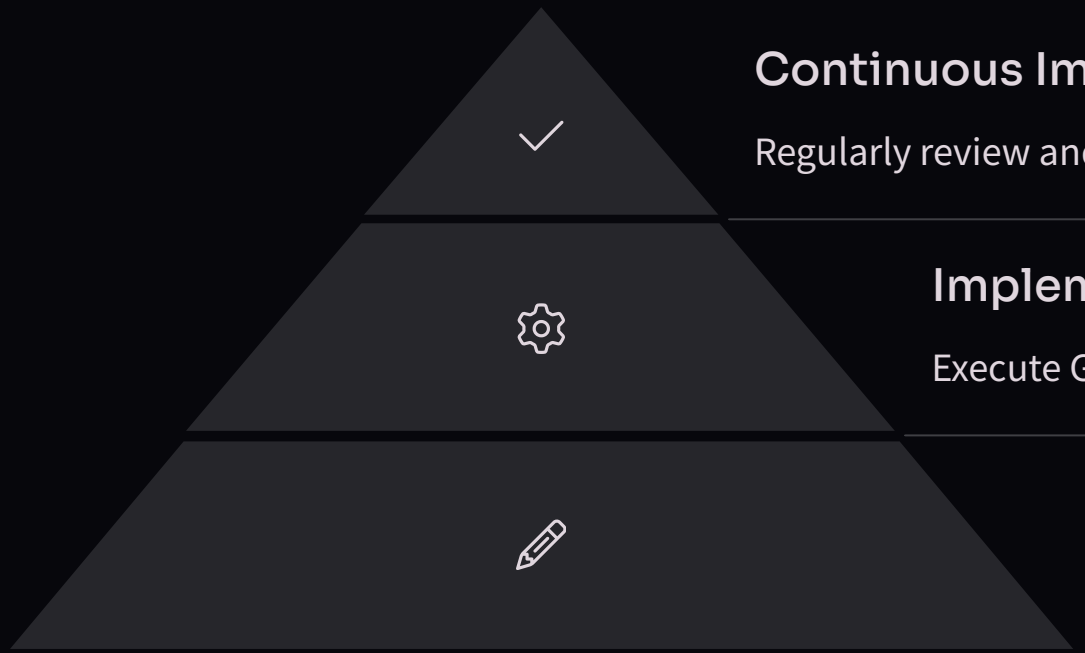
Start with enabling MFA across all accounts



Stay Informed

Subscribe to regulatory newsletters

GRC by Design



Continuous Improvement

Regularly review and enhance your GRC practices

Implementation

Execute GRC controls in cloud systems

Planning

Design GRC into architecture from the start

"Build GRC into the foundation—it's not an afterthought." This approach parallels "security by design" but extends to governance and compliance.

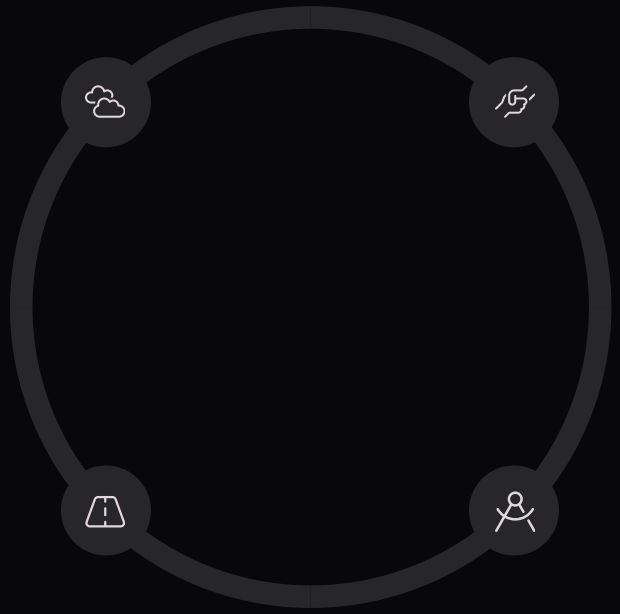
Conclusion

Essential for Success

GRC is fundamental to cloud security and business continuity

Continuous Journey

Adapt and improve your GRC approach as you grow



Shared Responsibility

Understand your obligations versus your provider's duties

GRC by Design

Embed governance and compliance from the beginning

Resources and Further Learning

Standards

- ISO 27001
- NIST CSF 2.0 & 800-53
- FedRAMP

Provider Resources

- AWS Well-Architected Framework
- Azure Security Center
- Google Cloud Security Best Practices

Organizations

- Cloud Security Alliance (CSA)
- ISACA
- OWASP Cloud Security Project



Q&A

? Discussion

? Share Your Experience

? Tool Talk

Questions? Let's discuss! Connect w/ me: **https://www.linkedin.com/in/cwhitlock95/**