Information Security Governance and IT Governance

Overview

NC State is redesigning its IT governance process (see external document, “NC State IT Governance Redesign” at http://go.ncsu.edu/it-governance-redesign-final). The integration of information security governance with IT governance in the new structure is a change from the prior model in which security matters were addressed by an IT governance subcommittee. In the new model, information security is embedded throughout an IT governance structure that is designed to be aligned with the mission and business of the university.

Relationship of IT Governance to Information Security Governance

ISACA, an international professional association focused on IT governance, describes information security governance in this way:

> Information security governance consists of the leadership, organisational structures and processes that safeguard information. Critical to the success of these structures and processes is effective communication amongst all parties based on constructive relationships, a common language and shared commitment to addressing the issues.[1]

When we refer to IT governance at NC State, we are referring to a process that is centered on the functional areas of the university: academics, research, business and technology support. We pursue an **embedded model** for the integrating into governance certain key elements of information technology that span these functions. This includes information security, and to some extent, infrastructure.

Embedding information security throughout IT governance helps us achieve the key objectives ISACA identifies: ensuring effective communication, building constructive relationships, and ensuring a shared commitment to realizing the university’s information security strategy. We believe that this integration of information security within a functionally-oriented IT governance process will produce better results than segregating information security into a standalone governance subcommittee with no connection to the other governance bodies.

[1] ISACA. (2006). Information security governance: Guidance for boards of directors and executive management (2nd ed.). Rolling Meadows, IL: IT Governance Institute, p. 11. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/Information-Security-Govenance-for-Board-of-Directors-and-Executive-Management_res_Eng_0510.pdf

ISACA further explains the relationship of information security with an organization's governance processes:

> Information security should be an integral part of enterprise governance, aligned with IT governance and integrated into strategy, concept, design, implementation and operation.[2]

The essential elements of the relationship of information security and IT governance are the needs for **alignment and strategic integration**.

Strategic Integration of Information Security with IT Governance

The strategic importance of information security should not be understated. IT strategy must consider information security in all decisions, whether it's a matter of policy or services. It is critical that information security have a direct connection with the university's decision-making process at the highest level.

- In this model, the CISO should be seated on the Strategic IT Committee.
- As the service owner for information security functions, the CISO is responsible for conveying critical information to the Strategic IT Committee and for advocating for an appropriate enterprise security posture.
- The CISO ensures that information security strategy, decisions and policies are reviewed by the Strategic IT Committee.
- Information security representation throughout IT governance serves to ensure that a two-way flow of information informs strategy. As new IT projects, policies and strategies are considered, information security considerations can be integrated into decision-making.

Alignment of Information Security with IT Governance

In the proposed IT governance model, we view security as integral to all functions, both in the subcommittees' domains and clearly at the level of the Strategic IT Committee. For this reason alone, we do not recommend segregating security functions into a separate governance subcommittee, but instead propose an **embedded model** in which information security interests are represented at every level of IT governance.

We have found that in practice, even under the current model, that in order for information security to be considered by the relevant stakeholders, the Security & Compliance unit has had

[2] ISACA. (2006). Information security governance: Guidance for boards of directors and executive management (2nd ed.). Rolling Meadows, IL: IT Governance Institute, p. 15.

to be engaged with all of the governance subcommittees in order to get buy-in for policies and to ensure adequate communication.

To some extent, the recommended structural changes do not change that. However, by embedding information security into the work of the mission and business focused IT governance subcommittees, we hope to ensure that security is not an afterthought and that the business needs of the various domains are considered when security policies and practices are developed.

While committee membership is outside the scope of the IT governance design phase, we have specific recommendations for security:

1. The CISO will be a member of the Strategic IT Committee
2. The membership of each of the subcommittees should include security/compliance representation. The CISO should appoint appropriate representatives.
    a. We recommend including a security representative as an *ex officio* member on each subcommittee.
    b. Alternatively, the CISO could choose to employ an ad hoc approach and send representatives as subject matter experts when the agenda requires
3. As the service owner for information security, the CISO should maintain an advisory group made up of campus stakeholders who have enough knowledge of the institution and information security issues to advise the CISO effectively.

Information Security Advisory Group Role

Some best practices guides suggest executives should appoint a steering committee to which information security responsibilities are assigned. ISACA suggests a steering team composed of business executives, such as the CEO, CFO, CIO, CISO, and functional area executives.[3] At NC State, we rely on the CIO to communicate directly with the university's executive leadership as needed; we have found it less effective in the past to try to schedule regular meetings with a committee of executives to discuss IT issues exclusively. There is room for the university's top leadership in functional areas such as HR, audit, legal, etc. to be represented in IT governance, either on the Strategic IT Committee or in an appropriate subcommittee. Because security is embedded throughout this new structure, the goal of engaging this group with information security issues can be met.

Others describe a steering committee that serves in an advisory role. Brotby[4] describes the responsibilities of such a committee:

- Review and assist security strategy and integration efforts

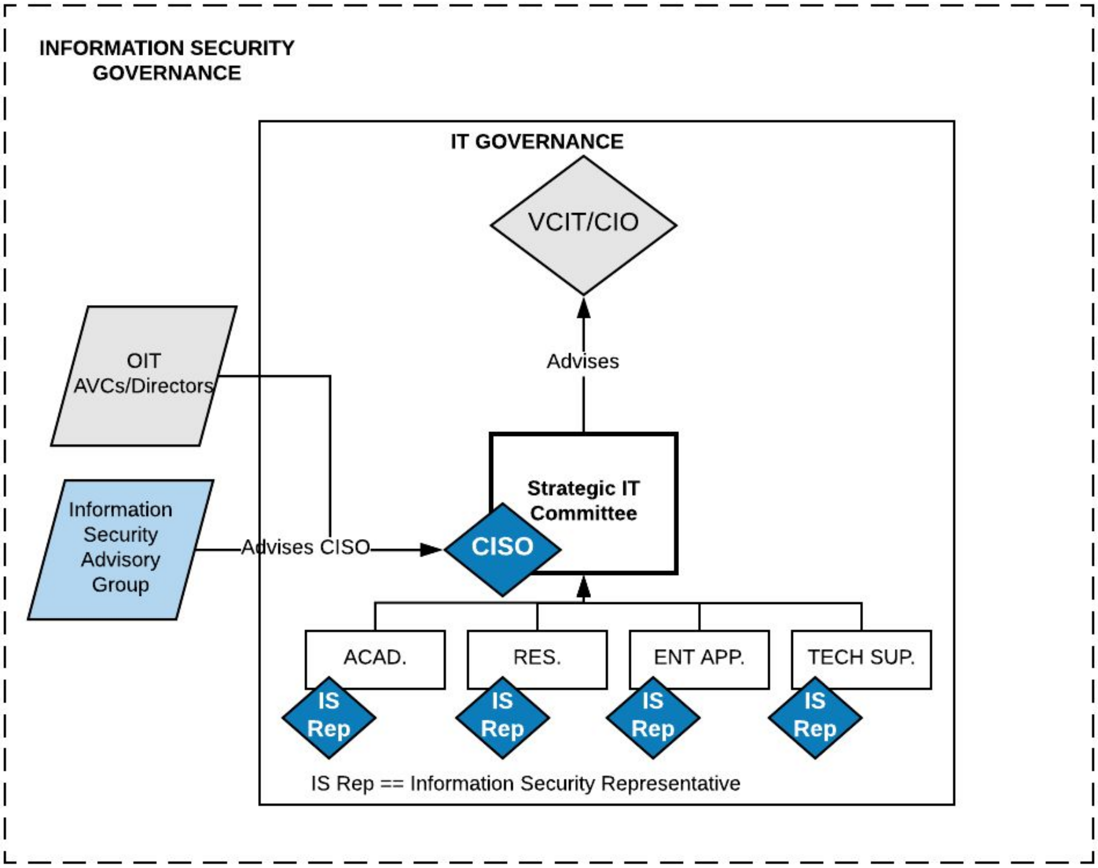
[3] ISACA. (2006). Information security governance: Guidance for boards of directors and executive management (2nd ed.). Rolling Meadows, IL: IT Governance Institute, p. 21.
[4] Brotby, K. (2009). Information security governance: A practical development and implementation approach. Hoboken, NJ: Wiley, p. 23.

- Ensure business unit managers and process owners support integration
- Identify emerging risks
- Promote business unit security practices
- Identify compliance issues
- Review and advise adequacy of security initiatives to serve business functions and value delivered in terms of enabled services
- Review and assure that security initiatives meet business objectives

In the model that we propose, the functions of such a steering committee are accomplished by the **information security advisory group** that advises the **CISO**, who is the service owner for information security functions of the university.

Conceptually, it is possible to think of that group as part of *information security governance* rather than *IT governance;* it is a superset of IT governance. In addition, there may be other groups that play a role in the development of information security strategy and policy such as the OIT assistant vice chancellors/directors that might be considered a part of information security governance.

Figure 1. Information Security Governance and IT Governance



Example: Cybersecurity Incident Response PRR

It may be helpful to trace a hypothetical example through the proposed information security governance process to understand the roles of the information security advisory group and IT governance.

Example: RUL 08.00.17 – Cybersecurity Incident Response Procedure

1. CISO determines that a need exists for a Cybersecurity Incident Response Plan
2. CISO consults the information security advisory group for input into considerations for the plan.
3. (Optionally) A working group is charged by the information security advisory group or the CISO to create a draft of the incident response plan. (This draft could be produced by a working group, the information security advisory group, or by OIT Security & Compliance staff.)

4. In parallel, *ex officio* information security staff on IT governance subcommittees inform them that work is being done in this area.
5. Technology Support subcommittee requests to review the draft when it is complete. This is consistent with the charter of the subcommittee.
6. Draft is reviewed by advisory group, in consultation with personnel on the security service team.
7. Information security advisory group makes a recommendation to CISO recommending acceptance of the draft.
8. CISO reviews the draft and approves.
9. CISO determines whether this should go to IT governance using the IT governance scorecard. This meets the criteria in the Risk category that require governance review.
10. CISO sends draft to the Technology Support subcommittee for review.
11. Technology Support subcommittee reviews and endorses with minor changes, which the CISO agrees to.
12. CISO brings completed proposed incident response plan to Strategic IT Committee for review.
13. Strategic IT Committee reviews and endorses.
14. VCIT/CIO takes incident response plan forward and it becomes a rule.