Chapter 3: Governance and Strategic Planning

Gonzalo De La Torre Parra, Ph.D.

Fall 2021

Objectives

- Identify the key organizational stakeholders that are actively involved in planning and compare their roles
- Explain strategic organizational planning for information security (InfoSec) and describe its relationship to organization-wide and IT strategic planning
- Discuss the importance, benefits, and desired outcomes of information security governance and how such a program would be implemented
- Describe the principal components of InfoSec system implementation planning within the organizational planning scheme

Certification Recommendations

- Agile
- Scrum
- Kanban

Agile

- Agile is a structured and iterative approach to project management and product development.
- It recognizes the volatility of product development, and provides a methodology for self-organizing teams to respond to change without going off the rails.
- Today, agile is hardly a competitive advantage. No one has the luxury to develop a product for years or even months in a black box.
- This means it’s more important than ever to get it right.

Scrum

- Scrum teams commit to shipping working software through set intervals called sprints.
- Their goal is to create learning loops to quickly gather and integrate customer feedback.
- Scrum teams adopt specific roles, create special artifacts, and hold regular ceremonies to keep things moving forward. Scrum is best defined in The Scrum Guide.

Kanban

- Kanban is all about visualizing your work, limiting work in progress, and maximizing efficiency (or flow).
- Kanban teams focus on reducing the time a project takes (or user story) from start to finish.
- They do this by using a kanban board and continuously improving their flow of work.

Planning

- Planning usually involves many interrelated groups and organizational processes.
- The groups involved in planning represent the three communities of interest discussed in Chapter 1.
- These groups may be internal or external to the organization and can include employees, management, stockholders, and other outside stakeholders.

Planning Cont.

- Planning is the dominant means of managing resources in modem organizations.
- It entails the enumeration of a sequence of actions intended to achieve specific goals during a defined period of time, and then controlling the implementation of these steps.
- Planning provides direction for the organization's future.

Planning Precursors

Mission Statement (How?)

- The mission statement explicitly declares the business of the organization and its intended areas of operations. It is, in a sense, the organization's identity card.
- A mission statement should be concise, should reflect both internal and external operations, and should be robust enough to remain valid for a period of four to six years. Simply put, the mission statement must explain what the organization does and for whom.
- Some internal departments sometimes have their own mission stamenets.

Department Mission Statement Example

- The Information Security Department is charged with identifying, assessing, and appropriately managing risks to Company X's information and information systems. It evaluates the options for dealing with these risks, and works with departments throughout Company X to decide upon and then implement controls that appropriately and proactively respond to these same risks. The Department is also responsible for developing requirements that apply to the entire organization as well as external information systems in which Company X participates (for example, extranets) {these requirements include policies, standards, and procedures]. The focal point for all matters related to information security, this Department is ultimately responsible for all endeavors within Company X that seek to avoid, prevent, detect, correct, or recover from threats to information or information systems

Vision Statement (Where?)

- The vision statement is an idealistic expression of what the organization wants to become and works hand in glove with the mission statement.
- The vision statement expresses where the organization wants to go, while the mission statement describes how it wants to get there.

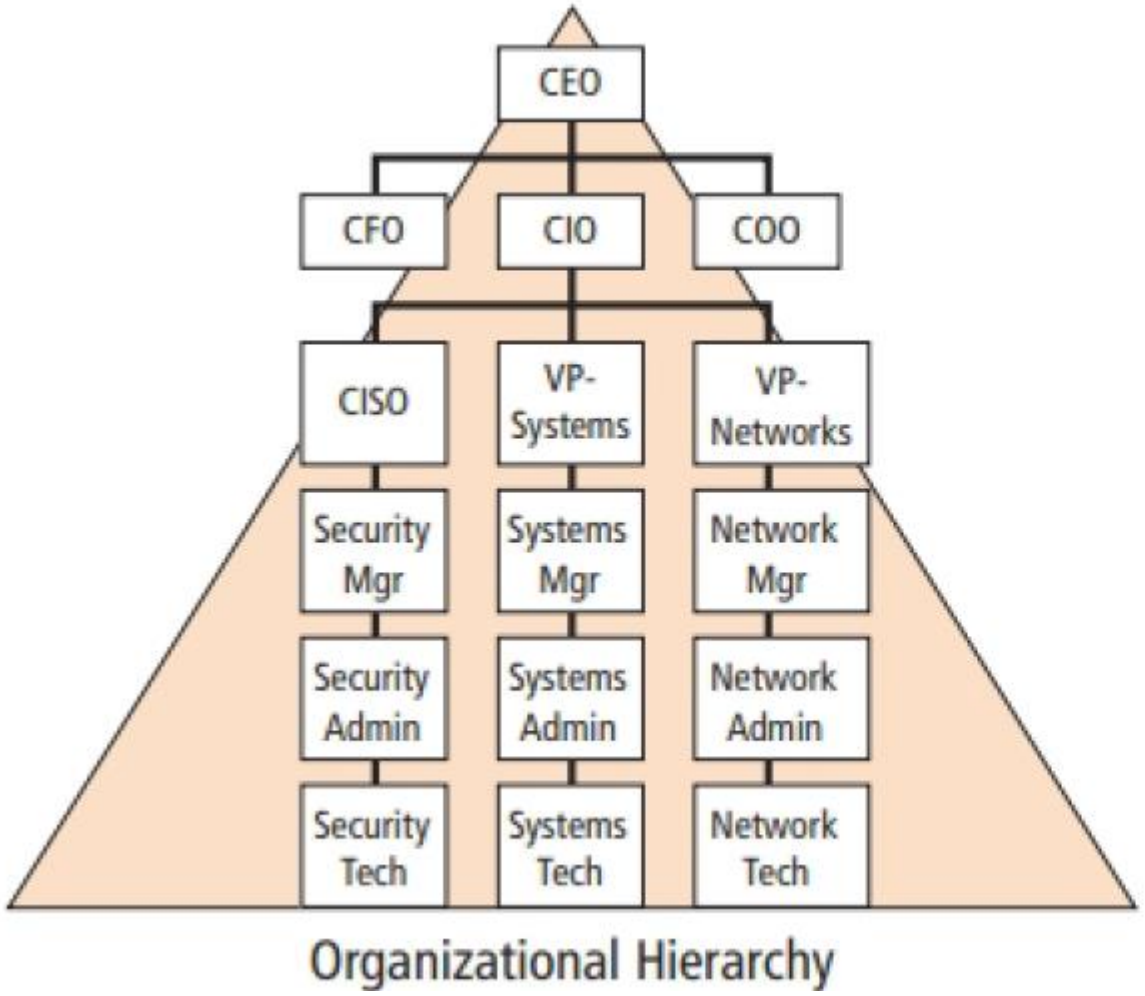
Values Statement

- The trust and confidence of stakeholders and the public are important factors for any organization.
- By establishing a formal set of organizational principles and qualities in a values statement, as well as benchmarks for measuring behavior against these published values, an organization makes its conduct and performance standards clear to its employees and the public.

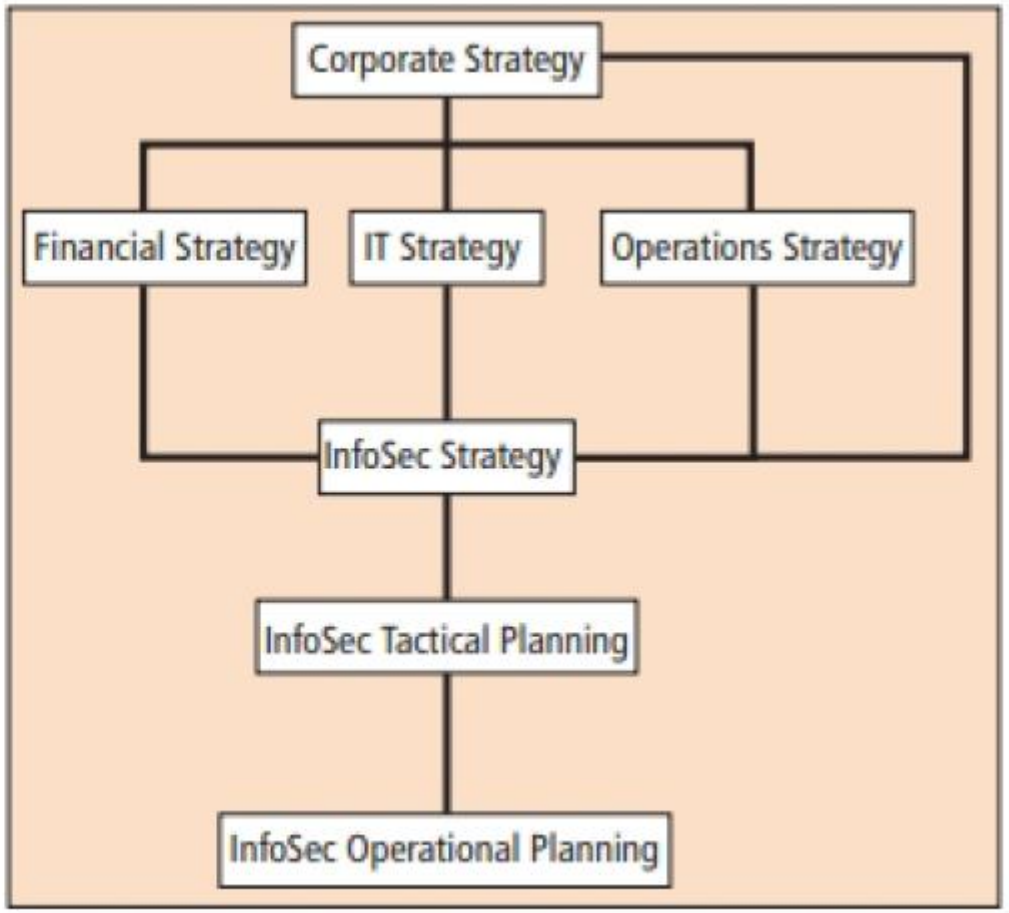

NATIONAL ARCHIVES
Blogs - Bookmark/Share - Contact Us
Search Archives.gov
Search
RESEARCH OUR RECORDS
VETERANS' SERVICE RECORDS
EDUCATOR RESOURCES
VISIT US
AMERICA'S FOUNDING DOCUMENTS
About the National Archives
Home > About > Vision and Mission
About Us
Visit Us
Vision & Mission
Organization
History
Budgets, Plans, & Reports
Strategic Plans
Performance Plans
Performance Budgets
Performance & Accountability Reports
E-Gov Report
State of the Archives and other Speeches & Writings
All Reports & Plans
Rules & Regulations
Laws & Authorities
Regulatory Process
NARA's Regulations
Significant Guidance
Feedback
Contact Us
Comment on Draft Policy & Regulations
Inspector General Hotline
Customer Service Commitment
Employment
Vision and Mission
Mission
We drive openness, cultivate public participation, and strengthen our nation's democracy through public access to high-value government records.
Our Mission is to provide public access to Federal Government records in our custody and control. Public access to government records strengthens democracy by allowing Americans to claim their rights of citizenship, hold their government accountable, and understand their history so they can participate more effectively in their government.
Vision
We will be known for cutting-edge access to extraordinary volumes of government information and unprecedented engagement to bring greater meaning to the American experience.
Our Vision is to transform the American public's relationship with their government, with archives as a relevant and vital resource. This vision harnesses the opportunities to collaborate with other Federal agencies, the private sector, and the public to offer information—including records, data, and context—when, where, and how it is needed. We will lead the archival and information professions to ensure archives thrive in a digital world.
Values
Collaborate: Create an open, inclusive work environment that is built on respect, communication, integrity, and collaborative teamwork.
Innovate: Encourage creativity and invest in innovation to build our future.
Learn: Pursue excellence through continuous learning and become smarter all the time about what we know and what we do in service to others.
Our Values reflect our shared aspirations that support and encourage our long-standing commitment to public service, openness and transparency, and the government records that we hold in trust."

Strategic Planning

- Strategic planning guides organizational efforts and focuses resources toward specific, clearly defined goals in the midst of an ever-changing environment.
- First, an organization identifies a goal for an area of improvement or a need for a new capability
- Documents the current progress toward accomplishing that goal (where are we now?).
- Leadership articulates where the organization seeks to be with regard to the goal (where are we going?).
- Finally, plans can be made for how to achieve that goal (how will we get there?).



Organizational Hierarchy



Planning Hierarchy

General

Strategic Planning

Lower-level tactical and operational planning

Example: General Strategy

Strategy: To provide the highest-quality, most cost-effective widgets in the industry.

Goals: To increase revenue by 10 percent annually.
To increase market share by 5 percent annually.
To decrease expenses by 5 percent annually.

C-Level Executive Team

- CEO - Chief Executive Officer
- COO - Chief Operating Officer
- CFO – Chief Financial Officer
- CIO - Chief Information Officer
- CISO - Chief Information Security Officer

CIO

Strategy: To provide high-level, cost-effective information service in support of the highest-quality, most cost-effective widgets in the industry.

Goals: To reduce IT-related expenses by 5 percent annually while maintaining systems, networks, and service capabilities to meet business needs.

To support corporate reduction in the cost of production through cost-effective systems development and implementation.

To recruit and retain highly competent IT professionals.

COO

Strategy: To provide the highest-quality, industry-leading widget development, manufacture, and delivery worldwide.

Goals: To reduce the cost of manufacture by 10 percent per year through the development of improved production methods.

To reduce the cost of distribution and inventory management by 10 percent per year through improved ordering methods with just-in-time delivery to our largest customers.

To improve the quality of products through research and development of better and more efficient product design and materials acquisition.

CISO

Strategy: To provide effective information service at minimal cost in support of the highest-quality, most cost-effective widgets in the industry.

Goals: To reduce costs associated with information breaches to near zero through improved security assessments and controls.

To support IT reduction in the cost of new information security technologies and systems through the implementation of 20 percent use of open source solutions

To support improvements in all business units through improved security measures that support research and development without concern over the loss of intellectual property due to corporate espionage

To maintain ongoing organizational efforts for the prevention of breaches and information disclosures.

Planning Levels

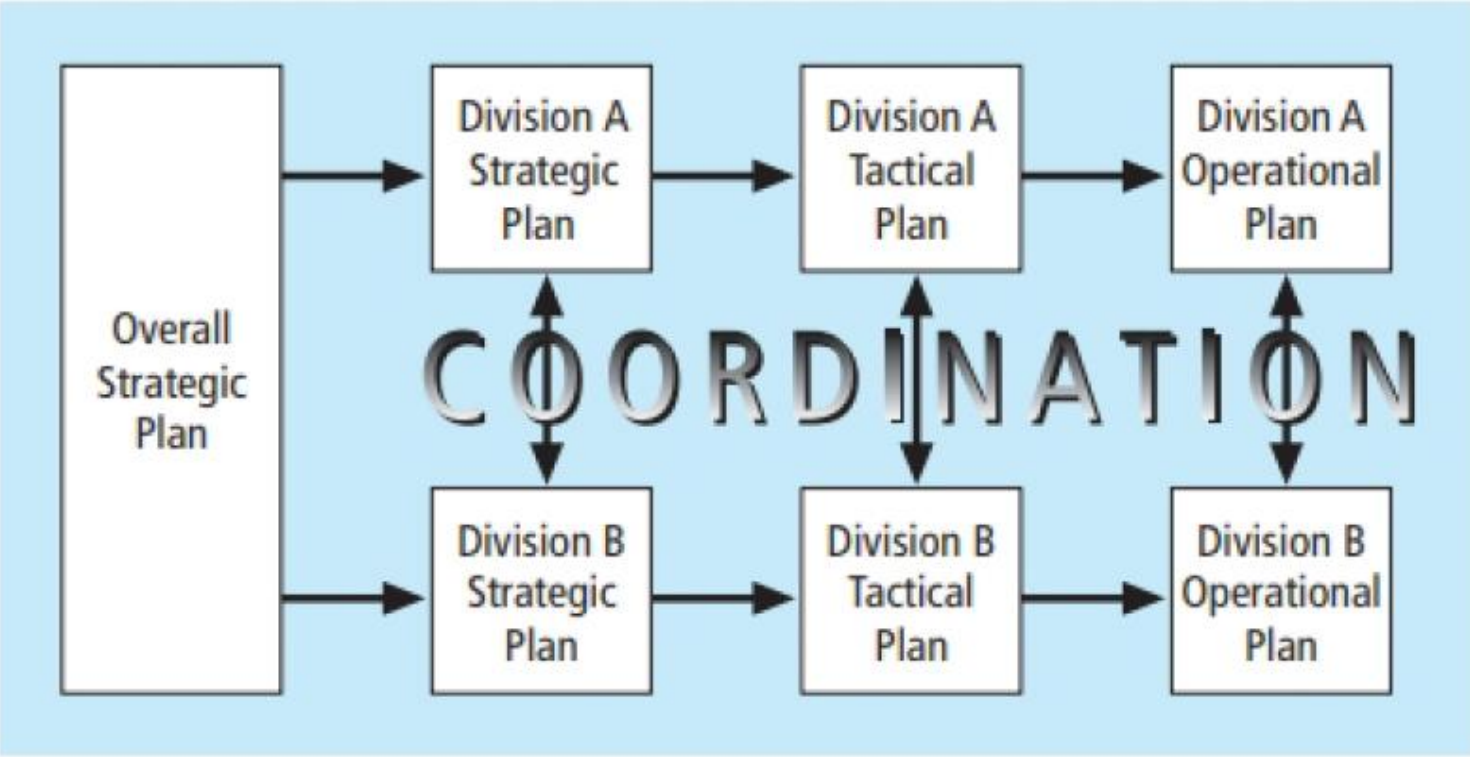


Figure 3-3 Strategic planning levels

Personality Test

- https://www.truity.com/test/type-finder-personality-test-new

Planning and the CISO

- The first priority of the CISO and the InfoSec management team should be the structure of a strategic plan.

Basic Components of InfoSec

- 1. Executive Summary
- 2. Mission, Vision, and Values Statements
- 3. Organizational Profile and History
- 4. Strategic Issues and Challenges
- 5. Organizational Goals and Objectives
- 6. Major Business Unit (or Product/Service) Goals and Objectives
- 7. Appendices (as applicable, including market analyses, internal/external surveys, budgets, and R&D projections)

Information Security Governance

- Strategic planning and corporate responsibility are best accomplished using an approach industry refers to as governance, risk management, and compliance (GRC).

Key Terms

governance The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

governance, risk management, and compliance (GRC) An approach to information security strategic guidance from a board of directors or senior management perspective that seeks to integrate the three components of information security governance, risk management, and regulatory compliance.

Information Security Governance

- InfoSec is all too often regarded as a technical issue when it is, in fact, a strategic management issue.
- In order to secure information assets, an organization's management must integrate InfoSec practices into the fabric of the organization, expanding corporate governance policies and controls to encompass the objectives of the InfoSec process.

The ITGI Approach to Information Security Governance

- Information Technology Governance Institute (ITGI) to address the recognized need for the intellectual development and advancement of Governance of Enterprise IT (GEIT).

- Created by ISACA: organization founded to support the development and certification of auditing programs in computer systems.

ITGI recommends that boards of directors supervise strategic InfoSec objectives:

- 1. Creating and promoting a culture that recognizes the criticality of information and InfoSec to the organization
- 2. Verifying that management's investment in InfoSec is properly aligned with organizational strategies and the organization's risk environment
- 3. Mandating and assuring that a comprehensive InfoSec program is developed and implemented
- 4. Requiring reports from the various layers of management on the InfoSec program's effectiveness and adequacys

Expected Outcomes

- Strategic alignment of InfoSec with business strategy to support organizational objectives
- Risk management by executing appropriate measures to manage and mitigate threats to information resources
- Resource management by utilizing InfoSec knowledge and infrastructure efficiently and effectively
- Performance measurement by measuring, monitoring, and reporting InfoSec governance metrics to ensure that organizational objectives are achieved
- Value delivery by optimizing InfoSec investments in support of organizational objectives

National Association of Corporate Directors (NACD) Recommendations

1. Place InfoSec on the board's agenda.
2. Identify InfoSec leaders, hold them accountable, and ensure support for them.
3. Ensure the effectiveness of the corporation's InfoSec policy through review and approval.
4. Assign InfoSec to a key committee and ensure adequate support for that committee.[6]

Benefits of Information Security Governance

- *An increase in share value for organizations*
- *Increased predictability and reduced uncertainty of business operations by lowering information-security-related risks to definable and acceptable levels*
- *Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care*
- *Optimization of the allocation of limited security resources*
- *Assurance of effective InfoSec policy and policy compliance*
- *A firm foundation for efficient and effective risk management, process improvement, and rapid incident response*
- *A level of assurance that critical decisions are not based on faulty information*
- *Accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response*[7]

Make sure the program includes:

- An InfoSec risk management methodology
- A comprehensive security strategy explicitly linked with business and IT objectives
- An effective security organizational structure
- A security strategy that talks about the value of information being protected and delivered
- Security policies that address each aspect of strategy, control, and regulation
- A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy
- Institutionalized monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk
- A process to ensure continued evaluation and updating of security policies, standards, procedures, and risks

NCSP Industry Framework for Information Security Governance

- Generated in 2004
- National Cyber Security Partnership (NCSP)
- The CGTF framework applies the IDEAL model to information security governance
- Originally published in a 1996 report on software process improvement by Bob Mcfeeley for the Software Engineering Institute of Carnegie Mellon University.

IDEAL

I	**Initiating**	Lay the groundwork for a successful improvement effort.
D	**Diagnosing**	Determine where you are relative to where you want to be.
E	**Establishing**	Plan the specifics of how you will reach your destination.
A	**Acting**	Do the work according to the plan.
L	**Learning**	Learn from the experience and improve your ability to adopt new improvements in the future.

Figure 3-4 IDEAL model use as a general governance framework

Responsibilities by Functional Role

Figure 3-5 Information security governance responsibilities[10]

Source: IT Governance Institute.

CERT Governing for Enterprise Security Implementation

- Governance activities should be driven by a Board Risk Committee (BRC) in addition to the organization's executive management and select key stakeholders.

The GES includes three supporting documents, referred to as Articles:

- Article 1: Characteristics of Effective Security Governance
- Article 2: Defining an Effective Enterprise Security Program
- Article 3: Enterprise Security Governance Activities

CERT Governing for Enterprise Security Implementation

Figure 3-6 CERT GES hierarchy[13]

Source: Carnegie Mellon University, Software Engineering Institute, CERT.

ISO/IEC 27014:2013 Governance of Information Security

- A set of international standards for the certification of an Information Security Management System (ISMS)

The six high-level "action-oriented" information security governance principles.

- 1. Establish organization-wide information security.
- 2. Adopt a risk-based approach.
- 3. Set the direction of investment decisions.
- 4. Ensure conformance with internal and external requirements.
- 5. Foster a security-positive environment.
- 6. Review performance in relation to business outcomes.

Five Governance Processes

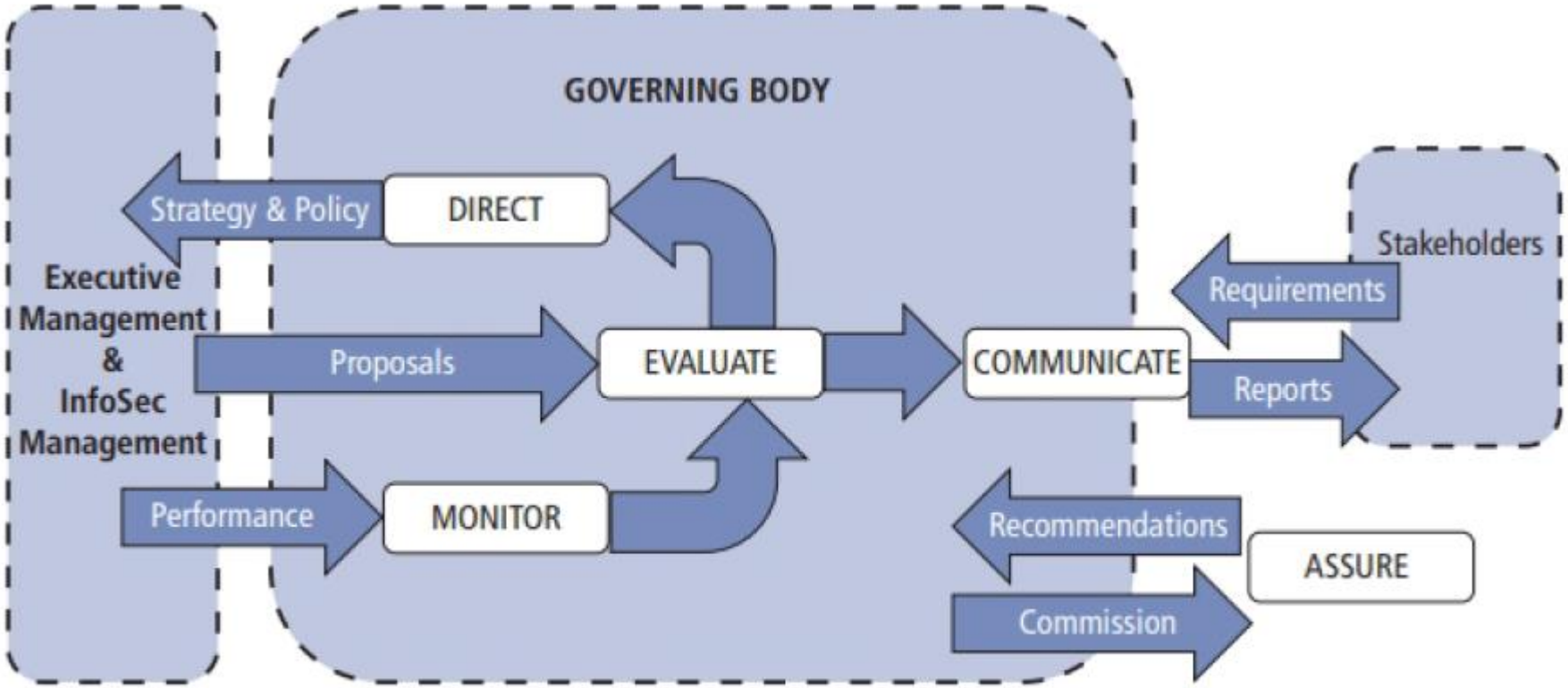


Figure 3-7 ISO/IEC 27014:2013 governance processes[19]

Source: R. Mahncke, Australian eHealth Informatics and Security Conference, December 2013.

Five Governance Processes

- *Evaluate*—Review the status of current and projected progress toward organizational information security objectives, and make a determination whether modifications of the program or its strategy are needed to keep on track with strategic goals.
- *Direct*—The board of directors provides instruction for developing or implementing changes to the security program. This could include modification of available resources, structure of priorities of effort, adoption of policy, recommendations for the risk management program, or alteration to the organization's risk tolerance.
- *Monitor*—The review and assessment of organizational information security performance toward goals and objectives by the governing body. Monitoring is enabled by ongoing performance measurement.
- *Communicate*—The interaction between the governing body and external stakeholders, where information on organizational efforts and recommendations for change are exchanged.
- *Assure*—The assessment of organizational efforts by external entities like certification or accreditation groups, regulatory agencies, auditors, and other oversight entities, in an effort to validate organizational security governance, security programs, and strategies.[18]