



GRC: Governance, Risk & Compliance

@themadbit

Living, with a degree of madness/<

11-08-2023



My Agenda:



GRC?



The GRC Components



Importance of GRC



**Challenges of GRC
implementation**



**Implementing an
effective GRC strategy**



What's next?

Hey there!
I'm Mark
Tanui.



Computer Science Student
Junior Security Analyst (intern), Yelbridges



*fake woke. very unserious. not mediocre
(anymore)*



GRC?

Governance, Risk, and Compliance

A **structured** way to align IT with **business goals** while managing risks and meeting all industry and government regulations.



The GRC components

Governance

Governance is a company's policies, rules, or frameworks to achieve its business goals.

Example:

- Responsibilities of critical stakeholders,
- Resource Management,
- Ethics and accountability



The GRC components...

Risk management

Risk - a situation involving exposure to danger.

Types of risk:

- Financial,
- legal, strategic,
- and security risks.

Proper risk management helps businesses identify risks and find ways to remediate any found.

For example, you can use risk assessment to find security loopholes in your computer system and apply a fix.



The GRC components

Compliance

Compliance is the act of following rules, laws, and regulations.

It applies to legal and regulatory requirements set by industrial bodies and internal corporate policies. In GRC, compliance involves implementing procedures to ensure business activities comply with regulations.

For example, Managed Security Service Providers must comply and adhere to **ISO 270001**



Regulations & Standards

Governance:

- COSO Framework (Committee of Sponsoring Organizations)

Risk Management:

- ISO 31000
- COSO ERM Framework

Compliance:

- GDPR (General Data Protection Regulation)
- NDPR (Nigeria Data Protection Regulation)
- DPA (Data Protection Act) - Kenya

Industry-Specific Regulations:

- PCI-DSS (Payment Card Industry Data Security Standard)
- ISO 270001



Why is GRC important?

Data-driven decision-making

Make data-driven decisions within a shorter time frame by monitoring your resources, setting up rules or frameworks, and using GRC software and tools.

Responsible operations

GRC promotes ethical values and guides solid culture development for growth.

Improved cybersecurity

The integrated GRC approach helps protect customer data from cyber risks and comply with data privacy regulations like GDPR, building customer trust and avoiding penalties.



Challenges of GRC implementation?

Change management

- GRC reports provide valuable insights, but change management is needed to act on them quickly.

Data management

- Departments in companies keep their own data, which creates duplicates and makes managing information challenging.

Lack of a total GRC framework

- Without a seamless integration of GRC components, the implementation will likely be fragmented and ineffective.



Challenges of GRC implementation?

Ethical culture development

- Getting every employee/stakeholder to share an ethically compliant culture takes great effort.

Clarity in communication

- Information sharing must be transparent between GRC compliance teams, stakeholders, and employee



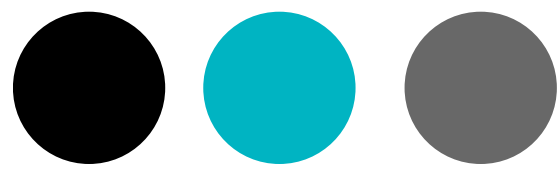
Implementing an effective GRC strategy

- Define clear goals
- Assess existing procedures
- Start from the top
- Use GRC solutions
- Test the GRC framework
- Set clear roles and responsibilities



What areas has GRC influenced?

- System audit
- Vulnerability Management
- IT Governance
- Risk Management
- Business Continuity Management



People/Companies to follow

GRCAfriq - <https://www.linkedin.com/company/grcafric/>

ISACA - <https://www.linkedin.com/company/isaca/>

Solape - <https://www.linkedin.com/in/oluwasolape-akinde-94b07081/>



Talk to me

I'm ready to figure it out
together with you.

Email

marktanui75@gmail.com

Website

www.marktanui.com

Twitter

[@themadbit](https://twitter.com/themadbit)

