Paweł Rajba
pawel@cs.uni.wroc.pl
http://itcourses.eu/

Application Security
Security Architecture

Agenda

- Introduction
- Security requirements
- Security principles
- Frameworks
  - OSA
  - SABSA

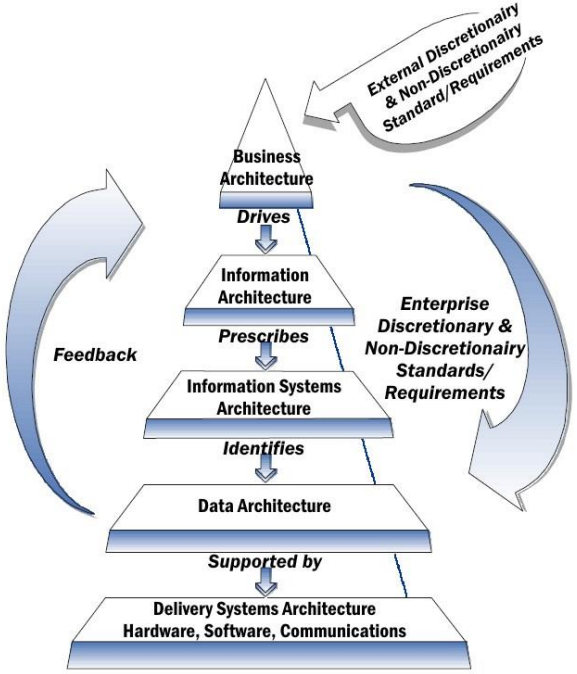
Introduction

- Architecture definition from ISO/IEC 42010

Fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution

Introduction

- Architecture can be considered on different levels
  - Enterprise
  - Information
  - Solution
  - Software
  - Integration
  - Infrastructure
- … and described in different ways
  - Artifacts (diagrams, matrix)
  - Viewpoints and Views
  - ArchiMate, UML, BPMN, …



Introduction

- Why architecture?
  - Support business needs
    - including non-functional requirements
  - Managing complexity
  - Maintanability and interoperability
    - Support change management
  - Reusability of components
  - Cost control

Introduction

- What about Security Architecture?
  - Part of Enterprise/IT Security
  - Support business needs
  - Security is a property of something else
    - There is always a context
  - There is no general „secure" meaning
    - Dependent on context and threats
  - Is about applying security controls to meet the risk apetite

Introduction

- Definition of IT Security Architecture from OSA (Open Security Architecture)

  The design artifacts that describe how the security controls are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system's quality attributes, among them confidentiality, integrity, availability, accountability and assurance.

Security requirements

- Security is usually considered as a part of non-functional requirements
- Most often we can consider 2 main sources
  - Customer's expectations
    - Authorizations, SSO, authentication method
  - Law and regulations
    - PCI-DSS, HIPPA, GDPR, internal policies & directives
- Needs to be part of business requirements

Security requirements

- Clear, explicit and complete documentation
  - E.g. importance of shared understanding of authZ
- Prototypes (authZ matrix, flows)
- Part of definitione of done in product backlog
- How to test security requirements?
  - Part of test strategy
  - Concept of abuse bases:
    - Use case: The system allows bank managers to modify an account's interest rate
    - Abuse case: A user is able to spoof being a manager and thereby change the interest rate on an account

Security principles

A Support the business	
PRINCIPLE	OBJECTIVE
A1 Focus on the business	To ensure that information security is integrated into essential business activities.
A2 Deliver quality and value to stakeholders	To ensure that information security delivers value and meets business requirements.
A3 Comply with relevant legal and regulatory requirements	To ensure that statutory obligations are met, stakeholder expectations are managed and civil or criminal penalties are avoided.
A4 Provide timely and accurate information on security performance	To support business requirements and manage information risks.
A5 Evaluate current and future information threats	To analyse and assess emerging information security threats so that informed, timely action to mitigate risks can be taken.
A6 Promote continuous improvement in information security	To reduce costs, improve efficiency and effectiveness and promote a culture of continuous improvement in information security.

B Defend the business	
PRINCIPLE	OBJECTIVE
B1 Adopt a risk-based approach	To ensure that risks are treated in a consistent and effective manner.
B2 Protect classified information	To prevent classified information (eg confidential or sensitive) being disclosed to unauthorised individuals.
B3 Concentrate on critical business applications	To prioritise scarce information security resources by protecting the business applications where a security incident would have the greatest business impact.
B4 Develop systems securely	To build quality, cost-effective systems upon which business people can rely (eg that are consistently robust, accurate and reliable).

C Promote responsible security behaviour	
PRINCIPLE	OBJECTIVE
C1 Act in a professional and ethical manner	To ensure that information security-related activities are performed in a reliable, responsible and effective manner.
C2 Foster a security-positive culture	To provide a positive security influence on the behaviour of end users, reduce the likelihood of security incidents occurring, and limit their potential business impact.

Security principles

- Solution & Software oriented
  - Minimize attack surface area
  - Establish secure defaults
  - Principle of Least privilege (or deny by default)
  - Principle of Defense in depth
  - Fail securely
  - Don’t trust services
  - Separation of duties
  - Avoid security by obscurity
  - Keep security simple & Usable
  - Fix security issues correctly

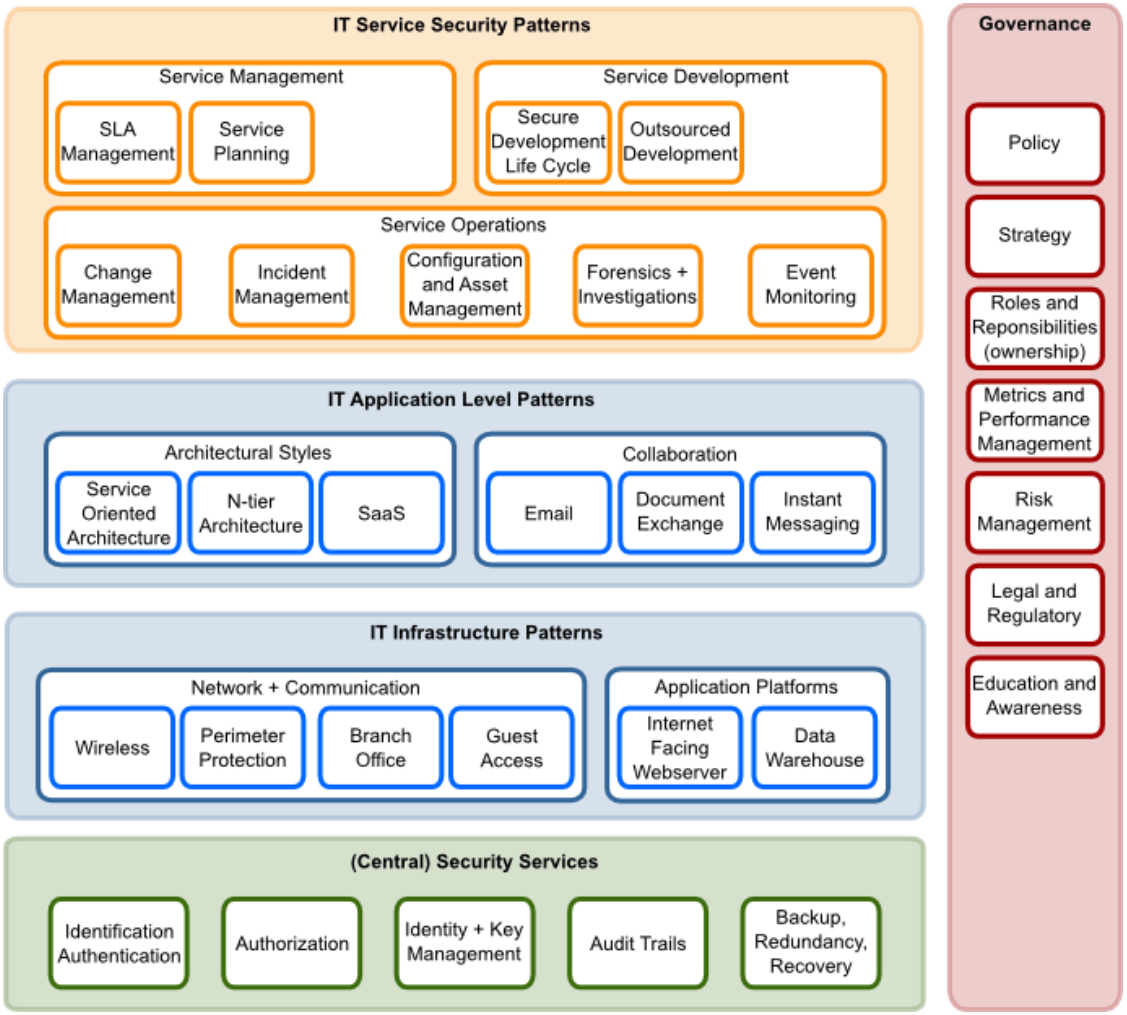
Frameworks

- There are different frameworks and models
- The most popular ones we will cover shortly
  - SABSA
  - OSA

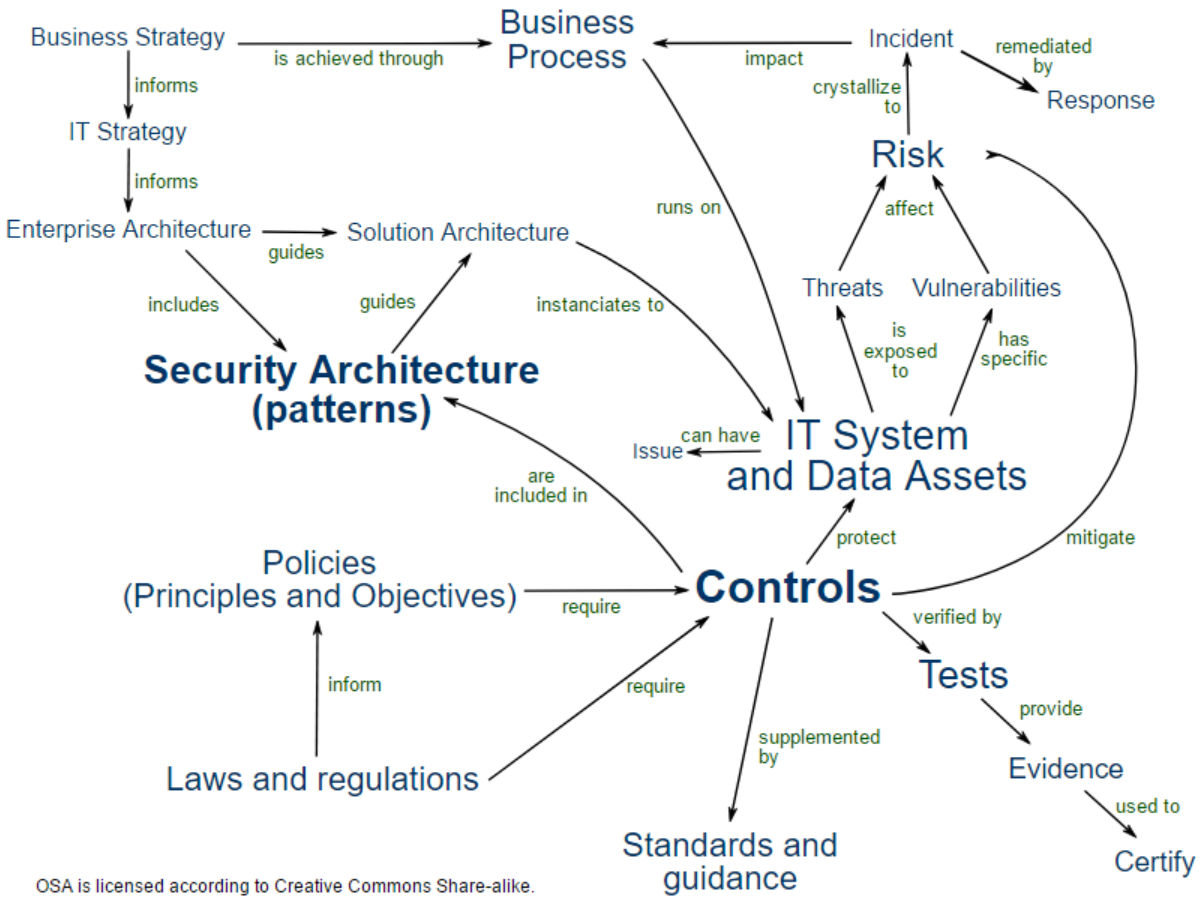
OSA

- OSA stands for
  - Open Security Architecture
- The OSA vision
  - OSA distills the know-how of the security architecture community and provides readily usable patterns for your application. OSA shall be a free framework that is developed and owned by the community.
- Different aspects covered, let's look at some of them

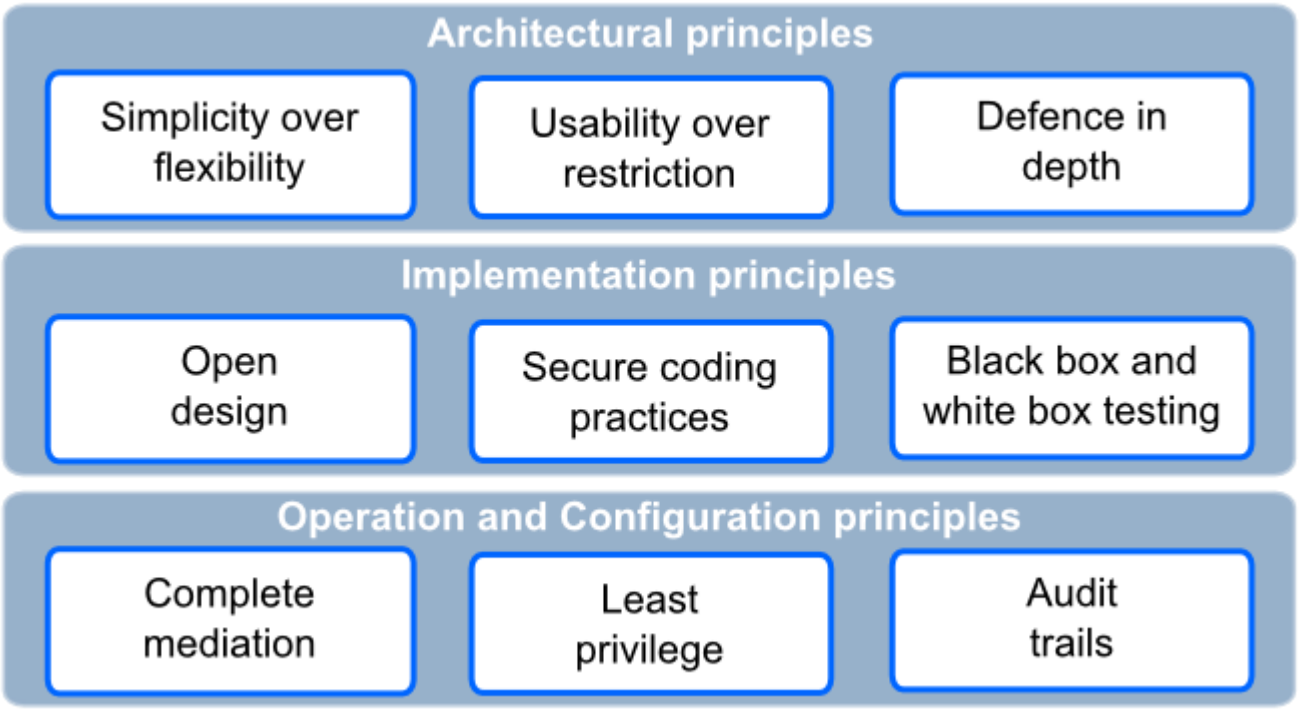
Landscape


IT Service Security Patterns
Service Management
SLA Management
Service Planning
Service Development
Secure Development Life Cycle
Outsourced Development
Service Operations
Change Management
Incident Management
Configuration and Asset Management
Forensics + Investigations
Event Monitoring
IT Application Level Patterns
Architectural Styles
Service Oriented Architecture
N-tier Architecture
SaaS
Collaboration
Email
Document Exchange
Instant Messaging
IT Infrastructure Patterns
Network + Communication
Wireless
Perimeter Protection
Branch Office
Guest Access
Application Platforms
Internet Facing Webserver
Data Warehouse
(Central) Security Services
Identification Authentication
Authorization
Identity + Key Management
Audit Trails
Backup, Redundancy, Recovery
Governance
Policy
Strategy
Roles and Reponsibilities (ownership)
Metrics and Performance Management
Risk Management
Legal and Regulatory
Education and Awareness

Taxonomy



Design principles



Actors

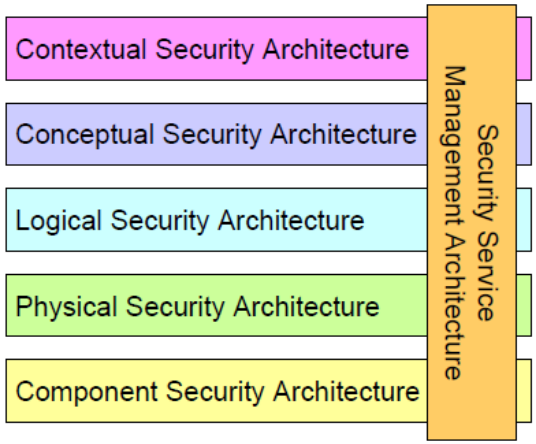
Icon	Name	Main Responsibilities
	IT Security manager (CISO, CSO,...)	Planning, policies and procedures, guidelines
	IT Security specialist	Security assessment and certifications, training, scans,
	IT Operations manager	Capacity management, configuration management, monitoring and incident management, backup and recovery management, maintenance scheduling and execution, Data-centre physical security.
	Information asset owner	Determines entitlements to access a given data set or resource for a specific role. Specifies or approves the classification and privacy requirements.
	Service / product owner	Risk assessments Role models
	Project manager	Responsible for project risk analysis, both in terms of original project risks related to time, and budget but also in terms of quality risks concerning the project deliverable that is then handed over as a service into production.
	Human resources	Trigger changes in the identity life cycle. Responsible for personnel security.
	ID administrations	Identifier management, authenticator management, role management
	Risk officer, controller & manager	Facilitate, Monitor and evaluate risk assessments
	Requirements analyst	Analyses how functional security components (e.g. authentication, audit trail) fit into usability requirements

	Developer	Follow security engineering principles
	SW architect	Responsible that all application security controls are added to the application design. Coordinates security specialist and developers.
	Infrastructure architect	Maintenance planning and prioritisation. Planning for security infrastructure such as directories and networks.
	Quality manager	Ensures that the products meets (security) specifications.
	External auditor	Security accreditation
	Internal auditor	Security assessments
	End user	The user of an IT-Service, can be internal business person or customer.
	Data privacy officer	Responsible to ensure that customer and employee data is managed according to privacy regulations in the jurisdictions where the data is processed or accessed. These responsibilities may be performed by the information asset owner, or delegated to Data Privacy Officer in larger organisations.
	Facility manager	Responsible for the physical security.

SABSA

- SABSA stands for
  - Sherwood Applied Business Security Architecture
- Definition from SABSA:
  - Methodology for developing business-driven, risk and opportunity focused enterprise security & information assurance architectures, and for delivering security infrastructure solutions that traceably support critical business initiatives
  - Comprised of a number of integrated frameworks, models, methods and processes

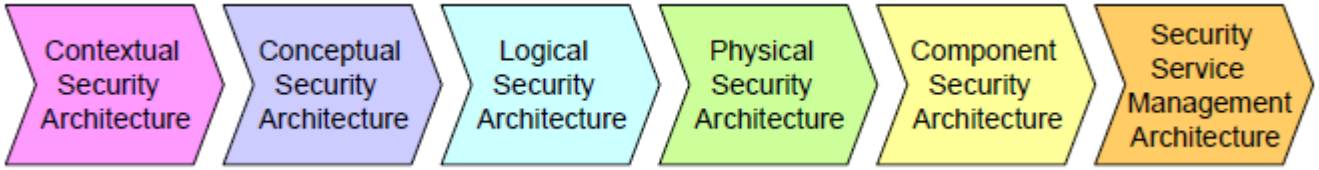
Layered model



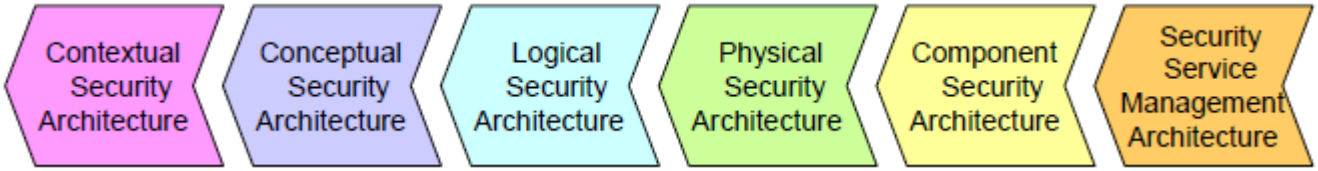
The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Service Manager's View	Security Service Management Architecture

2-way traceability

- Completeness:
  - Has every business requirement been met?

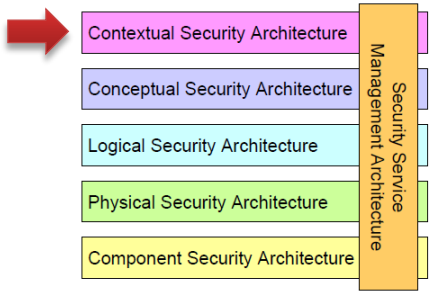


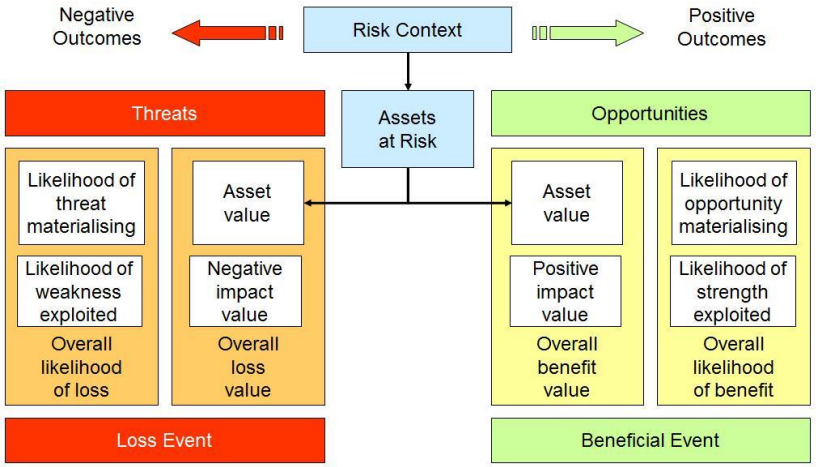
- Business Justification:
  - Is every component of the architecture needed?



Contextual (Business' View)

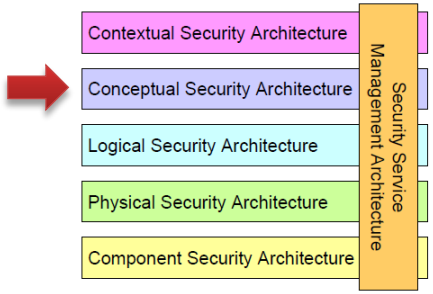
- Business objectives
- Business drivers
- Risk and opportunities





Driver No	Business Drivers
BD1	Protecting the reputation of the Organization, ensuring that it is perceived as competent in its sector
BD2	Providing support to the claims made by the Organization about its competence to carry out its intended functions
BD3	Protecting the trust that exists in business relationships and propagating that trust across remote electronic business communications links and distributed information systems
BD4	Maintaining the confidence of other key parties in their relationships with the Organization
BD5	Maintaining the operational capability of the Organization's systems
BD6	Maintaining the continuity of service delivery, including the ability to meet the requirements of service level agreements where these exist
BD7	Maintaining the accuracy of information
BD8	Maintaining the ability to govern
BD9	Preventing losses through financial fraud
BD10	Detecting attempted financial fraud

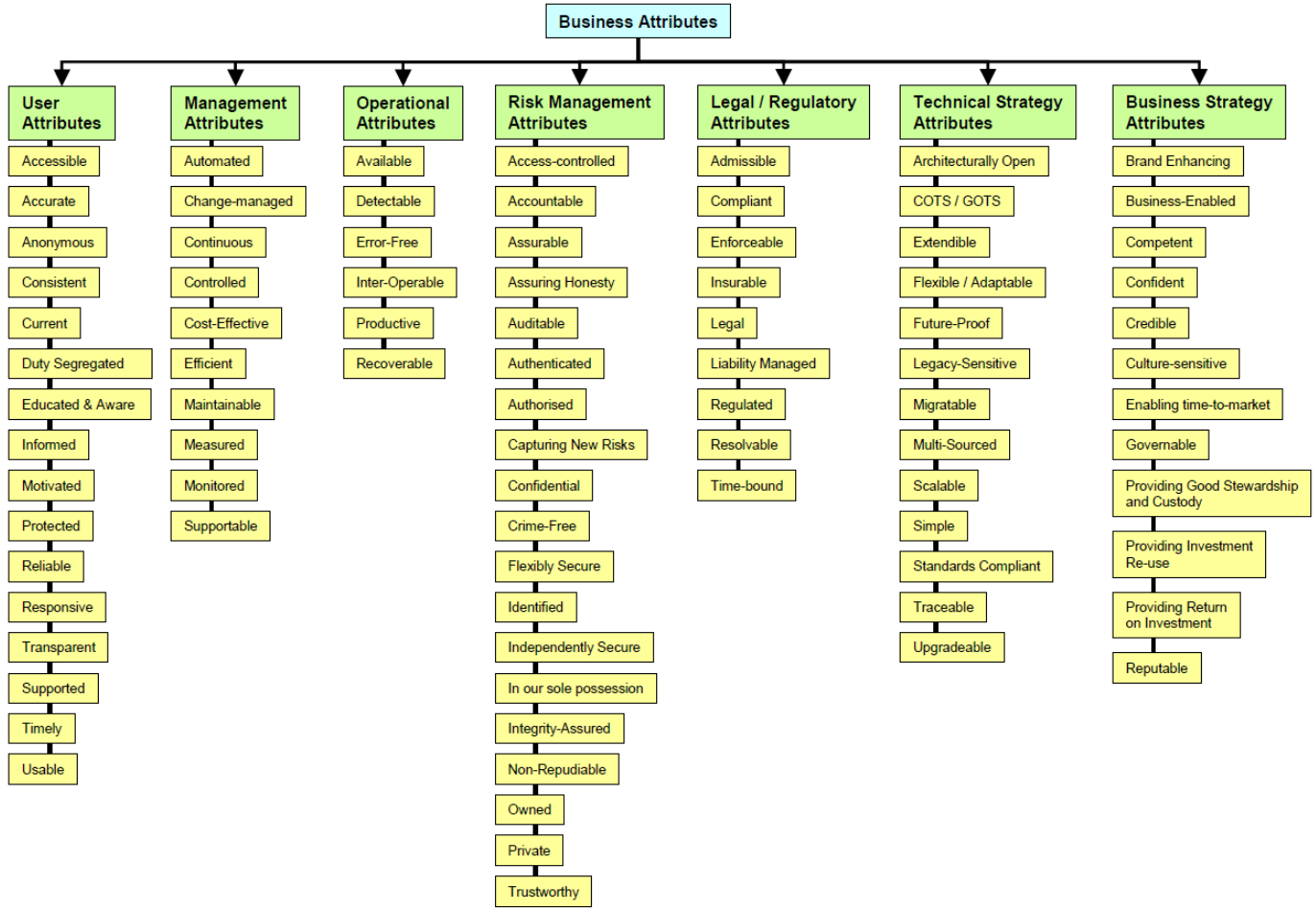
Conceptual (Architect's View)

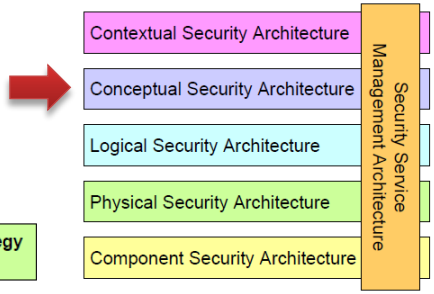


- High level architecture
- Translate business goals in terms of Business Attributes Profile
- Define strategies for different aspects, e.g.
  - Application Security
  - Network Security
  - Defence in depth

Conceptual (Architect's View)

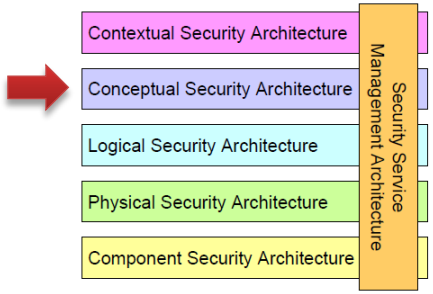
- Business Attribute Profile





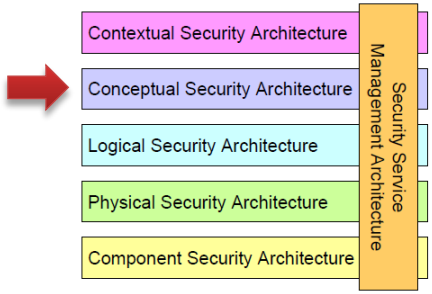
Conceptual (Architect's View)

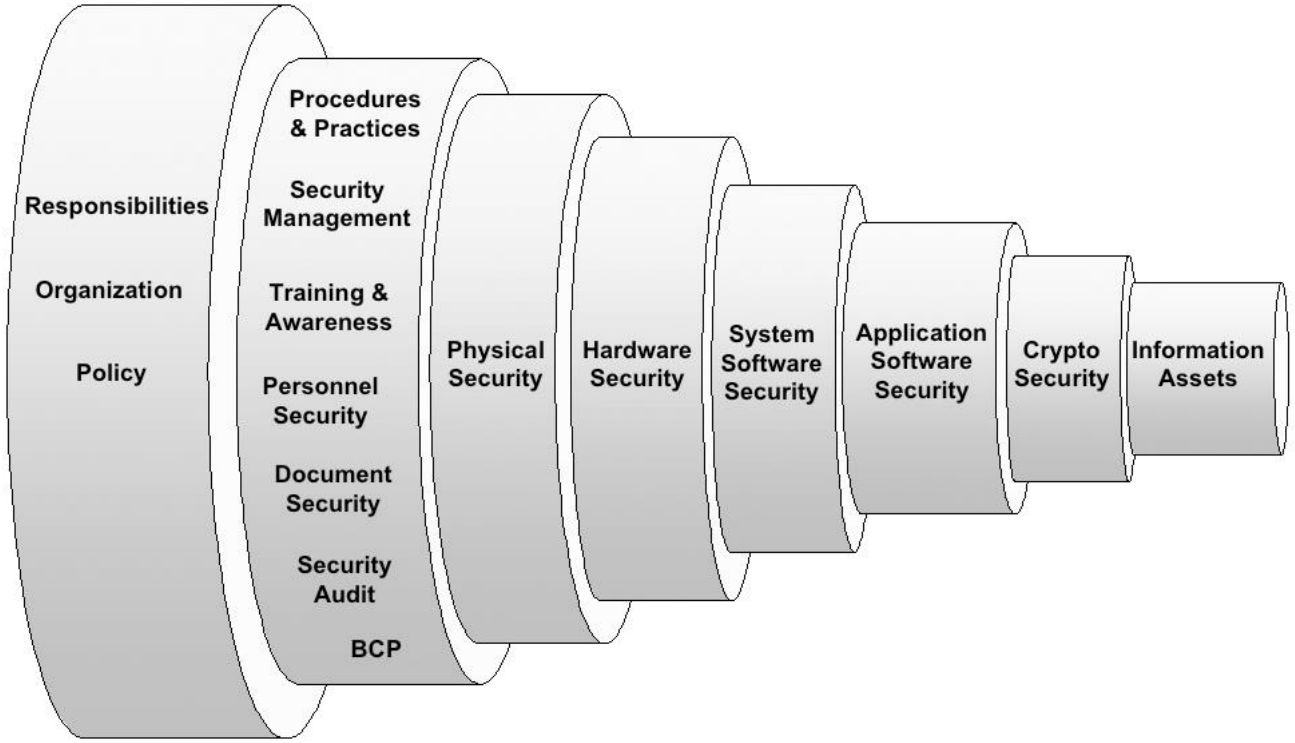
- Most common attributes
  - Confidentiality
  - Integrity
  - Availability
  - Privacy
  - Traceability
  - Non-repudiation



Conceptual (Architect's View)

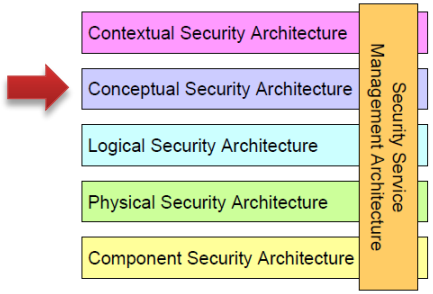
- Defense in depth





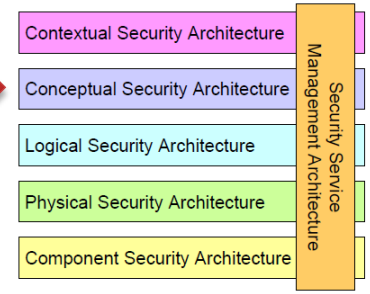
Conceptual (Architect's View)

- Categories of controls
  - Deterence
  - Prevention
  - Containment
  - Detection and Notification Services
  - Recovery and Restoration Services
- It is up to architect to decide what to put in every layer of defence

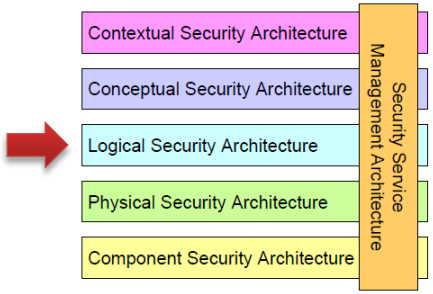


Conceptual (Architect's View)

- Strategies and services should be defined for chosen business attributes and areas
- Example areas and services
  - Application Security
    - Authorisation, Authentication, Access control, Audit, Administration,
  - Network Security
    - Entity authentication, gateways (firewalls), bandwidth control, intrusion detection and prevention, security zones
  - Data Management Security
    - Retention time, backup & restoration strategy
  - Platform Security
    - Hardening details, available services, virtualization modes, separation strategies

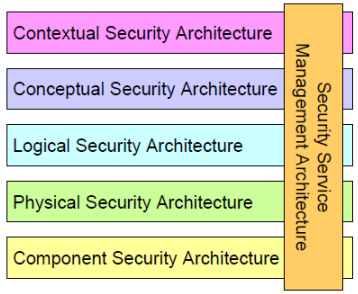


Logical (Designer's View)



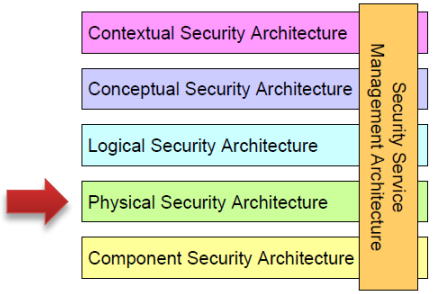
- Focus on the information assets
- Security Services needs to defined in details and integrated
- End-to-end protection of information flows
- Examples of security services:
  - Entity Registration, User & Device authentication
  - Session authentication, Message integrity protection
  - Entity authorisation, Audit trails, Data confidentiality, Data replication and backup, Intrusion detection

Physical (Builder's View)



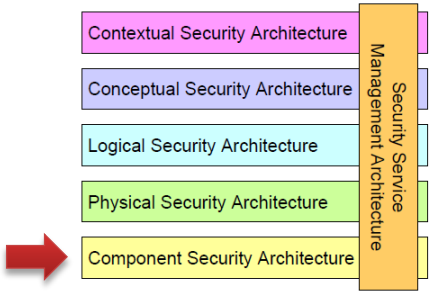
- Turn security services into physical security mechanisms
- Logical information convert into data model
  - Tables, messages, certificates, signatures, etc.
- The following areas should be covered:
  - Platform security, Hardware security, Network Topology, Directory Topology, etc.
  - Proper usage of cryptography including key management

Physical (Builder's View)



- Examples of converting security services into mechanisms
  - Authorisation: Roles
  - Entity Authentication: Login procedure, Passwords, Multi-factor authentication
  - Message Origin Authentication: Message integrity checksums, Digital signatures
  - Non-Repudiation: Digital signatures, Audit logs
  - Stored Data Confidentiality: Access control mechanisms, Stored data encryption

Component (Tradesman's View)



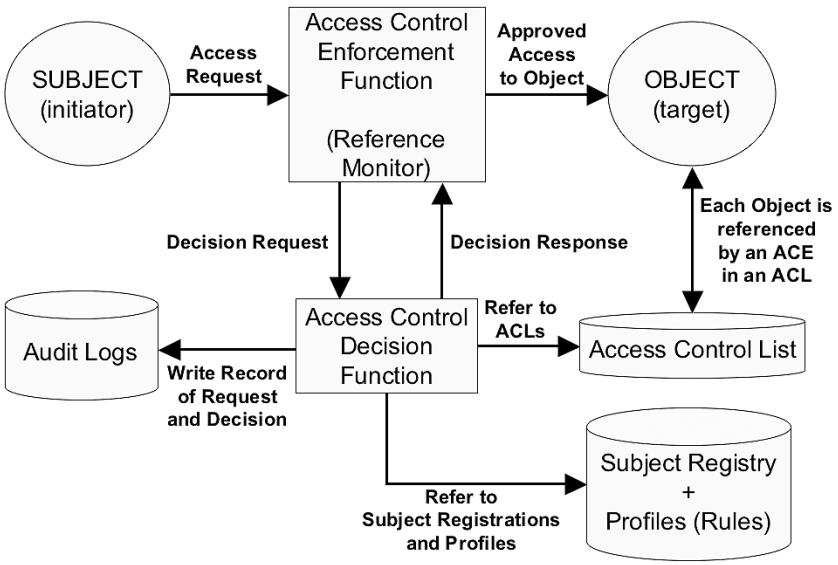
- Work with components that are
  - hardware items, software items,
  - interface specifications and standards.
- The lowest level when we need to elaborate, e.g.
  - Products, tools, including data repositories or CPUs
  - Configuration, technical details
  - Standards, tools and protocols both hardware and software, e.g. NIST, ISF, W3C, ECMA
  - Personnel management tools and products

Example: Access Control

- Contextual
  - Intention that there are assets which needs to be protected, clasification of prioritized items
  - First attempt to authorization & roles

Example: Access Control

- Conceptual
  - Potential Federations
  - General flows and components
  - Strategy



Example: Access Control

- Logical
  - Which entity authenticates where
    - both on user and devices level
  - Authentication flows, location of authentication and authorization services
  - Where are the enforcement and decision for ACS
  - Which authorization rules are executed where

Example: Access Control

- Physical
  - Authentication protocols (e.g. SAML2, OID Connect), methods (user name/password) vs. SSO
  - Directory services (user store: LDAP or local DB?)

Example: Access Control

- Component
  - Exact products to be used, configuration details
  - URL's and IP addresses
  - Signature algorithm for tokens
  - User logon screen prototypes

Additional questions

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

Complete matrix

The SABSA matrix

SABSA	Assets (WHAT)	Motivation (WHY)	Process (HOW)	People (WHO)	Location (WHERE)	Time (WHEN)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation 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 Lifetime 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 and Procedures	Security Mechanisms	Users, Applications and User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions 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 and Platforms	Security Operations Schedule

SDL perspective