Security Methodology

Secure Solution Design

William (Bill) Blake, CISSP

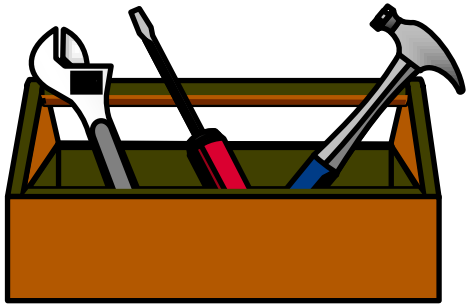
ISSA Senior Member

Creating a Security Solution can be described as:

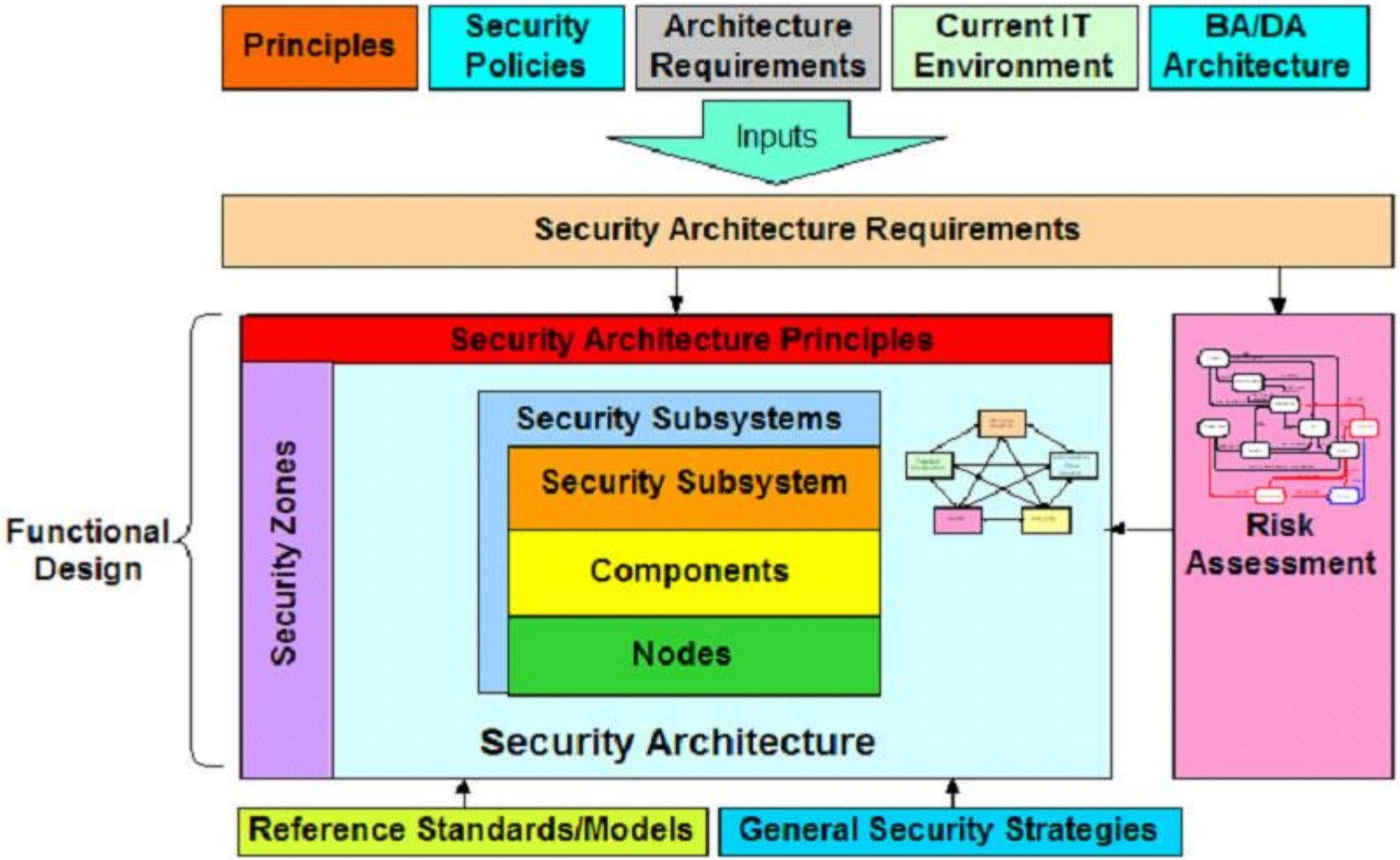
- Given the requirements expressed as:
  - a description of the Solution Environment
  - a set of business requirements
  - a set of security assumptions for the IT environment
  - countermeasures to mitigate the risks
- Document
  - a set of security architecture principles for the Solution
- Design and deploy
  - a set of Security subsystems, components placed on nodes in the operational environment, which is sectioned into security zones

The Secure Solution Design Toolbox

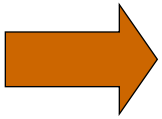
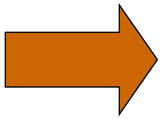
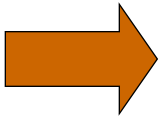
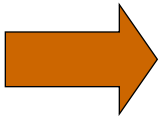
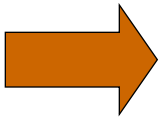
- Common Criteria
- ISO 27001: Information technology — Security techniques — Information security management systems — Requirements
- ISO 27002: Information technology — Security techniques — Code of practice for information security controls
- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
- ITIL V3



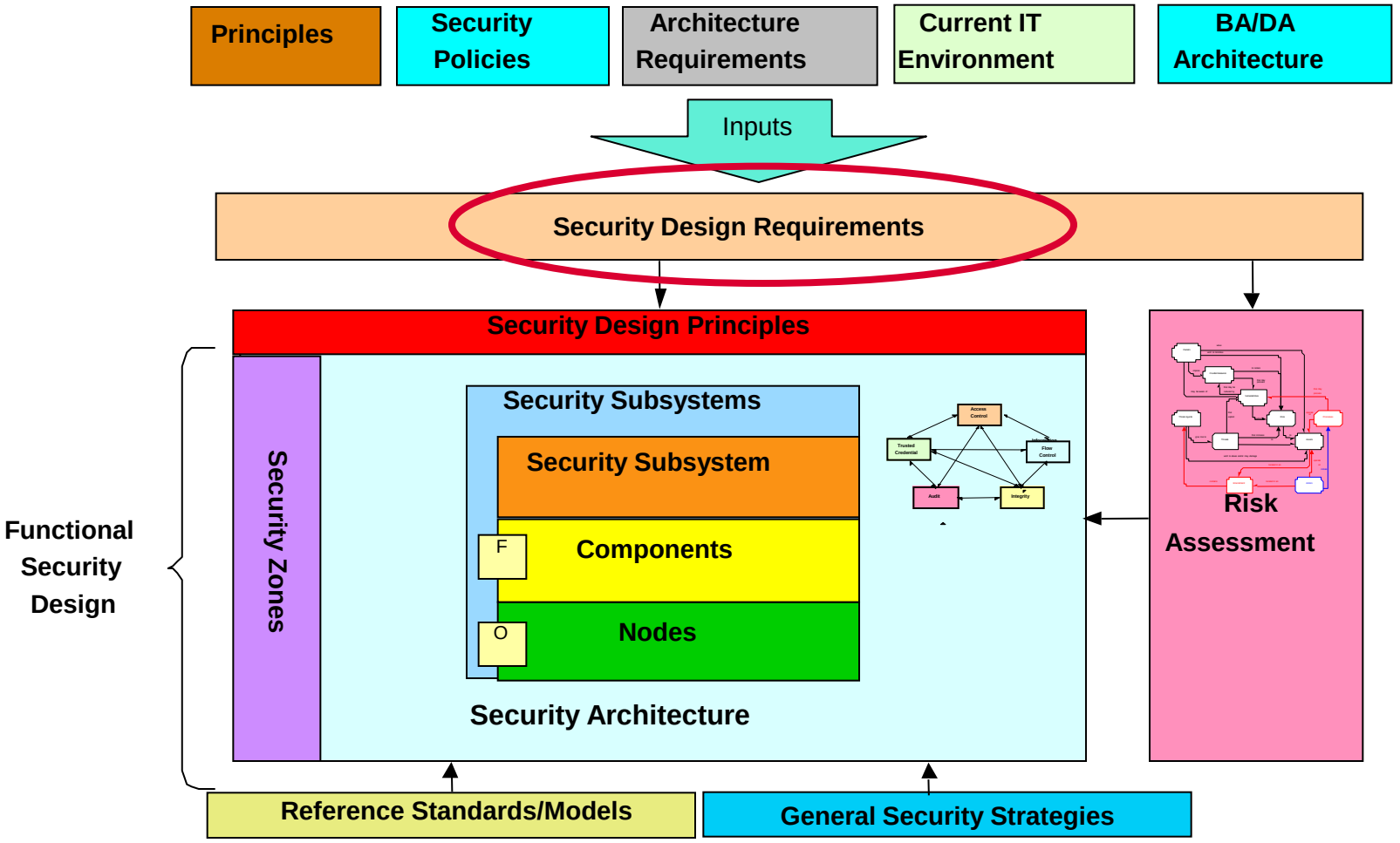
- Secure solution design helps us design and implement business solutions in the context of the client's overall Security Strategy and Enterprise Security Program



How does this help a solution type engagement?

Components		Benefits
Common Criteria - Functions, Assurance, Protection Profiles		Requirements are comprehensive, because they are based on a known standard
Security Architecture Principles		Raises the quality of the result and saves you time
Security Zones		Provides clear, efficient way of organizing the security architecture
Security Sub-systems		Breaks down a large problem into manageable parts
Risk Assessment		This approach provides a logical flow from the threats to the countermeasures which should be designed into the Architecture

Security Design Requirements



Security Requirements Steps

Understand Environment

- Business context
- Current IT Environment
- Policies

Actors and Processes

- Users and environment
- Initiate processes
- Create transaction flows

Assets and Owners

- Assets and owners
- Classify
- User access policy

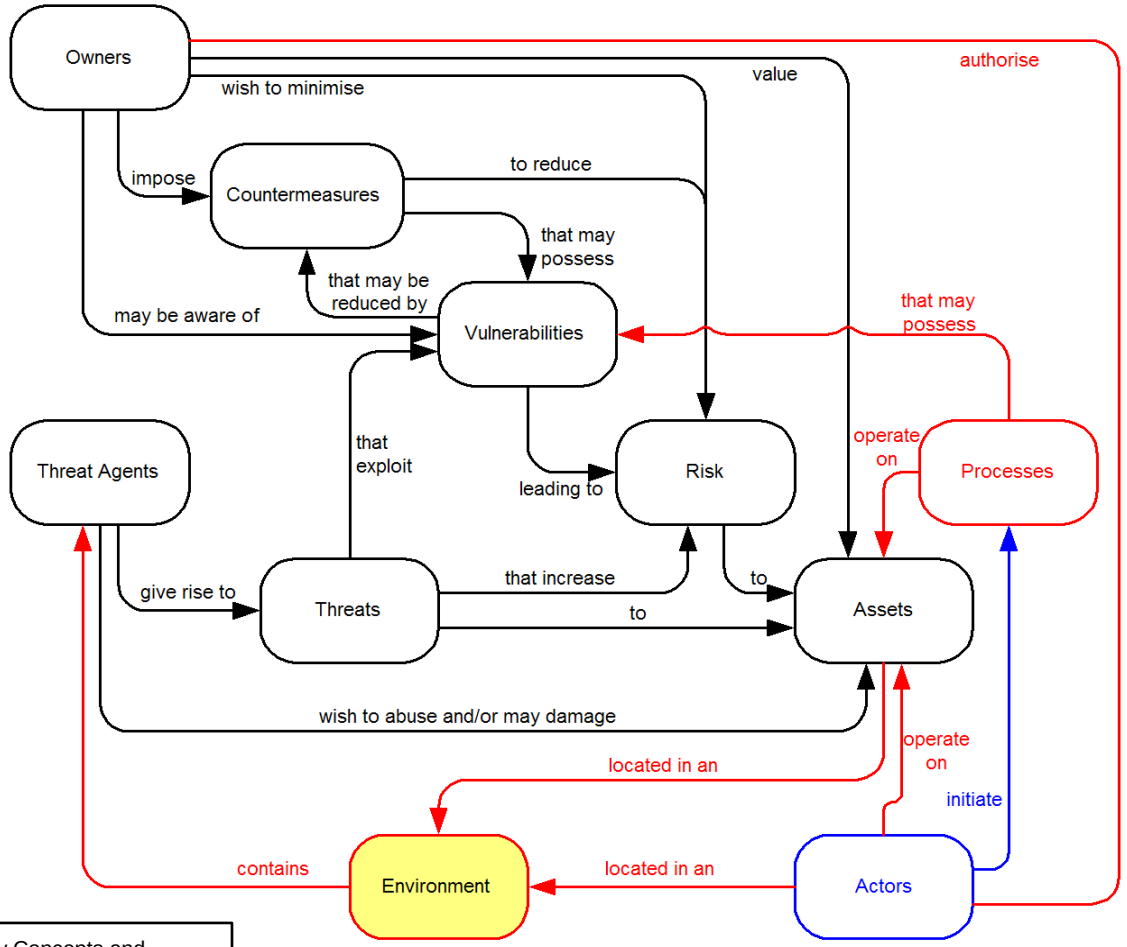
Security Zones

- Zones in current IT or ‘as-is’ environment

Risk Assessment

- Identify business risks, with threats and vulnerabilities

- The Common Criteria provides a comprehensive risk management model which we have extended to link this technology-based standard to a client's business



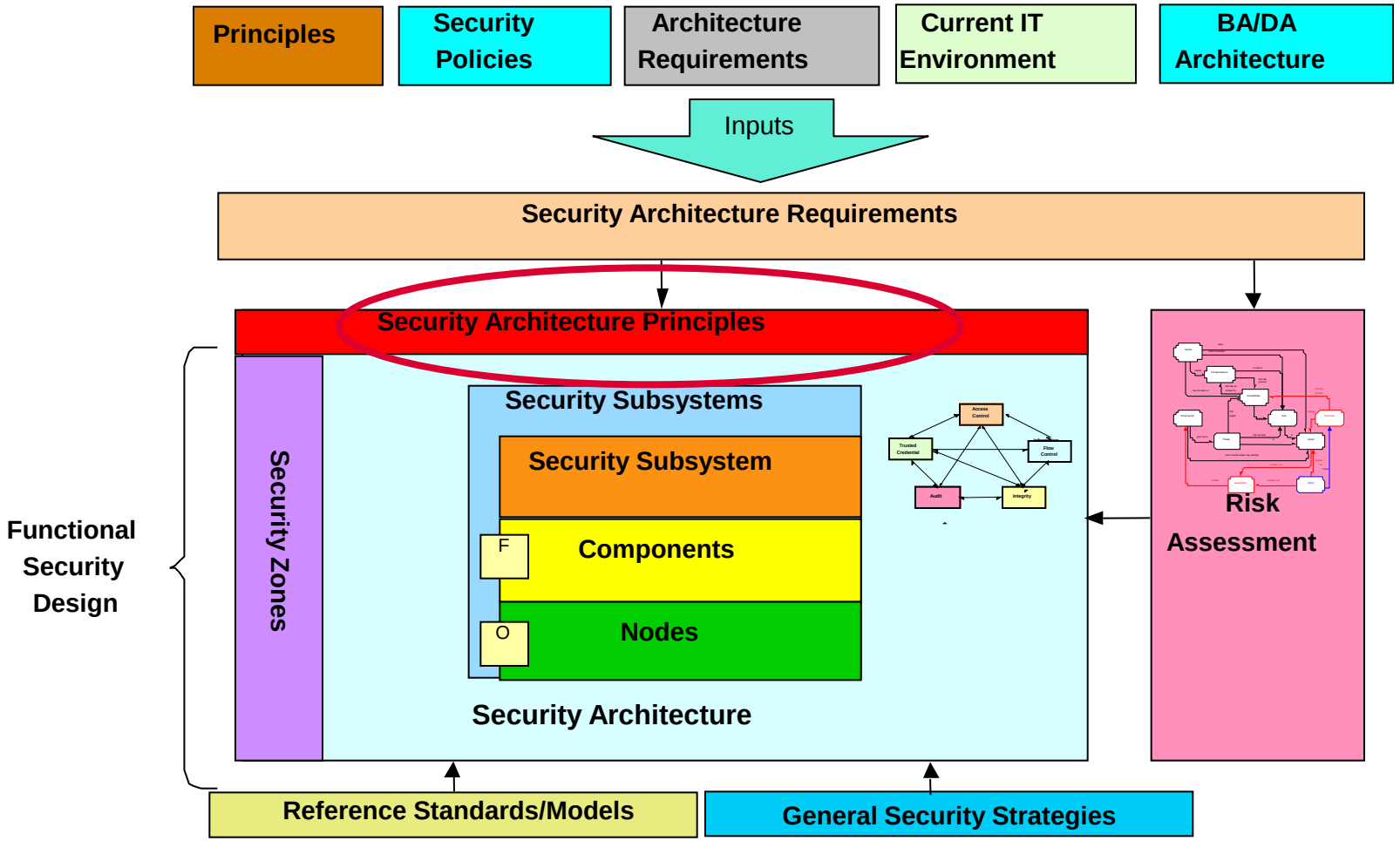
Line Colour Key

From CC V2.1 Part 1 Fig 4.1 Security Concepts and Relationships

Architecture Description Standard meta-model

Architecting Secure Solutions additions

Security Design Objectives: Principles



Security Architecture Principles enable consistent Architectural Decisions

Principles

The Security Architecture Principles work product documents security principles that can be used to make management and technology decisions consistent with an organization's security policies and standards.

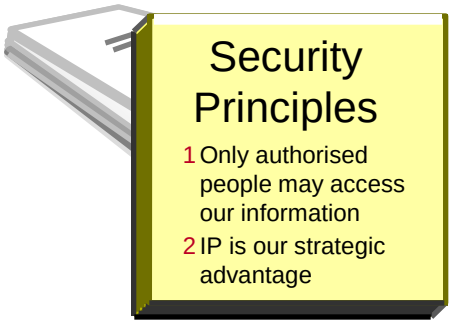
Links the Business Strategy and Requirements to Architecture Design Decisions

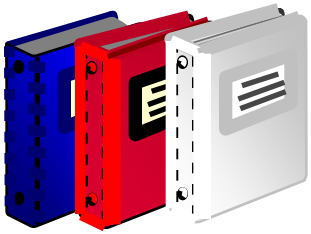
Architectural Decisions

An Architectural Decisions work product documents important decisions about any aspect of the architecture including the structure of the system, the provision and allocation of function, the contextual fitness of the system and adherence to standards

- The final security solution design must support the Enterprise Level Security Requirements as well as any specific security capability requirements or objectives

Enterprise Requirements

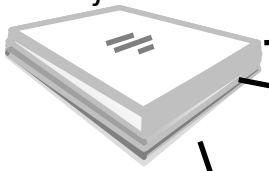




- Information Asset Profile
- Trust Model
- Security Policy
- Standards

The 'Rules'

Specific Capability Project



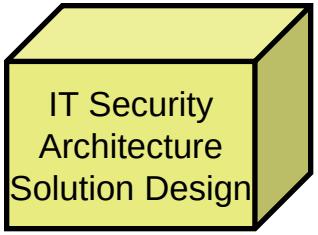
Requirements / Objectives

Process & Procedures

Organization, People and skills

Technology Solution Design

Architectural Decisions



To distill the requirements, the principles need to be gathered in two broad categories – Guiding Principles and Design Principles

Categories of Principles

- Information Security Guiding Principles are umbrella guidelines that form the terms of reference in determining what to do in relation to the security of corporate information
- Information Security Design Principles are specific Technical guidelines that form terms of reference for the Architecture. They must comply with the Guiding Principles.
  - A spectrum of security design principles can be defined
    - enterprise wide
    - part of a specific architecture component
    - part of a specific system
    - related to a specific security issue

General Guiding Principles

- Least Privilege
- Defense in Depth
- Choke Point
- Weakest Link
- Fail-Safe Stance
- Universal Participation
- Diversity of Defense
- Simplicity
- Compartmentalization
- Protect Against Insider and Outsider Threats

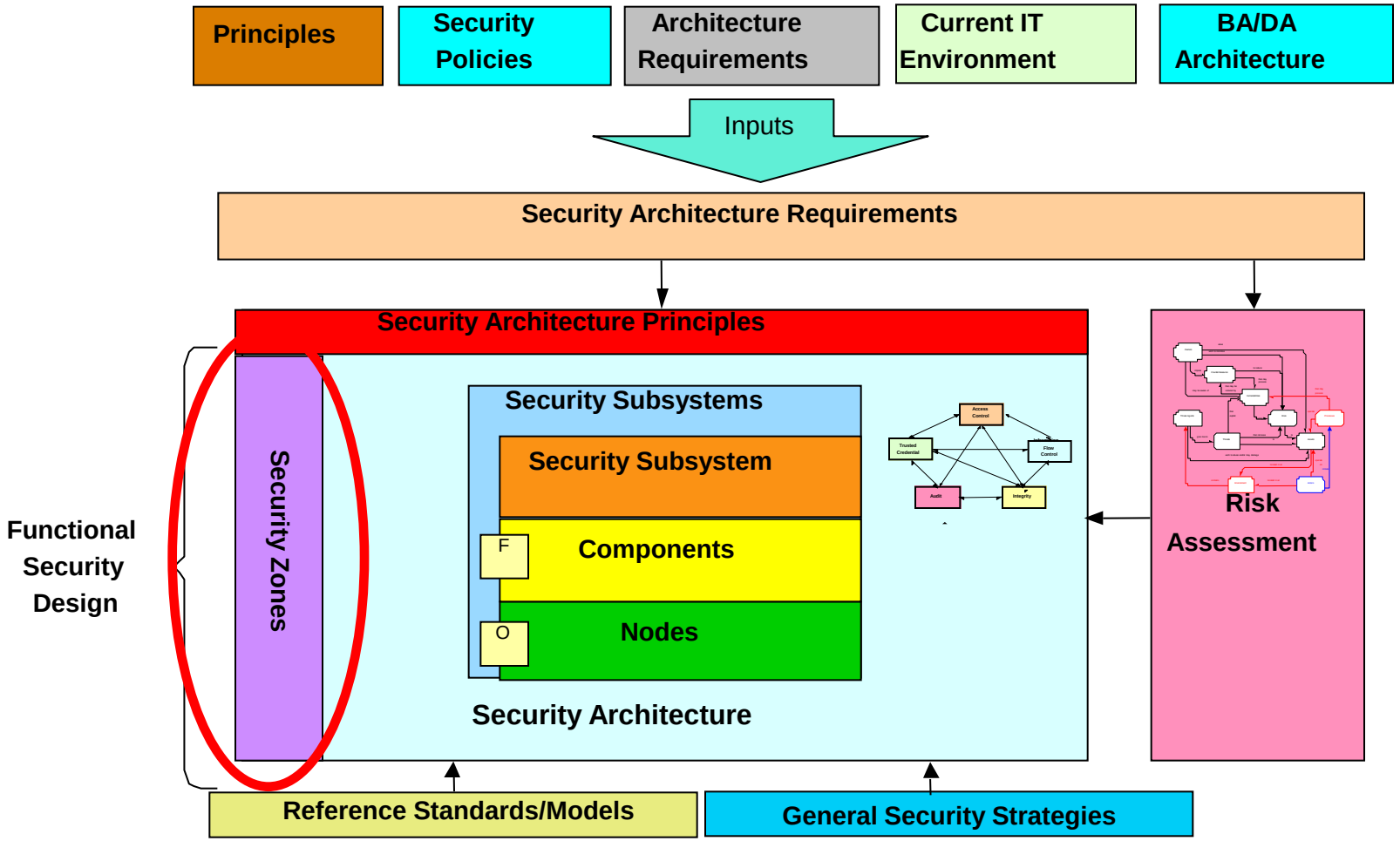
The construction of a Principle should capture the reasoning behind a decision as well as the associated cost or impact

Principle Format

Principle Topic: (1 or 2 words)

- Principle sentence: that defines the principle. The basic intent. The guidance that helps you make decisions
- Motivation: Sentences that explain why make this decision. It forms the business case. It is the benefits statement for the investment. If there is none, then why do it.
- Implication: This is the cost to do what you have decided. It becomes the project list and set of initiatives you need to do. This should link all the areas that need to be addressed to ‘make it happen.’ You need to define what is required for:
  - Technology
  - People
  - Process and Policies
- This gives direction and business justification for the architecture

Security Zones



Defining Security Zones

- Within a security zone you will have the same **security environment** (vulnerabilities, threats, etc)
- Rules on placement of assets into security zones are key architectural decisions, for each security zone will have consistent **security policy.**
- Boundaries of security zones are critically important, needing definition of:
  - interconnection requirements
  - security controls (information flow controls, access controls) at boundaries
- **Questions:** How can we define security zones in structured, re-usable way?
- **Answer:** Use standard categories to describe the security zones

Security Domain - A set of subjects, their information objects, and a common security policy. (NIST SP 800-33)

Security Zones – Basic Definitions

External Sensitive

External Restricted

External Controlled

Uncontrolled
The Uncontrolled environment is anything outside the control of CLIENT. Systems and networks that make up the Internet proper, client systems external to the CLIENT network, home systems that access the CLIENT network, etc.

Controlled
The Controlled / External Controlled are where the lowest levels of control are applied to filter traffic into and out of the networks controlled by CLIENT.

Restricted
The Restricted / External Restricted Zones are the next higher level of security.

It is where access is restricted to authenticated users or processes using stronger authentication mechanisms than found in the Controlled Zone.

It is where most processing will occur and where data that is needed near at hand should be stored.

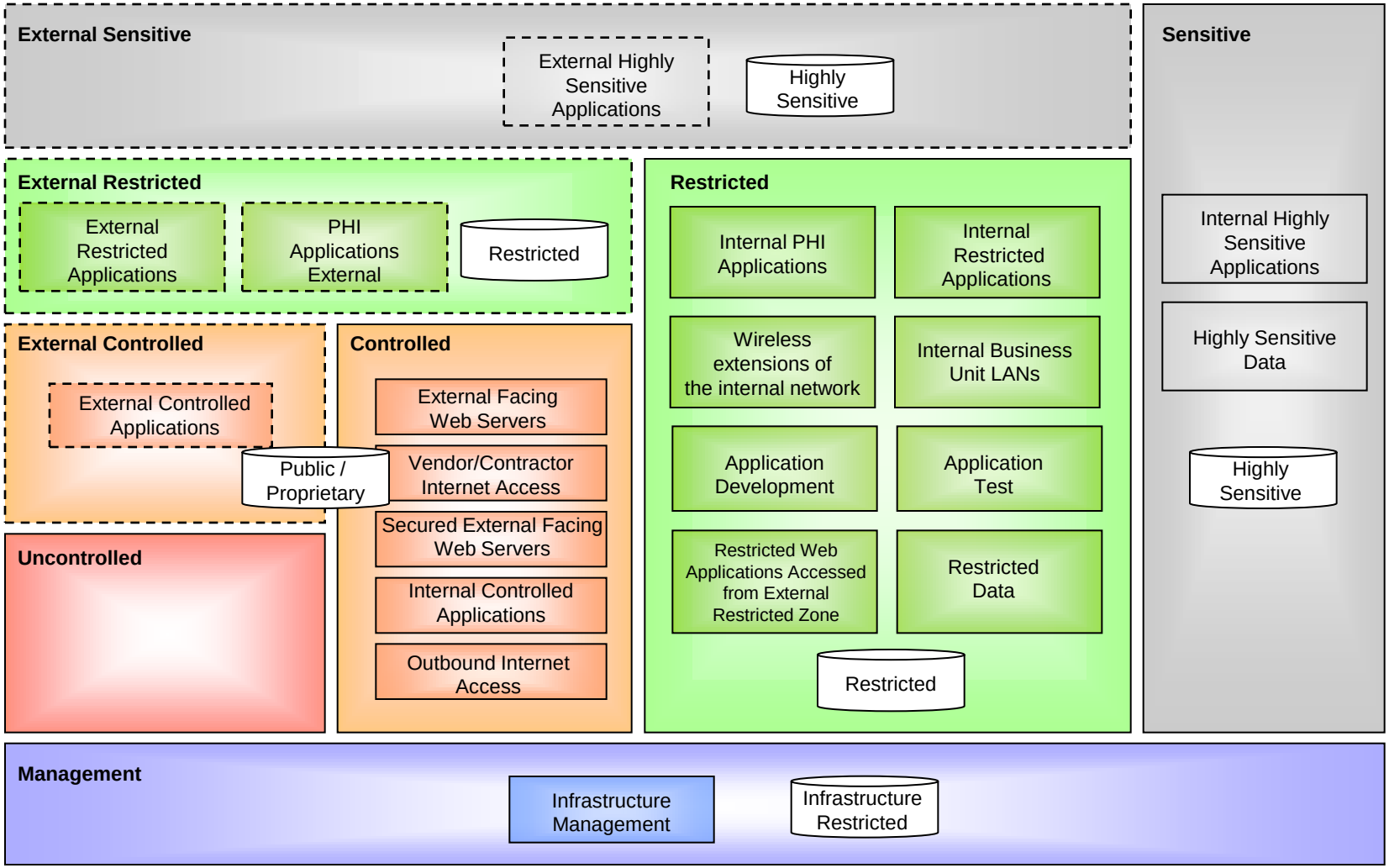
Sensitive
The Sensitive / External Sensitive Zones are the most secure area within the architecture.

Here access should be limited to a small group of highly trusted users / processes.

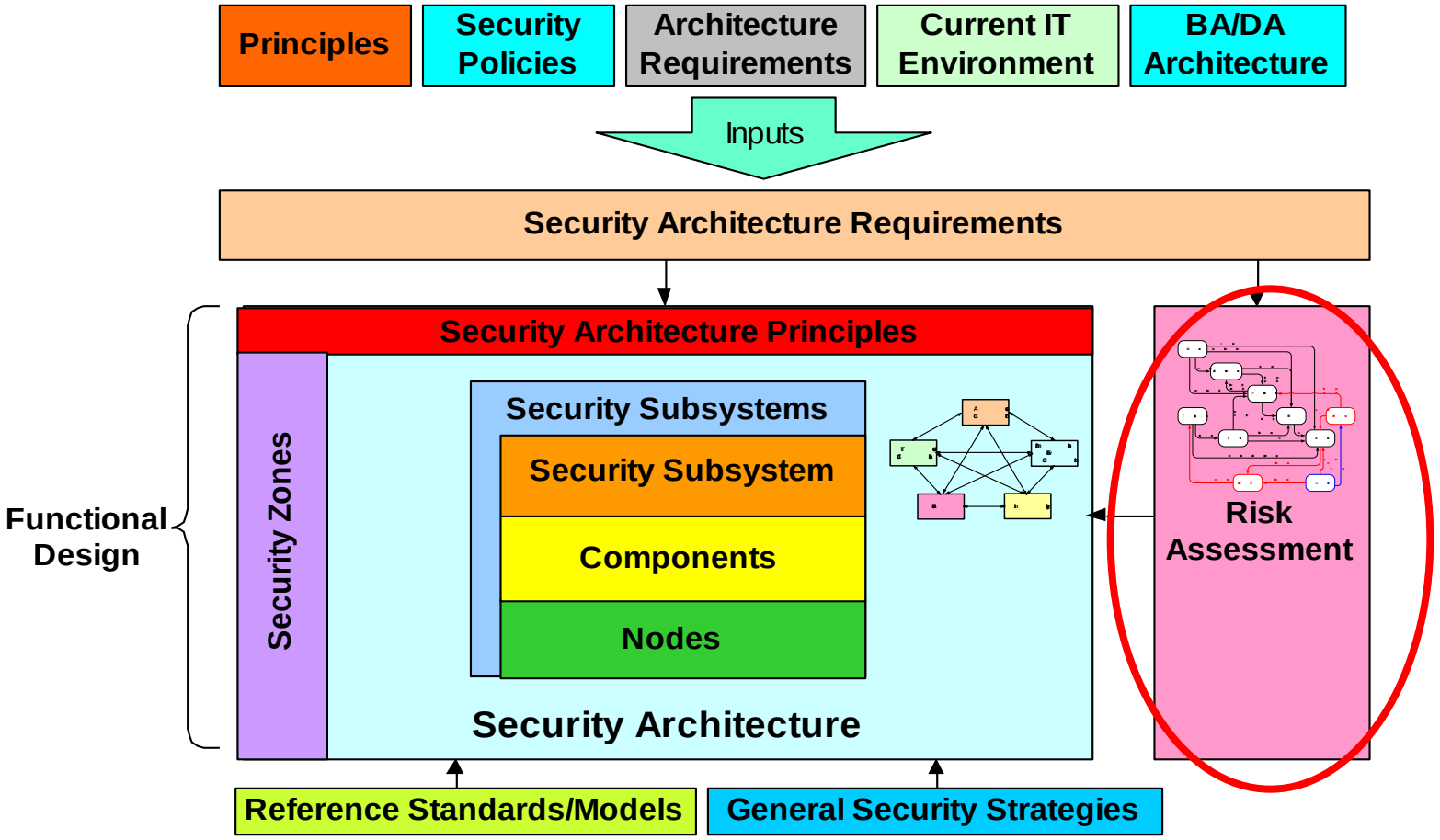
Management The Management zone belongs to IT. It is used to administer the servers, network devices, firewalls and other managed devices within the enterprise.

Security Zones

Zones, Enclaves and Data Classifications



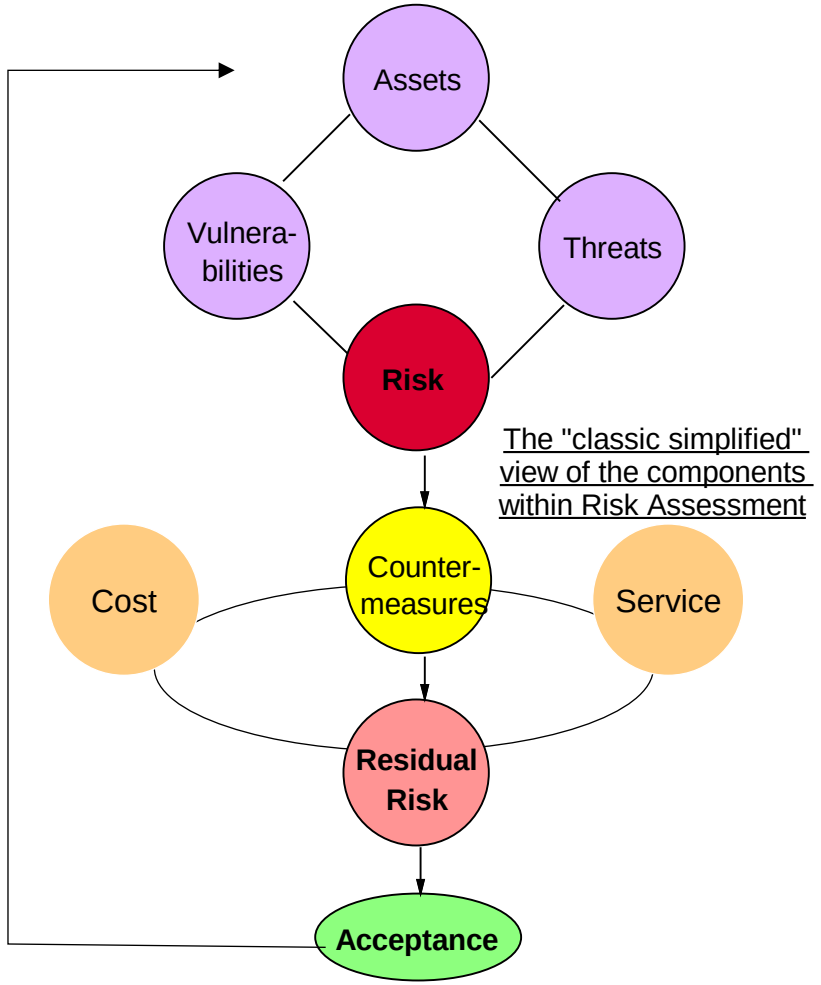
A Threat Risk Assessment is required at the Business level and later at a technical level



What is Risk Assessment?

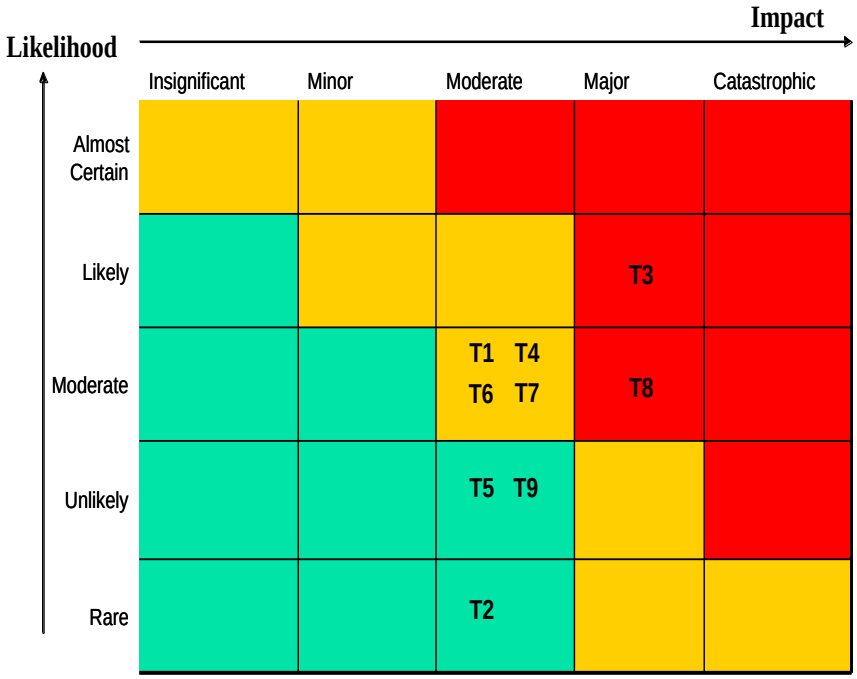
from http://www.itsecurity.com/

- **Assets –** Information or resources to be protected by the countermeasures of a system.
- **Vulnerability –** A weakness in the software and/or hardware design that allows circumvention of the system security.
- **Threat –** An action or event that might prejudice security.
- **Risk –** The likelihood that a given vulnerability will be exploited by a particular threat.
- **Countermeasure –** A measure designed to reduce or eliminate a security threat or vulnerability. [Common Criteria]



Threat and Risk: Loss of Confidentiality Risk Grid

Assessment example:

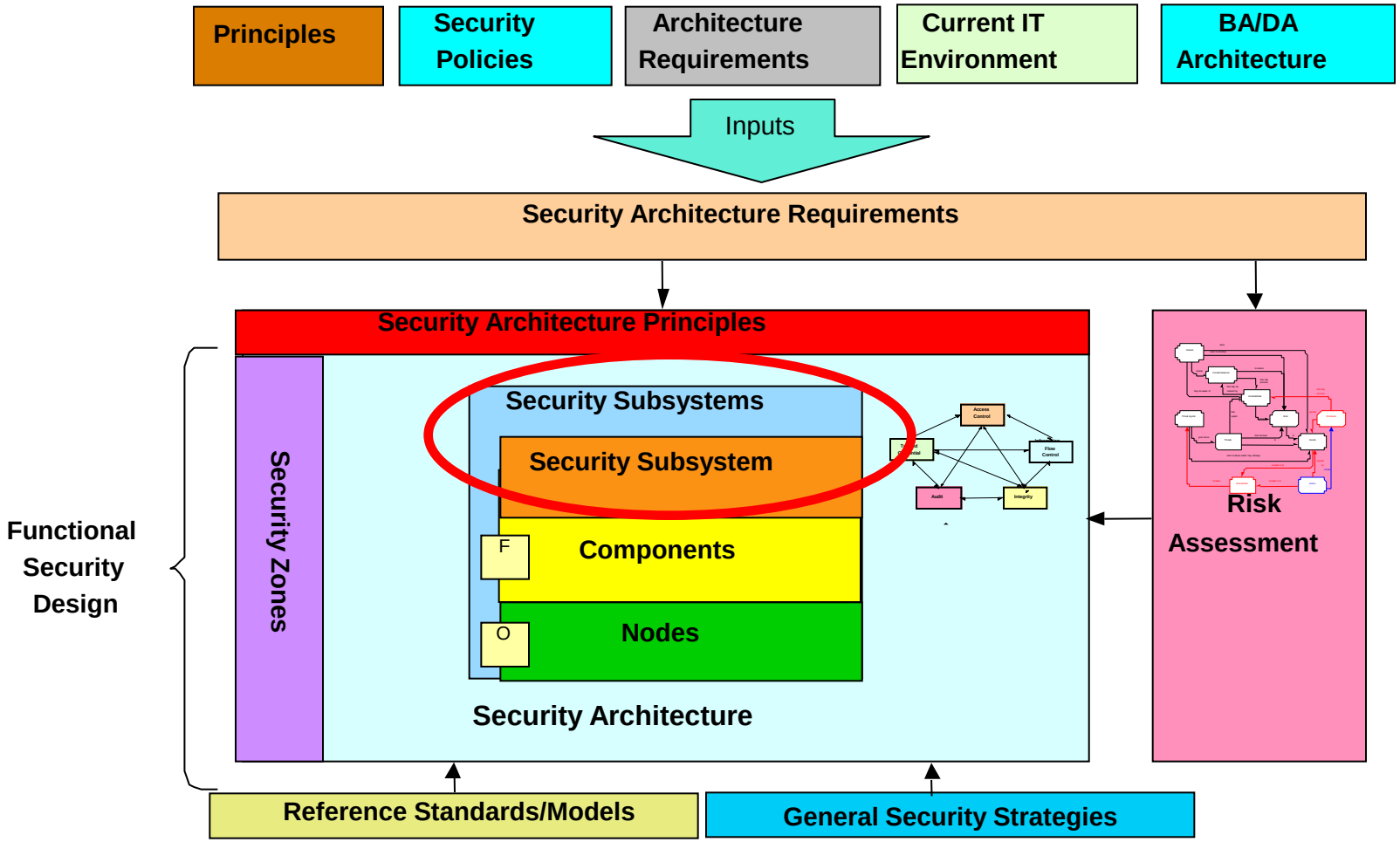


Threats	XREF #
Electromagnetic radiation	T2
Misrouting or rerouting messages	T5
Unauthorized access to storage media	T9
Eavesdropping	T1
Masquerading of user identity	T4
Software failure	T6
Theft	T7
Malicious code	T3
Unauthorized access to computers, data, services, applications	T8

Legend :

Green = Low Ri sk
Yellow = Medium Risk
Red = High Risk

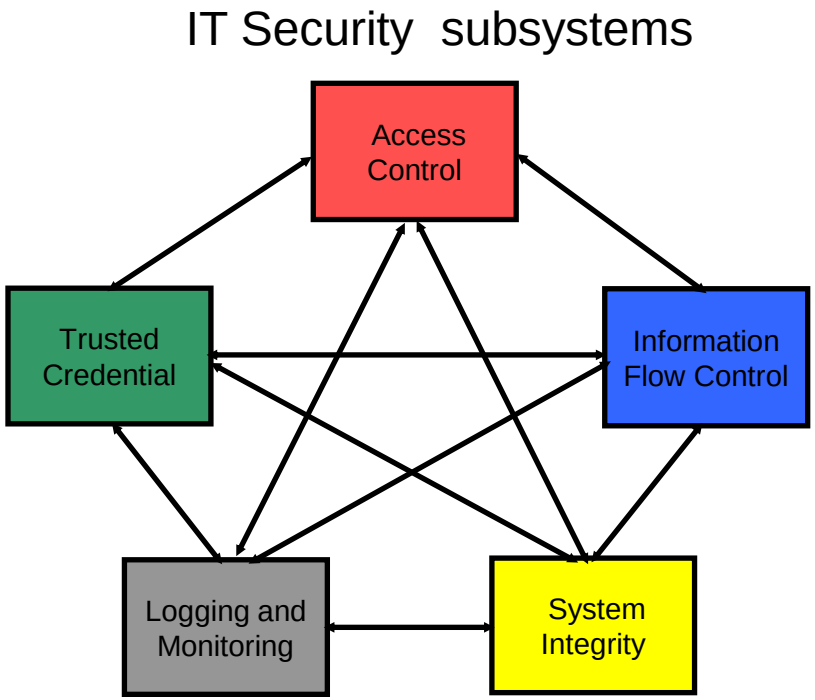
Security Subsystems



There are so many aspects to security that working with them is confusing and complex: some of them are components, some processes, some use cases, some are properties of the foregoing

- User enrollment
- Management of identities and secrets
- Credential creation
- Credential distribution
- Credential lifecycle management
- Specification of secrets
- Cryptographic services
- Cryptographic algorithms
- Verification of secrets
- Credential validation
- Identification
- Authentication
- Authorization
- Access control
- n-tier user to process binding
- n-tier session / state management
- Anonymity (property)
- Pseudonymity (property)
- Unlinkability (property)
- Unobservability (property)
- Information flow control
- Data confidentiality (property)
- Data integrity (property)
- Guaranteed delivery (POO / POR)
- Import / export between domains
- Event awareness
- Event data capture
- Event data collection
- Event data aggregation
- Event monitoring & analysis
- Detection of anomalous events or conditions
- Alarms and alerts
- Continuity of operations
- Resource allocation
- Priorization of service
- Component integrity
- Component recovery
- Rollback
- Fault tolerance
- Function separation
- Trusted path / channel
- Automated policy enforcement
- Policy enforcement
- Policy administration
- Systems management
- Anomaly handling
- Event data archival
- After-the-fact analysis and reporting

The security subsystems provide a way of breaking down the complex security domain into five meaningful areas of security responsibility

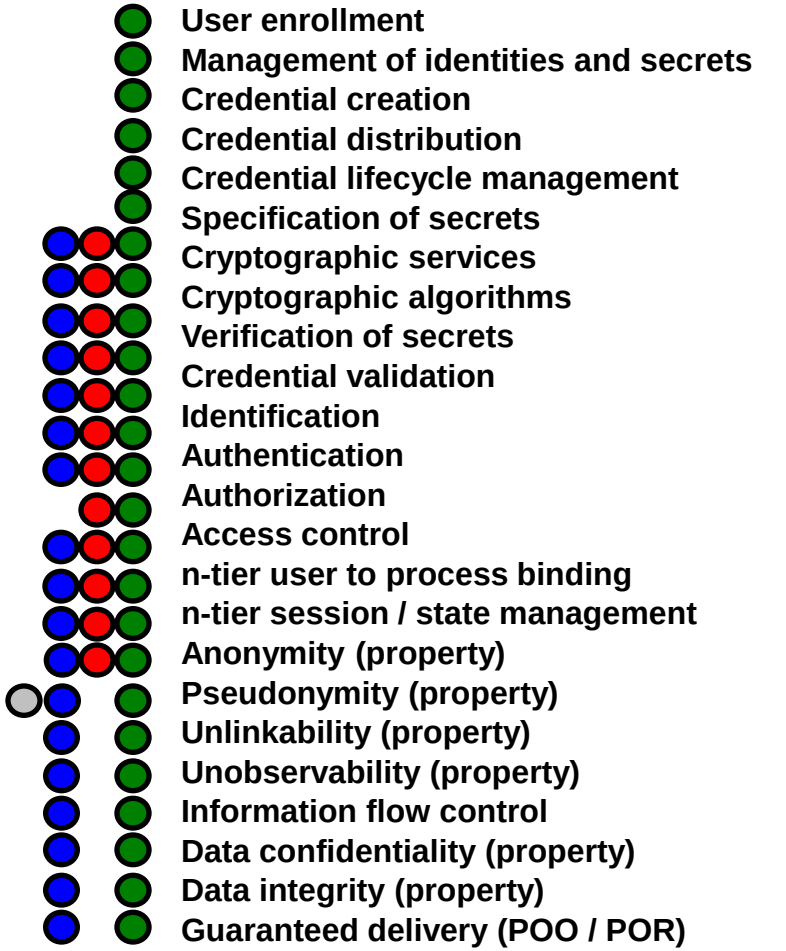


Security sub-systems are defined as collections of components; but they also have associated business processes, use cases and properties.

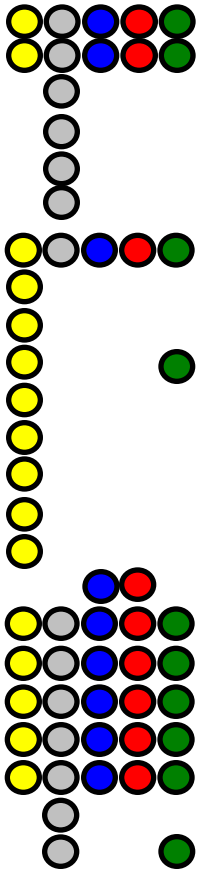
- **Trusted Credentials** – is responsible for generating, distributing and managing the object (e.g., user id, key fob) which conveys identity and permissions among the platforms, to the processes and the security subsystems within a computing solution. The object used by the trusted credential subsystem can be in whatever form, format or placement required to make a trust decision.
- **Information Flow Control** – is responsible for gating the flow of info within a computing solution, affecting the visibility of info within a computing solution and ensuring the integrity of information within a computing solution.
- **Access Control** – is responsible for gating access to and execution of processes and services within a computing solution via identification and authentication processes and security mechanisms, which use credentials and attributes.
- **Logging and Monitoring** – Audit- is responsible for capturing, analyzing, reporting, archiving and retrieving records of events and conditions within a computing solution.
- **Integrity** – is responsible for maintaining the correct and reliable operation of critical components and processes within the computing solution.

The different aspects need to be grouped so that we can work with them efficiently and easily

Integrity Logging and Monitoring Information Flow Control Access Control Trusted Credentials

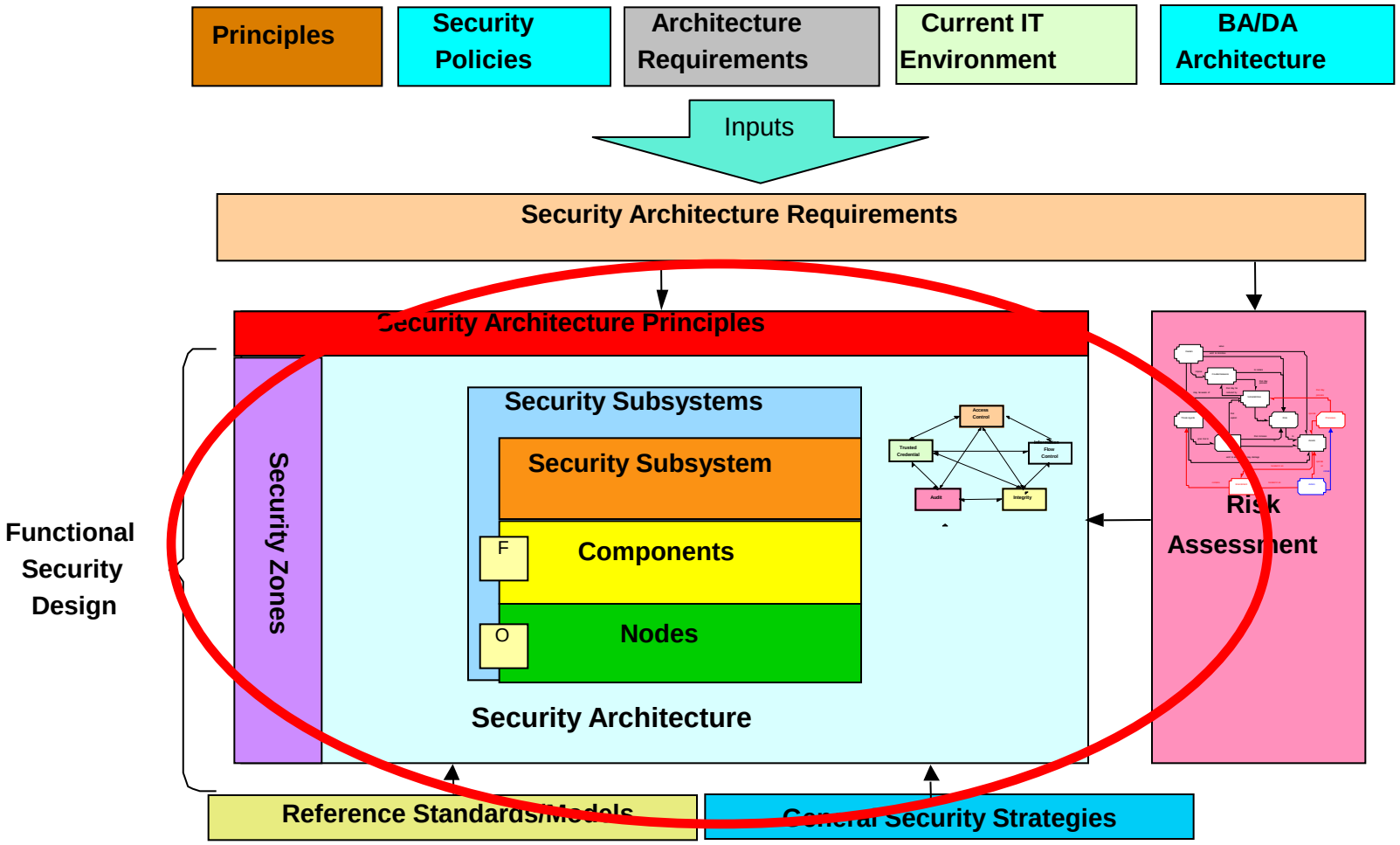


User enrollment
Management of identities and secrets
Credential creation
Credential distribution
Credential lifecycle management
Specification of secrets
Cryptographic services
Cryptographic algorithms
Verification of secrets
Credential validation
Identification
Authentication
Authorization
Access control
n-tier user to process binding
n-tier session / state management
Anonymity (property)
Pseudonymity (property)
Unlinkability (property)
Unobservability (property)
Information flow control
Data confidentiality (property)
Data integrity (property)
Guaranteed delivery (POO / POR)
Import / export between domains



Event awareness
Event data capture
Event data collection
Event data aggregation
Event monitoring & analysis
Detection of anomalous events or conditions
Alarms and alerts
Continuity of operations
Resource allocation
Priorization of service
Component integrity
Component recovery
Rollback
Fault tolerance
Function separation
Trusted path / channel
Automated policy enforcement
Policy enforcement
Policy administration
Systems management
Anomaly handling
Event data archival
After-the-fact analysis and reporting

Security Design Solution



IT security design consists of six design steps

1. Design security zones
2. Design trusted credential subsystems
3. Design access control subsystems
4. Design information flow control subsystems
5. Design audit subsystems
6. Design integrity subsystems

Each subsystem contains components, which interact with other security subsystems to provide security services to the components of the system, and are deployed on nodes which communicate via connections

Steps to define Security Solution

1. Derive Security Zones, put onto Architecture Overview diagram
2. Derive Security Subsystems, map requirements to them and place in Security Zones
3. Derive component Models of Security Subsystems (i.e., create component architecture for each subsystem)
4. Derive the use cases for the security operations of the application/network
5. Derive operational Models of Security Subsystems (i.e., create operational architecture for each subsystem)
6. Map subsystems to nodes (security specific nodes, application specific nodes and enterprise nodes)
7. Map nodes to zones/enclaves

Questions

Design Objectives Example

SUMMARY - Security Design Objectives			
Trusted Credentials			Requirements
SO	001	User identities should be consistent across all business applications whenever possible	5, 6, 9, 10, 69
SO	002	Authenticated credentials will be used to access any information asset, process, or component.	5, 6, 8, 9, 10, 11, 16, 72, 73
SO	003	Any use of a credential will be traceable to an individual or process	2, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16, 72, 73, 96
SO	004	The credential system will be able to support multiple roles per individual and be scalable to support the number of potential users.	6, 8, 9, 10, 11, 16, 54, 67, 69, 72, 73, 75
SO	005	Access to systems and information assets will be controlled by role, context, and individual credentials.	5, 6, 8, 10, 11, 16, 17, 26, 28, 37, 44, 67, 72, 73, 87, 88, 89

Requirements Example

005	Public logons such as "Guest" or "Anonymous" (those not assigned to a specific individual) are reviewed for appropriateness. If account deemed unnecessary, it should be removed or disabled. If deemed necessary, compensating controls should be established, such as monitoring account usage.
006	System Administrator accounts are tightly controlled and audited.
007	System maintenance logs are maintained to log all work carried out on critical systems. This includes but is not limited to OS, application and hardware updates, user account adds, changes and deletes and system restoration.
008	Access to sensitive data is authorized on a "need-to-know," least-privilege basis, providing users only the access they need to do their jobs.
009	System Administrator passwords are changed from the "default" password to a strong password, immediately upon implementation. A documented procedure exists for changing (less than 60 days), securely maintaining, and distributing systems admin passwords.
010	User IDs and strong passwords are required for users before accessing any system or application.
011	System Administrator userids are changed from the default when possible.