Governance Requirements for Cyber Security

CK Bruce, CISA, CISM, CRISC
Changing nature of cyberspace

Cyber Security Strategy: Focus Areas

- Governance
- Incident Management
- Culture
- Collaboration
- Legislation
Cyber Security Strategy: Focus Areas

Legislation
LEGISLATION: FOCUS

- Criminalization of offences related to computer crime and cybercrime
- Institution of investigation mechanisms
- Use of electronic evidence in prosecution
- Creation of an environment that defines the obligations and restricts the liability of ISPs
Collaboration
Cyber Security Strategy: Focus Areas

Culture
Multi-disciplinary and multi-stakeholder approach

Promote awareness of risks at all levels

Embedding cyber security in wider aspects of policy formulation

Certification programs through public and private education institutions

Research and development
Cyber Security Strategy: Focus Areas

Incident Management
INCIDENT RESPONSE

Establishment of a Computer Security Incident Response Team

The first point of contact to address cyber incidents that may affect national critical information infrastructure

- detection, tracking, mitigation

- Alerts and warnings

-a part of hemispheric and international network of CSIRTS
CSX training and certifications offered for skill levels and specialties throughout a professional’s career.

www.isaca.org/csx-certifications
Cyber Security Strategy: Focus Areas

Governance
Frameworks helps build or augment a security program that equips the enterprise to keep pace with the evolving threats.

- Harmonize cybersecurity approaches and provide a common language
- Establish the *right* level of security for your environment
- Inform cybersecurity budget planning
- Communicate cyber risks comprehensively to Senior Leadership
IT’s Stakeholders

Board and Executive
- Set direction for IT, monitor key results and insist on corrective measures

IT Management
- Delivers and improves IT services as required by the business

Business Management
- Defines business requirements for IT and ensures that value is delivered and risks are managed

IT Audit
- Provides independent assurance to demonstrate that IT delivers what is needed

Risk & Compliance
- Measures compliance with related policies and focuses on identification/mitigation of new risks
IT Governance Road Map Overview

Obtain support from senior management

Develop a strong service management capability to ensure that IT services is supporting enterprise strategic objectives

Further strengthen environment with specific Cybersecurity Frameworks

Cascade and strengthen stakeholder roles and responsibilities

Instill project management practices

Establish the ISMS to create a secure, smooth operating environment
Thank you