Information Security and Security Architecture: Two Complementary Ambits

The Open Group

3rd Security Practitioners Conference

July 22 – 23, 2009

Toronto, Ontario

Murray Rosenthal, CISA
Risk Management & Information Security
I&T Strategic Planning & Architecture
City of Toronto
mrosent@toronto.ca

Problem Statement: Intent vs. Reality

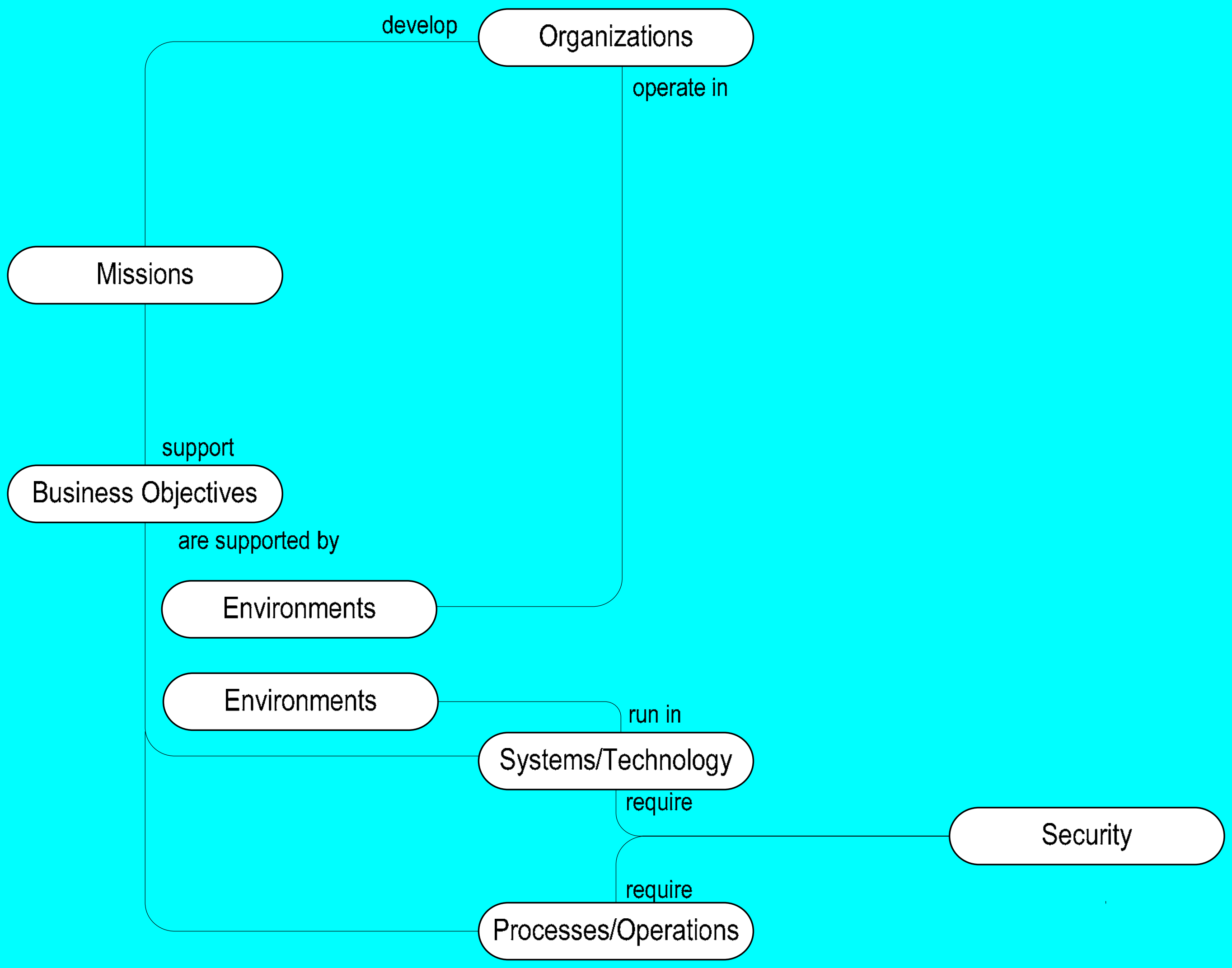
Intent

- Organizations stand up information security and security architecture as essential risk management practices, in line with “due care” standards.
  - Requirement to design, develop and stand up programmatic approaches to information security on an authoritative, sustainable basis.
  - Requirement to design, develop and deploy systems that comply with generally accepted architectural standards.

Reality

- Obfuscation of practice “edges”.
- Obfuscation of organizational spans of control.
- Obfuscation of authority.
- Obfuscation of professional skill sets.
- Information security ≠ security architecture.
- Security architecture ≠ information security.
- Ready-Fire-Aim.
  - Absence of a strategic plan and strategic planning for information security and security architecture.
- Organizational marginalization of information security and security architecture.

Information Security Metamodel



Organizations

develop

operate in

Missions

support

Business Objectives

are supported by

Environments

Environments

run in

Systems/Technology

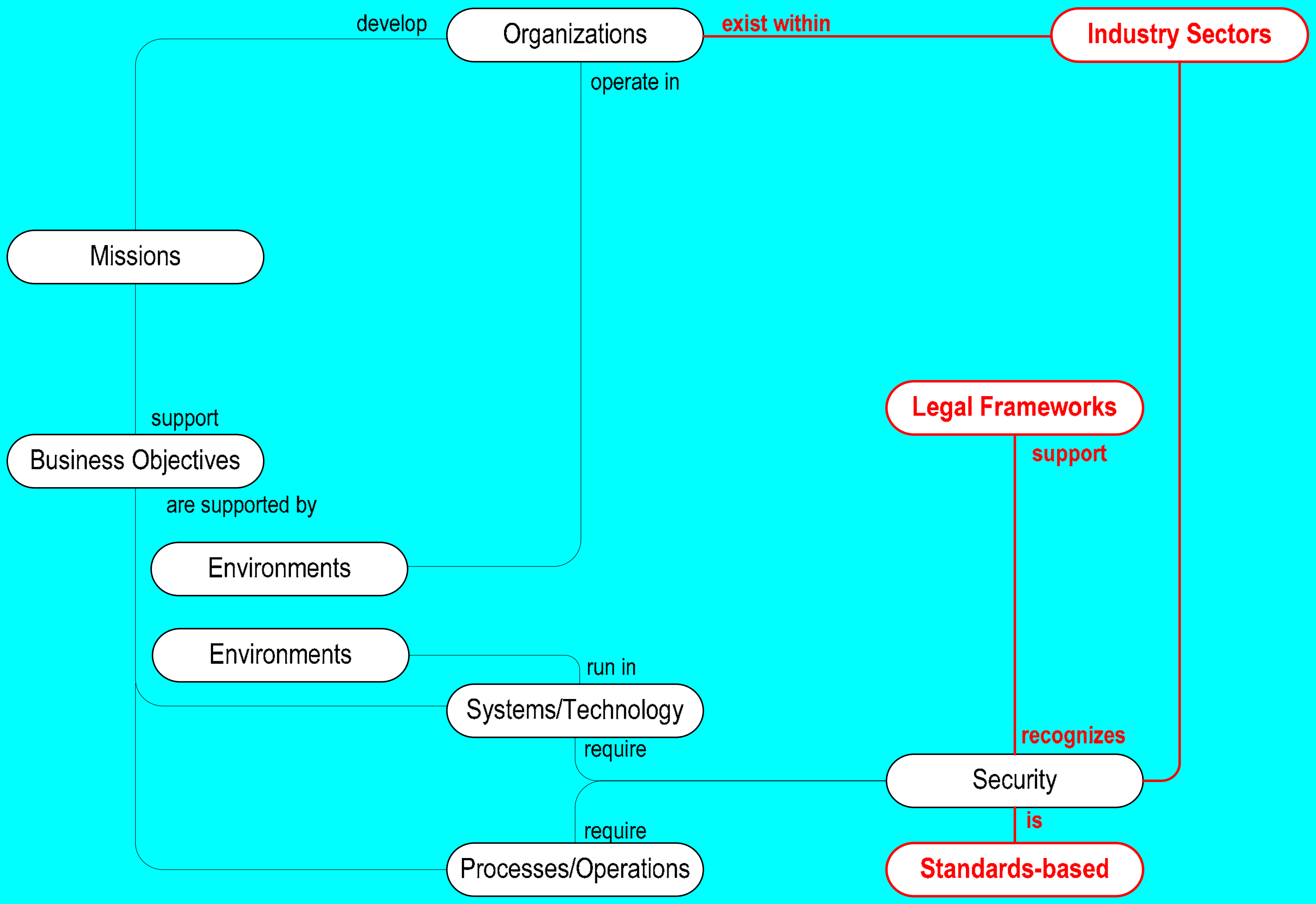
require

Security

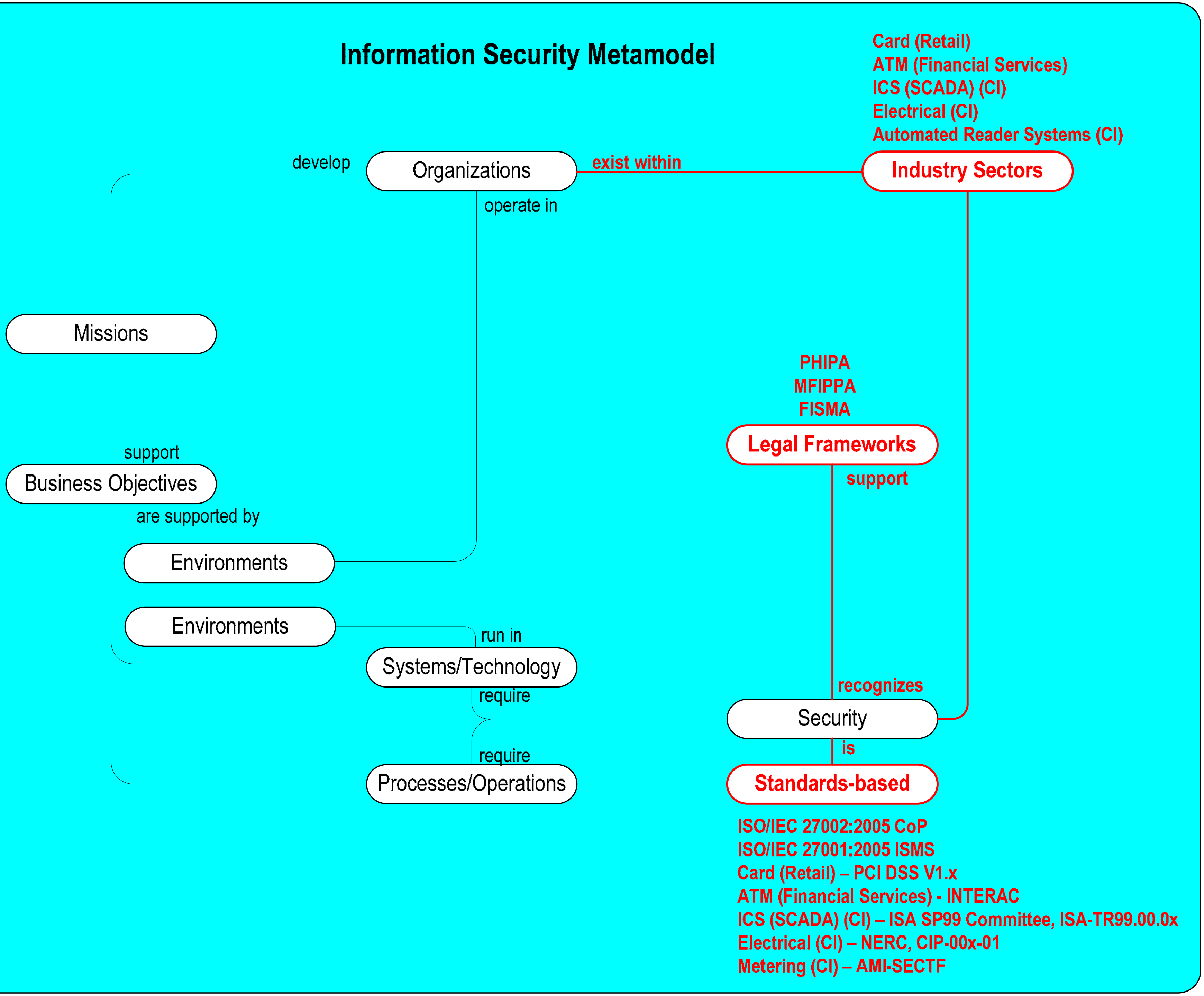
require

Processes/Operations

Information Security Metamodel



Information Security Metamodel



Organizations develop Missions

Missions support Business Objectives

Business Objectives are supported by Environments

Organizations operate in Environments

Systems/Technology run in Environments

Systems/Technology require Security

Processes/Operations require Security

Organizations exist within Industry Sectors

Card (Retail)
ATM (Financial Services)
ICS (SCADA) (CI)
Electrical (CI)
Automated Reader Systems (CI)

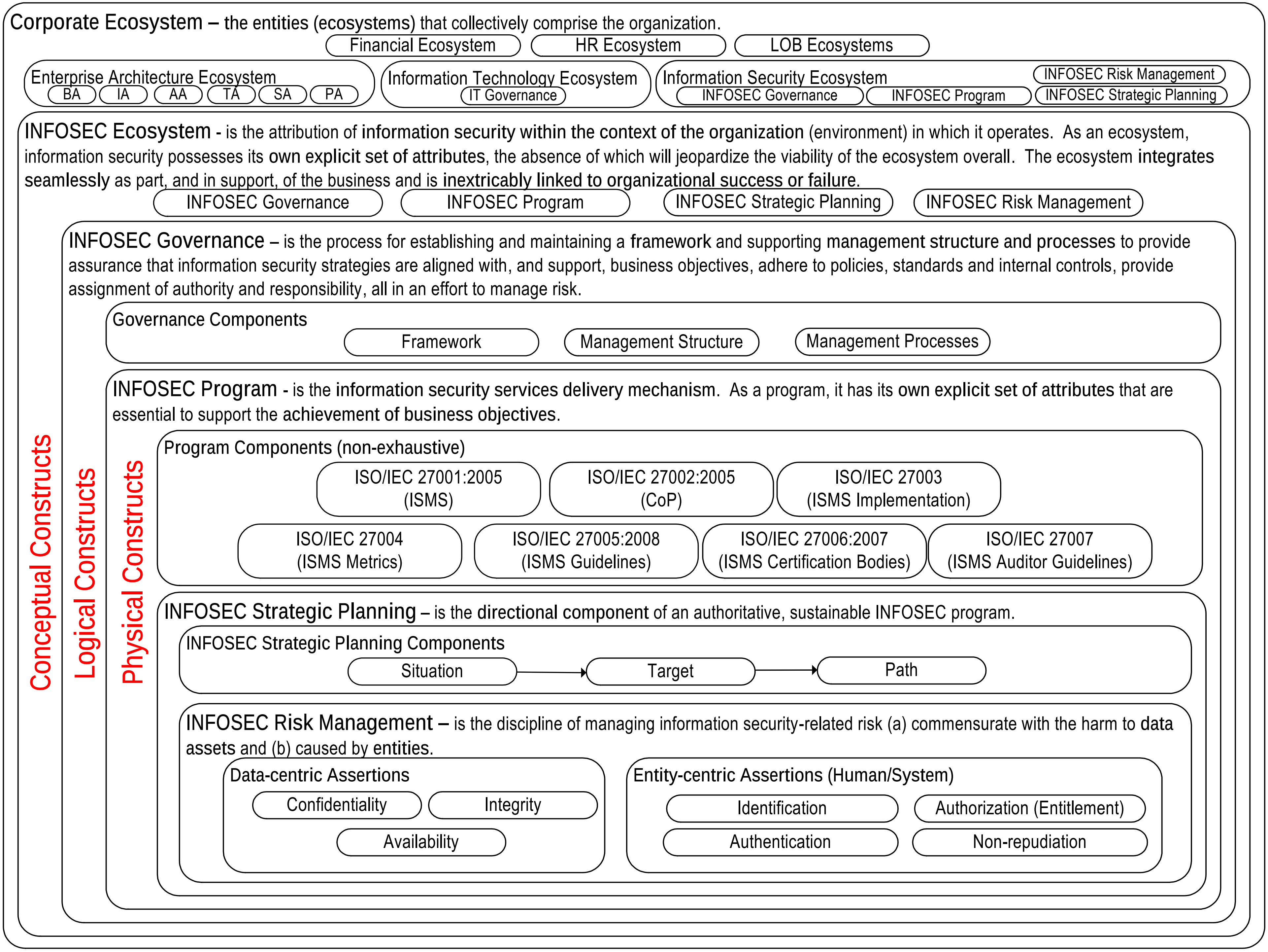
PHIPA
MFIPPA
FISMA

Legal Frameworks support

Security recognizes

Security is Standards-based

ISO/IEC 27002:2005 CoP
ISO/IEC 27001:2005 ISMS
Card (Retail) – PCI DSS V1.x
ATM (Financial Services) - INTERAC
ICS (SCADA) (CI) – ISA SP99 Committee, ISA-TR99.00.0x
Electrical (CI) – NERC, CIP-00x-01
Metering (CI) – AMI-SECTF



Corporate Ecosystem – the entities (ecosystems) that collectively comprise the organization.

Financial Ecosystem | HR Ecosystem | LOB Ecosystems

Enterprise Architecture Ecosystem: BA | IA | AA | TA | SA | PA

Information Technology Ecosystem: IT Governance

Information Security Ecosystem: INFOSEC Governance | INFOSEC Program | INFOSEC Risk Management | INFOSEC Strategic Planning

INFOSEC Ecosystem - is the attribution of information security within the context of the organization (environment) in which it operates. As an ecosystem, information security possesses its own explicit set of attributes, the absence of which will jeopardize the viability of the ecosystem overall. The ecosystem integrates seamlessly as part, and in support, of the business and is inextricably linked to organizational success or failure.

INFOSEC Governance | INFOSEC Program | INFOSEC Strategic Planning | INFOSEC Risk Management

INFOSEC Governance – is the process for establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with, and support, business objectives, adhere to policies, standards and internal controls, provide assignment of authority and responsibility, all in an effort to manage risk.

Governance Components: Framework | Management Structure | Management Processes

INFOSEC Program - is the information security services delivery mechanism. As a program, it has its own explicit set of attributes that are essential to support the achievement of business objectives.

Program Components (non-exhaustive)

- ISO/IEC 27001:2005 (ISMS)
- ISO/IEC 27002:2005 (CoP)
- ISO/IEC 27003 (ISMS Implementation)
- ISO/IEC 27004 (ISMS Metrics)
- ISO/IEC 27005:2008 (ISMS Guidelines)
- ISO/IEC 27006:2007 (ISMS Certification Bodies)
- ISO/IEC 27007 (ISMS Auditor Guidelines)

INFOSEC Strategic Planning – is the directional component of an authoritative, sustainable INFOSEC program.

INFOSEC Strategic Planning Components: Situation → Target → Path

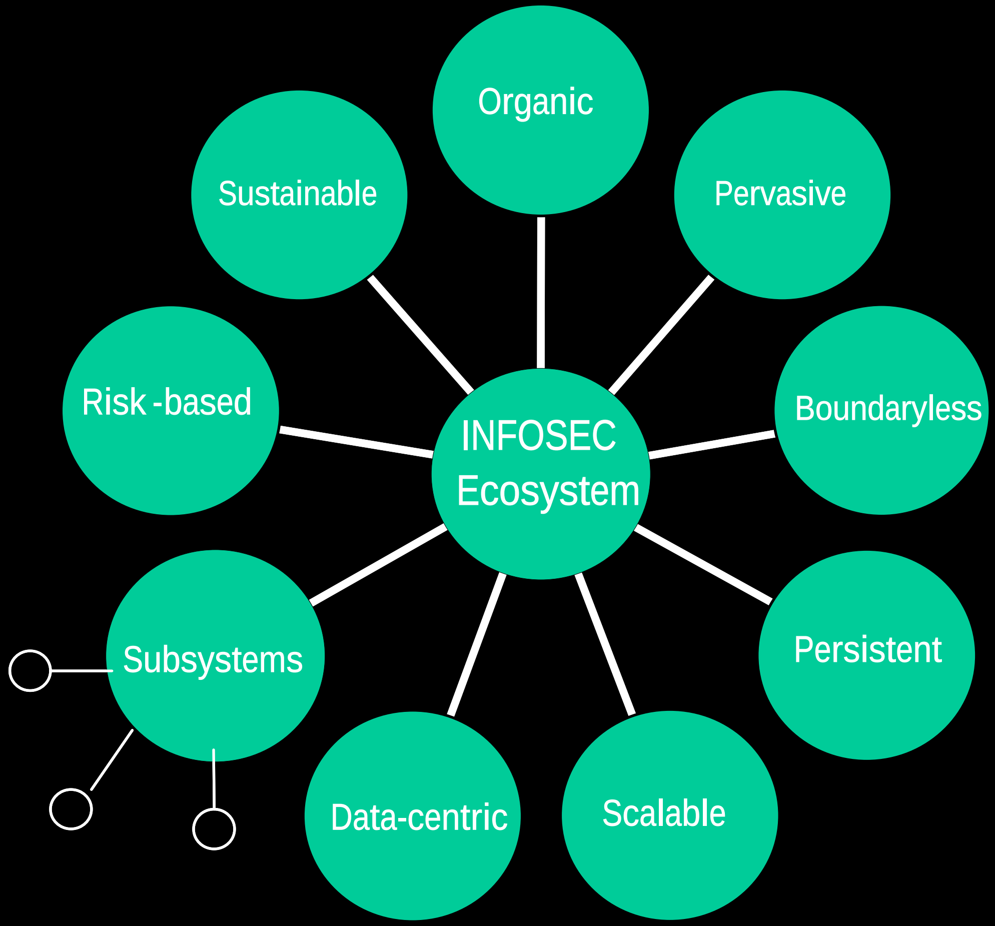
INFOSEC Risk Management – is the discipline of managing information security-related risk (a) commensurate with the harm to data assets and (b) caused by entities.

Data-centric Assertions: Confidentiality | Integrity | Availability

Entity-centric Assertions (Human/System): Identification | Authorization (Entitlement) | Authentication | Non-repudiation

Information Security Ecosystem

Information Security Ecosystem Attribution



Generally Accepted INFOSEC Assertions

Data-centric

- Confidentiality
- Integrity
- Availability

Entity-centric (human/system)

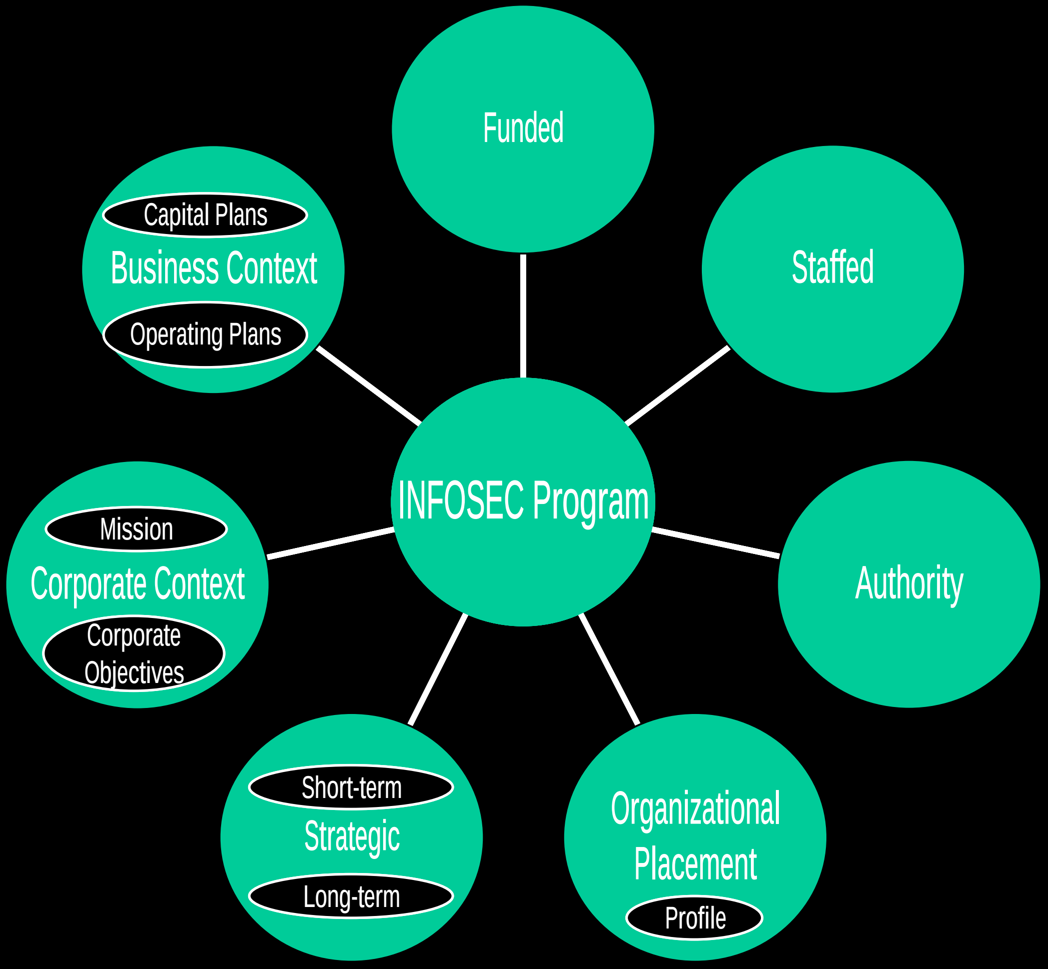
- Identification
- Authentication
- Authorization
- Non-repudiation

Risk Mitigation Approaches

Deterrence Avoidance Acceptance Transfer Recovery Restoration

Information Security Program

Information Security Program Attribution



INFOSEC Program

Funded

Staffed

Authority

Organizational Placement

Profile

Strategic

Short-term

Long-term

Corporate Context

Mission

Corporate Objectives

Business Context

Capital Plans

Operating Plans

Generally Accepted INFOSEC Assertions

Data-centric

- Confidentiality
- Integrity
- Availability

Entity-centric (human/system)

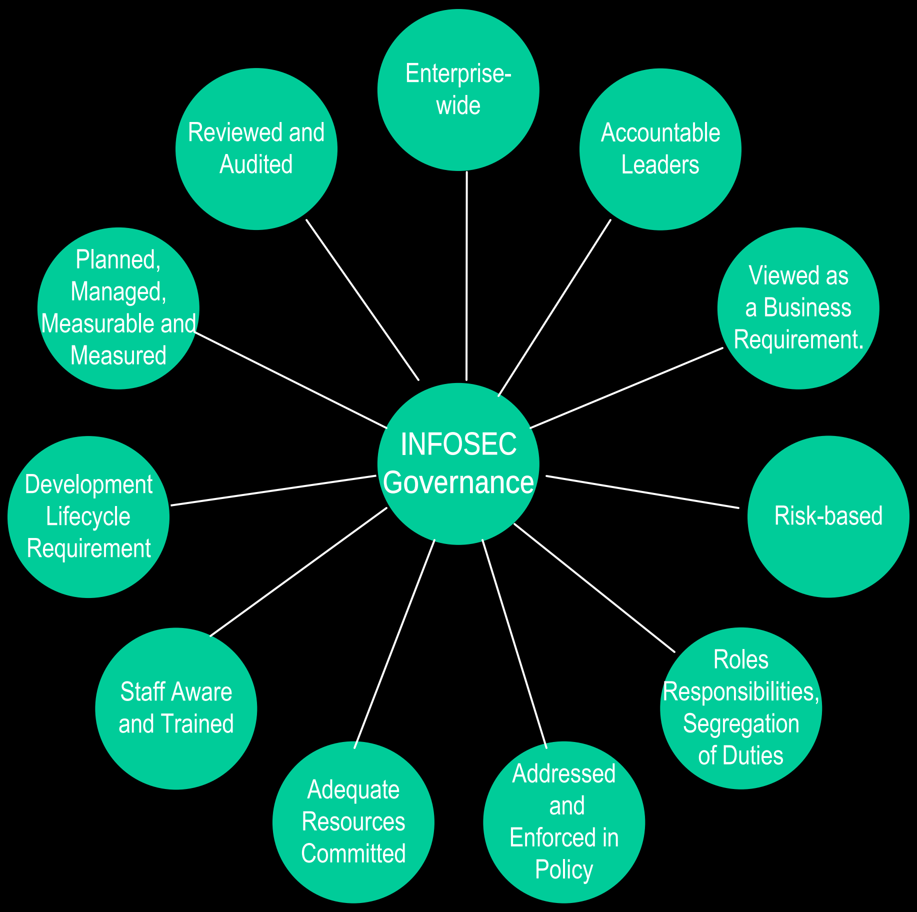
- Identification
- Authentication
- Authorization
- Non-repudiation

Risk Mitigation Approaches

- Deterrence
- Avoidance
- Acceptance
- Transfer
- Recovery
- Restoration

Information Security Governance

Information Security Governance Attribution



INFOSEC Governance

Enterprise-wide

Accountable Leaders

Viewed as a Business Requirement.

Risk-based

Roles Responsibilities, Segregation of Duties

Addressed and Enforced in Policy

Adequate Resources Committed

Staff Aware and Trained

Development Lifecycle Requirement

Planned, Managed, Measurable and Measured

Reviewed and Audited

Generally Accepted INFOSEC Assertions

Data-centric

- Confidentiality
- Integrity
- Availability

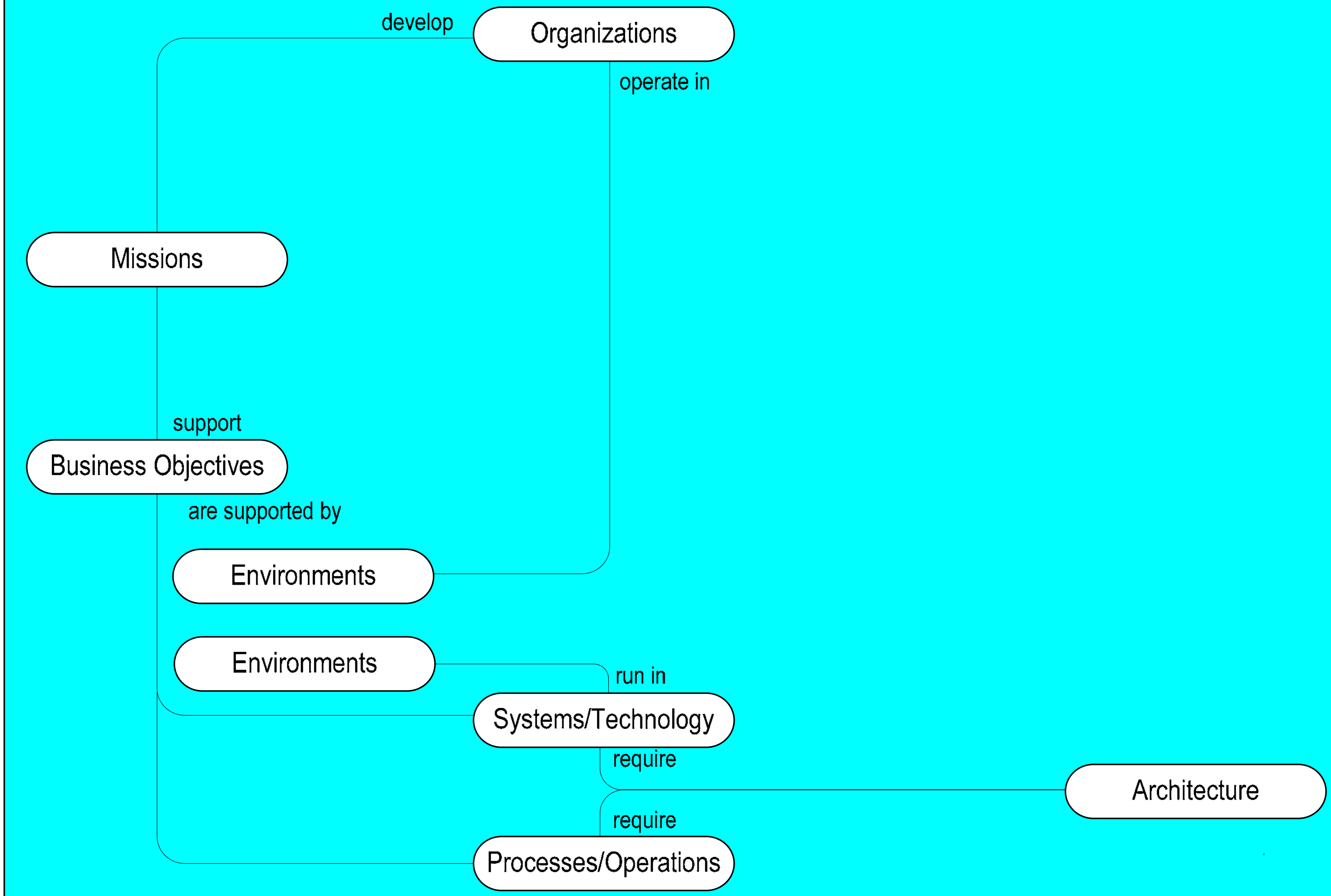
Entity-centric (human/system)

- Identification
- Authentication
- Authorization
- Non-repudiation

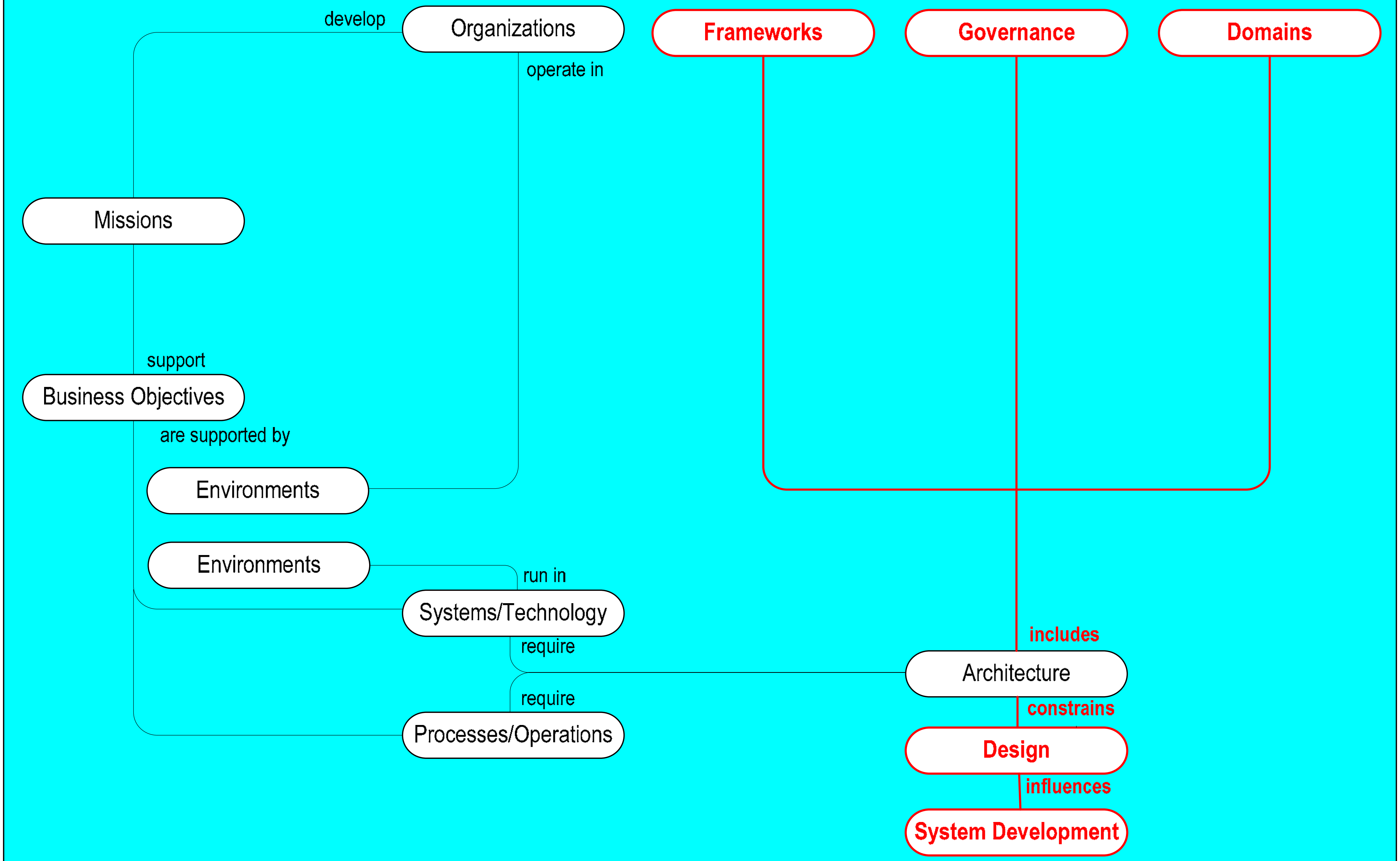
Risk Mitigation Approaches

Deterrence | Avoidance | Acceptance | Transfer | Recovery | Restoration

Architecture Metamodel

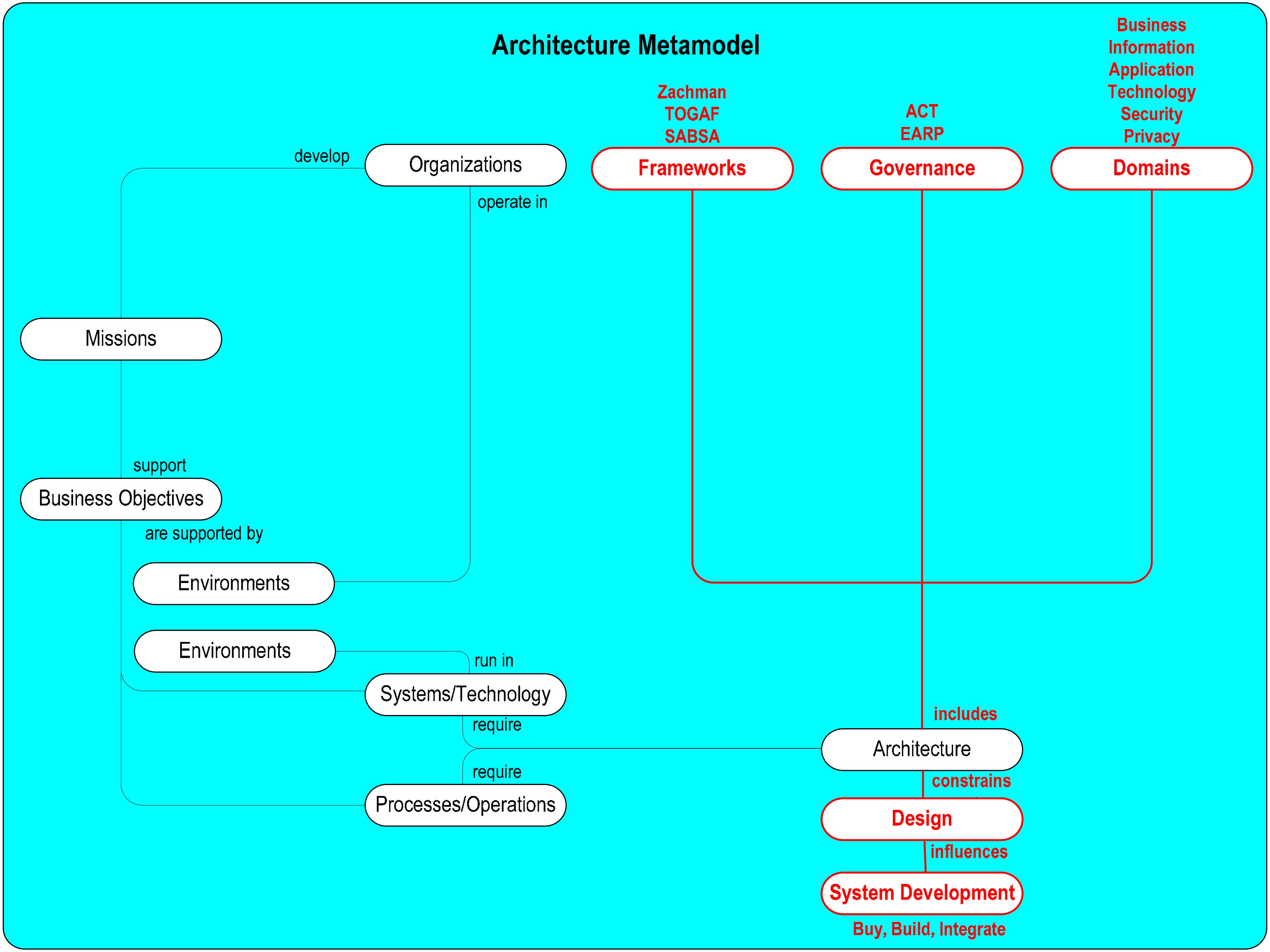


Architecture Metamodel



Organizations
develop
Missions
support
Business Objectives
are supported by
operate in
Environments
Environments
run in
Systems/Technology
require
require
Processes/Operations
Frameworks
Governance
Domains
includes
Architecture
constrains
Design
influences
System Development

Architecture Metamodel



Business
Information
Application
Technology
Security
Privacy

Zachman
TOGAF
SABSA

ACT
EARP

develop

Organizations

Frameworks

Governance

Domains

operate in

Missions

support

Business Objectives

are supported by

Environments

Environments

run in

Systems/Technology

require

includes

Architecture

require

constrains

Processes/Operations

Design

influences

System Development

Buy, Build, Integrate

Taxonomy of Architecture Attribution

Domain Architecture	Solutions Architecture
□ strategic orientation	□ delivery/operational orientation □ enterprise architecture *applied*
□ precursor (pre-dates)	□ dependent, extension, outgrowth (ante-dates)
□ framework-based	□ framework-agnostic
□ raw-state artefacts	□ contextualized artefacts
□ artefact commoditization	□ artefact componentization
□ loose artefact assembly	□ tight artefact integration
□ vertical artefact arrangements	□ horizontal, converged artefact arrangements
□ fixed domain boundaries	□ fuzzy edges
□ authoritative compilation of enterprise models	□ authoritative compilation of enterprise models *constrained by project* □ state models o conceptual o logical o physical
□ fine-grain abstraction o enterprise normalization o enterprise ambit	□ finer-grain abstraction o project normalization o project ambit
□ authoritative artefact set	□ authoritative, derivative subset

If You Don’t Have Security Architecture…

Program Level	Project Level
Trial-and-Error Security artefacts are created informally, or not at all, and are not authoritative.	Trial-and-Error Application of security artefacts is ad hoc, or not at all.
Reverse-engineer the enterprise’s “as is” models from the existing enterprise Takes time and costs money.	Reverse-engineer the project’s “as is” models Takes time and costs money.
Let the enterprise go out of business Security architecture becomes a poster child as the business tailspins out of control.	Let the project lapse and not go forward Lack of artefacts = lack of security design credibility.

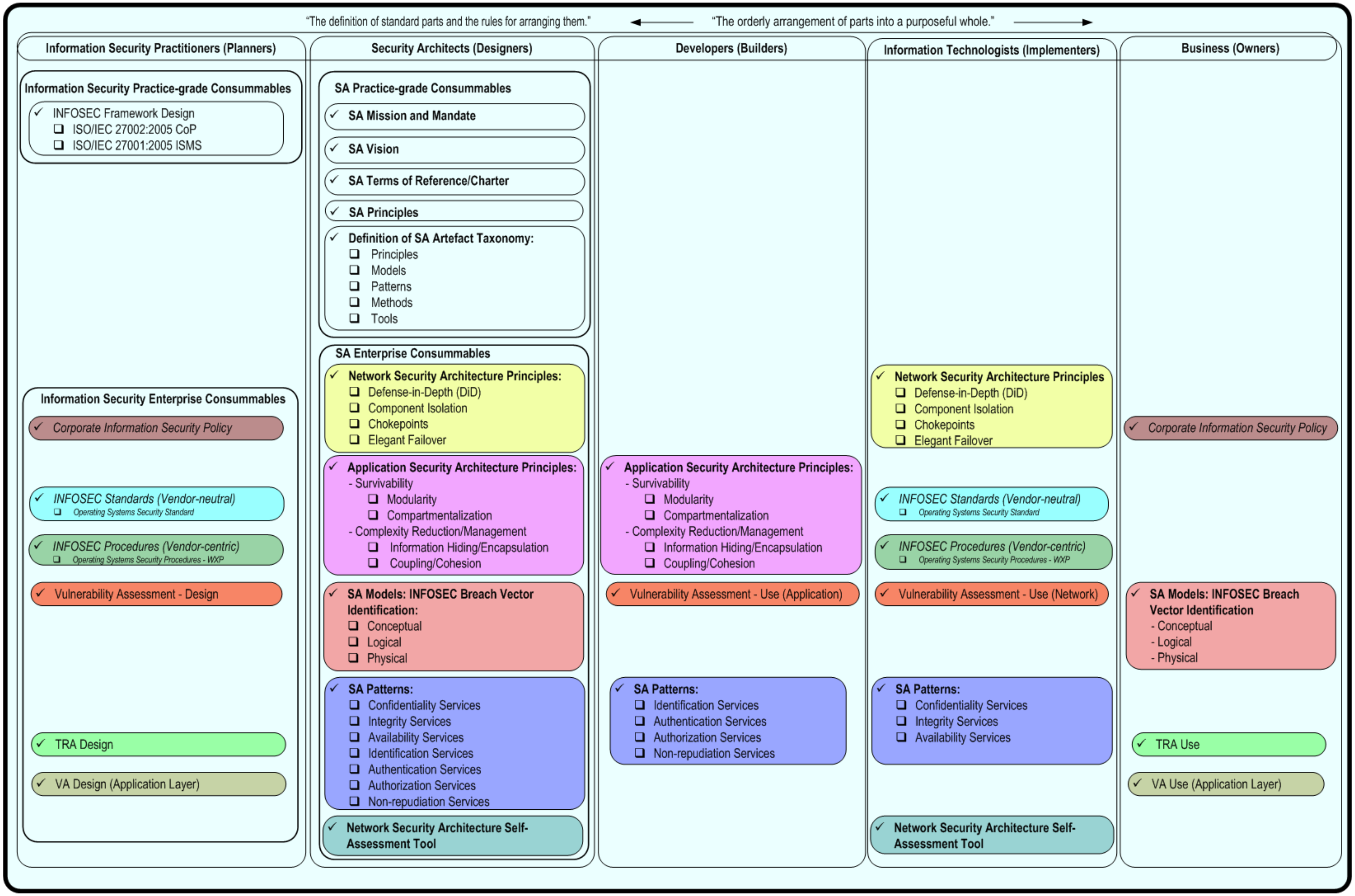
SABSA Framework

	Assets	Motivation	Process	People	Location	Time
	(What)	(Why)	(How)	(Who)	(Where)	(When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices & Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Action and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

Disentangling Two Complementary Ambits

Information Security	Security Architecture
The establishment of an authoritative, sustainable approach to information security on a programmatic basis.	The definition of standard parts and the rules for arranging them.
“Program Design”	“System Design”
□ Corporate Information Security Policy	□ SA Design Principles
□ Information Security Standards for IT Components (Assertions)	□ SA Design Patterns o Confidentiality Services o Integrity Services o Availability Services o Authentication Services o Authorization Services o Non-repudiation Services o Identification Services
□ Information Security Procedures for IT Components	□ SA State Models: INFOSEC Vector Identification o Conceptual o Logical o Physical
□ Threat Risk Assessment Design	□ Inventory of Authoritative INFOSEC Technologies
□ Vulnerability Assessment Design	
□ Consultative Services for Projects o INFOSEC Risk Identification and Remediation	
□ INFOSEC Framework Design o ISO/IEC 27002:2005 CoP Adoption o ISO/IEC 27001:2005 ISMS Certification	
□ INFOSEC Strategic Planning	

Conceptual Reference Model



"The definition of standard parts and the rules for arranging them." ← "The orderly arrangement of parts into a purposeful whole." →

Information Security Practitioners (Planners)

Information Security Practice-grade Consummables

- ✓ INFOSEC Framework Design
  - ❑ ISO/IEC 27002:2005 CoP
  - ❑ ISO/IEC 27001:2005 ISMS

Information Security Enterprise Consummables

- ✓ *Corporate Information Security Policy*
- ✓ *INFOSEC Standards (Vendor-neutral)*
  - ❑ *Operating Systems Security Standard*
- ✓ *INFOSEC Procedures (Vendor-centric)*
  - ❑ *Operating Systems Security Procedures - WXP*
- ✓ Vulnerability Assessment - Design
- ✓ TRA Design
- ✓ VA Design (Application Layer)

Security Architects (Designers)

SA Practice-grade Consummables

- ✓ **SA Mission and Mandate**
- ✓ **SA Vision**
- ✓ **SA Terms of Reference/Charter**
- ✓ **SA Principles**
- ✓ **Definition of SA Artefact Taxonomy:**
  - ❑ Principles
  - ❑ Models
  - ❑ Patterns
  - ❑ Methods
  - ❑ Tools

SA Enterprise Consummables

- ✓ **Network Security Architecture Principles:**
  - ❑ Defense-in-Depth (DiD)
  - ❑ Component Isolation
  - ❑ Chokepoints
  - ❑ Elegant Failover
- ✓ **Application Security Architecture Principles:**
  - - Survivability
    - ❑ Modularity
    - ❑ Compartmentalization
  - - Complexity Reduction/Management
    - ❑ Information Hiding/Encapsulation
    - ❑ Coupling/Cohesion
- ✓ **SA Models: INFOSEC Breach Vector Identification:**
  - ❑ Conceptual
  - ❑ Logical
  - ❑ Physical
- ✓ **SA Patterns:**
  - ❑ Confidentiality Services
  - ❑ Integrity Services
  - ❑ Availability Services
  - ❑ Identification Services
  - ❑ Authentication Services
  - ❑ Authorization Services
  - ❑ Non-repudiation Services
- ✓ **Network Security Architecture Self-Assessment Tool**

Developers (Builders)

- ✓ **Application Security Architecture Principles:**
  - - Survivability
    - ❑ Modularity
    - ❑ Compartmentalization
  - - Complexity Reduction/Management
    - ❑ Information Hiding/Encapsulation
    - ❑ Coupling/Cohesion
- ✓ Vulnerability Assessment - Use (Application)
- ✓ **SA Patterns:**
  - ❑ Identification Services
  - ❑ Authentication Services
  - ❑ Authorization Services
  - ❑ Non-repudiation Services

Information Technologists (Implementers)

- ✓ **Network Security Architecture Principles**
  - ❑ Defense-in-Depth (DiD)
  - ❑ Component Isolation
  - ❑ Chokepoints
  - ❑ Elegant Failover
- ✓ *INFOSEC Standards (Vendor-neutral)*
  - ❑ *Operating Systems Security Standard*
- ✓ *INFOSEC Procedures (Vendor-centric)*
  - ❑ *Operating Systems Security Procedures - WXP*
- ✓ Vulnerability Assessment - Use (Network)
- ✓ **SA Patterns:**
  - ❑ Confidentiality Services
  - ❑ Integrity Services
  - ❑ Availability Services
- ✓ **Network Security Architecture Self-Assessment Tool**

Business (Owners)

- ✓ *Corporate Information Security Policy*
- ✓ **SA Models: INFOSEC Breach Vector Identification**
  - - Conceptual
  - - Logical
  - - Physical
- ✓ TRA Use
- ✓ VA Use (Application Layer)

Harvestable Nuggets

❶Develop strategic plans and implementation schedules for information security and security architecture, respectively.

❷Disentangle spans of control and authorities.

❸Institute practice “edge” management and relevant anti-collision protocols.

❹Recruit based on differentiated skill sets and individuated practice requirements.

Information Security and Security Architecture: Two Complementary Ambits

The Open Group
3rd Security Practitioners Conference

July 22 – 23, 2009
Toronto, Ontario

Murray Rosenthal, CISA
Risk Management & Information Security
I&T Strategic Planning & Architecture
City of Toronto
mrosent@toronto.ca