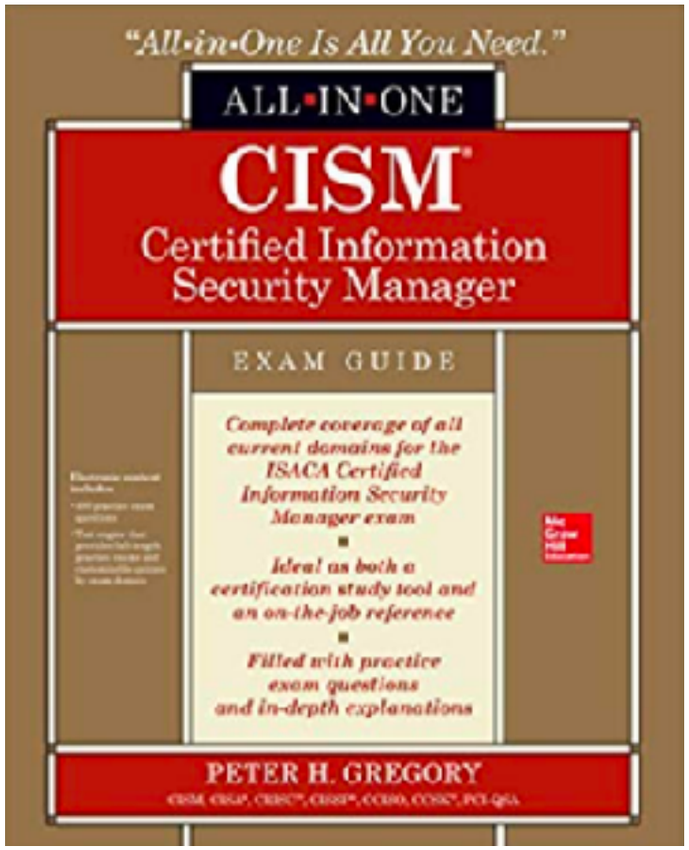
CNIT 160: Cybersecurity Responsibilities

4. Information Security Program Development Part 1

Pages 190 - 202



Chapter Topics

- **Information Security Programs**
- **Security Program Management**
- **Security Program Operations**
- **IT Service Management**
- **Controls**
- **Metrics and Monitoring**
- **Continuous Improvement**

Information Security Programs

Information Security Programs

- **Outcomes**
- **Charter**
- **Scope**
- **Information Security Management Frameworks**
- **Defining a Road Map**
- **Information Security Architecture**
  - **The Open Group Architecture Framework**
  - **The Zachman Framework**
  - **Implementing a Security Architecture**

Developing an Information Security Program

- **Four steps**
  - **Developing a security strategy**
  - **Gap analysis**
  - **Developing a road map**
  - **Developing a security program**

Information Security Programs

- **The collection of activities to identify, communicate, and address risks**
- **Consists of controls, processes, and practices**
- **To increase resilience of computing environment, and**
- **Ensure that risks are known and handled effectively**

Enabling Business

- **Security program acts as a business enabler**
  - **Allowing it to consider new business ventures**
    - **While being aware of risks that can be mitigated**
- **Like the brakes on a race car**
  - **Allowing it to move faster and stay on the road**

Outcomes

- **Strategic alignment**
- **Risk management**
- **Value delivery**
- **Resource management**
- **Performance management**
- **Assurance process integration**

Strategic Alignment

- **Program must work in harmony with the rest of the organization**
  - **Being aware of new initiatives**
  - **Developing risk tolerance criteria that business leaders agree with**
  - **Establishing mutual trust**
  - **Use a security council or governance committee**
    - **With stakeholders across the business**

Risk Management and Value Delivery

- **Risk Management**
  - **Identifies risks**
    - **Facilitates desired outcomes**
      - **Through appropriate risk treatment**
- **Value Delivery**
  - **Reducing risk in critical activities**
    - **To an acceptable level**

Resource Management

- **Permanent and temporary staff, external service providers, and tools**
- **Must be managed so they are effectively used**
    - **To reduce risks in alignment with the risk management program**
- **"Rightsizing" information security program budget**
    - **Assist with resource requests from security manager**

Performance Management

- **Measure key activities**
  - **To ensure the are operating as planned**
- **Security metrics**

Assurance Process Integration

- **Information security program aligns with other assurance programs and processes**
  - **HR, finance, legal, audit, enterprise risk management, IT, and operations**
  - **Influences those activities to protect them from harm**

Charter

- **Formal written definition of**
  - **Objectives of the program**
  - **Main timelines**
  - **Sources of funding**
  - **Names of principal leaders and managers**
  - **Business executives who are sponsoring the program**
- **Gives security manager authority, shows support from leadership team**

Security Manager Functions

- **Develop and**
- **Enforce *security policy***
- ***Risk management* process**
- ***Security governance***
- ***Controls* across business unit boundaries**

Security Manager Functions

- **Develop and direct implementation of key security processes**
    - **Vulnerability management**
    - **Incident management**
    - **Third-party risk**
    - **Security architecture**
    - **Business continuity planning**
    - **Security awareness training**

Team Sport

- **Security charter is ratified by executive management**
- **Security manager can't dictate the program to others**
  - **Must lead and guide program through collaboration and consensus by stakeholders**
- **Executive leaders and board of directors hold the ultimate responsibility or ownership for protecting information**

Scope

- **Define departments, business units, affiliates, and locations**
  - **Included in information security program**
- **More relevant in larger organizations**

Information Security Management Frameworks

- **Business process models**
  - **Include essential processes and activities**
  - **Needed by most organizations**
- **Risk-centric**

Three Most Popular Security Management Frameworks

- **ISO/IEC 27001:2013**
- **COBIT 5**
- **NIST CSF**

ISO/IEC 27001:2013

- **International standard**
- **"Information technology - Security techniques - Information security management systems - Requirements"**
- **Processes used to**
  - **Assess risk**
  - **Develop controls**
  - **Manage typical processes such as vulnerability management and incident management**

COBIT 5

- **From ISACA**
- **Controls and governance framework**
  - **For managing an IT organization**
- **COBIT 5 for Information Security**
  - **Additional standard to extend COBIT 5**

NIST CSF

- **US National Institute of Standards and Technology (NIST)**
- **Cyber Security Framework (CSF)**
  - **Developed in 2014 to address rampant security breaches and identity theft in the US**

Ch 4a-1

Defining a Road Map

- **Required steps to achieve an objective**
  - **In support of the business vision and mission**
- **Consists of various tasks and projects**
  - **Creating and implementing capabilities**
  - **Reducing information risk**

Enterprise Architecture

- **Both a business function and a technical model**
- **Business function**
  - **Activities ensuring that important business needs are met by IT systems**
- **Model**
  - **Mapping business systems into IT environment and systems**

Information Security Architecture

- **A subset within Enterprise Architecture**
- **Concerned with two things**
  - **Protective characteristics in components in the enterprise architecture**
  - **Specific components n the enterprise architecture that provide preventive or detective security functions**

Enterprise Architecture Ensures:

- **All hardware and software components fulfill a stated specific business purpose.**
- **All components work well together.**
- **There is overall structure and consistency in infrastructure throughout the organization.**
- **Infrastructure resources are used efficiently.**
- **Infrastructure is scalable and flexible.**
- **Existing elements can be upgraded as needed.**
- **Additional elements can be added as needed.**

Two Layers of Information Security Architecture

- **Policy**
  - **Necessary characteristics of overall environment**
    - **Ex: centralized authentication, endpoint-based web filtering**
- **Standards**
  - **Vendor standards**
  - **Protocol standards**
  - **Configuration or hardening standards**

Centralized Functions

- **Operate more effectively than isolated, local instances**
- **Amplify workforce**
  - **So a small staff can manage hundreds or thousands of devices**

Centralized Functions

- **Authentication**
  - **Microsoft Active Directory (AD)**
  - **Lightweight Directory Access Protocol (LDAP)**
- **Monitoring**
  - **SIEMs like Splunk**
- **Device Management**
  - **Consistency for servers, workstations, mobile devices, and network devices**

Two Enterprise Architecture Frameworks

- **The Open Group Architecture Framework (TOGAF)**
- **Zachman Framework**

- **These are *Enterprise Architecture* models, not *Enterprise Security Architecture* models**

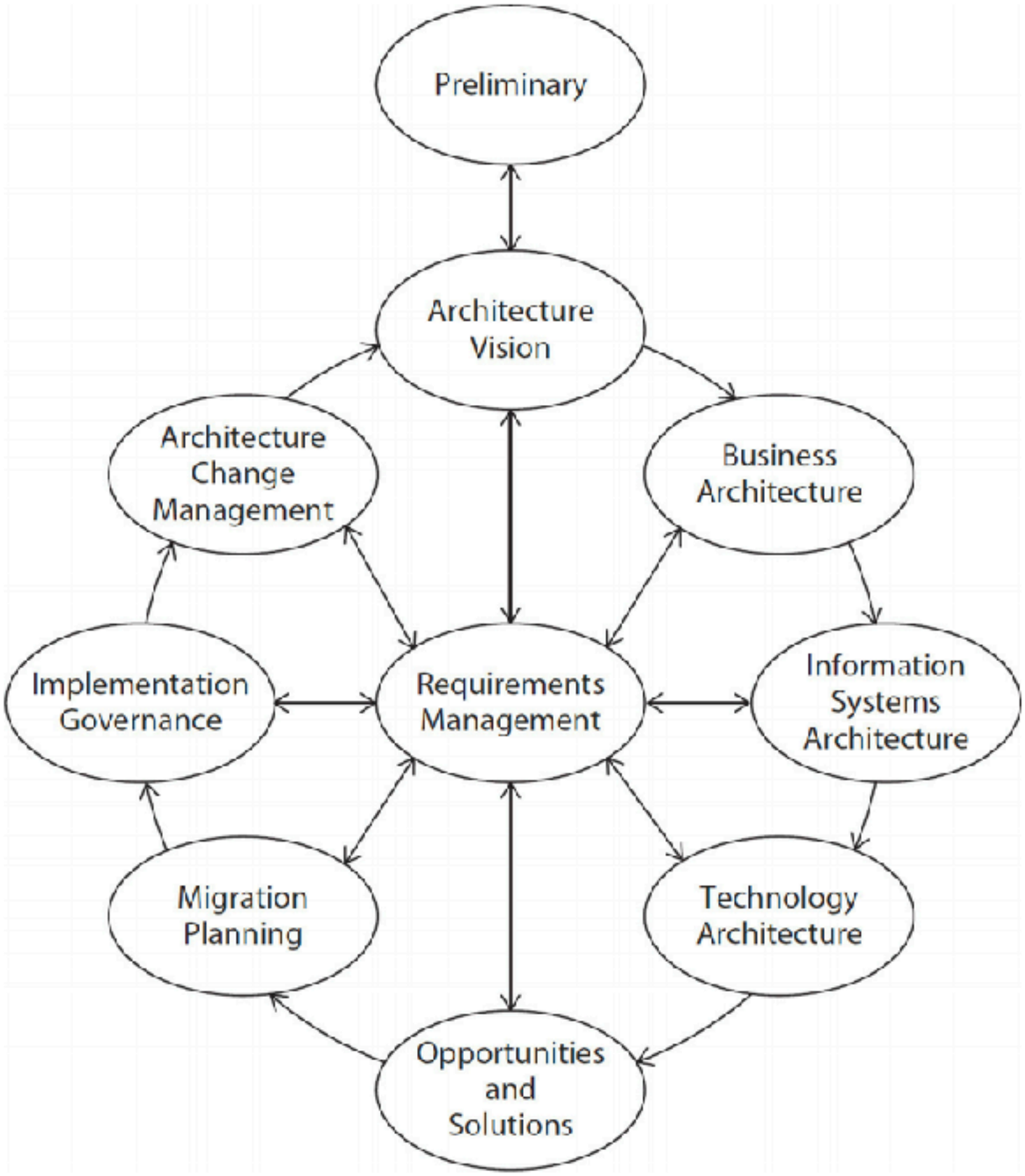
The Open Group Architecture Framework (TOGAF)

- **Life-cycle enterprise architecture framework**
  - **For designing, planning, implementing, and governing**
  - **An enterprise technology architecture**
- **A high-level approach**

Phases in TOGAF

- **Preliminary**
- **Architecture vision**
- **Business architecture**
- **Information systems architecture**
- **Technology architecture**
- **Opportunities and solutions**
- **Migration planning**
- **Implementation governance**
- **Architecture change management**
- **Requirements management**

TOGAF Components



Zachman Framework

- **Established in the 1980s**
  - **Still dominant today**
- **Likens IT enterprise architecture to construction and maintenance of an office building**

Zachman Framework

	Data	Functional (Application)	Network (Technology)	People (Organization)	Time	Strategy
Scope	List of data sets important in the business	List of business processes	List of business locations	List of organizations	List of events	List of business goals and strategy
Enterprise Model	Conceptual data/object model	Business process model	Business logistics	Workflow	Master schedule	Business plan
Systems Model	Logical data model	System architecture	Detailed system architecture	Human interface architecture	Processing structure	Business rule model
Technology Model	Physical data/ class model	Technology design	Technology architecture	Presentation architecture	Control structure	Rule design
Detailed Representation	Data definition	Program	Network architecture	Security architecture	Time definition	Rule speculation
Function Enterprise	Usable data	Working function	Usable network	Functioning organization	Implemented schedule	Working strategy

Implementing a Security Architecture

- **Both a big-picture and a detailed plan**
- **At enterprise level**
- **Policy and governance**
- **Decisions about major aspects**
- **Such as brands of servers, workstations, and network devices**

Implementing a Security Architecture

- **At detail level**
  - **Configuration and change management on devices or groups of devices**
- **Ex: Upgrade to DNS infrastructure**
  - **Might increase number of name servers**
  - **Requiring updates to most or all devices**

Changes to Architecture Models

- **Software-Defined Networking (SDN)**
- **Virtualization**
- **Microservices**
  - **Small, independent services that communicate over networks**
  - **Often in containers**

Security Program Management

Security Program Management Topics

- **Security Governance (in this lecture)**
  - **Activities and Results**
- **For later lectures:**
  - **Risk Management**
  - **The Risk Management Program**
  - **The Risk Management Process**
    - **Identifying and Grouping Assets**
    - **Risk Analysis**
    - **Risk Treatment**

Security Program Management Topics (continued)

- **For later lectures**
  - **Audits and Reviews**
    - **Control Self-Assessment**
    - **Security Reviews**
- **Policy Development**
- **Third-Party Risk Management**
- **Administrative Activities**

Security Governance

- **Assemblage of management activities that**
- **Identify, analyze and treat risks to key assets**
- **Establish key roles and responsibilities**
- **Measure key security processes**

Security Governance Personnel

- **Board of Directors**
  - **Establishes tone for risk appetite and risk management**
- **Information Steering Committee**
- **Chief Information Security Officer (CISO)**
- **Audit**
- **Chief Information Officer (CIO)**
- **Management**
- **All employees**

Information Steering Committee

- **Establishes operational strategy**
  - **For security and risk management**
  - **Sets strategic and operational roles and responsibilities**
  - **Security strategy should align with strategy for IT and the business overall**

Chief Information Security Officer (CISO)

- **Responsible for**
  - **Developing security policy**
  - **Conducting risk assessments**
  - **Developing processes for**
    - **Vulnerability management**
    - **Incident management**
    - **Identity and access management**
    - **Security awareness and training**
    - **Compliance management**

Audit

- **Responsible for examining selected business processes and information systems**
- **To verify that they are designed and operating properly**

Chief Information Officer (CIO)

- **Responsible for overall management of the IT organization, including**
  - **IT strategy**
  - **Development**
  - **Operations**
  - **Service desk**

Management

- **Every manager should be at least partially responsible for the conduct of their employees**
- **This establishes a chain of accountability**

All Employees

- **Required to comply with**
  - **Security policy**
  - **Security requirements and processes**
  - **All other policies**
- **Compliance with policy is a condition of employment**

Reasons for Security Governance

- **Organizations are completely dependent on their information systems**
- **Ineffective security governance can lead to negligence, and breaches**

Security Governance Activities and Results

- **Risk management**
- **Process improvement**
- **incident response**
- **Improved compliance**
- **Business continuity and disaster recovery planning**
- **Effectiveness measurement**
- **Resource management**
- **Improved IT governance**

Results of Security Governance

- **Increased trust**
  - **From customers, suppliers, and partners**
- **Improved reputation**

Ch 4a-2