Introduction to G.R.C

Governance, Risk and Compliance

KamiLimu cohort 9 - Cybersecurity

Check-in slide!

How is everyone doing?

Introduction

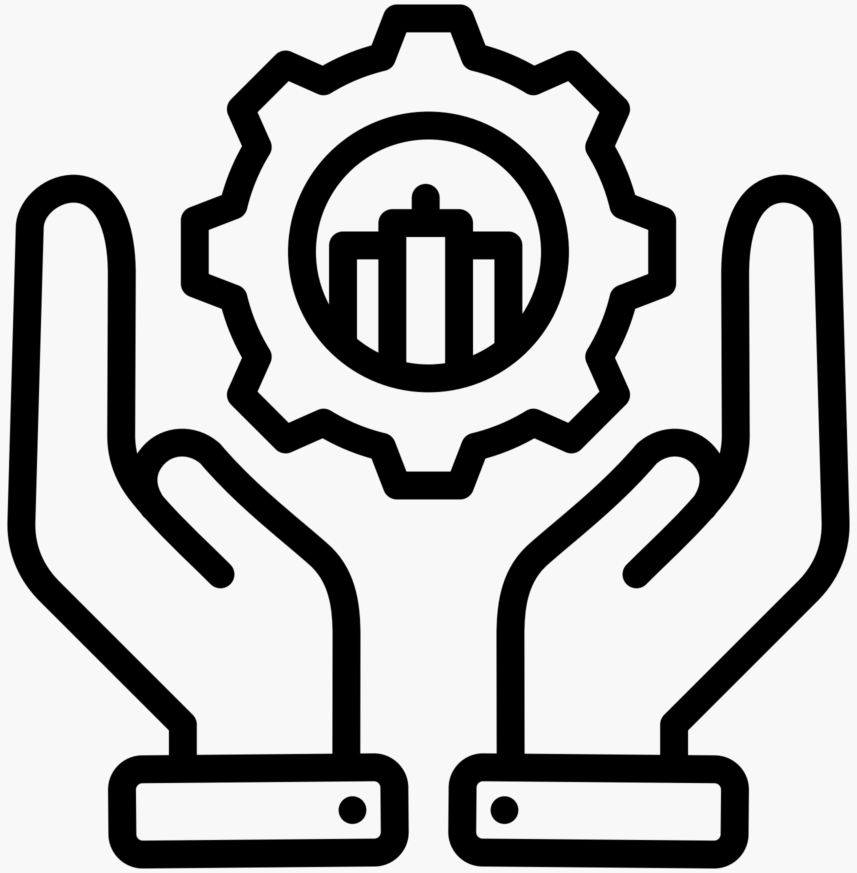
G.R.C - **Governance, Risk and Compliance** works to align IT and business - ensuring that policies, processes and regulation structures meet an organization's risk and business objectives.

People, Process & Technology - core tenets of cyber security

Governance

Governance is the leadership and key processes of an organization that allow it to function as it needs to.

Why should we “measure” governance and what do you think this looks like? Why should governance matter in cyber security?



Risk

Risks are all the potential “bad” things that can happen to an organization. These can stem from the environment e.g. tsunamis, hackers, loss of power (electricity) etc.

Consider a common business scenario, like launching a new product. What are some of the key risks involved, and how might a company mitigate them?

Compliance

What are all the elements an organization is expected to adhere to - think, laws, regulations etc.

Which are some you can think of and how can a new business understand and comply with these?

Key frameworks

ISO27001

Created by the International Organization for Standardization, 27001 represents a framework to assess ISMS

COBIT

The Control Objectives for Information and Related Technologies developed by ISACA

NIST - Cyber Security Framework - CSF

An American framework that has seen widespread adoption. It guides companies on managing cyber security risks.

Other frameworks: industry specific

PCI-DSS

- The Payment Card Industry Data Security Standard.
- Protects and recommends best practice for any entities that manage cards e.g. Visa

SWIFT

- Applies to inter-bank messaging and transactions.
- Managed by SWIFT - Society for Worldwide Inter-bank Financial Telecommunication

Cloud/AI/Crypto frameworks

- Frameworks governing new and emerging technologies
- Companies and governments are racing to develop and address key issues in new tech.

Emerging area: Data Protection

Kenya - Data Protection Act, 2019 & accompanying regulations

- Developed in 2019 to meet a majority (kind of) of the requirements of the GDPR but for Kenyan citizens
- Causing a regulatory headache for companies locally due to non-compliance.

General Data Protection Regulations - (GDPR) - EU

- Developed by the European Union - around 2016.
- In place to address data protection for EU citizens - regardless of their location/jurisdiction.
- Groundbreaking law on Data Privacy.

Global data protection frameworks & regulations

- Frameworks governing new and emerging Carlifonia Consumer Privact Act (CCPA) - USA
- Lei Geral de Proteção de Dados (LGPD) - Brazil - Data Protection law from Brazil that applies if data processing is handled in Brazil.
- etc....

Analysis methodology

Assessment Questionnaires - interviews

- Most provided frameworks have an element of available assessment questionnaires that can be used for assessment.

Evidence gathering & validation

- It is hard to be sure about a client's posture without seeing - seeing is believing
- Gather evidence in the form of seeing, hearing, testing etc.

Reporting

- Explain to the organization where their "gaps" are
- Give recommendations on areas they can improve

Practice lab - TryHackMe

cybergovernanceregulation

Further study (resources)

Frameworks

ISO - https://iso.org
NIST - https://www.nist.gov/cyberframework
COBIT: https://www.isaca.org/resources/cobit

Further study - certifications

- ISC2 https://www.isc2.org/certifications/cgrc
- CIPP (privacy): https://iapp.org/certify/cipp/
- ISO audit certificates: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27001

Questions?

Thank you