CERT Governing for Enterprise Security (GES)
Implementation Guide

"Governance and management of security are most effective when they are systemic – woven into the very culture and fabric of organizational behaviors and actions."

Chapter 1: Governing for Enterprise Security

The focus is on governance definitions, effective characteristics and comparison contrast of effective versus ineffective behaviors. There is strong emphasis on senior leadership's commitment to information security being the most important aspect of any successful enterprise security governance model and implementation.

It is stated that enterprise security governance results from duty of care owed by leadership towards fiduciary requirements. This position is based on judicial rationale and reasonable standard of care. The five general governance areas are

1. govern the operations of the organization and protect its critical assets
2. protect the organization's market share and stock price (perhaps not appropriate for education)
3. govern the conduct of employees (educational AUP and other policies that may apply to use of technology resources, data handling, etc.)
4. protect the reputation of the organization
5. ensure compliance requirements are met

The definition of enterprise governance and the list of effective strategies are very good and mirror information, best practices and methodologies developed by the Security Task Force and its working groups. Some definitions provided in the document are from IFAC, ISACA and The Business Roundtable.

The eleven characteristics of effective security governance are spot on to all the elements necessary for an effective enterprise security information program. They are

1. it's an enterprise-wide issue
2. leaders are accountable
3. viewed as business requirement (cost of doing business)
4. it is risk-based
5. roles, responsibilities and segregation of duties defined
6. addressed and enforced in policy
7. adequate resources committed
8. staff aware and trained
9. a development life cycle requirement
10. planned, managed, measureable and measured
11. reviewed and audited

Table 1 Effective versus Ineffective Security Governance is an excellent example to use as a benchmark for any enterprise security governance initiative. It is refreshing one of the elements addresses application life cycle development as an important component of enterprise security. The table information can be made available as is to serve as a basis for assessing the institution's governance effectiveness. Security metrics are generally considered to be somewhat technical in nature. Table 1 information can definitely be turned into a measureable instrument, even if only measured by a Likert Scale.

Following the Table 1 effective and ineffective criteria is a list of challenges to consider that relate to the ineffective or absent category. The challenges listed are

1. understanding the implications of ubiquitous access and distributed information
2. appreciating the enterprise-wide nature of the security problem
3. overcoming the lack of a game plan
4. establishing the proper organizational structure and segregation of duties
5. understanding complex global legal compliance requirements and liability risks (the word global may or may not apply to education)
6. assessing security risks and the magnitude of harm to the organization
7. determining and justifying appropriate levels of resources and investment
8. dealing with the intangible nature of security
9. reconciling inconsistent deployment of security best practices and standards
10. overcoming difficulties in creating and sustaining a security-aware culture

Each of the challenges in the document is addressed separately with more detailed explanation as to why these are challenges. Challenges information would be very useful in presenting rationale to leadership for implementing an effective enterprise security governance model.

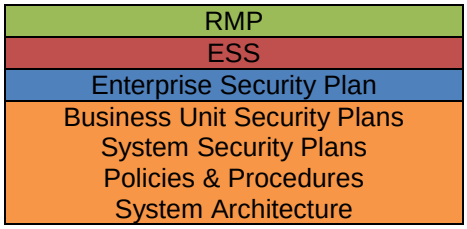
Chapter 2: Defining an Effective Enterprise Security Program

"The governance structure is the defining activity that serves as the foundation and sustains all others."

This chapter focuses on the tenants of an enterprise security plan (ESP), key development players and its relationship within the organization. Activities of an ESP support an enterprise risk management plan (RMP). Results are defined as the development and maintenance of

1. a long-term enterprise security strategy (ESS)
2. an overarching enterprise security plan (which may be supported by underlying business unit security plans and security plans for individual systems)
3. security policies, procedures, and other artifacts
4. the system architecture and supporting documentation

For the purposes of the review of this chapter, a reasonable facsimile of Figure 1 Enterprise Security Program hierarchical relationship is represented below.



Some colleges and universities employ risk managers, and some do not. Of those institutions that do employ a Risk Manager, there are few that appear to have an enterprise risk management plan.

The reference to an ESP serving as a business plan for securing digital assets is a simple yet effective communication technique. This document defines digital assets as

1. information and data
2. applications
3. networks

Figure 2 Enterprise Security Program Inputs is a good graphical representation of components of an ESP. The definitions of the various types of security policies and their relation to the organization are clear and easy to understand.

There are four categories of an ESP

1. governance
2. integration and operation
3. implementation and evaluation
4. capital planning and reviews/audits

It would be interesting to see how accepted educational categories (policies, executive buy-in, tools, incident response, risk assessment, etc.) of an effective security program may relate to the categories in Chapter 2.

Roles and personnel involvement are based on alignment with the four categories of an ESP. It is extraordinarily complex, assumes a board risk committee at the highest level and may not be realistic for higher education models. The explanation and example give for each role or team consisting of multiple institutional roles is good. The information could be used to assist in building an ESP for higher education.

The most useful information in this chapter is Table 2 Categories, Activities, Responsibilities/Roles, and Artifacts. Table 2 could serve as an effective matrix, with appropriate editing, for establishing an ESP in education.

Chapter 3: Enterprise Security Governance Activities

"Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business."

If one makes it through Chapter 2, the reward in Chapter 3 is well worth the wait. This chapter expands on the ESP categories, activities, roles and responsibilities, and artifacts listed in Table 2, Chapter 2. Each activity within each category is mapped out with extraordinary detail with the focus of governance for each of the ESP parts.

The examples are excellent and provide some real world resources and situations that can translate directly into strategies and activities for higher education. As an example, 3.2.5 Governance Activities during Integration and Operations #1 – Categorization and Controls has 3 parts.

1. Categorize Assets by Levels of Risk and Magnitude of Harm

   Categorization of assets is referred to as one of the most important steps in the sustainment of an ESP. CERT uses confidentiality, availability and integrity as three risk factors. Table 3 Categorization of a Medical Claim System is a good example of using the three risk factors to rank an asset.

2. Determine and Update Necessary Controls

   Technical, managerial and operational are defined as the three classes of controls. The three components of security controls are well defined and useful.

3. Develop and Update Key Performance Indicators and Metrics

This section reinforces that Chief Security Officers must establish key performance indicators and measure the effectiveness of security controls, and metrics can be assigned at the organizational and system level. NIST is referenced as having an excellent guide for assessment.

Artifacts are listed after each section that clarifies what end result should be expected.

There are many references throughout this chapter to outside standards and entities that have developed detailed indicators, assessments and other helpful resources. Section 3.3.2 Best Practice and Standards provides a list of some of the better-known standards and guidelines.

There is still an issue of roles driving the ESP, in particular the governance approach and its reliance on an enterprise risk management (ERM) environment in place. Others may see issues with terminology related to specific roles and responsibilities. The information presented in this chapter, however, is thorough and useful.

Appendices

Appendices A, B and C offer more detail on selected artifacts. They are as follows:

1. Appendix A: Board Risk Committee: Missions, Goals, Objectives, and Composition
2. Appendix B: Cross-Organizational Team (X-Team): Missions, Goals, Objectives, and Composition
3. Appendix C: Roles and Responsibilities for an Enterprise Security Program

Other Document Elements

There four podcasts available at http://www.cert.org/podcast/#govering The subject areas are

1. Getting Real About Security Governance
2. The Legal Side of Global Security
3. Why Leaders Should Care About Security
4. Compliance vs. Buy-in

There is a list of Acronyms, Glossary and a list of references.

Conclusion

The CERT Governing for Enterprise Security (GES) Implementation Guide is a very comprehensive, detailed guide that contains many elements that can and should be used by institutions of higher education. The guide definitely sets the ideal stage for ESP.