Policy, Strategy and Operations

IWOSI: The Information Warfare, Cyber Warfare and Open Sources Intelligence – Yasar University Izmir, Turkey 2012

Part I-1: 2012.04.18, 10:00-12:00

Dr. Nikolaj Goranin, CISM, CISA
Vilnius Gediminas Technical University

About this course

- Covers non-technical aspects of information security insurance.
- “CISM-oriented” (Based on CISM 2011 Review manual).
- A Short Primer for Developing Security Policies (SANS Institute).
- Open-source documentation.
- Not the official ISACA course for CISM certification.

Importance of Information Security Governance

- Governance – continuous process of decision-making and managing processes, based on specific expectations and power.
- Information and knowledge – "crown jewels" in digital age.
- Losses due to security breaches.
- Information security insurance can not be based only on technical people.
- Governance allows understanding where you are and what do you want to achieve.

Julia Allen @ Carnegie Mellon

- *Governing for enterprise security means viewing adequate* ***security as a non-negotiable requirement of being in business****. If an organization’s management – including boards of directors, senior executives and all managers – does not establish and reinforce the business need for effective enterprise security, the organization’s desire to state of security will not be articulated, achieved, or sustained. To achieve a sustainable capability,* ***organizations must make enterprise security the responsibility of leaders*** *at a governance level, not of other organizational roles and that lack the authority, accountability and resources to act and enforce compliance.*

Outcomes of Information Security Governonce

- □ Strategic alignment.
  - ■ Aligning inf.sec. with business strategy.
- □ Risk management.
  - ■ Executing measures to mitigate risks and reduce impacts.
- □ Value delivery
  - ■ Optimizing security investments in support of business objectives.
- □ Resource management
  - ■ Effective usage of available resources
- □ Performance measurement
  - ■ Monitoring and reporting status
- □ Integration
  - ■ All processes operate as intended

Governance Framework

- □ Security strategy
- □ Governing security policies
- □ Complete set of standards for each policy
- □ Effective security organizational structure with no conflicts of interest
- □ Metrics for monitoring process efficiency.

Roles and Responsibilities of Senior Management – /I/

- Information security management requires:
  - Strategic direction
  - Commitment
  - Resources
  - Responsibilities
  - Monitoring

Roles and Responsibilities of Senior Management – /II/

- Senior management:
  - Board of directors
  - Executive management
  - Steering committee
  - CISO / Information security manager
  - Audit executives

Board of Directors

Strategic Alignment	Require demonstrable alignment.
Risk Management	Establish risk tolerance; Oversee a policy of risk; Ensure regulatory compliance.
Value Delivery	Require reporting of security activity costs.
Performance Measurement	Require reporting of security effectiveness.
Resource Management	Oversee a policy of knowledge management and resource utilization.
Process Assurance	Oversee a policy of assurance process integration.

Executive Management

Strategic Alignment	Institute processes to integrate security with business objectives
Risk Management	Ensure that roles and responsibilities include risk management in all activities; Monitor compliance.
Value Delivery	Require business case studies of security initiatives.
Performance Measurement	Require monitoring and metrics for security activities.
Resource Management	Ensure processes for knowledge capture and efficiency metrics.
Process Assurance	Provide oversight of all assurance functions and plans for integration.

Steering committee

Strategic Alignment	Review and assist security strategy and integration efforts; Ensure that owners support integration.
Risk Management	Identify emerging risks, promote business unit security practices and identify compliance issues.
Value Delivery	Review and advise on the adequacy of security initiatives to serve business functions.
Performance Measurement	Review and advise whether security initiatives meet business objectives.
Resource Management	Review processes for knowledge capture and disseminations.
Process Assurance	Identify critical business processes and assurance providers; Direct assurance integration efforts.

CISO / Information security manager.

Strategic Alignment	Develop security strategy; oversee the security program and initiatives; Get the support.
Risk Management	Ensure that risk assessments are conducted; Develop risk mitigation strategies; Enforce compl.
Value Delivery	Monitor utilization and effectiveness of security resources.
Performance Measurement	Develop and implement monitoring and metrics approaches, direct and monitor activities.
Resource Management	Develop methods for knowledge capture and dissemination.
Process Assurance	Liaise with other assurance providers; Ensure the gaps are indentified and addressed.

Audit Executives

Strategic Alignment	Evaluate and report on degree of alignment.
Risk Management	Evaluate and report on corporate risk management practices and results.
Value Delivery	Evaluate and report on efficiency.
Performance Measurement	Evaluate and report on efficiency or resource management.
Resource Management	Evaluate and report on efficiency or resource management.
Process Assurance	Evaluate and report effectiveness of assurance processes performed by management.

CISO Responsibilities

- Position in hierarchy

- Getting senior management commitment:
  - Aligning business and security objectives;
  - Identifying potential consequences of failing;
  - Identifying budget;
  - Total cost of ownership (TCO) and Return on investment (ROI) methods;
  - Defining monitoring methods.

- Establishing Reporting and Communication Channels with:
  - Management;
  - Business Process Owners;
  - Employees.

Information Security Governance Metrics – /I/

- □ It is impossible to manage something if you can not measure it.
- □ How secure is organization?
- □ What impact is lack of security on productivity?
- □ What impact will security solutions have on productivity?

Information Security Governance Metrics – /II/

Strategic Alignment	Reverse evaluation of business strategy being found in security strategy.
Risk Management	Determined risk tolerance; Defined mitigation objective; Trends of risk assessments.
Value Delivery	Key goal and performance (KGI and KPI) indicators; Asset and protection cost proportions.
Performance Measurement	Time to identify an incident; Number of detected unreported incidents; Number of incidents.
Resource Management	Number of standardized processes; Number of assets covered by security resources.
Process Assurance	Number of gaps/overlapping controls; Number of defined roles and reponsibilities.

Information Security Strategy

- *Corporate **strategy is the pattern of decisions** in a company that **determines and reveals its objectives**, purposes, or goals, produces the principal policies and plans for achieving those goals, and **defines the range of business** the company is to pursue, the kind of economic and human **organization it is or intends to be**, and the nature of the economic and non-economic contribution it intends to make to its stakeholders, employees, customers, and communities.*

    - Kenneth Andrews The Concept of Corporate Strategy, 2nd Edition.

Answers to be Answered

- □ What?
- □ Why?
- □ When?
- □ How?
- □ Who?
- □ Where?

Strategy Constraints

- Legal
- Physical
- Ethics
- Culture
- Costs
- Personnel
- Organizational structure
- Resources
- Capabilities
- Time
- Risk tolerance

Pitfalls in Developing Strategy

- Overconfidence (*Sure I am right*)
- Optimism (*Sure I can*)
- Anchoring (*Once defined we will not change*)
- The *status quo* bias (*I do not want to change something*)
- Mental accounting (*We'd better spend on "innovation"*)
- The herding instinct (*I won't make "original" mistake*)
- False consensus (*Everyone supports me*)

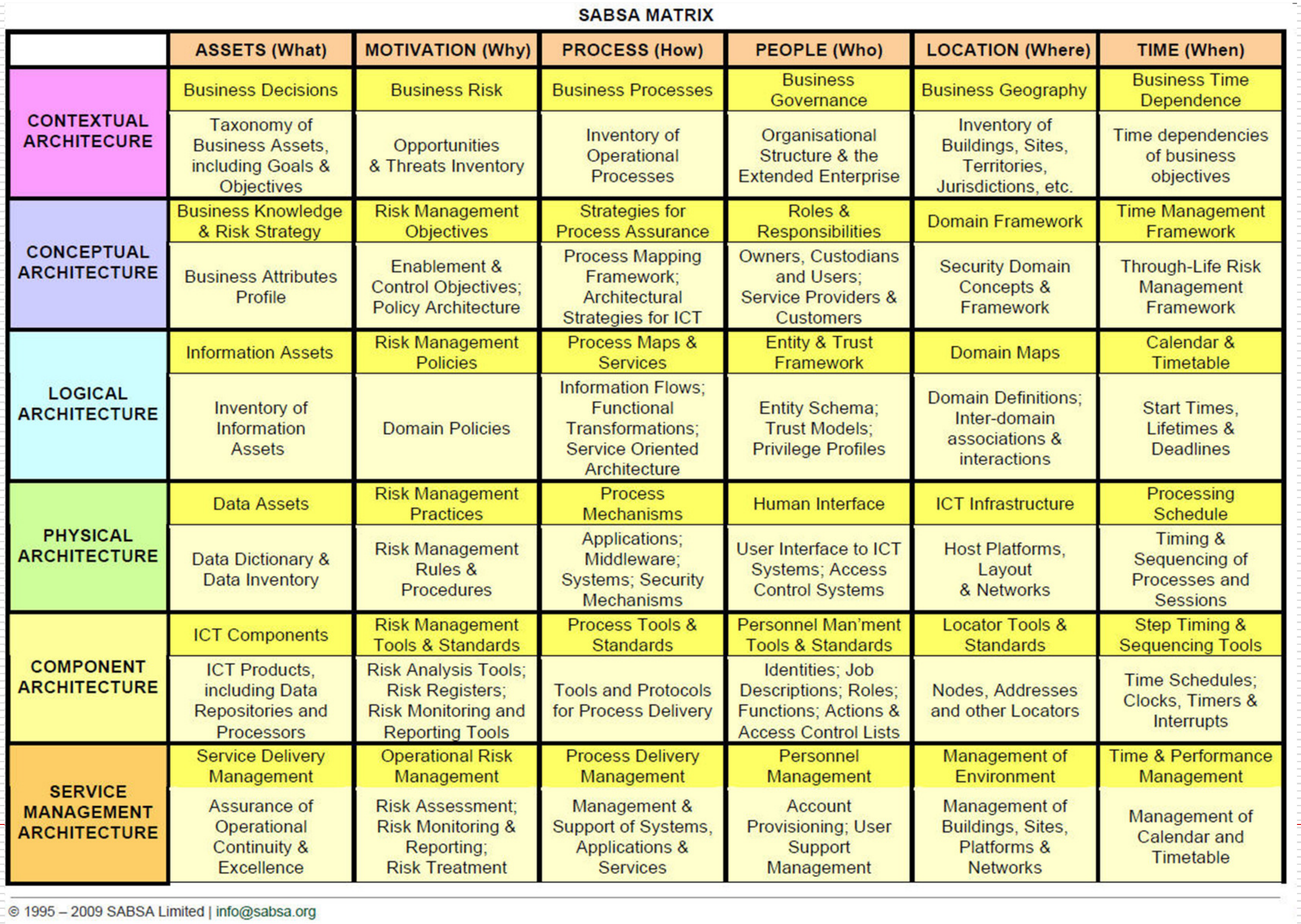
Strategy Implementation Steps

- Business case calculation:
  - Value
  - Focus
  - Deliverables
  - Dependencies
  - Workload
  - Resources
  - Commitments

- **N.B.** Business case should be adaptable, business oriented, understandable, measurable, REALISTIC.

- Defining the desired state
- Road-map
- Action plan based on a gap analysis

SABSA Security Architecture



SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Policy and Strategy

- Policy
- Procedures
- Standards

- As a strategy evolves, it is vital that supporting policies are developed to articulate the strategy.

Policy Aims

- □ Policies define appropriate behavior.
- □ Policies set the stage in terms of what tools and procedures are needed.
- □ Policies communicate a consensus.
- □ Policies provide a foundation for HR action in response to inappropriate behavior.
- □ Policies may help prosecute cases.

Notices on Policy Development

- □ A sample of people affected by the policy should be provided an opportunity to review and comment.
- □ A sampling of the support staff effected by policy should have an opportunity to review it.
- □ Incorporate policy awareness as a part of employee orientation.
- □ Provide a refresher overview course on policies once or twice a year.

Requirements for Policy Development

- Policies must:
  - be implementable and enforceable
  - be concise and easy to understand
  - balance protection with productivity
- Policies should:
  - state reasons why policy is needed
  - describe what is covered by the policies
  - define contacts and responsibilities
  - discuss how violations will be handled

Level of Control

- Security needs and culture play major role.
- Security policies MUST balance level of control with level of productivity.
- If policies are too restrictive, people will find ways to circumvent controls.
- Technical controls are not always possible.
- You must have management commitment on the level of control.

Policy Structure

- Dependent on company size and goals.
- One large document or several small ones?
  - smaller documents are easier to maintain/update
- Some policies appropriate for every site, others are specific to certain environments.
- Some key policies:
  - acceptable use
  - remote access
  - information protection
  - perimeter security
  - change management

Procedures

- Policies only define "what" is to be protected.
- Procedures define "how" to protect resources are the mechanisms to enforce policy.
- Procedures define detailed actions to take for specific incidents.
- Procedures provide a quick reference in times of crisis.
- Procedures help eliminate the problem of a single point of failure (e.g., an employee suddenly leaves or is unavailable in a time of crisis).

Standards Development

- Standards set the permissable bounds for procedures and practices of technology and systems, people and events.
- Provide the measureing stick for policy compliance and basis for audit.
- Standards serve to interpret policies.
- Standards must be disseminated to those governed and impacted by them.

Demonstration of Supplementing Documents

Discussion