Information Security Governance:
Guidance for Boards of Directors and Executive Management

Review by :Cheryl Washington and Javier Torner

Overall evaluation:

This document can be used a starting point for a similar guide for higher education executive management. The guide is concise, easy to read and provides executives with enough information to be able to act.

The guide also provides content that may be adapted to create a "self-assessment" template for executives to assess their information security governance.

Section 1. What is information security governance? - An Overview
Desired Outcomes
- Strategic alignment of information security
- Risk management – manage and mitigate risks
- Resource Management
- Performance measurement - information security governance metrics
- Value delivery by optimizing information security investment

Knowledge and Protection of Information Assets
Benefits of Information security Governance
Process Integration

Section 2. Why are information security and information security governance important?
Information security concepts
- Information Security program elements

Information Security Governance defined
- subset of enterprise governance
  - provides strategic direction
  - ensures objectives are achieve
  - manages risk appropriately
  - uses organizational resources responsibly
  - monitors the enterprise security program

Information Security Governance framework – conceptual diagram – figure 1 – must see

Section 3. Who should be concerned with information security governance?
- Board of directors/trustees
- Executives
- Steering committee
- CISO

Essential security practices directors:
- Place information security on the agenda
- Identify info sec leaders
  - ensure support
  - hold them accountable
- ensure the effectiveness of the corporation's info sec policies through review and approval

assign information security to a key committee

Section 4. What should the board of directors/trustees and senior executives be doing?
Understand why information security needs to be governed
Take board level action
Take senior level action
Responsibilities of outcomes with management directives – figure 2 – must see

Section 5. What are some of the thought-provoking questions to ask?
Questions to uncover information security (governance?) issues
Questions to find out how management addresses information security (governance?) issues
Questions to self-assess information security governance

Section 6. what should information security governance deliver?
Strategic alignment
Risk management
Resource Management
Performance Management – metrics!
Value delivery
Process integration – ensure that processes and activities operate as intended from end to end minimizing hidden risks
no gaps exist in information asset protection
unnecessary security overlaps are eliminated
assurance activities are seamlessly integrated
roles and responsibilities are well defined
assurance providers understand their relationship to other assurance functions and regularly liaise with each other

Section 7. How is security governance evolving?
Reason why is evolving – increasing risk, security breaches, etc

Section 8. What can be done to successfully implement information security governance?
Question for directors
Question for Management

Section 9. How does my organization compare on information security governance?
Information security governance maturity model
conduct a Self-assessment to set future developments
planning projects to reach targets – based on gap analysis
prioritizing project work
Maturity levels - see chart
Level 0 – non-existent
Level 1 – Initial/Ad Hoc
Level 2 – Repeatable but intuitive
Level 3 – defined process
Level 4 – Managed and Measurable
Level 5 - Optimized