TOGAF® Series Guide

Integrating Risk and Security within a TOGAF® Enterprise Architecture

Prepared by the Security Forum, a Forum of The Open Group®, in collaboration with The SABSA® Institute

TOGAF® Series Guide

Integrating Risk and Security within a TOGAF® Enterprise Architecture

ISBN: 1-937218-66-9

Document Number: G152

Published by The Open Group, April 2022.
Figure 1 corrected March 2023 to reinstate the underscores, as mentioned in the preceding text.

This document was originally published in March 2016 by The Open Group Security Forum, in collaboration with The SABSA® Institute, having completed its Company Review in September 2015. It was republished in April 2019 to align with the TOGAF Standard, Version 9.2.

In 2019, it was agreed to reclassify the document as a TOGAF Series Guide. This TOGAF Series Guide does not change the content of the previous edition(s).

Comments relating to the material contained in this document may be submitted to:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. With more than 870 member organizations, we have a diverse membership that spans all sectors of the technology community – customers, systems and solutions suppliers, tool vendors, integrators and consultants, as well as academics and researchers.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry's premier certification service and encouraging procurement of certified products

Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, most of which is focused on development of Standards and Guides, but which also includes white papers, technical studies, certification and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/library.

The SABSA® Institute

The SABSA Institute is the professional member and certification body for Enterprise Security Architects of all specialisms and at all career levels. It governs the ongoing development and management of SABSA intellectual property and the associated certification and education programs worldwide.

The SABSA Institute envisions a global business world of the future, leveraging the power of digital technologies, enabled in the management of information risk, information assurance, and information security through the adoption of SABSA as the framework and methodology of first choice for commercial, industrial, educational, government, military, and charitable enterprises, regardless of industry sector, nationality, size, or socio-economic status, and leading to enhancements in social well-being and economic success.

Further information on The SABSA Institute can be found at www.sabsa.org.

The TOGAF® Standard, a Standard of The Open Group

The TOGAF Standard is a proven enterprise methodology and framework used by the world's leading organizations to improve business efficiency.

This Document

This document is a TOGAF® Series Guide to Integrating Risk and Security within a TOGAF Enterprise Architecture. It provides guidance for security practitioners and Enterprise Architects who need to work with the TOGAF Standard, a standard of The Open Group, to develop an Enterprise Architecture. It has been developed and approved by The Open Group Security Forum.

Integrating security and risk management in Enterprise Architecture strongly supports The Open Group vision of Boundaryless Information Flow™, by informing well-justified design decisions, which maximize business opportunity whilst minimizing business risk.

This document is structured as follows:

- Chapter 1 provides a high-level introduction to this Guide, introducing the topic of Enterprise Security Architecture, how it relates to Enterprise Architecture, and how this Guide supports the TOGAF Standard
- Chapter 2 describes the relationship with other IT security and risk standards
- Chapter 3 describes the concept of Enterprise Security Architecture in detail; it describes Information Security Management (ISM) and Enterprise Risk Management (ERM), two processes used by Security Architects
- Chapter 4 describes Security Architecture, which is a cross-cutting concern, pervasive through the whole Enterprise Architecture
- Chapter 5 explains in detail the core security concepts and how they can be applied for each phase of the TOGAF ADM

The intended audience for this document is as follows:

- Enterprise Architects, Security Architects

More information is available, along with a number of tools, guides, and other resources, at www.opengroup.org/architecture.

About the TOGAF® Series Guides

The TOGAF® Series Guides contain guidance on how to use the TOGAF Standard and how to adapt it to fulfill specific needs.

The TOGAF® Series Guides are expected to be the most rapidly developing part of the TOGAF Standard and are positioned as the guidance part of the standard. While the TOGAF Fundamental Content is expected to be long-lived and stable, guidance on the use of the TOGAF Standard can be industry, architectural style, purpose, and problem-specific. For example, the stakeholders, concerns, views, and supporting models required to support the transformation of an extended enterprise may be significantly different than those used to support the transition of an in-house IT environment to the cloud; both will use the Architecture Development Method

(ADM), start with an Architecture Vision, and develop a Target Architecture on the way to an Implementation and Migration Plan. The TOGAF Fundamental Content remains the essential scaffolding across industry, domain, and style.

Trademarks

ArchiMate, DirecNet, Making Standards Work, Open O logo, Open O and Check Certification logo, Platform 3.0, The Open Group, TOGAF, UNIX, UNIXWARE, and the Open Brand X logo are registered trademarks and Boundaryless Information Flow, Build with Integrity Buy with Confidence, Commercial Aviation Reference Architecture, Dependability Through Assuredness, Digital Practitioner Body of Knowledge, DPBoK, EMMM, FACE, the FACE logo, FHIM Profile Builder, the FHIM logo, FPB, Future Airborne Capability Environment, IT4IT, the IT4IT logo, O-AA, O-DEF, O-HERA, O-PAS, Open Agile Architecture, Open FAIR, Open Footprint, Open Process Automation, Open Subsurface Data Universe, Open Trusted Technology Provider, OSDU, Sensor Integration Simplified, SOSA, and the SOSA logo are trademarks of The Open Group.

COBIT is a registered trademark of ISACA, registered in the United States and other countries.

SABSA is a registered trademark of The SABSA Institute.

All other brands, company, and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

Acknowledgements

(Please note affiliations were current at the time of approval.)

The Open Group gratefully acknowledges the contribution of the following people in the development of this Guide (in alphabetical order):

- Geoff Besko, Seccuris: Co-lead
- Randy Caraway, HP
- Piotr Ciepiela, Ernst & Young
- Pascal de Koning, i-to-i: Co-lead
- Thorbjørn Ellefsen, DIFI
- Brian Golumbeck, HP
- Kirk Hansen, Kirk Hansen Consulting
- Jim Hietala, The Open Group: VP, Business Development and Security
- David Hornford, Conexiam
- Andrew Josey, The Open Group: VP, Standards and Certification
- Christian Mark, IBM Security: Co-lead
- Robert Martin, MITRE
- Martin W. Murhammer, IBM
- Matthew Olsen, Ernst & Young
- Miroslaw Ryba, Ernst & Young
- John Sherwood, Founder, The SABSA Institute: Lead SABSA Contributor
- John Sluiter, PricewaterhouseCoopers (PwC)
- Eric Stephens, Oracle
- Tony Yin, HP

Where appropriate, this Guide includes excerpts from the SABSA® Blue Book [2] and the TOGAF® and SABSA® Integration White Paper [13], with the full approval and permission of The SABSA Institute.

Referenced Documents

The following documents are referenced in this TOGAF® Series Guide:

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

[1] The TOGAF® Standard, 10th Edition, a standard of The Open Group (C220), published by The Open Group, April 2022; refer to: www.opengroup.org/library/c220.

[2] SABSA® Blue Book: Enterprise Security Architecture: A Business-Driven Approach, by John Sherwood, Andy Clark, David Lynas, 2005.

[3] The SABSA® Institute: www.sabsa.org.

[4] ISO/IEC 27001:2013: Information Security Management; refer to: www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[5] ISO/IEC 27002:2013: Information Technology – Security Techniques – Code of Practice for Information Security Controls; refer to: www.iso.org/iso/catalogue_detail?csnumber=54533.

[6] ISO 31000:2009: Risk Management – Principles and Guidelines; refer to: www.iso.org/iso/home/standards/iso31000.htm.

[7] IEC 31010:2009: Risk Management – Risk Assessment Techniques; refer to: www.iso.org/iso/catalogue_detail?csnumber=51073.

[8] ArchiMate® 3.1 Specification, a standard of The Open Group (C197), published by The Open Group, November 2019; refer to: www.opengroup.org/library/c197.

[9] Open Information Security Management Maturity Model (O-ISM3), a standard of The Open Group (C102), published by The Open Group, February 2011; refer to: www.opengroup.org/library/c102.

[10] Control Objectives for Information and Related Technology (COBIT®), Version 5.0, IT Governance Institute, 2012.

[11] An Enterprise Architecture and Data Quality Framework, Jerome Capirossi, NATEA Consulting and Pascal Rabier, La Mutuelle Generale, 2007; accessed at: http://innovation-regulation2.telecom-paristech.fr/wp-content/uploads/2007/05/DEDM13_An-Enterprise-Architecture-and-Data-quality-framework.pdf.

[12] Modeling Enterprise Risk Management and Security with the ArchiMate® Language, White Paper (W150), published by The Open Group, January 2015; refer to: www.opengroup.org/library/w150.

[13] TOGAF® and SABSA® Integration: How SABSA and TOGAF complement each other to create better architectures, White Paper (W117), published by The Open Group, October 2011; refer to: www.opengroup.org/library/w117.

[14] Open Enterprise Security Architecture (O-ESA): A Framework and Template for Policy-Driven Security, The Open Group Guide (G112), published by Van Haren Publishing, April 2011; refer to: www.opengroup.org/library/g112.

[15] Risk Taxonomy (O-RT) Version 2.0, a standard of The Open Group (C13K), published by The Open Group, October 2013; refer to: www.opengroup.org/library/c13k.

[16] Risk Analysis (O-RA), a standard of The Open Group (C13G), published by The Open Group, October 2013; refer to: www.opengroup.org/library/c13g.

1 Introduction

Enterprise Architecture (including Security Architecture) is all about aligning business systems and supporting information systems to realize business goals in an effective and efficient manner (systems being the combination of processes, people, and technology). One of the important quality aspects of an Enterprise Architecture is information security and the way this can be managed. For too long, information security has been considered a separate discipline, isolated from the business processes and Enterprise Architecture.

A Security Architecture is a structure of organizational, conceptual, logical, and physical components that interact in a coherent fashion in order to achieve and maintain a state of managed risk and security (or information security). It is both a driver and enabler of secure, safe, resilient, and reliable behavior, as well as for addressing risk areas throughout the enterprise.

However, an Enterprise Security Architecture does not exist in isolation. As part of the enterprise, it builds on enterprise information that is already available in the Enterprise Architecture, and it produces information that influences the Enterprise Architecture. This is why a close integration of Security Architecture in the Enterprise Architecture is beneficial. In the end, doing it right the first time saves costs and increases effectiveness compared to bolting on security afterwards. To achieve this, Security Architects and Enterprise Architects need to speak the same language. That language is introduced in this Guide, which describes how to integrate security and risk into an Enterprise Architecture. It provides guidance for both security practitioners and Enterprise Architects working with the TOGAF® standard, a standard of The Open Group [1], to develop an Enterprise Architecture.

Figure 1 summarizes this Guide. It shows how Enterprise Architecture and Enterprise Security Architecture relate to each other, highlighting the core security and risk concepts that are used in Information Security Management (ISM) and Enterprise Risk Management (ERM). These concepts are listed in the center column, and form a set of foundation concepts that complement and enhance the TOGAF Standard. Concepts with an underscore in the figure are additions to the TOGAF framework and brought in by ISM or ERM.

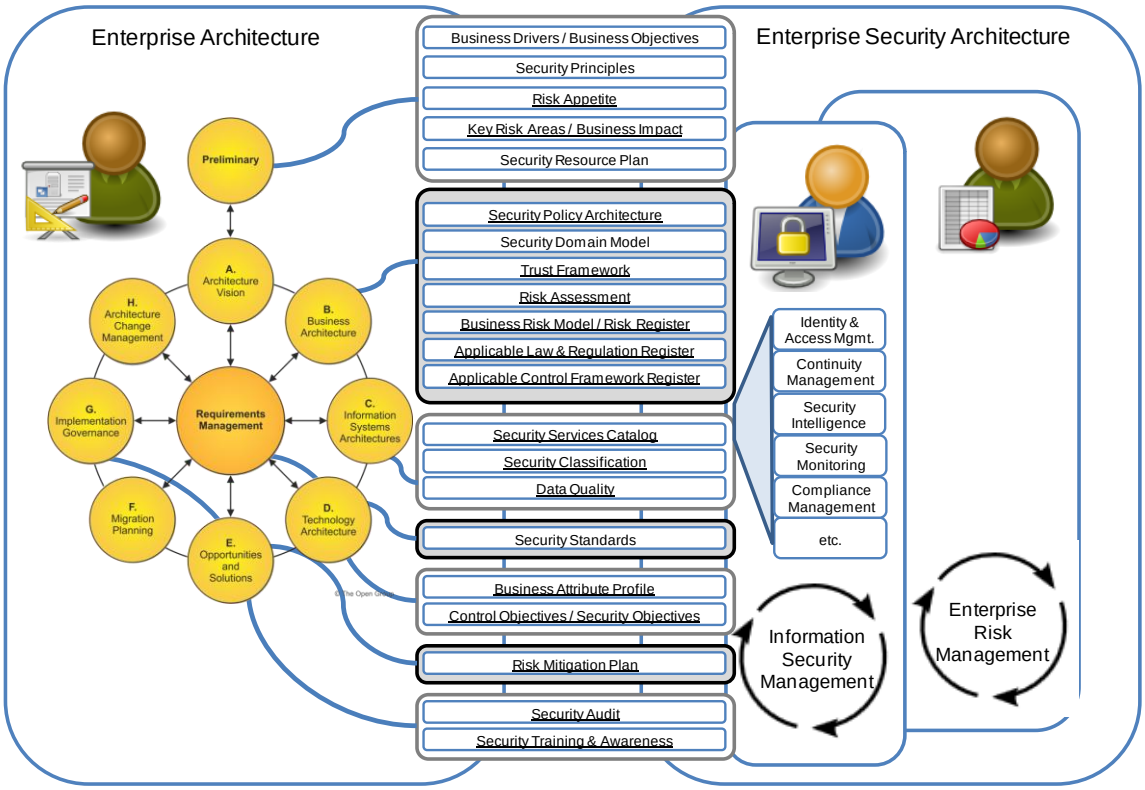

Figure 1: Essential Security and Risk Concepts and their Position in the TOGAF ADM

1.1 How does this Guide Support the TOGAF Standard?

This new content takes the security activities in the current TOGAF Standard [1] to a higher conceptual level. The goal of this approach is to explain how the TOGAF method and framework can be tailored to make use of an existing Enterprise Security Architecture in order to address security and risk properly.

This approach is business-driven and supports the integration of two processes: ISM and ERM. This process orientation will improve understanding of the security concepts and activities at different phases through the TOGAF Architecture Development Method (ADM). The business orientation will contribute to justification of the security components.

In this approach, it is foreseen that a lot of additional security practitioner guidance needs to be developed. This Guide provides the basis for that work. By using a common foundation this will deliver an internally consistent and practical way of working.

1.2 What about Risk Management?

Risk management in the TOGAF Standard primarily focuses on architecture project risk. This is only one type of risk. The scope of ERM, as presented in this Guide as part of the Enterprise Security Architecture, is much broader. It includes business, system, information, project, privacy, compliance, and organizational change risk, among other categories, too.

This Guide describes the broader concepts of ERM and how to integrate them into the TOGAF Standard. In particular, this work focuses on all aspects of operational risk – the risks that a business faces in day-to-day operations that are based on operational capabilities that are produced as the result of Enterprise Architecture work. It is intended that by paying more attention to operational risk downstream of the delivery of Enterprise Architecture work products, the utility, quality, and effectiveness of those work products will be improved and enhanced.

The Enterprise Security Architecture contains a balanced view on risk: negative consequences are kept to an acceptable level and positive opportunities are exploited to their maximum. The business-driven approach is key for the Security Architecture: business drivers offer the context for risk assessments; they define whether compliance with any control framework is necessary, and they justify the need for security measures.

This Guide is explicitly looking at risk within the context of best practice ERM. It is written for practitioners who expect to use best practices and are prepared to read and consider carefully the language within a profession. Like all professions, the risk management profession evolves and improves. Central to best practice ERM is a very precise definition of the term "risk". Over the last 15 years risk management has moved the professional definition from thought leadership, to leading practice, to well established best practice. Risk definition is embedded within mainstream risk management international standards, such as ISO 31000:2009 [6], best practice guides, and derived industry-specific guides, such as the Global Association of Risk Professionals Financial Risk Manager certification.

There is a difference between the commonly accepted definition of "risk" and the risk management professional definition of the term. Within the risk management profession "risk" is defined to be the "*effect that uncertainty has on the achievement of business objectives*". For many information security practitioners, this definition can feel uncomfortable: In their discipline, "risk" is usually regarded as threat-bound and therefore a negative attribute.

Since this Guide is aimed at the core concepts of the TOGAF Standard as an Enterprise Architecture framework, the definition of risk used is as defined in ISO 31000:2009. This definition allows for the usage of the term in subsequent practitioner guidance that focuses only on the narrower usage of risk as a negative; for example, in the information security risk management area, where the uncertainties are generally always negative outcomes.

1.3 Where is the Controls Checklist?

First of all, integrating security is not a matter of selecting controls from a checklist. We advocate a holistic approach towards security, so that a trustworthy, robust, reliable, secure, and risk-managed architecture is delivered. To do this, the Enterprise Security Architecture makes sure that tight cooperation is obtained between the ADM and the processes for ISM and ERM. Therefore, most of the security concepts in this Guide refer to things needed to set up security properly.

However, designing the operational security is part of the architecture as well. In the architecture context, security controls are bundled into security services. A security service can be seen as an Architecture Building Block (ABB). In the TOGAF Standard, ABBs capture architecture requirements that both direct and guide the development of Solution Building Blocks (SBBs). This can apply to all four of the TOGAF domain architectures: Business, Data, Application, and

Technology. In the same way, security services capture security requirements and guide the development of sub-services and components.

Examples of security services are:

- Identity & Access Management
- Continuity Management
- Security Intelligence
- Digital Forensics
- Audit
- Network Monitoring
- Compliance Management
- Training & Awareness Programs, etc.

The security services are positioned in the logical layer of the SABSA® architecture framework, which is developed in Phase C (Information Systems Architectures) of the TOGAF ADM. The Security Services Catalog provides the actual description of those security services.

To support security practitioners in actually designing and using the security services, a Security Services Catalog is needed. For Security Architects, the Security Services Catalog is a register that supports filling in the logical layer of the SABSA architecture framework with security controls. Unlike existing control frameworks that contain requirements, the Security Services Catalog describes security building blocks that actually deliver protection. This architecture approach enables smooth integration of information security in the Enterprise Architecture.

The standardized approach contributes to the professionalization of the security management organization and facilitates a more efficient, cost-effective way of working. One of the main advantages of the Security Services Catalog is that offers a common terminology and reference framework for the domain of security management allowing better cooperation between the parties concerned.

2 Relationship to Other IT Security and Risk Standards

This chapter documents relationships among selected standards in this subject area.

2.1 ISO/IEC 27001:2013: Information Security Management

"*ISO/IEC 27001:2013 is a standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.*" [4]

The core concepts of ISO/IEC 27001:2013 are taken as a basis for the ISM process in this Guide. This explains a sound security management process and helps readers to understand the logic behind specific risk concepts that are needed in the TOGAF framework. However, no fixed mapping has been made to that standard. It is seen as one of the good references that is very useful for this work.

2.2 ISO 31000:2009: Risk Management – Principles and Guidelines

ISO 31000:2009 [6] sets out principles, a framework, and a process for the management of risk that are applicable to any type of organization in the public or private sector. It does not mandate a "one size fits all" approach, but rather emphasizes the fact that the management of risk must be tailored to the specific needs and structure of the particular organization. It has a related standard IEC 31010:2009 [7] that describes examples of qualitative risk assessment methods.

The core concepts of ISO 31000:2009 are taken as a basis for the ERM process in this Guide. Just as with ISO/IEC 27001:2013, no fixed mapping has been made to that standard but it is seen as one of the good references that is very useful for this work.

2.3 National Cybersecurity Frameworks

Internationally there are many country-specific cybersecurity standards. A leading example is the NIST Cybersecurity Framework, introduced in 2014. This framework aims to help organizations in critical infrastructure sectors to reduce risk, and protect their critical infrastructure. The NIST Cybersecurity Framework groups security functions into these five areas: Identify, Protect, Detect, Respond, and Recover. Many of the security and risk concepts introduced in this Guide and in future work (including the Security Services Catalog) will be highly useful to Security Architects in critical infrastructure areas seeking to integrate security and risk into their TOGAF Standard practices, and into their Enterprise Architectures.

2.4 COBIT®

"*COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from Information Technology (IT) by maintaining a balance between realizing benefits and optimizing risk levels and resource use. COBIT 5 for Information Security builds on the COBIT 5 framework in that it focuses on information security and provides more detailed and more practical guidance for information security professionals and other interested parties at all levels of the enterprise.*" [10]

COBIT 5 for Information Security is regarded as a relevant framework for security governance. However, in this Guide the structure of ISO/IEC 27001:2013 is used because that is a broader recognized definition of a security management system.

2.5 O-ESA

The Open Enterprise Security Architecture (O-ESA) standard [14], published by The Open Group in 2011, is a reference Security Architecture and guide to building a security program. While it contains useful information on information security governance, security principles, and technology components and services needed in Security Architectures, this reference architecture can be also applied to support the implementation of security and risk in Enterprise Architectures using the TOGAF Standard.

2.6 O-ISM3

The Open Information Security Management Maturity Model (O-ISM3) standard [9], published by The Open Group in 2011, describes a process-based approach towards building and operating an Information Security Management System (ISMS). Successful operation of the ISMS is generally a prerequisite for Enterprise Architectures to meet the security objectives established by an organization. A chapter of the Security Architecture Practitioners Guide will be devoted to the relationship between Enterprise Architecture, the TOGAF Standard, and ISMSs. The O-ISM3 standard defines security services as strategic, tactical, or operational processes, and provides a metrics-based approach to continuous improvement of the processes. Many of the services or processes described in the O-ISM3 standard are expected to be referenced in the Security Services Catalog Project as well.

2.7 Open FAIR

The Open FAIR Body of Knowledge comprises the Risk Taxonomy (O-RT) Standard [15] and the Risk Analysis (O-RA) Standard [16]. These standards help organizations to better measure their information security and operational risks. The Open FAIR quantitative risk analysis approach is highly useful during threat assessments and helps to understand the impact of threat mitigation options during the ADM cycle. Open FAIR can be thought of as a tool or technique in analyzing risk throughout the TOGAF ADM.

2.8 SABSA®

SABSA is a methodology for developing risk-driven enterprise information security and information assurance architectures and for delivering security infrastructure solutions that support critical business initiatives. It is an open standard, comprising a number of frameworks, models, methods, and processes. As an Enterprise Security Architecture framework, it allows for the usage of existing standards and practices (such as ISO/IEC 27001:2013, COBIT, and ISO 31000:2009) within the Security Architecture. SABSA is free for use by all, with no licensing required for end-user organizations that make use of the standard in developing and implementing architectures and solutions.

SABSA is well described in the SABSA® Blue Book [2]. In addition, new SABSA thinking is published at www.sabsa.org [3]. The fundamental idea behind SABSA is that the Security Architecture is there to facilitate the business. This is in line with TOGAF concepts.

3 Enterprise Security Architecture

A Security Architecture is a structure of organizational, conceptual, logical, and physical components that interact in a coherent fashion in order to achieve and maintain a state of managed risk. It is an enabler/driver of secure behavior, safe behavior, resilient behavior, reliable behavior, and upholding of privacy at risk areas throughout the whole enterprise.

Security Architecture components always have a relationship with other elements in the architecture. Thus, although the Security Architecture might be *viewed* as one architecture, it can never *be* an isolated architecture.

The risks managed by the Security Architecture are of various kinds. Two important ones are business risk and operational risk. The Security Architecture contains a balanced view on risk: negative consequences are kept to an acceptable level and positive opportunities are exploited to their maximum. The business-driven approach is key for the Security Architecture: business drivers offer the context for risk assessments; they define whether compliance with any control framework is necessary, and they justify the need for security measures.

For true integration of security in the architecture, a system engineering approach should be used. This means that security and risk are considered as soon as possible in the system engineering development lifecycle of the subject in question. At each phase in the development lifecycle, appropriate security and risk-related activities are conducted. These activities might vary from high-level advice and guidance in the early phases up to detailed security checks in the final phase. In this way, a secure operational system can be achieved that is reliable, safe, resilient, and respectful of privacy concerns. In addition, it leads to secure behavior.

In the operational phase, the security aspects of the architectures should be monitored, assessed, and reported. Although this operational phase generally does not begin until the first iteration of the TOGAF ADM is complete, it is during the ADM Phases G and H that the capabilities to measure security need to be designed and incorporated.

The adjective “Enterprise” before “Security Architecture” indicates the abstraction layer that the Security Architecture addresses. The concept of “enterprise” implies business alignment at the highest level, rather than at local levels. The TOGAF Standard defines “enterprise” as the highest level of description of an organization and typically covers all missions and functions. It further states than an enterprise will often span multiple organizations. For example, an enterprise could be a government agency, a whole corporation, a division of a corporation, a single department, or a chain of geographically distant organizations linked together by common ownership.

The Enterprise Security Architecture seeks business alignment of the security measures with the business objectives. It does so by defining relationships between the components on the different architecture layers, thus providing traceability and justification. The Enterprise Security Architect typically makes use of ISM and ERM processes to develop the deliverables and to interact with stakeholders.

3.1 Enterprise Risk Management

The Information Technology security and information security industry has evolved over its lifetime a view of operational risk that is concerned only with threats, vulnerabilities, and loss events (negative impacts). However, as noted earlier in Section 1.2, this Guide uses the ISO 31000:2009 [6] definition of "risk", an "uncertainty of outcomes", and risk management is presented as striking a balance between positive and negative outcomes resulting from the realization of either opportunities or threats.

3.1.1 Definition of Risk

Risk is the "*effect of uncertainty on objectives*" (ISO 31000:2009 [6]).

The effect of uncertainty is any deviation from what is expected – positive and negative.

Understanding the term "risk" is central to understanding the broader concepts of ERM, and the role of effective Enterprise Architecture and Enterprise Security Architecture. In this Guide we define risk in line with ISO 31000:2009. Risk is the effect that uncertainty has on the achievement of business objectives. The uncertainty is concerned with predicting future outcomes, given the limited amount of information available when making a business decision. This information can never be perfect, although our expectation is that given better quality information we can make better quality decisions. Every decision is based on assessing the balance between potential opportunities and threats, the likelihood of beneficial outcomes *versus* damaging outcomes, the magnitude of these potential positive or negative events, and the likelihood associated with each identified outcome. Identifying and assessing these factors is known as "risk assessment" or "risk analysis". "Risk management" is the art and science of applying these concepts in the decision-making process. Risk can be seen at the strategic long-term level (overall direction of the business), the medium term tactical level (transformation projects and programs), and at the operational level (regular day-to-day operational decisions, processes, and practices). The objective of risk management is to optimize business outcomes to maximize business value and minimize business losses. Risk can be seen at any level in the business stack (see Figure 2), but is always driven top-down from assessment of business value and its optimization.

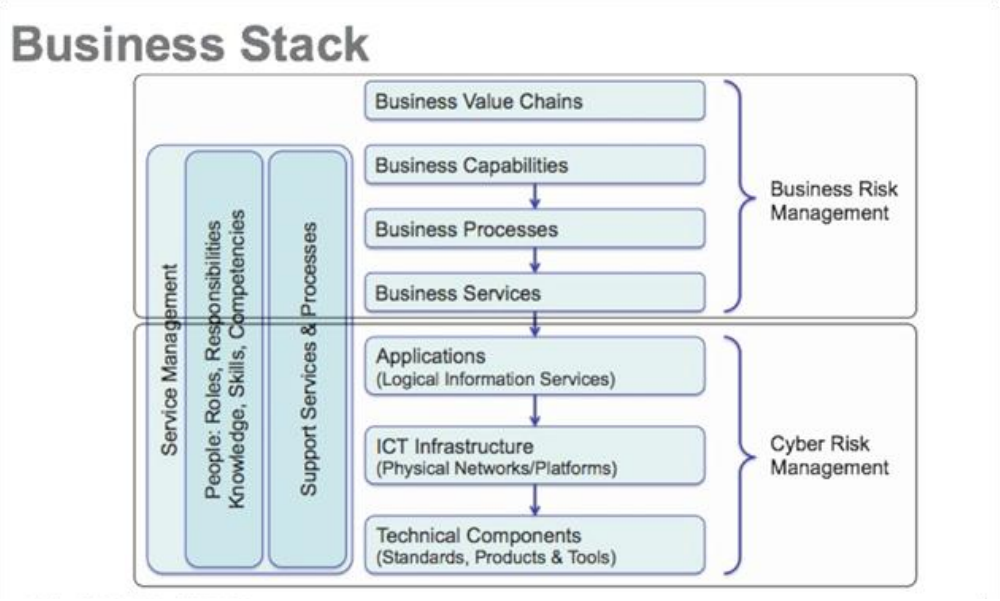

Figure 2: Business Risk *versus* Cyber Risk Areas

Uncertainty typically involves a deficiency of information and leads to inadequate or incomplete knowledge or understanding. In the context of risk management, uncertainty exists whenever the knowledge or understanding of an event, consequence, or likelihood is inadequate or incomplete.

This balanced view of risk is also embedded in SABSA, including the enabling of benefits arising from opportunities as well as the control of the effects of threats. Arguably, the sole role of the Enterprise Architect is to create an operational environment in which operational risk can be optimized for maximum business benefit and minimum business loss.

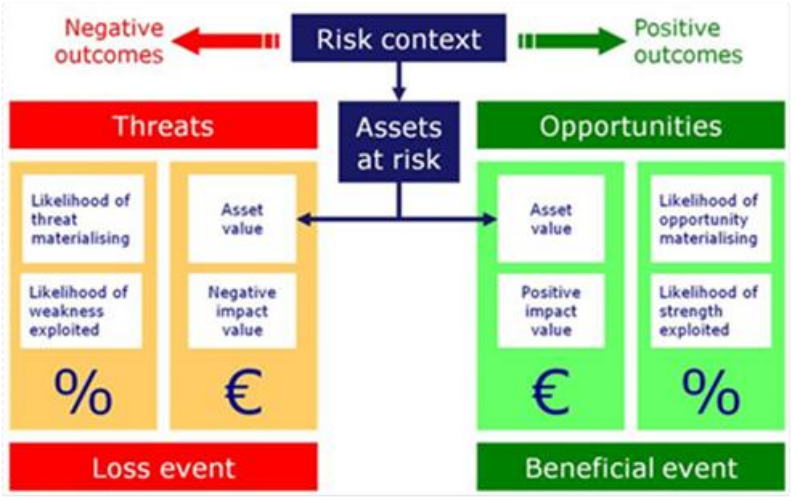

Figure 3: The SABSA Operational Risk Model

Operational risk is concerned with the threats and opportunities arising in business operations. SABSA is an architectural and operational framework for reaching out to opportunities and enabling positive outcomes to attain defined business targets and managing negative outcomes of loss events to within an enterprise's tolerance towards risk – namely their risk appetite.

3.1.2 Core Concepts for Enterprise Risk Management

According to ISO 31000:2009, the risk management process aids decision-making by taking account of uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives. It also gives a risk management process model, as illustrated in Figure 4. The ISO 31000:2009 approach makes it clear that risk management should be embedded deeply and firmly in all business activities. It also states that it is a continuous lifecycle rather than an isolated activity. This definition of risk management is adopted in this work.

The heart of this definition is that effective risk management is about managing to the expected objective. Every step has an element of risk that needs to be managed and every outcome is uncertain. ERM is about reducing uncertainty.

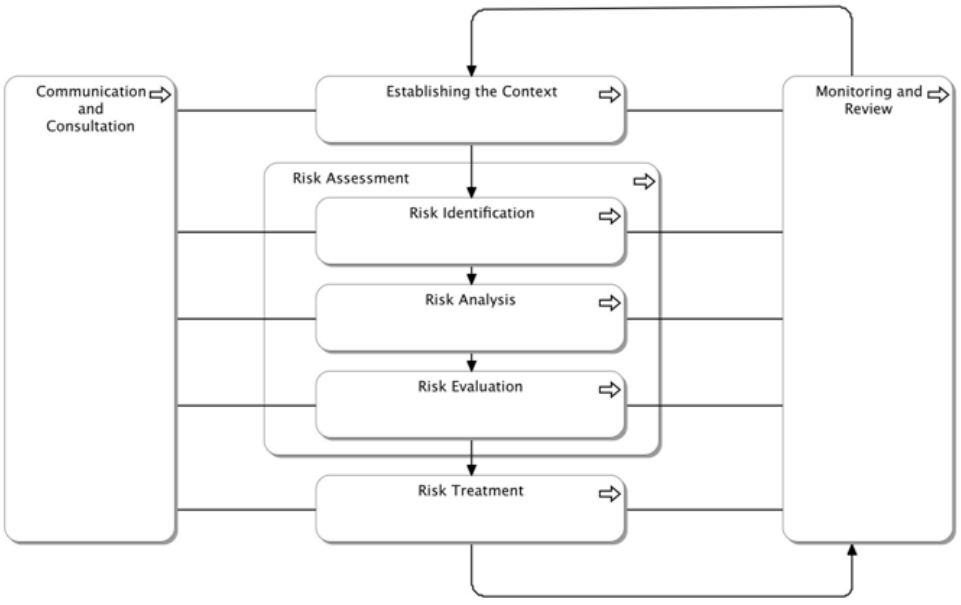

Figure 4: ISO 31000:2009 Model for Risk Management (Derived from[6])

The following concepts are important for ERM:

- Key Risk Areas
- Business Impact Analysis
- Risk Assessment
- Business Risk Model/Risk Register
- Risk Appetite

- Risk Mitigation Plan/Risk Treatment Plan

3.2 Information Security Management

Information Security Management (ISM) is a process that defines the security objectives, assigns ownership of information security risks, and supports the implementation of security measures. The security management process includes risk assessment, the definition and proper implementation of security measures, reporting about security status (measures defined, in place, and working), and the handling of security incidents.

3.2.1 Security

For many security practitioners, security is based on three core pillars: Confidentiality, Integrity, and Availability – also known as the CIA triad. These work pretty well in a technical environment where information systems need to be classified in order to determine the security requirements that apply. Classification can be achieved according to the confidentiality scheme (high-medium-low). Especially in the financial industry, these schemes for security classification based on the CIA triad are pervasive through the whole organization.

However, when talking with business owners it often turns out that these terms are meaningless to them. They have a clear understanding of which people are allowed to access which systems, but they don't use these "security" terms for that. In addition, the three terms are too broad. It's possible to rank every security concern under one of those three terms. The fact that they are so broadly defined is also their weakness: they can mean something completely different in two different environments.

For example, "Availability" can stand for:

- **Up-time** – a minimum up-time of a system of 99.9% during business hours
- **Responsiveness** – a minimum response time of 0,01 milliseconds for each transaction
- **Archived** – a guaranteed storage time of 7 years for healthcare data
- **Erased** – all data on servers should be made unrecoverable before they are sent to trash
- **Recoverable** – if the system fails due to a calamity, it should be restored within 24 hours

This example illustrates that Availability can have all kinds of meanings, depending on scope and context. It also illustrates that terms that are more specific are at our disposal that specify the type of concern we need to address. If the terms are so complex and need to be analyzed each time to determine what we really mean, then why should we keep using those terms? The terms Confidentiality, Integrity, and Availability are overloaded, used by many people for different purposes. We need a more specific concept.

Therefore, in this work we move away from the narrow CIA triad to a very rich terminology that is both specific and business-friendly. This is offered by the SABSA Business Attribute model, as described in the section "Requirements Management". Business Attributes offer a flexible and powerful way of expressing the security concerns of the business owners.

The Business Attribute model also allows for measurement of efficacy. The efficacy of a security measure is considered in relation to the risk it mitigates. An enterprise cannot determine

how much it will be willing to spend on securing an asset until it understands the asset value. For example, the use of that asset in an application and the concomitant risk the asset is exposed to as a result, will determine the true requirements for security. Additionally, the organization's tolerance for risk is a factor. In other words, the question asked should not be: "Is it secure?", but rather: "Is it secure enough?". The latter is ultimately a question to be answered by risk evaluation.

To give a more down-to-earth idea of what security encompasses, some generally accepted areas of concern for the Security Architect are given:

- **Asset Protection** – the protection of information assets from loss or unintended disclosure, and resources from unauthorized and unintended use
- **Risk Assessment** – determining what risks we face, measuring them to determine their likelihood and impact, and then accepting, mitigating, or transferring the risk according to the organization's risk appetite
- **Access Control** – who are you and what activity are you allowed to do under which conditions?
- **Audit** – does the operational environment operate in accordance with the requirements?
- **Availability** – the ability to function without service interruption or depletion despite abnormal or malicious events

3.2.2 Privacy

Privacy is the ability of an individual or group to seclude themselves, or information about themselves. The boundaries and content of what is considered private differ among cultures and individuals, but share common themes. The domain of privacy partially overlaps security, including, for instance, the concepts of appropriate use, as well as protection of information.

In general, directives on privacy demand that personal data should not be processed at all, except when certain conditions are met. These conditions fall into three categories: transparency, legitimate purpose, and proportionality.

3.2.3 Core Concepts for Information Security Management

According to ISO/IEC 27001:2013 [4], the ISM system preserves the security aspects of information by applying a risk management process, and it gives confidence to interested parties that risks are adequately managed. The ISM system is part of and is integrated with the organization's processes and overall management structure. The standard specifies the requirements for the ISM system.

The following core security concepts are relevant for the ISM process. Their descriptions as well as their relationship with the TOGAF ADM are given later in this Guide. Their role in the ISM process will be described in the Security Architecture Practitioners Guide. They are listed here in order to enumerate the core information security concepts that should be part of the TOGAF Standard. The main categories of ISO/IEC 27001:2013 are used to understand better how the concepts are related.

Context of the Organization

- Security Domain Model
- Business Drivers/Business Objectives
- Applicable Law and Regulation Register
- Applicable Control Framework Register
- Trust Framework

Leadership

- Security Policy Architecture

Planning

- Security Principles
- Business Attribute Profile
- Control Objectives/Security Objectives
- Data Quality
- Business Risk Model/Risk Register
- Security Services Catalog

Support

- Security Resource Plan
- Security Training & Awareness
- Security Standards

Operation

- Security Classification

Performance Evaluation

- Security Audit

Improvement

- (no new security concept)

3.2.4 Operational Security Processes

Operational controls are designed during TOGAF ADM Phases B, C, D, and E. ADM Phases F and G provide guidance on the definition of metrics that would be used later during the project operations. This is why the operational security processes are introduced in the design phase as part of the Security Services Catalog.

The consequence is that operational security processes, such as digital forensics, security intelligence, and security analytics, will be found in the architectures as part of the Security Services Catalog. Security intelligence provides the means to analyze and measure enormous amounts of data and deliver meaningful incident information to the right people across the organization.

4 Security as a Cross-Cutting Concern

Security Architecture is a cross-cutting concern, pervasive through the whole Enterprise Architecture. It can be described as a coherent collection of views, viewpoints, and artifacts, including security, privacy, and operational risk perspectives, along with related topics like security objectives and security services. The Security Architecture is more than a dataset; it is based on the ISM and ERM processes.

The TOGAF ADM covers the development of the four architecture domains commonly accepted as subsets of an Enterprise Architecture: Business, Data, Application, and Technology. The Security Architecture interacts with all four of them and is therefore called cross-cutting.

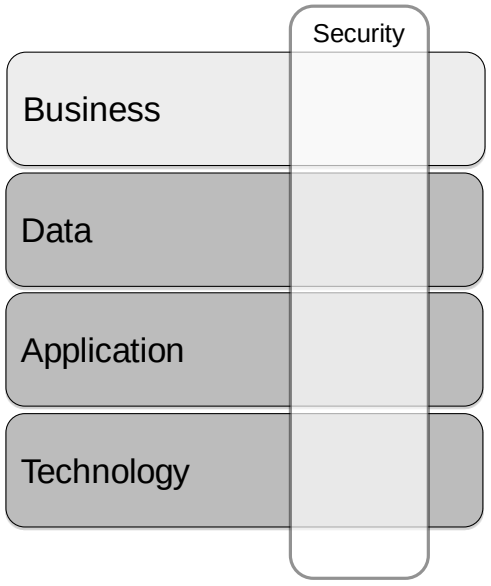

Figure 5: Security as a Cross-Cutting Concern through the Architecture

As a cross-cutting concern, the Security Architecture impacts and informs the Business, Data, Application, and Technology Architectures. The Security Architecture may often be organized outside of the architecture scope, yet parts of it need to be developed in an integrated fashion with the architecture. These touch-points will be explained in the next chapter.

5 Security and Risk Concepts in the TOGAF ADM

The TOGAF ADM contains the concept of "artifacts" (work products) that are consumed or produced by each phase. To match this, the core concepts of the Enterprise Security Architecture are expressed in TOGAF terminology and related to TOGAF concepts, which will ensure correct embedding of the relevant risk and security concepts at the appropriate ADM phases. A complete overview of all selected SABSA artifacts is given in Figure 1.

These core security concepts are explained in more detail in the following sections for each TOGAF ADM phase. Besides the description, the location in the "Architecture Framework" is given. That can be in the TOGAF Standard – if it's already there – or in the Enterprise Security Architecture. The Enterprise Security Architecture is used here as a generic Security Architecture concept, encompassing both ISM and ERM.

5.1 Preliminary Phase

The Preliminary Phase establishes the security context required to guide the Security Architecture design. 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.

5.1.1 Business Drivers/Business Objectives

Location in the Architecture Framework: This is the subset of TOGAF business drivers affecting security, presented as an integral part of the overall architecture business drivers (The TOGAF Standard – Architecture Content: Architecture Deliverables).

In O-ISM3 [9], this is called the business objectives. Every organization exists for specific purposes that require it to set goals and meet certain obligations. Business objectives, ranging from aspirational goals to regulatory compliance, may originate internally, or be imposed by an external party such as the government. Their achievement depends on many factors, one being information security. Some examples of business objectives are:

- Paying the payroll on the 1st of every month
- Paying all incoming invoices within a certain timeframe

5.1.2 Security Principles

Location in the Architecture Framework: Security Principles is the subset of Business Principles addressing Security Architecture. This is presented as an integral part of the overall Architecture Principles deliverable (The TOGAF Standard – Architecture Content: Architecture Deliverables).

Security Principles, like other Architecture Principles, will provide valuable guidance to making business decisions to comply with the enterprise's risk appetite. In essence, the usage of Security

Principles does not differ from the usage of Architecture Principles. Examples of Security Principles will be given in the Security Architecture Practitioners Guide.

5.1.3 Risk Appetite

Location in the Architecture Framework: Enterprise Security Architecture: ERM.

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 approve it specifically. It defines both the level of risk the organization is willing to accept as well as its strategy in defining this level. For risks above this acceptable level, it defines the strategy used for mitigation (transference, avoidance).

5.1.4 Key Risk Areas/Business Impact Analysis

Location in the Architecture Framework: Enterprise Security Architecture: ERM.

Note: Risk classification is described in the TOGAF Standard – ADM Techniques (Risk Management) and is focused on risk of the architecture projects. This document extends the concepts of risk and risk assessment.

During the Preliminary Phase, addressing key risk areas provides a context for architecture projects. During an architecture project in Phase A, this should be confirmed.

The business impact analysis can be applied in all domains and against the architecture roadmap, and is a powerful tool for determining fitness of the architecture and roadmap. A business impact analysis points out the potential damage (or profit) to the business that can be expected if inappropriate and insufficient information security is applied. It (only) defines what kind of impact is relevant to the business process and should be avoided, not the likelihood of this impact occurring. The deliverable is a list of the key risk areas within the architecture scope. This information is input to the risk assessment.

5.1.5 Security Resource Plan

Location in the Architecture Framework: the TOGAF Standard – Architecture Development Method, Preliminary Phase and Phase A.

Resource planning for architecture work for the entire architecture team is addressed in the Preliminary Phase when the Enterprise Architecture team is defined and established. In Phase A it is addressed where the capability of the architecture team is assessed against the architecture project.

Based on the scope of the Enterprise Architecture team's responsibility and the scope of any architecture project, it will identify the required security resources to deliver the security elements of the architecture.

A key part of defining the Enterprise Architecture team is establishing the expected role and mandate of the Security Architect. Best practice Security Architecture integrates security and

risk within all domains. Integral to this is establishing the governance process for the Security Architecture within the context of the Enterprise Architecture governance process.

Answering the following questions will assist in identifying the security and risk resources required in the team, and on an architecture project:

- What are the common security or risk-related concerns?
- Do key and influential security or risk-related stakeholders exist who require specific security views?
- Does the architecture address high-risk areas, or is the risk appetite low?
- Can security support be requested on an as-needed basis from an existing security team or are dedicated Security Architecture resources required as part of the overall architecture team?

During the Preliminary Phase it is decided which security artifacts are really needed in the Enterprise Architecture and which will be created by whom. It might not be necessary to deliver all security artifacts in order to address security properly. The reverse applies too: delivering all artifacts does not guarantee that security is taken care of properly – more artifacts may be required.

For enterprise-level architectures, the artifacts need to be created based on discussions with key stakeholders; preliminary assessments carried out by the architecture team; and assessing relevant statutes, applicable jurisdictions, legislation, and regulations.

For capability-level architectures, existing sources might be available. For instance, an enterprise-level security policy or risk assessment describes the security principles, risk appetite, and key risk areas for a particular context.

5.2 Phase A: Architecture Vision

In general, Phase A: Architecture Vision describes enough of the TOGAF ADM Phases B, C, and D to ensure that key stakeholders can agree to a vision of the end-state, which represents a solution to a defined problem.

In Phase A sufficient security-specific architecture design is carried out to:

- Satisfy the security stakeholders that the end-state does not represent any unknown or unacceptable risk and aligns with corporate policies, standards, and principles
- 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 with the right balance between risk, compliance, and business benefits

In Phase A, it is essential to identify the complete list of all stakeholders, their concerns, and associated requirements for approval of the architecture. All stakeholders will have security and risk concerns and associated requirements. Separating security stakeholders ensures that the architecture will address a subset of stakeholders and a subset of requirements.

The stakeholder requirements are gathered to determine the security blueprint needed to address the various concerns the stakeholders have. The security blueprint is defined at a level giving sufficient assurance to the stakeholders that the final artifacts and deliverables will address their concerns appropriately. The ADM phases related with architecture descriptions complete the blueprint and add the required detail.

Stakeholders typically have value concerns related to the Security Architecture. Value may be measuring items such as reduced risk and enablement of the overall architecture. The Business Attribute Profile[1] can be useful as a basis for the business case. As a specific Business Attribute Profile may not yet be available, the SABSA-provided Business Attribute Profile can be used as a starting point. A scenario-based approach may be used to obtain stakeholder approval.

The viewpoints and business cases must build on Security Principles, drivers, key risks, and risk appetite and should be an integral part of the overall Architecture Vision deliverables.

5.3 Phase 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.

The security-related Business Architecture artifacts are described below.

5.3.1 Security Policy Architecture

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

The Security Policy Architecture (or Framework) contains a set of security policies that express the security strategy. It assigns ownership and accountability for security and risk management. It also addresses the linkage and hierarchy of operational risk management in general with the various security aspects such as business continuity, information security, system security, and physical security.

5.3.2 Security Domain Model

Location in the Architecture Framework: the TOGAF Standard – Introduction and Core Concepts (Glossary of Supplementary Definitions: Information Domain). Complete text: "Grouping of information (or data entities) by a set of criteria such as security classification, ownership, location, etc. In the context of security, information domains are defined as a set of users, their information objects, and a security policy."

Note: The concept of information domain corresponds with the definition of a security domain below.

A security domain represents a set of assets that could be described by a similar set of business attributes. In other words, the security domain groups the assets with the same security level that fall under the jurisdiction of one security policy. In addition, the security domain model helps in defining responsibility areas where responsibility is exchanged with external parties. It can also

[1] See Chapter 6 (pp.87-97) of the SABSA® Blue Book [2].

be used to distinguish between areas of different security or trust levels. A security policy authority is responsible for setting and implementing the security policy within the domain.

If the business model of the organization does encompass federation with other organizations, the extent of the security federation should be established at this point in the process. This is the case when organizations have data objects or activities in common. Contractual federation agreements should be examined for their security implications and agreements. It may be necessary to establish joint architecture meetings with other members of a federation if they belong to the same security domain.

5.3.3 Trust Framework

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

Trust relationships are the basis for doing business with other parties. The trust framework describes trust relationships between various entities in the architecture domain 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) 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.[2]

5.3.4 Risk Assessment

Location in the Architecture Framework: Enterprise Security Architecture: ERM.

Although the TOGAF Standard – ADM Techniques (Initial Risk Assessment) describes one method of administrating the result of a risk assessment, the actual act of assessing risk and the ways to do that are not described. Therefore, this concept is augmented by this document for use with the TOGAF Standard.

A risk assessment is the activity of determining the risks that are relevant to an asset or objective. A qualitative risk assessment delivers a listing of relevant risk scenarios with a high-level prioritization (high-medium-low), whereas a quantitative approach seeks for numeric determination of the risk. This is commonly based on identified threats, their likelihood of materializing, and the impact of an incident. A deliverable of a risk assessment is the Business Risk Model.

5.3.5 Business Risk Model/Risk Register

Location in the Architecture Framework: Enterprise Security Architecture: ERM.

The Business Risk Model is a Risk Register. It 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. The classification of the

[2] The Open Group published a Guide to the Trust Ecosystem in January 2014 that describes the need for a trust ecosystem, a taxonomy for trust, as well as the impact of trust on business relationships and contracts (available at www.opengroup.org/library/g141).

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.

5.3.6 Applicable Law and Regulation Register

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

The Applicable Law and Regulation Register contains the specific laws and regulations that apply within the scope of the Enterprise Architecture engagement, based on the business function inventory. It is kept up-to-date, following legal and regulatory changes. This register is important for compliance purposes.

Whether the business function is subject to regulation depends upon the functionality of the system as a whole and the data collected or maintained. In addition, the jurisdiction where the supporting systems or services are deployed, where the users reside, etc. is relevant information. It may be wise to obtain legal counsel regarding these obligations at the outset of activities.

5.3.7 Applicable Control Framework Register

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

The Applicable Control Framework Register contains the suitable set of control frameworks that best satisfy the requirements and address the risks related to the engagement scope and context. Control frameworks contain requirements and/or mandatory security measures. Examples of control frameworks are ISO/IEC 27001:2013 [4], ISO/IEC 27002:2013 [5], COBIT [10], PCI-DSS, Common Criteria, etc.

Factors that drive the selection of control frameworks are:

- Mandatory certifications, due to the nature of the business process or the industry
- Way of working of the internal ISM process – this is often inspired by ISO/IEC 27001:2013 but might mandate additional control frameworks as well
- Marketing objectives – customers may ask for specific control framework certifications
- Support for security audits

5.4 Phase C: Information Systems Architectures

The security elements of Phase C: Information Systems Architectures comprise functional security services and their security classification.

The artifacts are described in more detail below.

5.4.1 Security Services Catalog

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

Note: The TOGAF Standard has a Business Services Catalog that is a list of the enterprise's business services and their functional and non-functional requirements. It is used to analyze the functional and non-functional requirements. The Security Services Catalog

stores and provides more kinds of information about each service, so this needs to be introduced.

The Security Services Catalog is a list of services that provide security-specific functionality as part of the overall architecture. Unlike control frameworks that contain requirements, the Security Services Catalog describes security building blocks that actually realize the security goals. It provides a common terminology and reference framework for the domain of security management. The Security Services Catalog contains conceptual definitions of the services, as well as operational information about implementation and usage.

Examples of security services are:

- Identity & Access Management
- Continuity Management
- Security Intelligence
- Digital Forensics
- Security Analytics
- Audit, Network Monitoring
- Compliance Management
- Training & Awareness Programs, etc.

This is the area of security that most security practitioners will recognize. One of the main advantages of the Security Services Catalog is that it is a common terminology and reference framework for the domain of security management allowing better cooperation between the parties concerned.

5.4.2 Security Classification

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

Security classification is a label attached to an asset, according to a classification scheme. In most cases, this scheme is defined and described in the corporate information security policy and the classification is based on one or more characteristics of the asset.

Keep in mind that the asset can be any relevant component of the architecture. Assets include business service, a capability, information, an information system service, physical data component, or physical technology component. The security classification determines the security requirements that apply to the asset; for example, regarding access control, confidentiality, or availability. It is a means to implement the security policy.

5.4.3 Data Quality

Note: From an Enterprise Security Architecture perspective, data quality[3] requirements are an integral part of the security requirements and so are the related risk assessment and selection of measures.

Data quality is a key factor in operational risk management. Some of the key attributes that contribute to data quality are accuracy, relevance, timeliness, currency, completeness, consistency, availability, and accessibility. Safeguarding data quality starts with a clear overview on the datasets in question. For each dataset, ownership and responsibility for the quality of data needs to be assigned. The owner authorizes people or processes that are trusted for a certain activity on the data under certain circumstances. It might also be necessary to change information systems in order to handle the data properly. Finally, each of the key attributes should be measured based on log and performance data.

5.5 Phase D: Technology Architecture

In most cases, the development of specific Technology Architecture security artifacts is not necessary, as long as it incorporates the relevant security controls and mechanisms defined in earlier phases. The Security Architect must ensure that the required controls are included in the Technology Architecture and verify whether the controls are used in an effective and efficient way. This includes the technology for the provision and regulation of system resources, such as electric power, processing capacity, network bandwidth, and memory.

A security stakeholder may request the creation of a specific Technology Architecture security view or deliverable that describes all security-related technology components and how they inter-relate. This view should explain which business risks are mitigated by what technology, providing justification for the technology.

5.6 Phase E: Opportunities and Solutions

In defining the roadmap, where the sequence of gaps to be addressed is determined, it is imperative that security and risk are evaluated. Ensure the stakeholders' security and risk concerns are addressed in the analysis. Confirm that risk owners are consulted. The value expected to be delivered by work packages should include measures related to security and risk value to ensure the roadmap addresses the complete set of business goals and drivers.

The security building blocks defined in the previous phases become SBBs in this phase so that more specific implementation-oriented requirements and specifications are defined. A whole solution design might be needed at this stage.

The Security Services Catalog of the Baseline Security Architecture probably contains existing security services or security building blocks that meet the requirements. For example, if the requirement exists for application access control, an existing central authentication service might be used to fill that in. The efficacy of existing security services and controls earmarked for re-use must be verified to ensure that the end-state contains security measures, which work and integrate well.

[3] This document addresses the TOGAF Standard, 10th Edition which does not sustain a distinction between data and information. When your architecture makes a clear distinction, all references to data are appropriate for information.

5.6.1 Risk Mitigation Plan

Location in the Architecture Framework: Enterprise Security Architecture: ERM.

Note: In the TOGAF Standard, 10th Edition risk mitigation is done for transition risks, but it is not explained how this should be created or what possible risk mitigation strategies there are, so this document provides additional guidance on this issue.

The Risk Mitigation Plan contains activities to mitigate risks. It is the implementation of the risk mitigation strategy, which could aim to increase the level of control, transfer the risk to another party, avoid the risk by changing the business activity, delay the risk, compensate for the risk, etc.

The broader sense of risk is addressed by the ERM process in this phase. The scope includes the latest information security risks as identified during the risk assessments that are done earlier in the ADM (in Phase B). This is where the risks get "solutioned" or "treated". The Risk Mitigation Plan should also consider risks that appear as a result of the new architecture.

5.7 Phase F: Migration Planning

Migration is itself a business process that needs to be secured. The migration strategy should include a risk assessment and a Risk Mitigation Plan. In Phase F, the Risk Mitigation Plan is limited to the transition. These concepts have already been mentioned in earlier phases of the ADM. Migration of live environments should always include regression planning so that there is a way to reverse out a failed migration. This is an essential part of risk management.

In addition, migration planning should include a security impact analysis to understand any security impacts of the target state of the change.

5.8 Phase G: Implementation 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 deviations from Architecture Principles and implementation guidelines don't create any unacceptable risk.

The following artifacts are relevant in this phase.

5.8.1 Security Audit

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

Security audit includes security reviews of implemented processes, technical designs, developed code, and configurations against policies and requirements. It also includes security testing, comprising functional security testing, performance testing, and penetration testing.

5.8.2 Security Training and Awareness

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

Security training and awareness means that sufficient training is provided to ensure correct deployment, configuration, and operations of security-relevant subsystems and components; including awareness training of all users and non-privileged operators of the system and/or its components. It is critical for a proper, continuous, and secure performance.

In many control frameworks, security training must be followed and results documented to demonstrate due diligence. Substantiated corrective actions or sanctions are needed in cases where exploits or errors compromise security objectives.

5.9 Phase H: Architecture Change Management

Phase H does not produce tangible security outputs but defines two processes essential for continued alignment between the business requirements and the architecture: risk management and architecture governance. Even though they are not formal artifacts, they are added here to emphasize their importance.

ERM is the process in which the existing architecture is continuously evaluated regarding changes to business opportunity and security threat. Based on the results of this process, the current architecture might deem it unsuitable to mitigate changed or new risks, or it might constrain the business too much in exploiting new opportunities. In that case, a decision on architecture change must be made.

Architecture governance is 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. This is explained in the TOGAF Standard – Enterprise Architecture Capability and Governance (Architecture Governance Framework). Changes related to risk and security should be an explicit part of that framework. Large changes to the architecture should include a security impact analysis.

Change is driven by new requirements or changes in the environment. For instance, changes in security requirements can 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.

Due care must be taken in deciding whether a security change triggers a new iteration though the TOGAF ADM cycle – for instance, when enterprise risk appetite changes – a seemingly small security requirement change can easily trigger a new architecture development cycle.

An example of where changes can be applied within the existing architecture is when security standards or requirements change. This is usually less disruptive since the trade-off for their adoption is based on the value of the change – that is, evaluation of the risk – the trade-off between the opportunity for business improvement, the perceived threat to the business in security terms, and the threat posed by the change itself, which would perhaps be very disruptive and expensive. This is an excellent example of where the SABSA concept of balancing risks can be applied to decision-making.

It is therefore essential that the architecture change board or any other governance structure that is responsible for applying appropriate architecture change management comprises suitable security skilled individuals.

5.10 Requirements Management

Requirements Management plays a central role in architecture work. This is recognized in the TOGAF Standard. The purpose of Requirements Management is to identify, store, maintain, and communicate business requirements through the different phases of architecture development by means of a controlled and repeatable process. In addition, operational performance is monitored against target requirements. This is not explicitly addressed in the TOGAF ADM but lies within Phase H: Architecture Change Management, and the continual validation of Requirements Management.

The TOGAF method validates and updates business requirements in every stage of an architecture development project. However, the TOGAF Standard does not provide a required technique for describing or documenting requirements. Such a technique is present in SABSA, which presents its unique Business Attribute Profiling technique as a means to describe requirements effectively. This section describes the use of Business Attribute Profiling with respect to security requirements management, along with the benefit this technique offers for Requirements Management in general.

5.10.1 Business Attribute Profile

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

Business Attribute Profiling is a SABSA requirements engineering technique that translates business goals and drivers into requirements using a risk-based approach. Some important advantages of this technique are:

- Executive communication in non-IT terms
- Traceability mapping between business drivers and requirements
- Performance measurement against business-defined targets
- Grouping and structuring of requirements, which facilitates understanding and oversight by architects

The SABSA Business Attribute Profile is at the heart of the SABSA methodology. It is this requirements engineering technique that makes SABSA truly unique and provides the linkage between business requirements and technology/process design. See the SABSA® Blue Book [2].

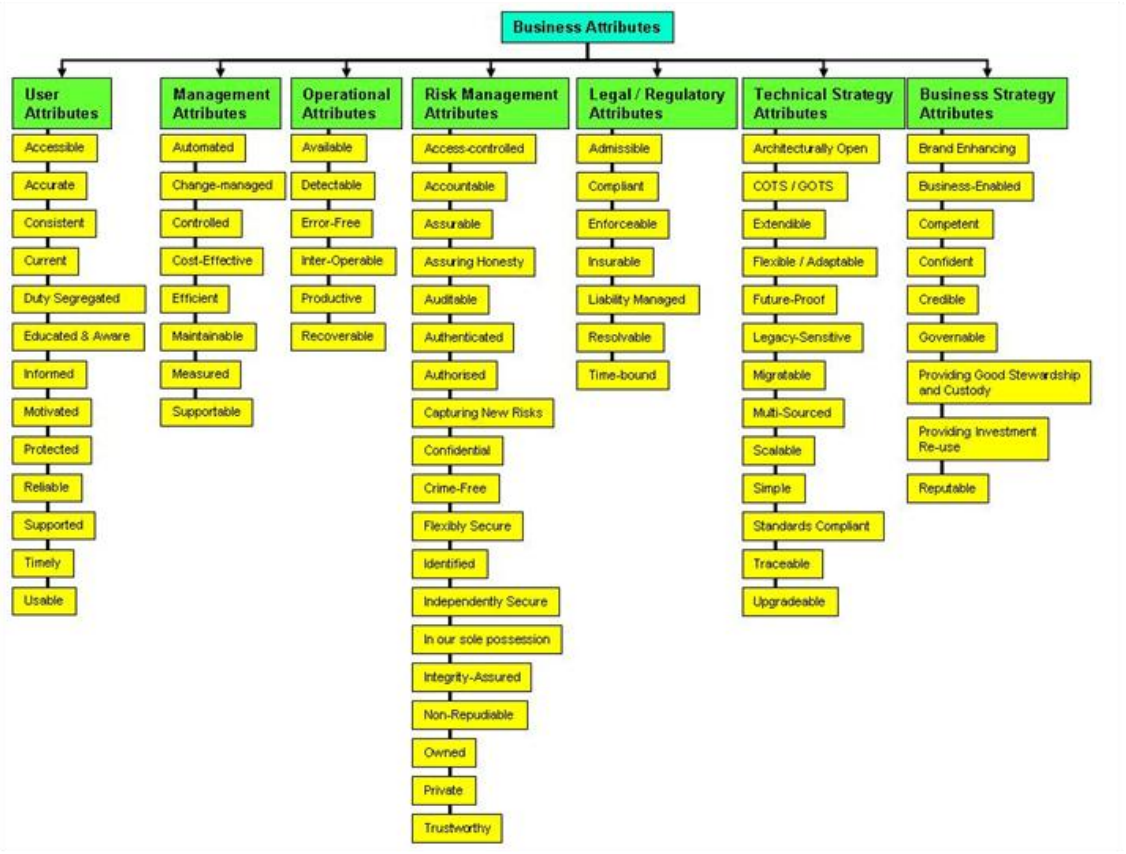

Figure 6: Example of a SABSA Business Attribute Taxonomy

Each SABSA Business Attribute in the example taxonomy of Figure 6 has a detailed generic definition and some suggested guidelines for applying metrics to that attribute, not included in this overview. A Business Attribute Profile is built by the architects, using the taxonomy as a guideline. The objective is to document the relevant attributes for the business case in hand, redefining each selected attribute in terms of the business case, developing a measurement approach, specific metrics, and performance targets, again related to the business case. The model is flexible and adaptive. When needed, new attributes and new definitions should be added to fulfill the business requirements. Thus, although the method is well defined, the Business Attribute taxonomy can be extended as much as is appropriate and each Business Attribute Profile is highly customized according to the business case being considered by the architecture team.

An integral part of the SABSA Business Attribute Profile is the selection of metrics to set targets, so that performance can be measured in the operational phase ("did you hit the target?"). The business analyst can choose to either use the suggested metrics in the detailed examples, or create new metrics if that seems more appropriate. Eventually, the creation of a real-time operational risk dashboard is possible that monitors performance of operational capabilities against the predetermined performance targets, and provides early warnings of up-coming risk events that may require management intervention.

In O-ISM3, performance targets are called "security targets". As well as expressing security objectives in terms of what matters to the business, O-ISM3 defines the tolerable deviations. All O-ISM3 objectives (business and security) must include their security target. This is the maximum deviation from the desired outcome that management tolerates before taking corrective action. O-ISM3 can support any specified variance. This enables the O-ISM3 program to support and manage both aspirational objectives (whose allowable deviations may be very high) and critical objectives (where there is usually a very narrow compliance range).

Security targets are normally defined in terms of frequency of occurrence and threshold cost. The allowable business impact of missing objectives reflects the trade-off against other priorities and objectives. Security targets show what the organization expects from its information security investment. In a way, management's act of defining security targets also specifies its risk appetite.

5.10.2 Control Objectives/Security Objectives

Location in the Architecture Framework: Enterprise Security Architecture: ISM.

A control objective (sometimes called a security objective) is a desired state of security for a given process, person, activity, system, or dataset. It differs from a security requirement since an objective is a goal that the ISM process aims to fulfill. This control objective might not exactly match the security requirement. Control objectives are linked to business attributes.

O-ISM3 documents the contribution of information security towards meeting business objectives through using a dependency analysis. The output of the dependency analysis is a list of security objectives that form the basis for design, implementation, and monitoring of the ISMS. They also form the business objectives for the security component when planning Enterprise Architecture. Security objectives, derived from business objectives, state explicitly how information security contributes to business objectives.

Some examples of security objectives derived from the business objective "Invoicing all products and services provided" are:

- Invoices are accessible only to the accountancy and collection teams
- Paid invoices are kept for three years and destroyed after no more than four years

5.10.3 Security Standards

Location in the Architecture Framework: the TOGAF Standard – Architecture Content (Standards Library) provides a repository area to hold a set of specifications to which architectures must conform. The standards can apply at every architecture domain in the TOGAF Standard. Security standards can be added to this existing catalog as well.

The Security Architecture provides guidance on which security standards to use in which situation. Whether a security standard applies is decided by the business owner or business analyst. If so, the standard is applied to the architecture work through the Requirements Management process. The standard can dictate security controls for the Business, Data, Application, or Technology Architecture.

Standards are needed to ensure that many different components can be integrated to form a larger system. Different types of standards exist, such as regulatory standards, technical

standards, etc. An example is the PCI-DSS standard that applies for businesses in the payment card industry, the ETSI standards that apply in the telecom industry, etc. It is also worth noting that security standards may be externally imposed, or they may be internally developed.

5.11 The TOGAF Architecture Content Metamodel

The TOGAF Architecture Content Metamodel includes the necessary concepts to model ISM and ERM. Existing entities, such as business service and information system service, are adapted by having ISM and ERM-specific attributes.

5.12 Use of the ArchiMate® Modeling Language

The ArchiMate language [8] supports ISM and ERM modeling. This is described in The Open Group White Paper: Modeling Enterprise Risk Management and Security with the ArchiMate® Language [12]. An example of the risk model in the ArchiMate language is given in Figure 7.

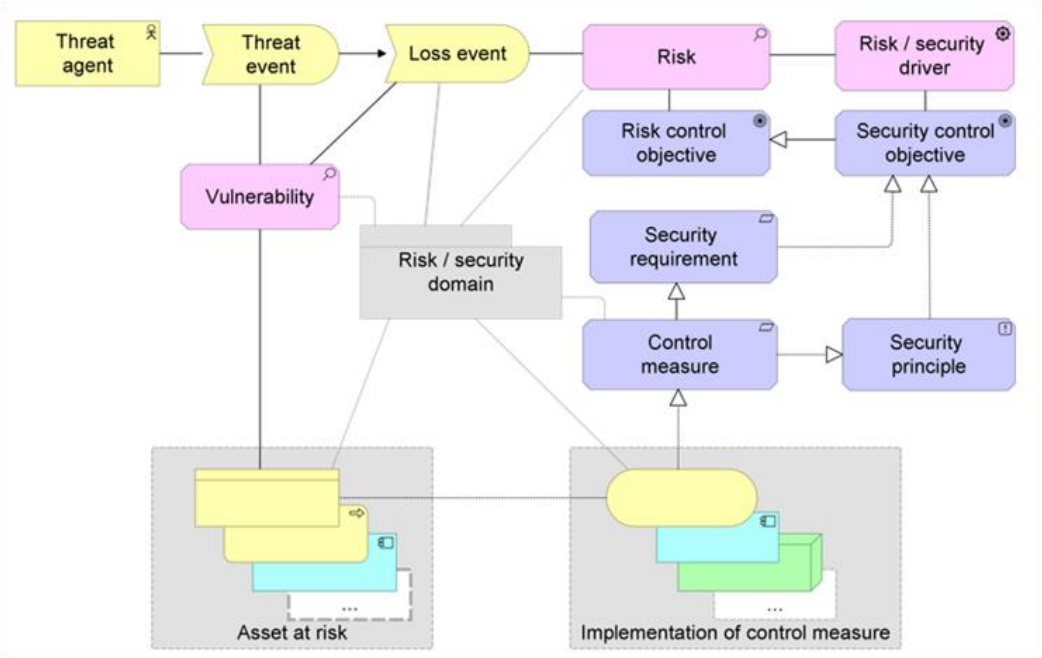

Figure 7: Modeling Risk and Security in the ArchiMate Language

Acronyms

ABB	Architecture Building Block
ADM	Architecture Development Method
ERM	Enterprise Risk Management
ETSI	European Telecommunications Standards Institute
ISM	Information Security Management
ISMS	Information Security Management System
O-ESA	Open Enterprise Security Architecture
O-ISM3	Open Information Security Management Maturity Model
O-RA	Risk Analysis Standard (Open FAIR)
O-RT	Risk Taxonomy Standard (Open FAIR)
PCI-DSS	Payment Card Industry Data Security Standard
SBB	Solution Building Block

Index