System Architecture Security

Week 7

Contents

Enterprise Architecture

- Ref: Chapter 02 – All-in-one CISSP 6th edition

PURPOSE

- Basic understanding of enterprise architecture framework
- Basic understanding of information governance
- Ability to measure the effectives of your efforts
- Ability to build an effective information security management program

TERMINOLOGY

Vision

A statement of what the business unit or organization would like to develop into

Strategic Planning

Defining direction and making decisions on allocating resources in pursuit of a strategic goal.

Framework

Serves as a guide for creating or expanding a structure into something of value.

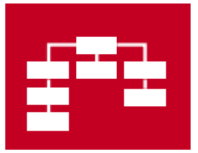
TERMINOLOGY

Deliverables

Any measureable, tangible, verifiable outcome, result, or item that must be produced to complete a project or part of a project

Standardization

The act of checking or adjusting (by comparison with a standard) the accuracy of a measuring instrument



Taxonomy

The science of classification according to a pre-determined system whose resulting catalogue is used to provide a conceptual framework

TERMINOLOGY

Risk

An uncertain event or set of events which, should it occur, will have an effect on the achievement of objectives. A risk consists of a combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives.

Risk Management

The systematic application of management policies, procedures, and practices to the tasks of communicating, establishing the context, identifying, analyzing, evaluating, treating, monitoring, and reviewing risk.

Business Driver

A resource, process or condition that is vital for the continued success and growth of a business.

TERMINOLOGY

Metadata

"Data about data". Structural metadata is about the design and specification of data structures and is more properly called "data about the containers of data"; descriptive metadata, on the other hand, is about individual instances of application data, the data content.

Metamodel

The analysis, construction and development of the frames, rules, constraints, models and theories applicable and useful for modeling a predefined class of problems.

Matrix

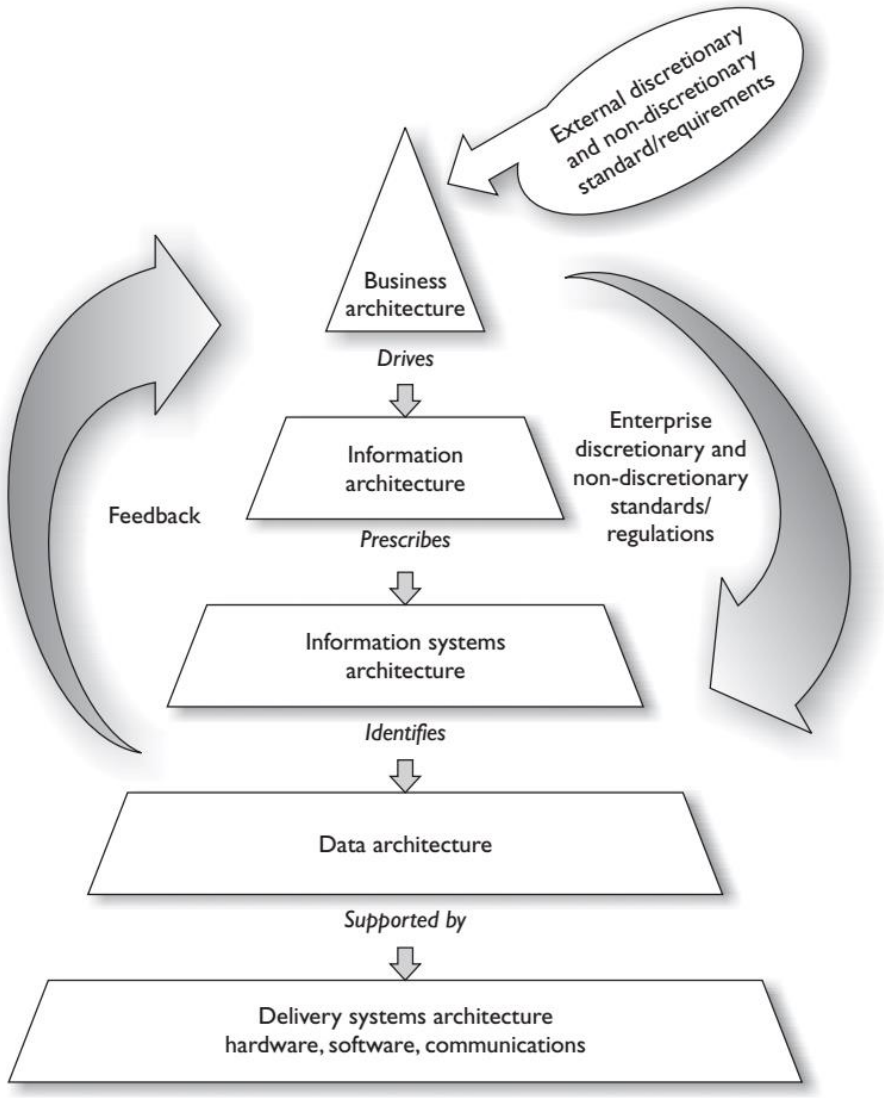
A matrix is a rectangular array of numbers, symbols, or expressions, arranged in rows and columns.

Enterprise Architecture Development

- Organizations have a choice when attempting to secure their environment as a whole. They can just toss in products here and there, which are referred to as point solutions or stovepipe solutions, and hope the ad bhoc approach magically works in a manner that secures the environment evenly and covers all of the organization's vulnerabilities.
- The second approach would be to define an enterprise security architecture, allow it to be the guide when implementing solutions to ensure business needs are met, provide standard protection across the environment, and reduce the amount of security surprises the organization will run into.
- An **enterprise architecture** encompasses the essential and unifying components of an organization. It expresses the enterprise structure (form) and behavior (function). It embodies the enterprise's components, their relationships to each other, and to the environment.

Example: NIST Enterprise Architecture Framework

Figure 2-4
NIST Enterprise Architecture Framework



- An enterprise architecture allows you to not only understand the company from several different views, but also understand how a change that takes place at one level will affect items at other levels.
- For example, if there is a new business requirement, how is it going to be supported at each level of the enterprise? What type of new information must be collected and processed? Do new applications need to be purchased or current ones modified? Are new data elements required? Will new networking devices be required?
- An architecture allows you to understand all the things that will need to change just to support one new business function. The architecture can be used in the opposite direction also. If a company is looking to do a technology refresh, will the new systems still support all of the necessary functions in the layers above the technology level? An architecture allows you to understand an organization as one complete organism and illustrate how changes to one internal component can directly affect another one.

Why Do We Need Enterprise Architecture Frameworks?

- Business and technical people use the term “risk,” but each group is focusing on very different risks a company can face—market share versus security breaches. This divide between business perspectives and technology perspectives can not only cause confusion and frustration—it commonly costs money.
- So we need a tool that both business people and technology people can use to reduce confusion, optimize business functionality, and not waste time and money. This is where business enterprise architectures come into play. It allows both groups (business and technology) to view the same organization in ways that make sense to them.
- Each organization is also made up of its own specialists (HR, marketing, accounting, IT, R&D, management). But there also has to be an understanding of the entity (whether it is a human body or company) holistically, which is what an enterprise architecture attempts to accomplish.

What is Enterprise Security Architecture?

- An ***enterprise security architecture*** is a subset of an enterprise architecture and defines the information security strategy that consists of layers of solutions, processes, and procedures and the way they are linked across an enterprise strategically, tactically, and operationally. It is a comprehensive and rigorous method for describing the structure and behavior of all the components that make up a holistic information security management system (ISMS).
- The main reason to develop an enterprise security architecture is to ensure that security efforts align with business practices in a standardized and cost-effective manner. The architecture works at an abstraction level and provides a frame of reference. Besides security, this type of architecture allows organizations to better achieve interoperability, integration, ease-of-use, standardization, and governance.
- Enterprise Security Architecture is the process of translating business security vision and strategy into effective enterprise change by creating, communicating and improving the key security requirements, principles and models that describe the enterprise's future security state and enable its evolution.

Enterprise Security Architecture (ESA) at a glance

- Enterprise Security Architecture (ESA) is essential to align your business strategy to IT security
- A successful ESA aligns risk management to business strategy, allowing technology to be embraced and support your organizational goals.

Enterprise Security Architecture (ESA)

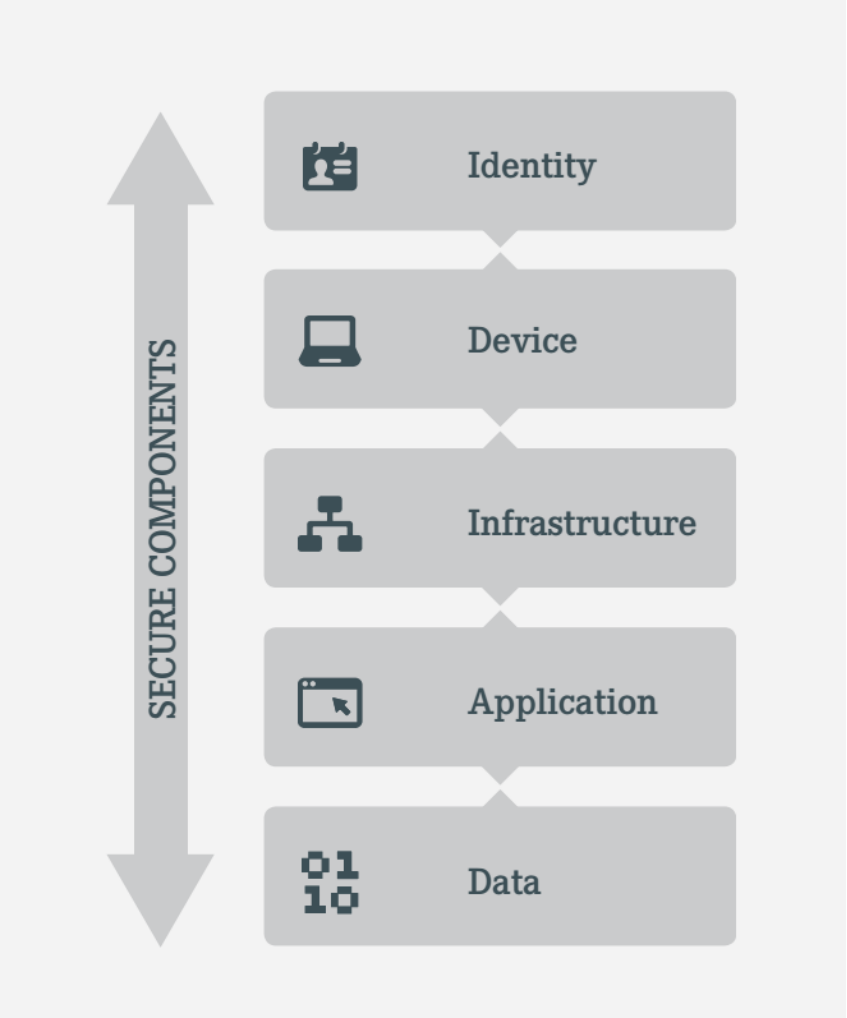
- The objective of enterprise security architecture is to provide the ***conceptual design*** of the network security infrastructure, related security mechanisms, and related security policies and procedures. The enterprise security architecture links the components of the security infrastructure as one **cohesive** unit. The goal of this cohesive unit is to protect corporate information.

- A mature ESA enables risk-based decision making for security objectives and provides a common framework to:
  - ✓Enable managers to visualize security capability gaps and prioritize security investments
  - ✓Establish a relationship between security capabilities, policies, and processes to better control and mitigate cybersecurity threats

Why it is so important?

- ESA is not about developing for a prediction. It is about assuring that we develop in a way that allow us to maintain and sustain our agility to change. We don’t know where we are going or how we are going to get there but we need to be ready.

Five components must be considered in ESA



Key Terms: Enterprise Security Architecture

- **Security through obscurity** Relying upon the secrecy or complexity of an item as its security, instead of practicing solid security practices.
- **ISO/IEC 27000 series** Industry-recognized best practices for the development and management of an information security management system.
- **Zachman framework** Enterprise architecture framework used to define and understand a business environment developed by John Zachman.
- **TOGAF** Enterprise architecture framework used to define and understand a business environment developed by The Open Group.
- **SABSA framework** Risk-driven enterprise security architecture that maps to business initiatives, similar to the Zachman framework.
- **DoDAF** U.S. Department of Defense architecture framework that ensures interoperability of systems to meet military mission goals.
- **MODAF** Architecture framework used mainly in military support missions developed by the British Ministry of Defence.

Key Terms (cont.): Security Controls Development

- **CobiT** Set of control objectives used as a framework for IT governance developed by Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI).
- **SP 800-53** Set of controls that are used to secure U.S. federal systems developed by NIST.
- **COSO** Internal control model used for corporate governance to help prevent fraud developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.
- **ITIL** Best practices for information technology services management processes developed by the United Kingdom's Office of Government Commerce.
- **Six Sigma** Business management strategy developed by Motorola with the goal of improving business processes.
- **Capability Maturity Model Integration (CMMI)** Process improvement model developed by Carnegie Mellon

ARCHITECTURE FRAMEWORKS

ZACHMAN	The Zachman Framework is an enterprise architecture framework which provides a formal and highly structured way of viewing and defining an enterprise. It consists of a two dimensional classification matrix based on the intersection of six communication questions (What, Where, When, Why, Who and How) with five levels of reification, successively transforming the most abstract ideas (on the Scope level) into more concrete ideas (at the Operations level).
TOGAF	The Open Group Architecture Framework (TOGAF) is a framework for enterprise architecture which provides a comprehensive approach for designing, planning, implementing, and governing an enterprise information architecture. TOGAF is a high level and holistic approach to design, which is typically modeled at four levels: Business, Application, Data, and Technology. It tries to give a well-tested overall starting model to information architects, which can then be built upon. It relies heavily on modularization, standardization, and already existing, proven technologies and products.
SABSA	SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. It was developed independently from the Zachman Framework, but has a similar structure. SABSA is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.

Zachman Framework for Enterprise Architecture

Order	Layer	What (Data)	How (Function)	Where (Network)	Who (People)	When (Time)	Why (Motivation)
1	**Scope context boundary** • Planner	List of things important to the business	List of processes the business performs	List of locations in which the business operates	List of organizations important to the business	List of events significant to the business	List of business goals/strategies
2	**Business model concepts** • Owner	e.g., semantic or entity-relationship model	e.g., business process model	e.g., business logistics model	e.g., workflow model	e.g., master schedule	e.g., business plan
3	**System model logic** • Designer	e.g., logical data model	e.g., application architecture	e.g., distributed system architecture	e.g., human interface architecture	e.g., processing structure	e.g., business rule model
4	**Technology model physics** • Builder	e.g., physical data model	e.g., system design	e.g., technology architecture	e.g., presentation architecture	e.g., control structure	e.g., rule design
5	**Component configuration** • Implementer	e.g., data definition	e.g., program	e.g., network architecture	e.g., security architecture	e.g., timing definition	e.g., rule specification
6	**Functioning enterprise instances** • Worker	e.g., data	e.g., function	e.g., network	e.g., organization	e.g., schedule	e.g., strategy

Sherwood Applied Business Security Architecture (SABSA)

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (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, 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 operation continuity	Operation risk management	Security service management and support	Application and user management and support	Security of sites, networks, and platforms	Security operations schedule

ARCHITECTURE FRAMEWORKS

- The Zachman and TOGAF are true Enterprise Architecture frameworks however SABSA is the main framework for Enterprise Security Architecture. More importantly The SABSA framework is most effective when integrated or linked with one of these more robust Enterprise Architecture frameworks. Today we will be talking about the integration to the Zachman and TOGAF frameworks.

ZACHMAN  SABSA

This is the traditional framework integration for SABSA and oldest. This framework integration is not nearly as effective as it used to be.

TOGAF  SABSA

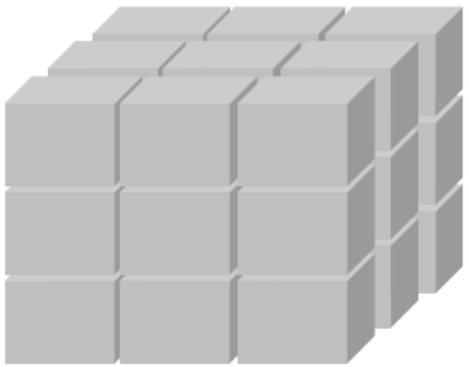
This is the new framework integration for SABSA. This framework carries with it many tools that exponentially increase its effectiveness.

ZACHMAN ⇔ SABSA

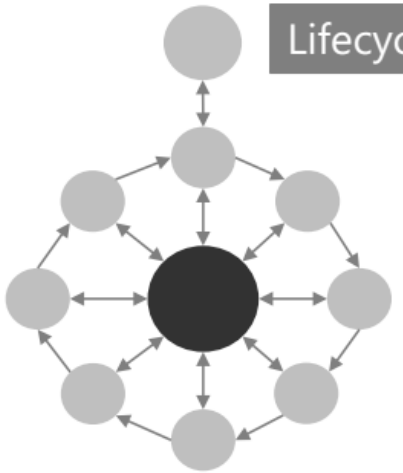
Matrix

There was a time when a company could leverage a single matrix for their information security risk management program but in today's rapidly changing and agile dependent world, this is no longer possible.

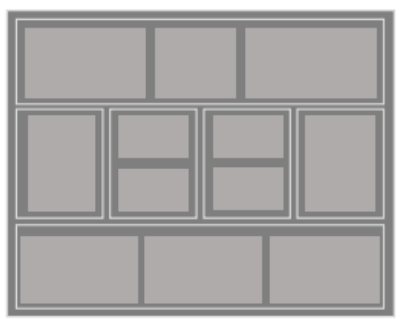
TOGAF ⇔ SABSA



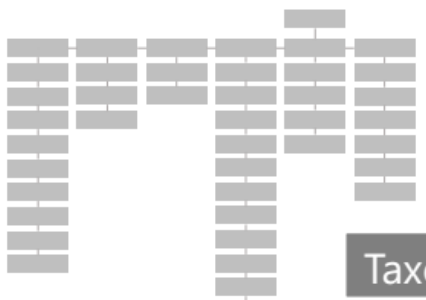
Matrix



Lifecycle



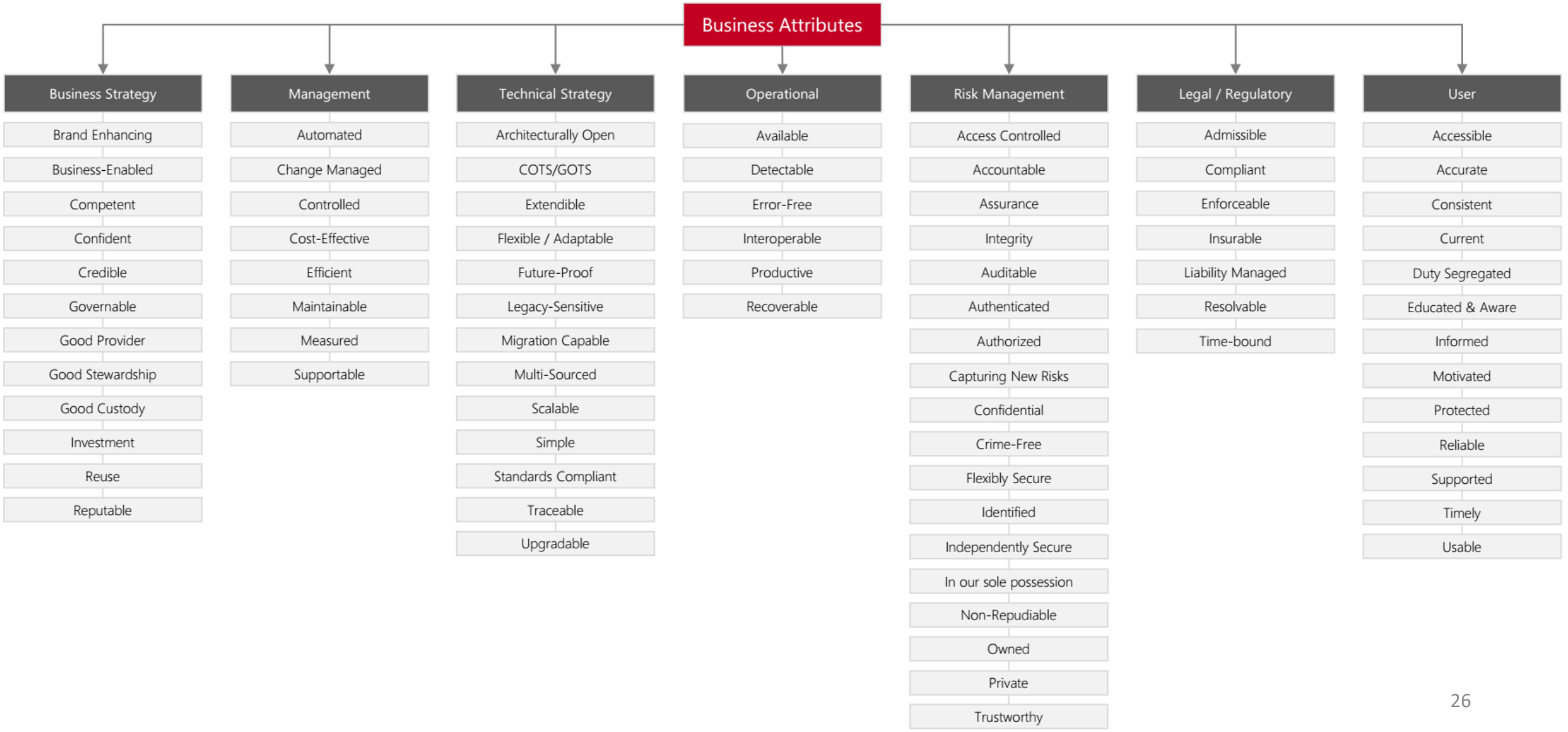
Metamodel

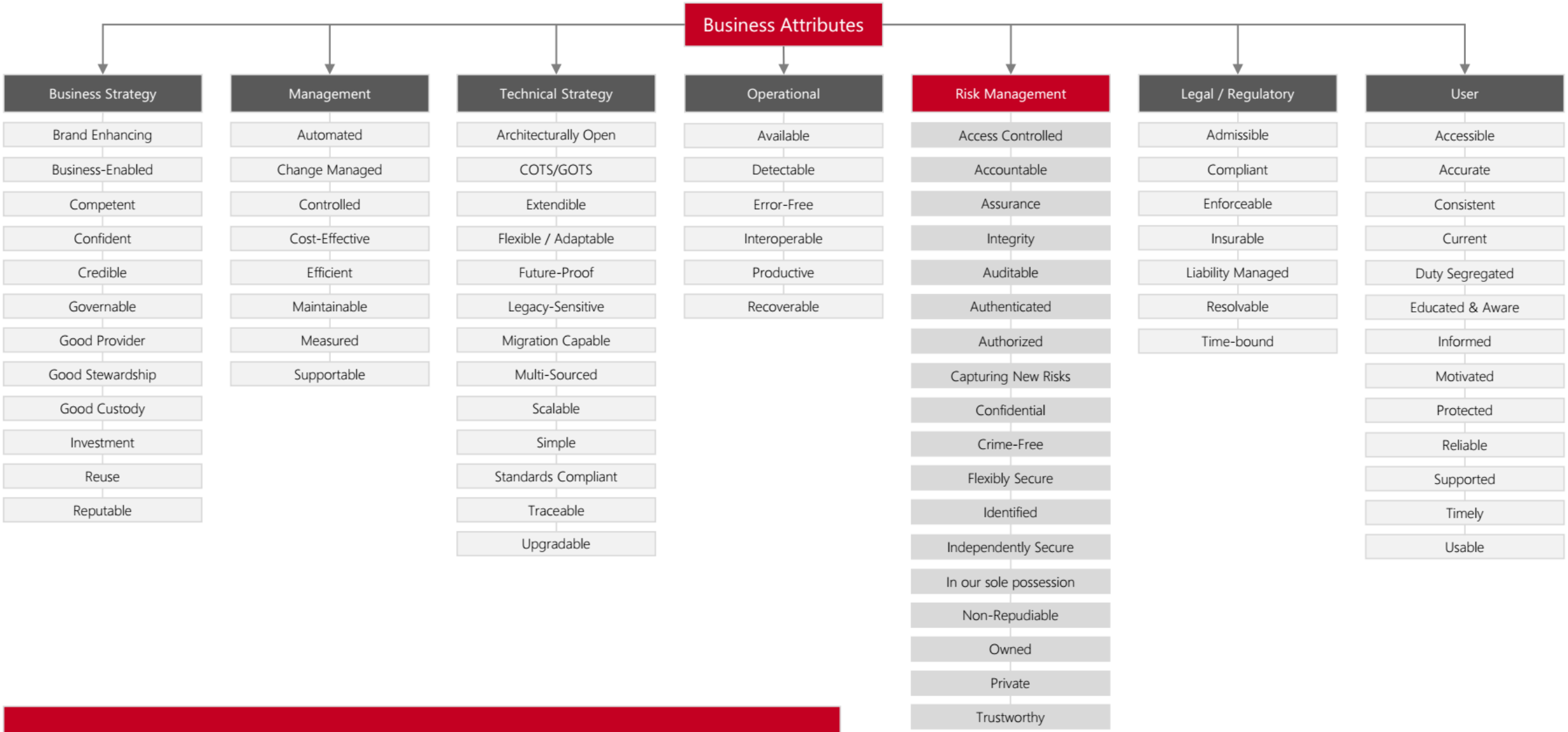


Taxonomy

This level of insight, detail, and complexity allows our business to remain agile and competitive in todays world.

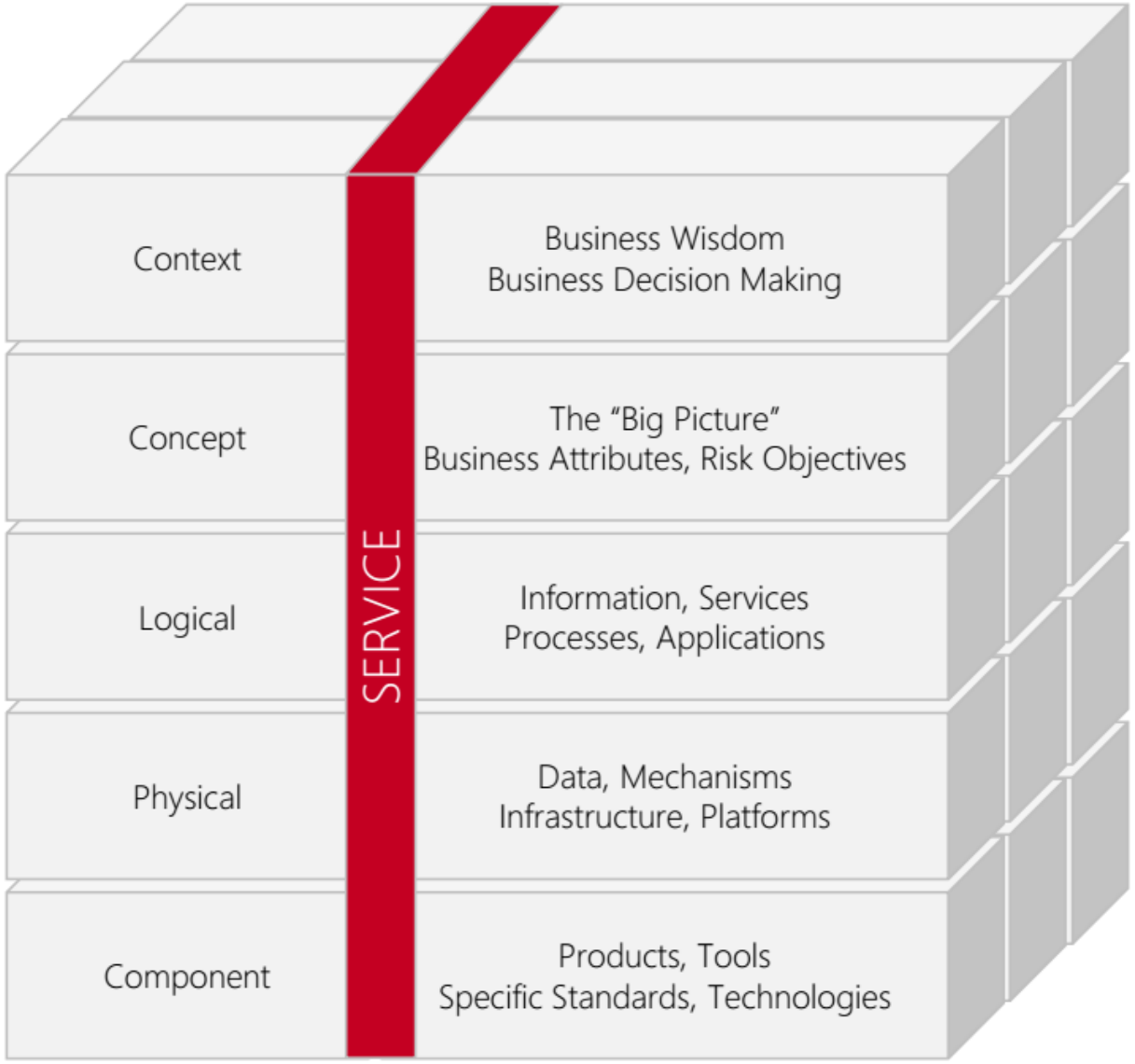
Taxonomy


Business Attributes
Business Strategy
Brand Enhancing
Business-Enabled
Competent
Confident
Credible
Governable
Good Provider
Good Stewardship
Good Custody
Investment
Reuse
Reputable
Management
Automated
Change Managed
Controlled
Cost-Effective
Efficient
Maintainable
Measured
Supportable
Technical Strategy
Architecturally Open
COTS/GOTS
Extendible
Flexible / Adaptable
Future-Proof
Legacy-Sensitive
Migration Capable
Multi-Sourced
Scalable
Simple
Standards Compliant
Traceable
Upgradable
Operational
Available
Detectable
Error-Free
Interoperable
Productive
Recoverable
Risk Management
Access Controlled
Accountable
Assurance
Integrity
Auditable
Authenticated
Authorized
Capturing New Risks
Confidential
Crime-Free
Flexibly Secure
Identified
Independently Secure
In our sole possession
Non-Repudiable
Owned
Private
Trustworthy
Legal / Regulatory
Admissible
Compliant
Enforceable
Insurable
Liability Managed
Resolvable
Time-bound
User
Accessible
Accurate
Consistent
Current
Duty Segregated
Educated & Aware
Informed
Motivated
Protected
Reliable
Supported
Timely
Usable



The highlighted areas are the items that we normally have the greatest interest and focus in when we consider information security

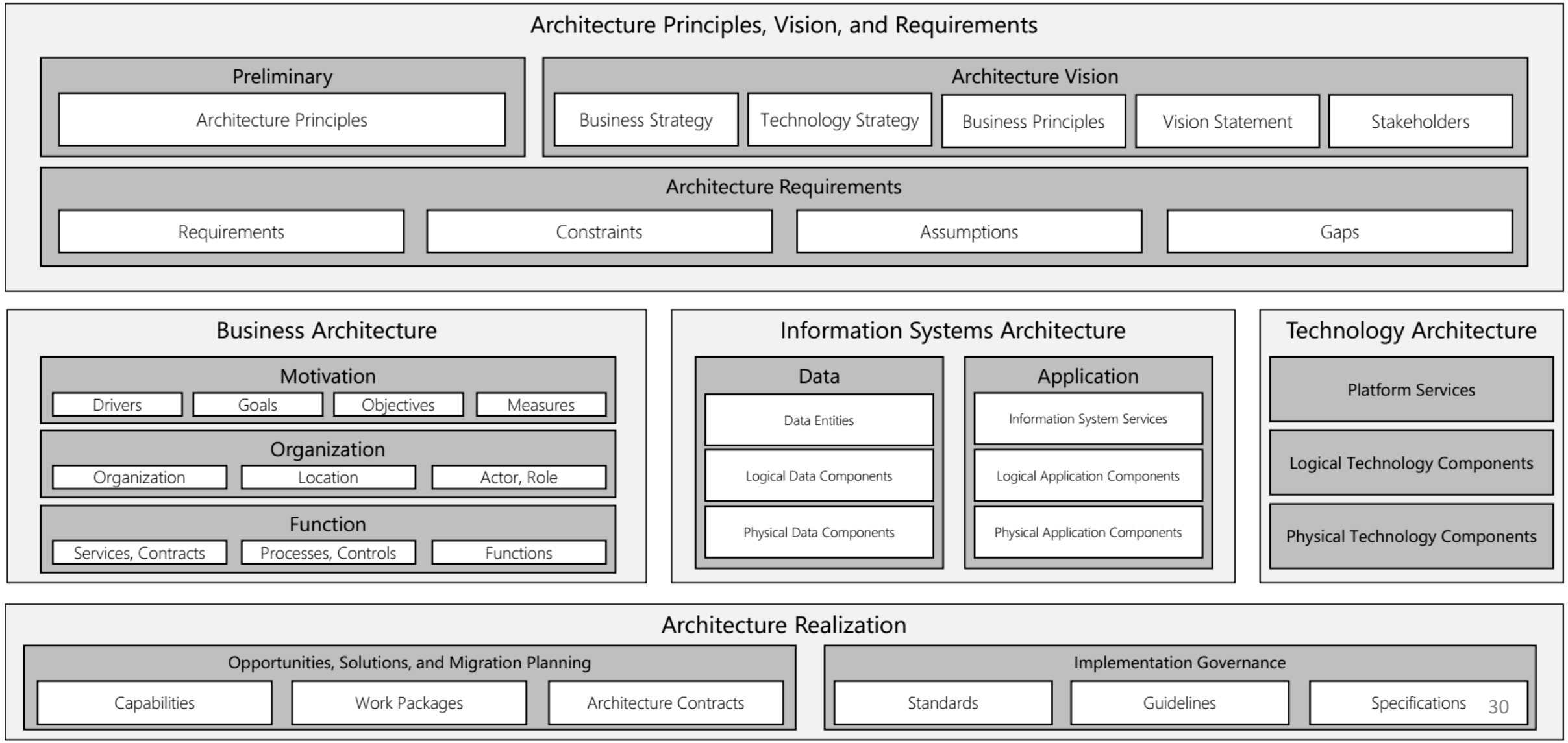
Matrix


Context
Business Wisdom
Business Decision Making
Concept
The "Big Picture"
Business Attributes, Risk Objectives
Logical
Information, Services
Processes, Applications
Physical
Data, Mechanisms
Infrastructure, Platforms
Component
Products, Tools
Specific Standards, Technologies
SERVICE

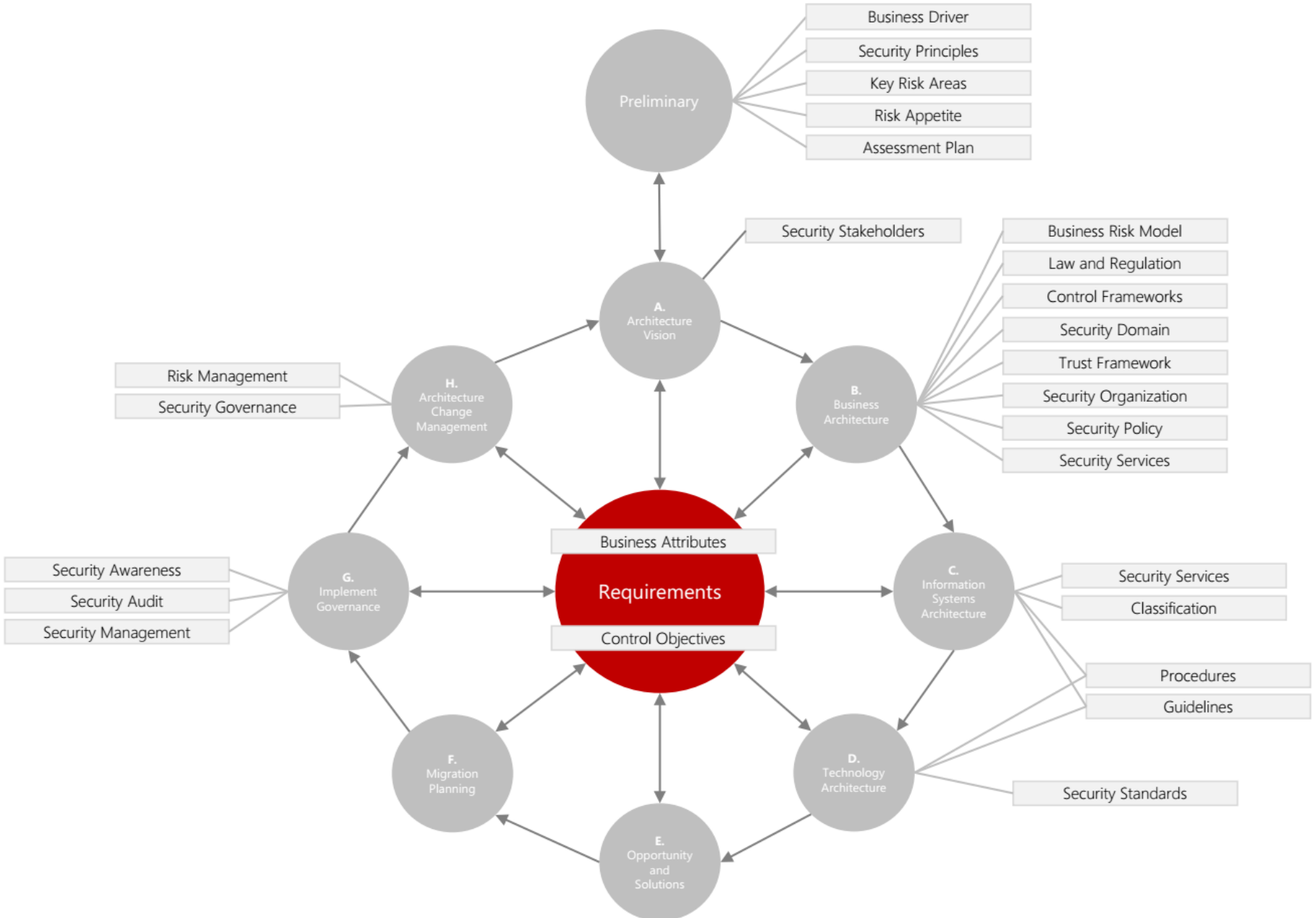
Matrix

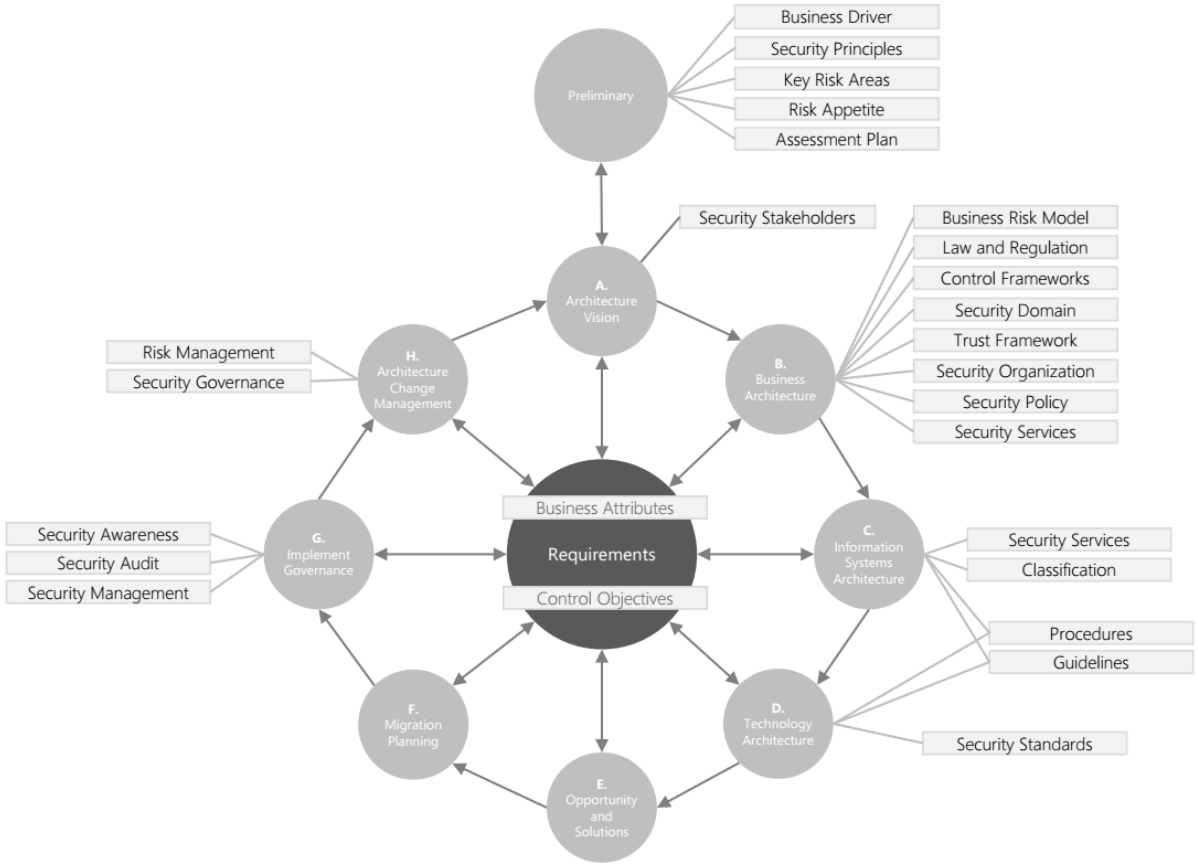
	Assets (what)	Motivation (why)	Process (how)	People (who)	Location (where)	Time (when)
Context	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Depends
	Business Asset Taxonomy, Goals, Objectives	Opportunities Exploits Threats	Inventory Of Operational Processes	Organizational Structure & Extensions	Buildings, Sites Jurisdictions, Territories	Time Dependencies with Objectives
Conceptual	Business Knowledge	Risk Management Objectives	Strategies for Assurance	Roles & Responsibilities	Domain Framework	Time Management
	Business Attributes Profile	Enablement & Control Objectives	Process Mapping Framework, Strategies	Owners, Custodians, Service Providers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
Logical	Information Assets	Risk Management Policies	Process Maps	Entity & Trusts	Domain Maps	Calendar & Timetables
	Inventory of Information Assets	Domain Policies	Information Flows, Service Architecture	Entity Schema, Trust Models, Privilege Profiles	Domain Definitions and Associations	Start Times, Lifetimes, Deadlines
Physical	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Procedures & Guidelines	Applications Systems, Security Mechanisms	User Interface, Systems, Access Control System	Host Platforms, Layouts, Network Topologies	Timing & Sequencing of Processes
Component	Compute	Risk Management Tools	Process Tools	Tools & Standards	Locator Tools	Step Timing & Sequences
	Products, Data, Repositories, Processors	Risk Analysis, Reports, Registers,	Tools, Protocols, Process Delivery	Identities, Job Descriptions, Roles, Functions	Nodes, Addresses, & other Locations	Time Schedules, Clocks, Timers, Interrupts
Service	Service Delivery	Operational Risk	Process Delivery	Personnel Management	Environment	Time & Performance
	Assurance of Operational Continuity	Risk Assessments, Monitoring, Treatment	Management & Support of Systems	Account Provisioning, User Support	Management of Building, Sites, Networks	Management of Calendar and Timetable

Metamodel


Architecture Principles, Vision, and Requirements
Preliminary
Architecture Principles
Architecture Vision
Business Strategy
Technology Strategy
Business Principles
Vision Statement
Stakeholders
Architecture Requirements
Requirements
Constraints
Assumptions
Gaps
Business Architecture
Motivation
Drivers
Goals
Objectives
Measures
Organization
Organization
Location
Actor, Role
Function
Services, Contracts
Processes, Controls
Functions
Information Systems Architecture
Data
Data Entities
Logical Data Components
Physical Data Components
Application
Information System Services
Logical Application Components
Physical Application Components
Technology Architecture
Platform Services
Logical Technology Components
Physical Technology Components
Architecture Realization
Opportunities, Solutions, and Migration Planning
Capabilities
Work Packages
Architecture Contracts
Implementation Governance
Standards
Guidelines
Specifications

Lifecycle

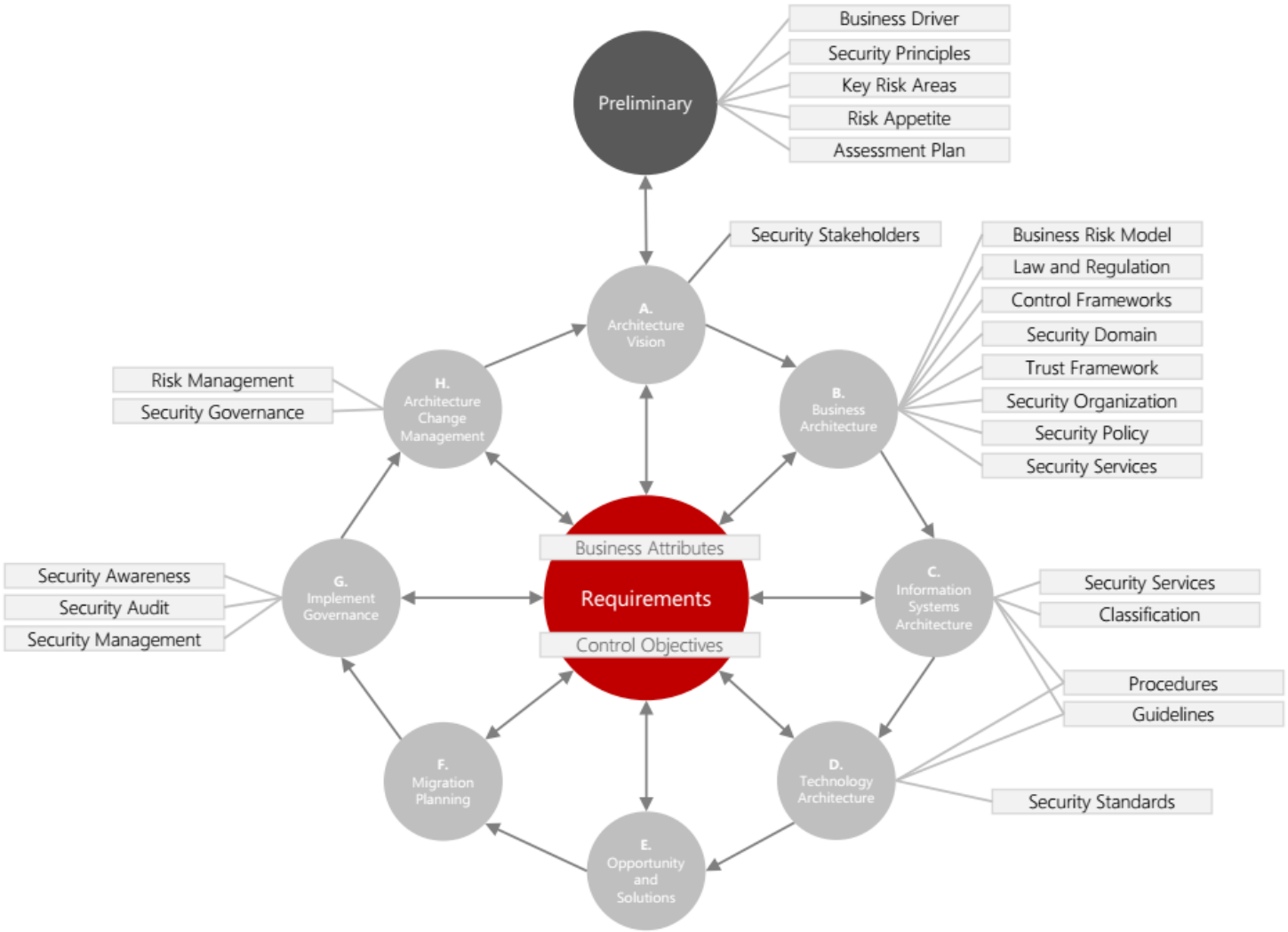

Preliminary
Business Driver
Security Principles
Key Risk Areas
Risk Appetite
Assessment Plan
A. Architecture Vision
Security Stakeholders
B. Business Architecture
Business Risk Model
Law and Regulation
Control Frameworks
Security Domain
Trust Framework
Security Organization
Security Policy
Security Services
C. Information Systems Architecture
Security Services
Classification
D. Technology Architecture
Procedures
Guidelines
Security Standards
E. Opportunity and Solutions
F. Migration Planning
G. Implement Governance
Security Awareness
Security Audit
Security Management
H. Architecture Change Management
Risk Management
Security Governance
Business Attributes
Requirements
Control Objectives



Requirements

Requirements management plays a central role in architecture work. This is recognized in both TOGAF and SABSA. The TOGAF method validates and updates business requirements in every stage of an architecture development project. However, TOGAF does not provide a concrete technique for describing or documenting requirements. In contrast, SABSA presents its unique Business Attribute Profiling technique as a means to effectively describe requirements. This section describes the use of Business Attribute Profiling with respect to security requirements management, along with the added value this technique offers for requirements management in general. Together, the TOGAF concept of validating architecture and validating and updating requirements based upon information uncovered during the development of the architecture and SABSA's Business Attribute Profiling improve requirements management, traceability, and architecture development.

Architecture in general should provide continuous alignment of capabilities with business goals and support achieving these goals in an effective and efficient manner, even when the environment or business goals change. This alignment is in many cases the major rationale for using methodologies such as TOGAF and SABSA and therefore both frameworks define a requirements management process to ensure this continuous alignment.



Preliminary

To build the security context, the following security artifacts need to be determined during this phase. These artifacts can be integrated into existing architecture documentation, but it is important that they be properly identified and that they convey the necessary information to make quality decisions:

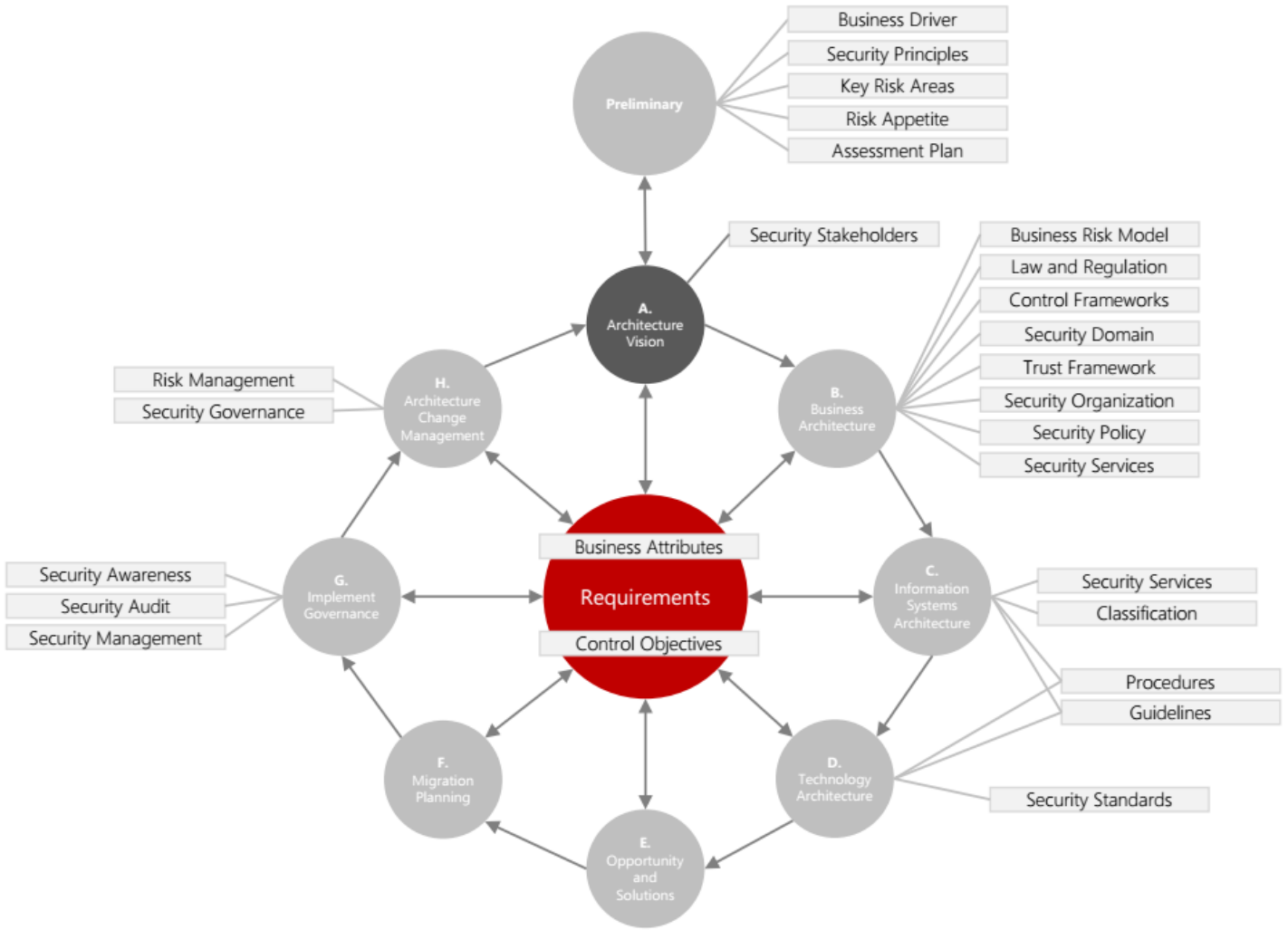
Business Drivers for Security – the subset of TOGAF business drivers impacting security, presented as an integral part of the overall architecture business drivers artifact or deliverable.

Security Principles – the subset of Business Principles addressing security architecture. This is presented as an integral part of the overall Architecture Principles artifact or deliverable. Security principles like other architecture principles will provide valuable guidance to making business decisions to comply with the enterprise's risk appetite.

Key Risk Areas – the list of the key risk areas within the architecture scope. The key risk areas should be related to the business opportunities which the security architecture enables using the risk appetite artifact which informs the balance of risk versus opportunity. The key risk area should be included in the overall architecture risk management deliverable produced during the Preliminary Phase.

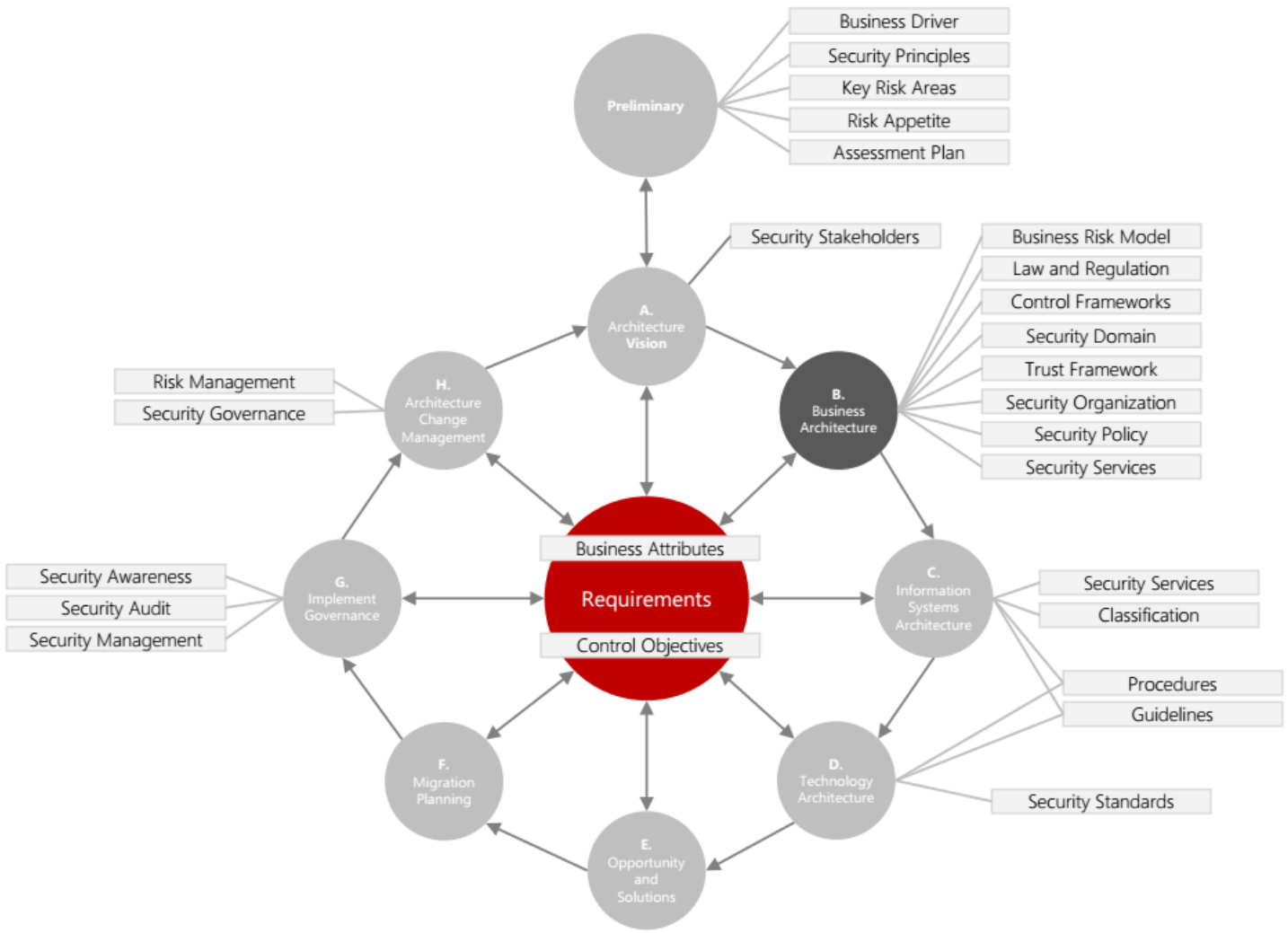
Risk Appetite – describes the enterprise's attitude towards risk and provides decision-making guidance to the organization to balance the amount of risk taken to achieve an expected outcome. The risk appetite could be expressed as, for example, a boundary on a risk/business impact and likelihood grid, profit, and loss measures or qualitative measures (zero tolerance for loss of life or regulatory compliance breaches). Risk appetite can also be represented by suitably worded security principles or produced as a stand-alone deliverable if a key stakeholder exists who needs to specifically approve it. It defines the level of risk (damage) that the organization is willing to accept and what their strategy is in defining this level. For risks above this acceptable level, it defines the strategy used for mitigation (transference, avoidance).

Security Resource Plan – based on the content of the artifacts and the characteristics of the planned architecture project, it must be decided during the Preliminary Phase which security resources are required to deliver the security elements. Finding answers to the following questions through sufficient stakeholder analysis in the Preliminary Phase can help determine the security-related effort required:



A.
Architecture Vision

Architecture Vision describes enough of the TOGAF ADM Phases B, C, and D to ensure that key stakeholders can agree to the end-state which represents a solution to a defined problem. In Phase A sufficient security-specific architecture design is carried out to... 1. Satisfy the security stakeholders that the end-state does not represent any unknown or unacceptable risk and aligns with corporate policies, standards, and principles and 2. Satisfy business stakeholders – in particular those who control the budget – that the security architecture is instrumental in enabling and supporting the overall architecture required to deliver the business opportunities and benefits identified.



B. Business Architecture

The security elements of Phase B: Business Architecture comprise business level trust, risk, and controls, independent from specific IT or other systems within the specific scope of the architecture engagement.

• Business Risk Model – the business risk model determines the cost (both qualitative and quantitative) of asset loss/impact in failure cases. It is the result of a risk assessment, based on identified threats, likelihood of materializing, and impact of an incident. Business impact should be aligned with the definitions in the Business Attribute Profile which act as pseudo-assets. Security classification should be carried out at this stage based on the risks identified. The business risk model is a detailing of the risk strategy of an organization. All information in the enterprise should have an owner and be classified against a business-approved classification scheme. The classification of the information determines the maximum risk the business is willing to accept, and the owner of the information decides what mitigation is enough for his/her information. These two aspects determine the context for the business risk model.

• Applicable Law and Regulation – determines the specific laws and regulations that apply within the scope of the enterprise architecture engagement.

• Control Frameworks – determine the suitable set of control frameworks that would best satisfy the requirements and address the risks related to the engagement scope and context.

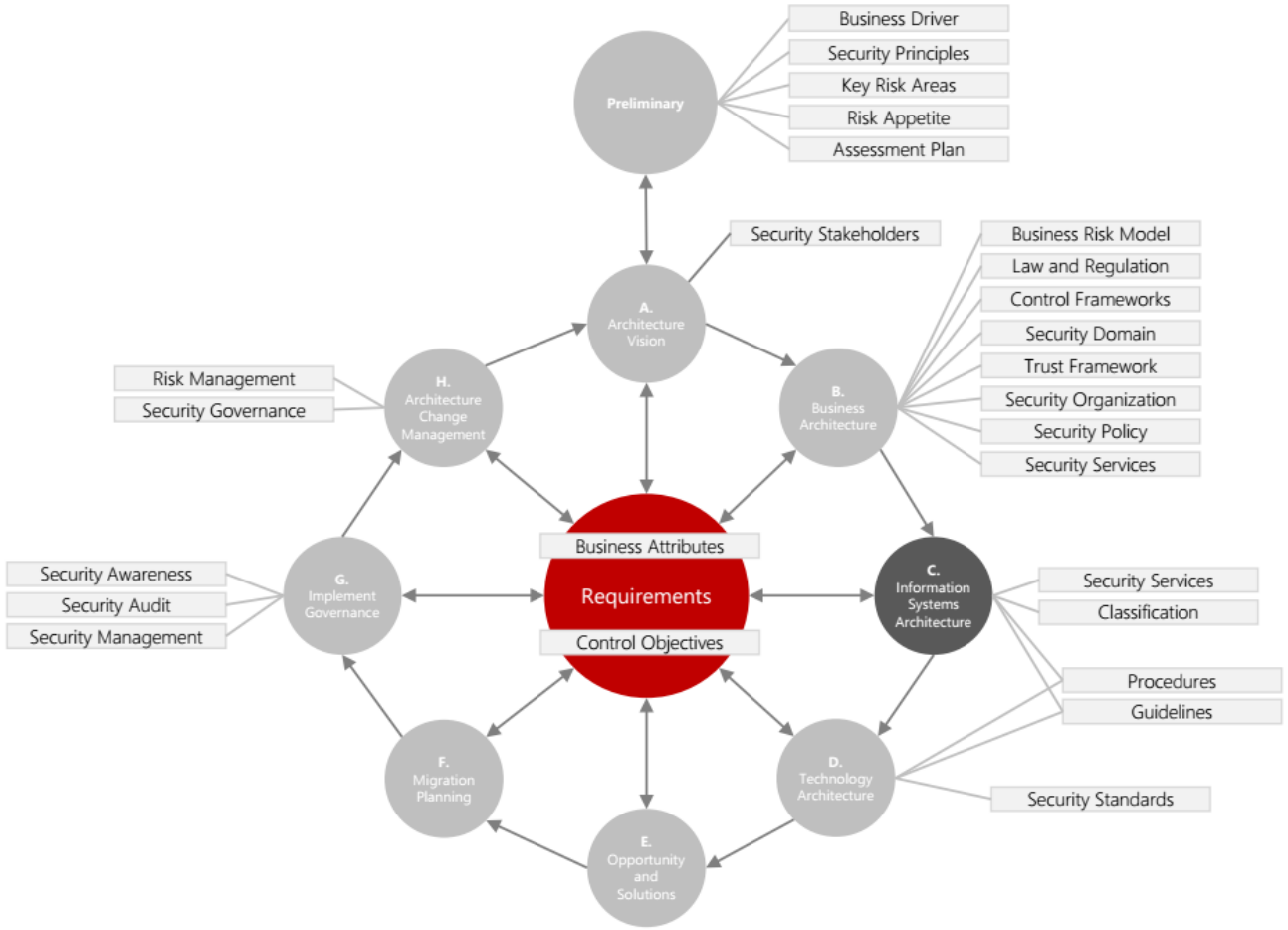
• Security Domain Model – a security domain represents a set of assets in the engagement scope which could be described by a similar set of business attributes (i.e., a security domain has a set of very similar business attributes for all entities in that domain). The security domain model describes the interactions between the various domains, parties, and actors and must be aligned with the Business Architecture model. This includes defining all people, processes, and system actors known at this stage, including third parties and external actors. The security domain model helps in defining responsibility areas, where responsibility is exchanged with external parties and distinguishes between areas of different security levels and can inform the engagement scope.

• Trust Framework – the trust framework describes trust relationships between various entities in the security domain model and on what basis this trust exists. Trust relationships can be unidirectional, bidirectional, or non-existent. The onus for assessing trust is the responsibility of those choosing to enter into the contracts and their legal counsel. It is important to note that technology (e.g., digital certificates, SAML, etc.) cannot create trust, but can only convey in the electronic world the trust that already exists in the real world through business relationships, legal agreements, and security policy consistencies.

• Security Organization – the corporate organization of risk management and information security which assigns ownership of security risks and defines the security management responsibilities and processes. Security management processes include risk assessment, the definition of control objectives, the definition and proper implementation of security measures, reporting about security status (measures defined, in place, and working) and the handling of security incidents.

• Security Policy – the security policy addresses the alignment of operational risk management in general with the various security aspects such as physical security, information security, and business continuity. Within the scope of the architecture engagement, decide which existing policy elements can be re-used or have to be developed new.

• Security Services – a list of security-related business services, defined as part of the Business Services.

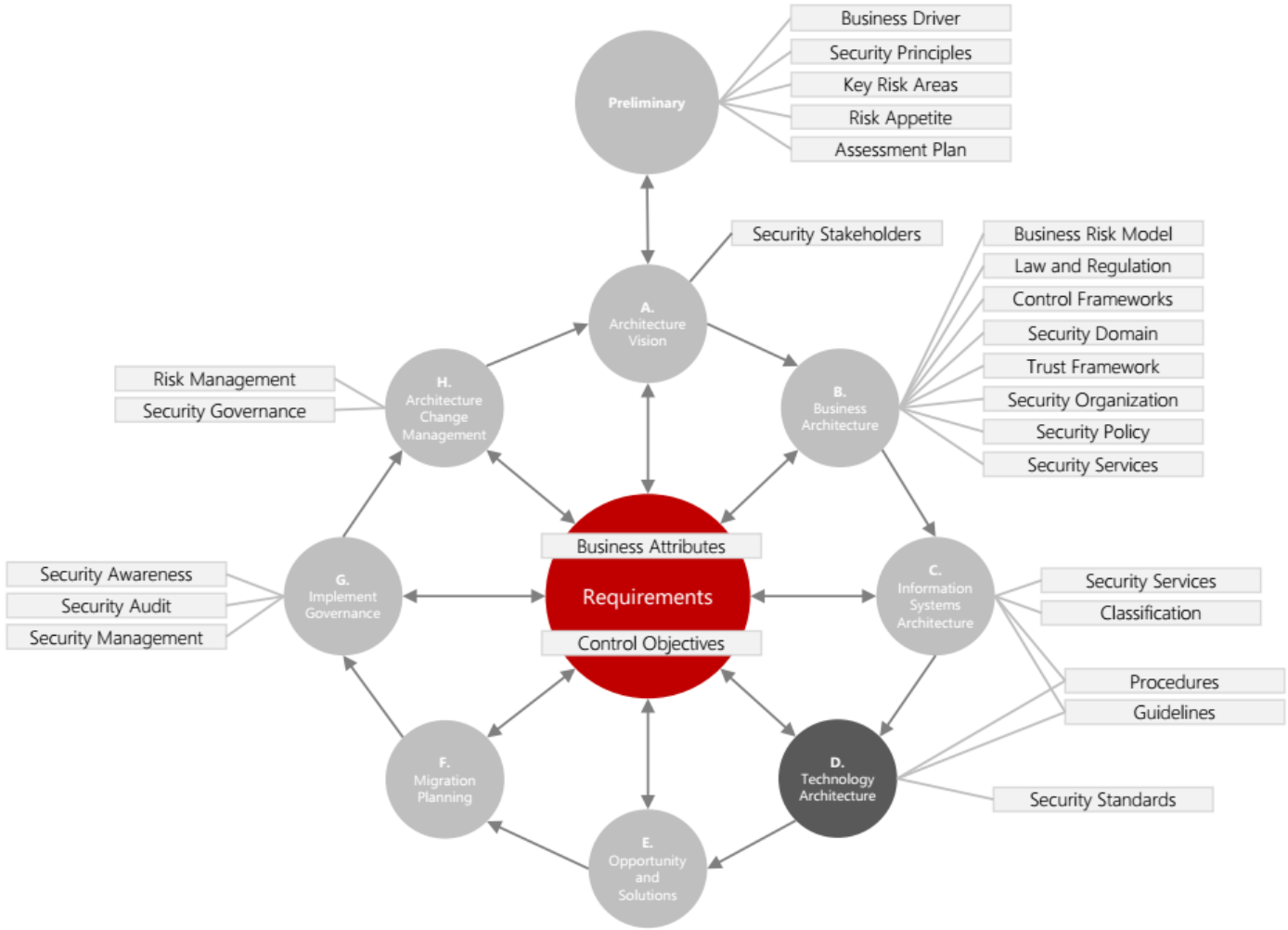


C. Information Systems Architecture

The security elements of Phase C: Information Systems Architectures comprise information system-related security services and their security classification.

- Classification of Services – the assignment of a security classification to the list of services in the Information System Services catalog according to the enterprise classification scheme. In most cases this scheme is defined and described in the corporate information security policy and is based on the information processed or stored by the service.

- Security Rules, Practices, and Procedures – are relevant artifacts for solution-level architectures. They are mentioned here because at the solution architecture level guidelines and designs for rules, practices, & procedures are expected to be produced in Phase C & D.



D. Technology Architecture

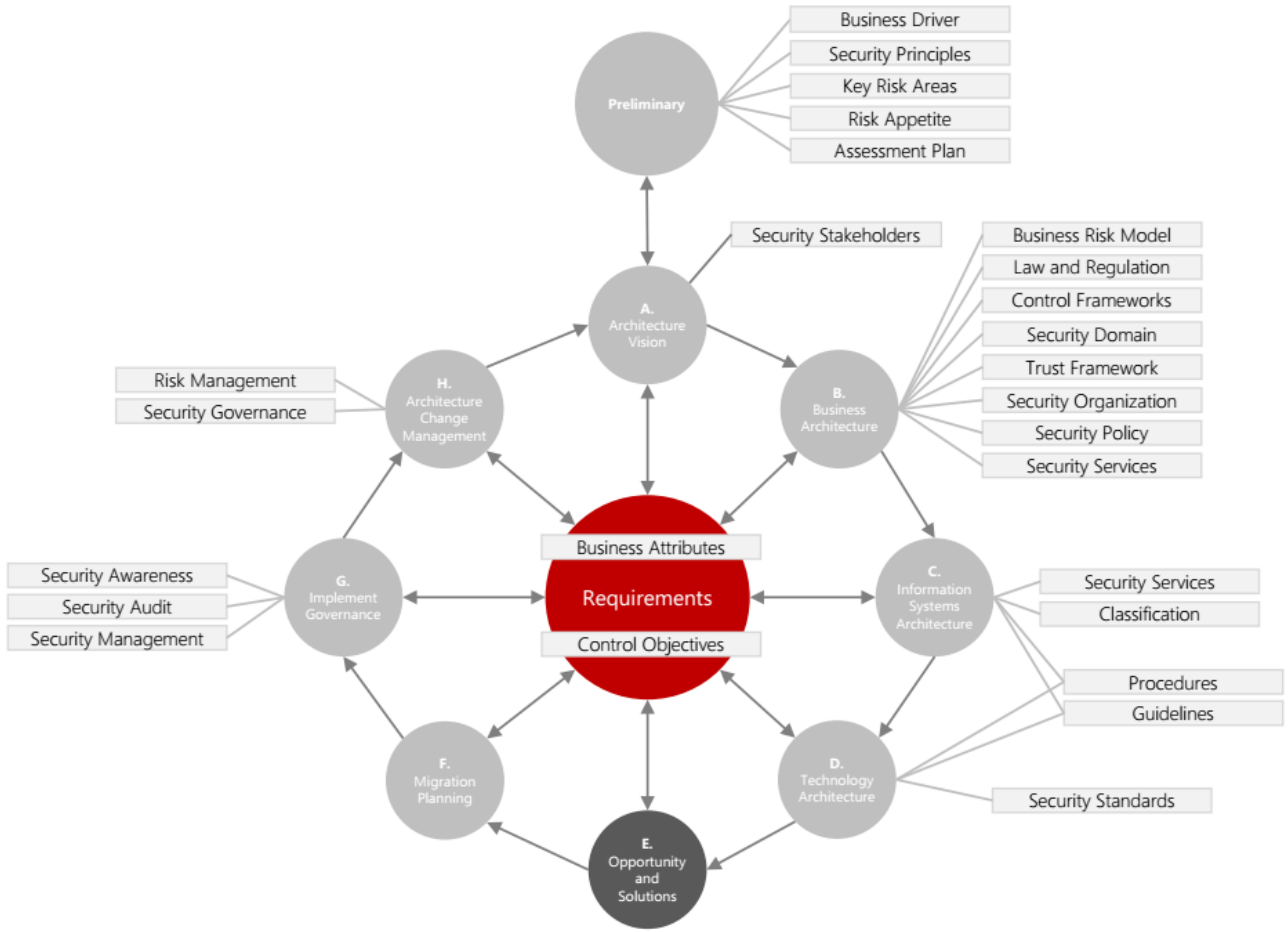
The security elements of Phase D: Technology Architecture comprise security rules, practices and procedures, and security standards:

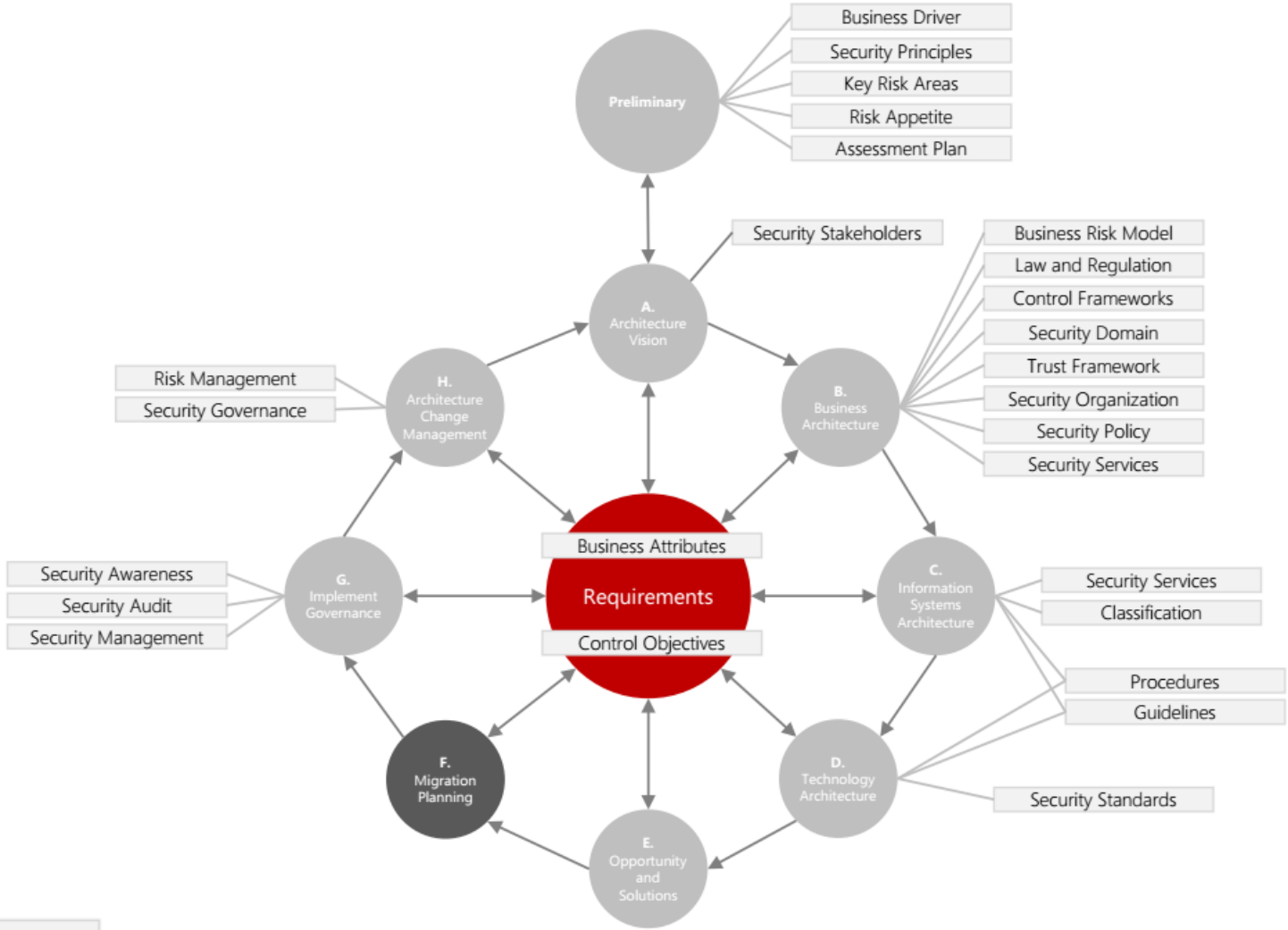
- Security Rules, Practices, and Procedures – artifacts mainly relevant for solution-level architectures, mentioned here because at solution architecture level guidelines and designs for rules, practices, and procedures are expected to be produced in Phase C and D.

- Security Standards – guide or mandate the use of technical, assurance, or other relevant security standards. The artifact is expected to comprise publicly available standards such as Common Criteria, TLS, and SAML.

E. Opportunity and Solutions

No specific security-related architecture artifacts are produced in this phase. However, in defining the roadmap and deciding which architecture elements must be implemented first, it is imperative that the security risks are evaluated and that risk owners are consulted when defining the place on the roadmap for high priority mitigations. This phase could also be used to verify the process and results, feeding back to the business goals and drivers.





F.
Migration Planning

No specific security architecture aspects apply to this phase; however, as part of the overall planning care must be taken to ensure that, for each stage on the roadmap, appropriate risks and associated controls are identified.

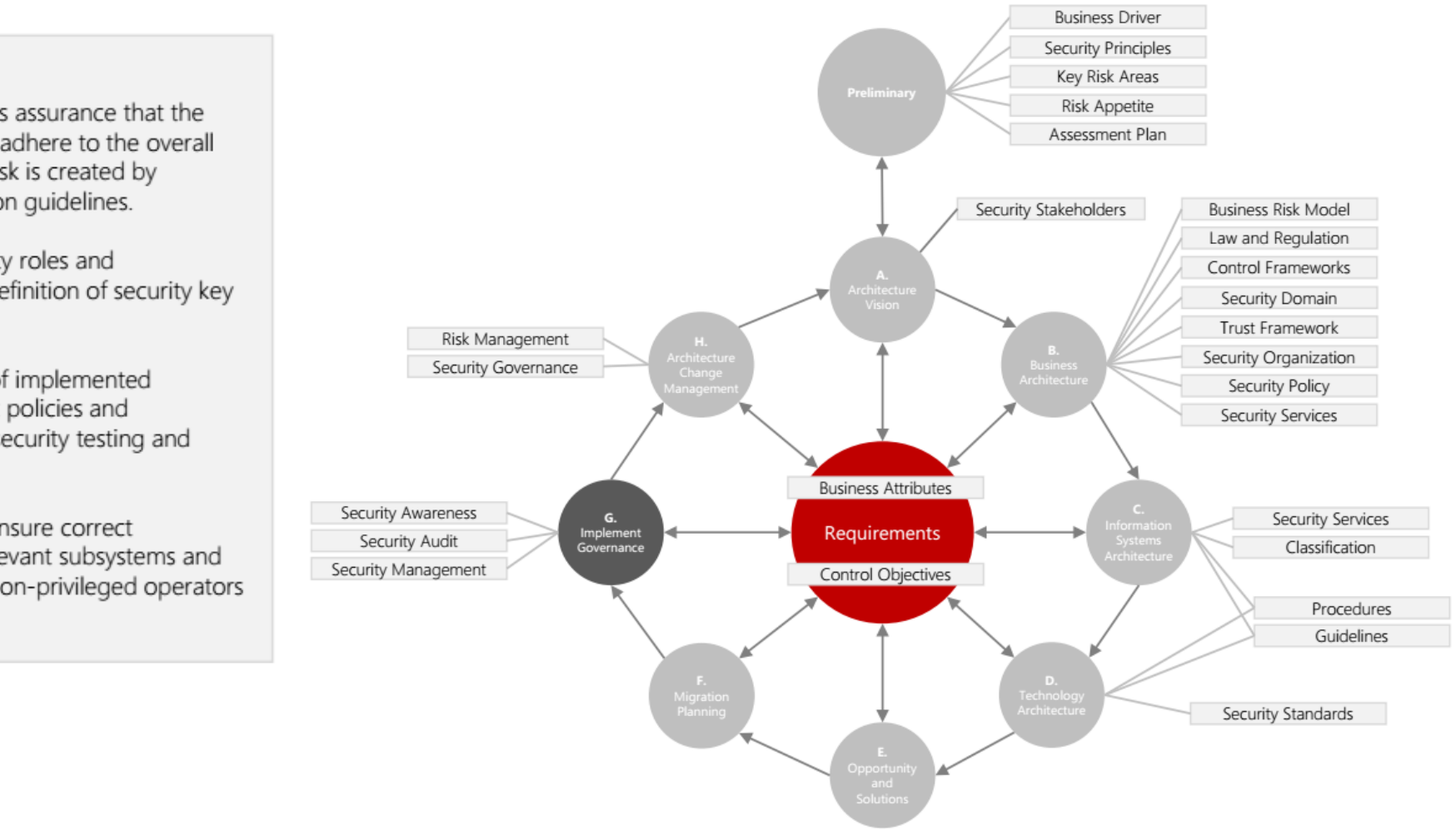
G. Implement Governance

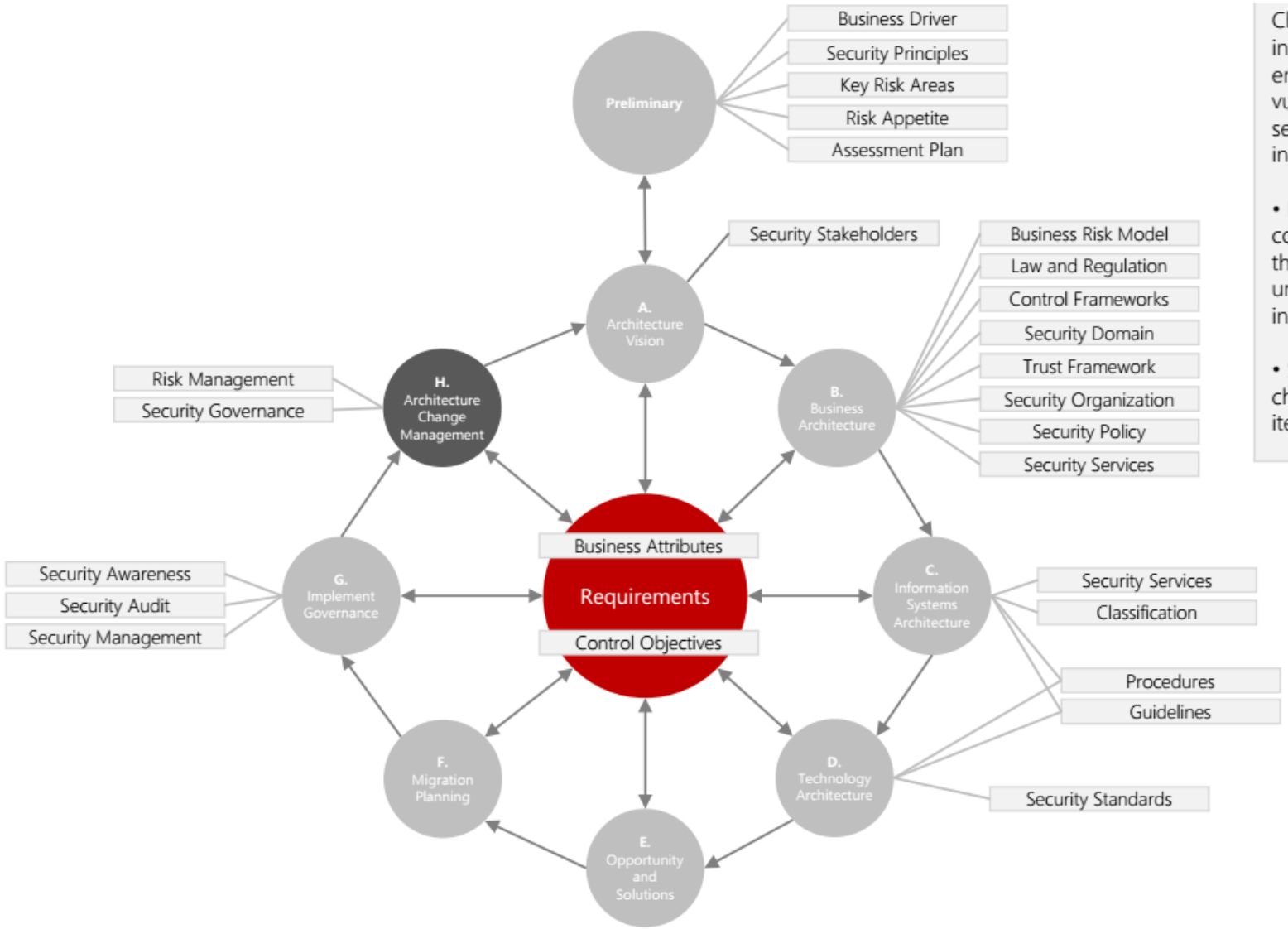
Security architecture implementation governance provides assurance that the detailed design and implemented processes and systems adhere to the overall security architecture. This ensures that no unacceptable risk is created by deviations from Architecture Principles and implementation guidelines.

• Security Management – definition of the detailed security roles and responsibilities, implementation of security governance, definition of security key performance and risk indicators, etc.

• Security Audit – reports which include security reviews of implemented processes, technical designs, and developed code against policies and requirements, and security testing comprising functional security testing and penetration testing.

• Security Awareness – implement necessary training to ensure correct deployment, configuration, and operations of security-relevant subsystems and components; ensure awareness training of all users and non-privileged operators of the system and/or its components.





Change is driven by new requirements or changes in the environment. Changes in security requirements can, for instance, be caused by changes in the threat environment, changed compliance requirements, or changes due to discovered vulnerabilities in the existing processes and solutions. Changes required due to security-related causes are often more disruptive than a simplification or incremental change.

- Risk Management – the process in which the existing architecture is continuously evaluated regarding changes to business opportunity and security threat. If based on the results of this process, the current architecture is deemed unsuitable to mitigate changed or new risks or constrains the business too much in exploiting new opportunities, a decision on architecture change must be made.

- Security Architecture Governance – the process in which decisions are made on changes to the existing architecture, either by minor changes in the current iteration or by means of a completely new iteration.

INFORMATION GOVERNANCE

- Why is Information Governance important?

Architecture will define the way. Governance will keep you on the path.

What does Information Governance mean?

Simple.

Organized.

Consistent.

Reliable.

Educated.

Measured.

Simple.

Policy	High-level statement of requirements. A security policy is the primary way in which management's expectations for security are provided to the builders, installers, maintainers, and users of an organization's information systems.
Standards	Specify how to configure devices, how to install and configure software, and how to use computer systems and other organizational assets, to be compliant with the intentions of the policy.
Procedures	Specify the step-by-step instructions to perform various tasks in accordance with policies and standards.
Guidelines	Advice about how to achieve the goals of the security policy, but the are suggestions, not rules. They are an important communication tool to let people know how to follow the policy's guidance or They convey best practices

Organized.

Standard

- Objectives
- Responsibilities
- Scope
- Measurement

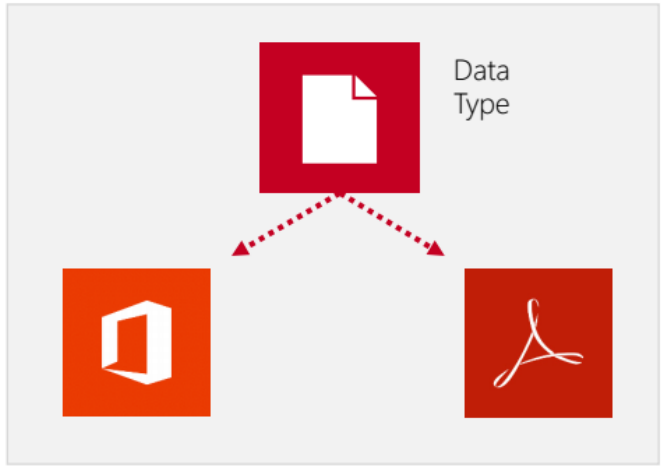
Procedures

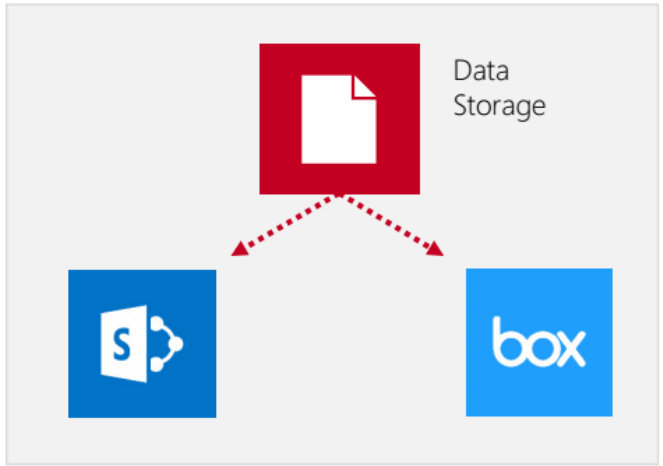
- Procedures for Activity 1
- Procedures for Activity 2
- Procedures for Activity 3
- Procedures for System 1
- Procedures for System 2
- Procedures for Process 1
- Procedures for Process

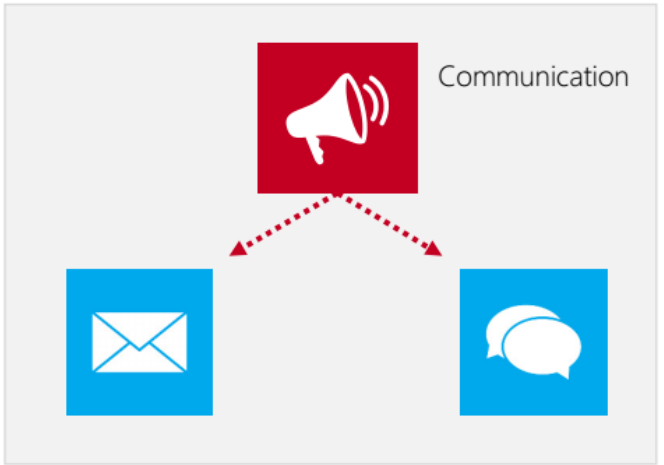
Guidelines

- Templates
- Flowcharts
- Best Practice
- Research
- Scenarios
- Visual Aids

Consistent.







Reliable.

Consistent Performance Metrics

Reduction in Risks

Proactive Users

Educated.

Clear and Concise Definitions

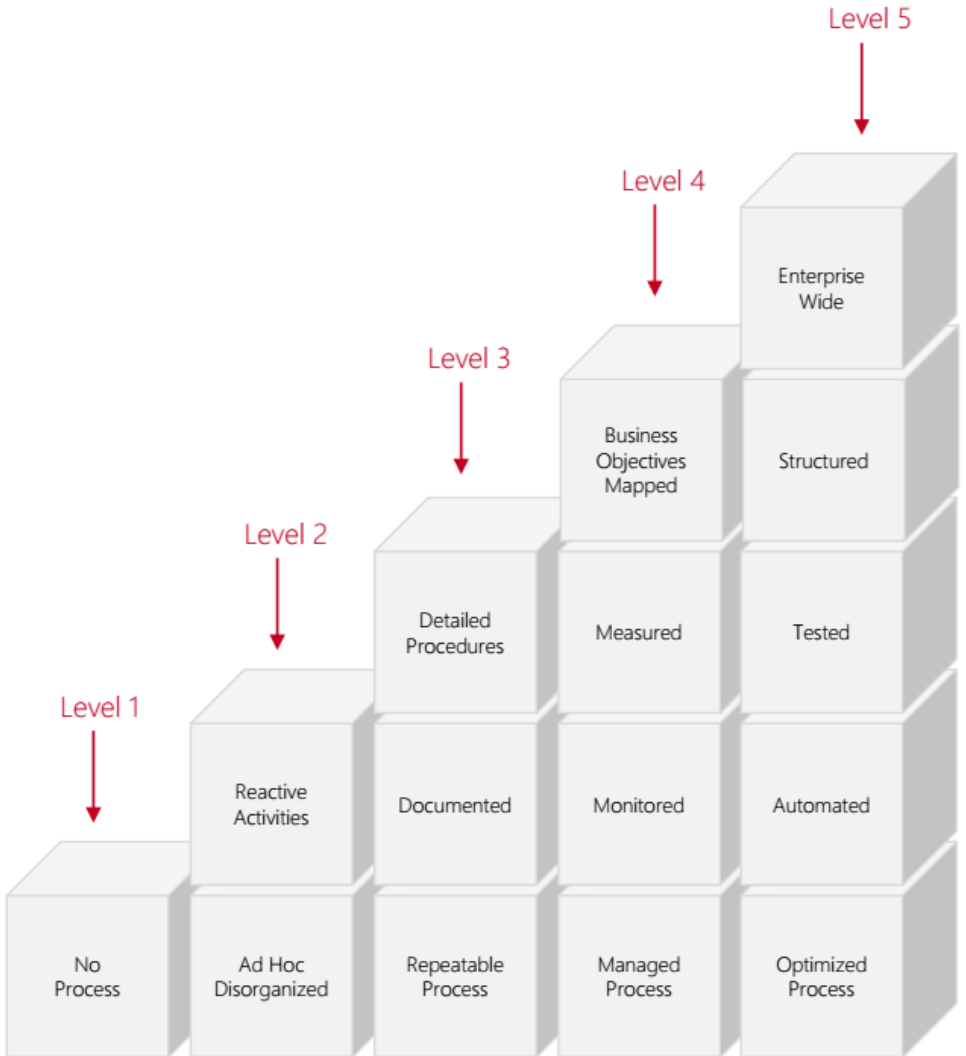
Effective Communicating

End User Awareness

Measured.

CAPABILITY MATURITY MODEL

Level 5 Optimizing	It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.
Level 4 Managed	It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.
Level 3 Defined	It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.
Level 2 Repeatable	It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.
Level 1 Initial (Chaotic)	It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.



Question

Conclusion

- The translation of the businesses vision and strategy into effective enterprise change by creating, communicating and improving the key requirements, principles and models that describe the enterprise's future information security state and enable its evolution.
- The discipline and framework to ensure simplicity, organization, consistency, reliability, education, and measurements are well-articulated and achievable.
- Enterprise Security Architecture + Information Governance = Successful & Robust Information Security Management Program