Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Modeling enterprise risk management and security with the ArchiMate language

Band, Iver; Engelsman, Wilco; Feltus, Christophe; González Paredes, Sonia; Hietala, Jim; Jonkers, Henk; Massart, Sébastien

Publication date:
2015

Document Version
Early version, also known as pre-print

Link to publication

Citation for pulished version (HARVARD):
Band, I, Engelsman, W, Feltus, C, González Paredes, S, Hietala, J, Jonkers, H & Massart, S 2015, *Modeling enterprise risk management and security with the ArchiMate language*.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 11. Nov. 2026

THE Open GROUP

Modeling Enterprise Risk Management and Security with the ArchiMate® Language

A White Paper by:

Iver Band, EA Principals

Wilco Engelsman, BiZZdesign

Christophe Feltus, Luxembourg Institute of Science and Technology

Sonia González Paredes, Dux Diligens

Jim Hietala, The Open Group

Henk Jonkers, BiZZdesign

Sebastien Massart, Arismore

January, 2015

Copyright © 2015, The Open Group

The Open Group hereby authorizes you to use this document for any purpose, PROVIDED THAT any copy of this document, or any part thereof, which you make shall retain all copyright and other proprietary notices contained herein.

This document may contain other proprietary notices and copyright information.

Nothing contained herein shall be construed as conferring by implication, estoppel, or otherwise any license or right under any patent or trademark of The Open Group or any third party. Except as expressly provided above, nothing contained herein shall be construed as conferring any license or right under any copyright of The Open Group.

Note that any product, process, or technology in this document may be the subject of other intellectual property rights reserved by The Open Group, and may not be licensed hereunder.

This document is provided "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Any publication of The Open Group may include technical inaccuracies or typographical errors. Changes may be periodically made to these publications; these changes will be incorporated in new editions of these publications. The Open Group may make improvements and/or changes in the products and/or the programs described in these publications at any time without notice.

Should any viewer of this document respond with information including feedback data, such as questions, comments, suggestions, or the like regarding the content of this document, such information shall be deemed to be non-confidential and The Open Group shall have no obligation of any kind with respect to such information and shall be free to reproduce, use, disclose, and distribute the information to others without limitation. Further, The Open Group shall be free to use any ideas, concepts, know-how, or techniques contained in such information for any purpose whatsoever including but not limited to developing, manufacturing, and marketing products incorporating such information.

If you did not obtain this copy through The Open Group, it may not be the latest version. For your convenience, the latest version of this publication may be downloaded at www.opengroup.org/bookstore.

ArchiMate®, DirecNet®, Jericho Forum®, Making Standards Work®, OpenPegasus®, The Open Group®, TOGAF®, UNIX®, and the Open Brand ("X Device") are registered trademarks and Boundaryless Information Flow™, Build with Integrity Buy with Confidence™, Dependability Through Assuredness™, FACE™, IT4IT™, Open Platform 3.0™, Open Trusted Technology Provider™, UDEF™, and The Open Group Certification Mark ("Open O") are trademarks of The Open Group.

UML® is a registered trademark and BPMN™ is a trademark of Object Management Group, Inc. in the United States and/or other countries.

SABSA® is a registered trademark of SABSA Limited.

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.

Modeling Enterprise Risk Management and Security with the ArchiMate® Language

Document No.: W150

Published by The Open Group, January 2015.

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

The Open Group, 44 Montgomery St. #960, San Francisco, CA 94104, USA

or by email to:

ogpubs@opengroup.org

Table of Contents

Introduction **6**

Risk and Security Standards, Frameworks, and Concepts **12**

Introduction to the ArchiMate Standard **19**

Modeling Risk and Security Aspects with the ArchiMate Language **22**

Case Studies and Examples **27**

Summary and Conclusions **37**

References **38**

About the Authors **40**

About The Open Group **42**

Boundaryless Information Flow ™
achieved through global interoperability
in a secure, reliable, and timely manner

Executive Summary

Enterprise Architects can use the ArchiMate® language to model Enterprise Risk Management (ERM) and security concepts and relationships. This widely accepted open standard provides the modeling constructs to describe and interconnect business and technical architectures. Applying the ArchiMate language to represent risk and security concepts results in the ideal vehicle to consider these aspects in an integral way. The ArchiMate language fits well with other Enterprise Architecture (EA) frameworks and standards, such as the TOGAF® standard and the Zachman framework, as well as enterprise security management frameworks such as the Sherwood Applied Business Security Architecture (SABSA).

Through its Motivation extension, the ArchiMate language makes it possible to link control measures to security requirements, principles, and goals, as well as to the results of a risk analysis. On the other hand, ArchiMate models can be linked to design languages for business processes and IT solutions such as BPMN and UML. These linkages enable precise gathering of a set of broadly accepted risk and security concepts, analysis of their semantics, and consensus regarding the most important ones of the full scope of enterprise risk.

This White Paper, a joint project of The Open Group ArchiMate Forum and The Open Group Security Forum, demonstrates this approach and identifies opportunities for future work that would enhance it.

After summarizing the ArchiMate 2.1 language, this White Paper reviews relevant standards and frameworks, including the TOGAF framework, the COSO ERM framework, the SABSA framework, and The Open Group Risk Taxonomy (O-RT) standard, upon which the Open FAIR risk analysis method is based. From these well-established paradigms, this White Paper extracts a broadly accepted set of risk and security concepts for expression in the ArchiMate language. These concepts cover:

- Vulnerability analysis: Asset at risk, vulnerability
- Risk management: Risk, threat, threat agent, loss event
- Security deployment: Control objective, control measure
- Classification: Risk domain

This White Paper examines three approaches to modeling risk and security concepts.

1. Using only the standard ArchiMate 2.1 language
2. Defining risk and security-specific specializations of ArchiMate 2.1 concepts
3. Defining risk and security concepts that complement ArchiMate 2.1 language concepts

This White Paper demonstrates, through concept mapping and case studies, that options 1 and 2 suffice for the majority of common risk and security concepts. The concepts that cannot readily be mapped, *domain* and *operational policy*, are also not specific to risk and security; they are specializations of concepts useful in a broader range of EA efforts.

Enterprise and security architects as well as risk and security analysts can benefit from this White Paper, which supports The Open Group vision of Boundaryless Information Flow™ by showing how ArchiMate models can help enterprises manage the myriad risks of our pervasively interconnected world while embracing its myriad opportunities.

Introduction

The importance of Enterprise Risk Management (ERM) and security rises with the progress of globalization and growth of the Internet. An increasing number of organizations interact with consumers and trading partners around the world, and are therefore exposed to an increasing variety of risks. Furthermore, they interact using electronic communications that can be compromised or abused. Many organizations are therefore facing complex risk scenarios that demand sophisticated planning and execution to protect their interests. Therefore, the ability to identify and manage risk has become a key priority in organizations no matter their size, industry, or region. Organizations need to understand the variables that affect their operations, so describing, classifying, managing, and mitigating risk factors is very important.

Enterprise Architecture (EA) builds transformative capabilities from people, processes, technology, and information. All of these capabilities can be threatened by diverse factors. Therefore, the assets that compose them must be protected. An EA approach that promotes systematic analysis, common understanding, and well-defined approaches to complex situations can therefore assist in the management of enterprise risk and security.

Enterprise Architects must help organizations manage risk through architectures that help avoid, transfer, mitigate, or accept adverse risks, because risks are not only inherent in the baseline state of every enterprise; they are inherent in any opportunities that the enterprise may embrace. ERM and security are therefore concerns that span all EA domains. Enterprise Architects can support ERM practices by:

- Understanding risk categories, the assets exposed to risks in each category, and the relationships between different risks
- Defining risk assessment methods
- Guiding risk management processes
- Integrating ERM into the EA practice

Risk and security models help organizations develop guidance and take action to embrace opportunity and manage risk. This White Paper examines a selection of well-established paradigms for risk and security modeling and analysis, extracts a set of core concepts from them, and maps most of the concepts to ArchiMate language elements.

This White Paper analyzes a representative sample of authoritative ERM and security frameworks and methods in order to gather a set of broadly accepted risk and security concepts, analyze their semantics, and reach consensus regarding the most important ones. The analyzed frameworks include the Casualty Actuary Society (CAS) ERM overview [10], the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework [9], Factor Analysis of Information Risk (Open FAIR) [3] and the Sherwood Applied Business Security Architecture (SABSA) [7,8]. This White Paper then models the Coldhard Steel case study from the CAS ERM overview, along with some original information security extensions. Based on the results of these modeling exercises, this White Paper describes the capabilities of the ArchiMate 2.1 language as specified, and as enhanced through its specified extension mechanisms (specialization of concepts, both from the ArchiMate core and the Motivation extension, and adding risk and security-specific attributes).

The TOGAF and ArchiMate Approach to Security

The TOGAF standard [20] presents security architecture as one of the important issues and organizational practices for Enterprise Architects. In the TOGAF Architecture Development Method (ADM), business requirements and drivers for security are mentioned as important issues for Phases A and B. The ADM focuses on generating requirements related to security, as well as for risk, by explaining how an organization's attitude towards risk determines the kind of protection that an asset needs and what the resulting security requirements are. It also mentions the need to define asset stewardship, especially for information assets, and the need to perform risk assessments and relate security to them.

The section of the TOGAF standard providing security guidance (Chapter 31: Risk Management) is mainly focused on security considerations and requirements for an EA iteration applying the ADM. It identifies specific areas of concern for security such as authentication, authorization, auditing, assurance, availability, asset protection, and administration, and relates them to risk management. All of these aspects are mainly presented as IT functions related to the information security discipline.

The TOGAF standard specifies security architecture viewpoints and frameworks, and also provides very general guidance for applying the Architecture Content Framework (ACF) and the TOGAF Metamodel to security views and patterns. The TOGAF standard presents examples like the data security diagram. In Chapter 35 (Architectural Artifacts) some basic patterns for security views are presented, and they are primarily focused on information systems security.

Regarding security management, the ADM recommends the integration of the EA effort with the security management organizational function along with other adjacent functions such as risk, project, and portfolio management.

This White Paper will extend the existing risk and security content of the TOGAF standard using relevant industry standards and leveraging the ArchiMate visual modeling language to:

- Cover risk assessment and protection of assets beyond information security
- Provide guidance and detailed tools and techniques for constructing specific models, viewpoints, and patterns that help practitioners to develop security architecture models
- Identify modeling patterns for functions such as authentication and authorization, security auditing, and monitoring
- Provide elements and mapping to the TOGAF ACF and Metamodel

The ArchiMate 2.1 specification makes very brief mentions of risk and security. It identifies risk and security as an important EA aspect that the language does not explicitly address, although it identifies the Infrastructure, Implementation, and Deployment and Project Viewpoints as useful for addressing risk or security concerns.

The TOGAF framework and the ArchiMate language can be extended and combined to help Enterprise Architects address risk and security. This White Paper provides specific guidance for risk and security modeling by extending the TOGAF standard and using the ArchiMate language.

Defining ERM and Security Together

This section gathers definitions for ERM, security, and related terms. It first summarizes a selection of leading definitions of ERM.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a coalition of professional organizations for accounting, auditing, and financial management. COSO issued its Enterprise Risk Management – Integrated Framework [9] in September 2004. The COSO ERM Framework includes key principles and concepts, a vocabulary, and guidance for evaluating and implementing ERM.

COSO defines ERM as:

"… a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Figure 1 assembles the definitions in this section into a generic ERM model. An enterprise contains stakeholders concerned with risk, who engage in ERM activity that assesses and manages risk.

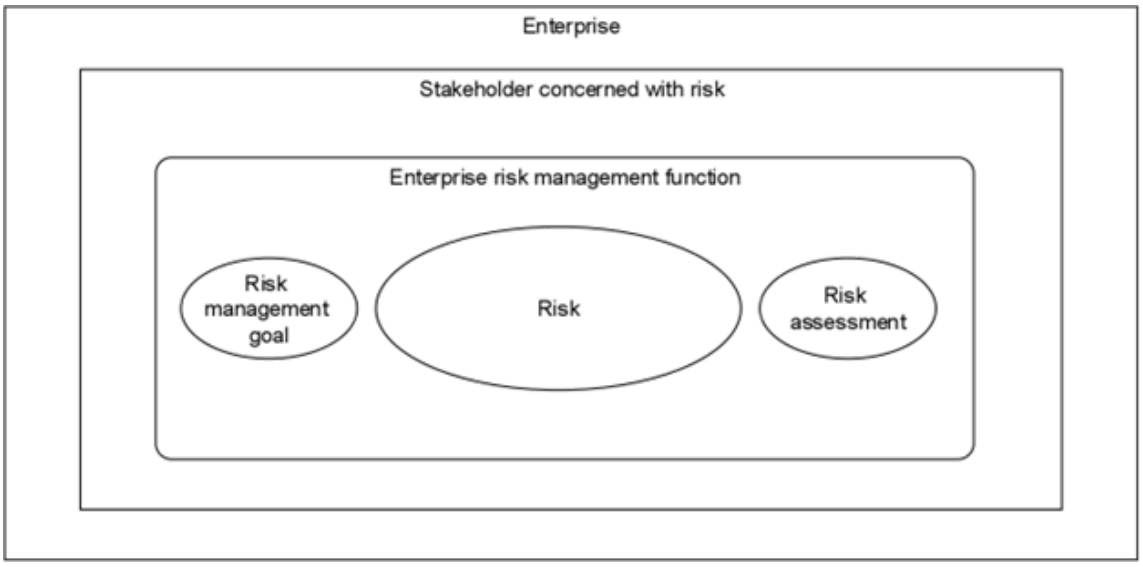

Figure 1: Generic Risk Model

Here is the Casualty Actuary Society (CAS) [10] definition:

"ERM is the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders."

The Institute of Risk Management (IRM) [4] defines risk management (clearly in an enterprise context) as follows:

"Risk management is a central part of any organization's strategic management. It is the process whereby organizations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities."

Each of these three ERM definitions discusses an enterprise engaging in risk-related activities that support or directly achieve organizational objectives. Each definition at least implies the existence of risk assessments, as well stakeholders concerned with risk. Therefore, they align with the ERM model in Figure 1.

This White Paper deals with modeling security as well as ERM. In relation to ERM, what does "security" mean? The Oxford English Dictionary (OED) [5] has a number of definitions that match typical goals of ERM:

- The state or condition of being or feeling secure
- Freedom from danger or threat:
    - The safety of an organization, establishment, or building from espionage, criminal activity, illegal entrance, or escape
    - With reference to encryption, or telecommunications or computer systems: the state of being protected from unauthorized access; freedom from the risk of being intercepted, decoded, tapped, etc.

The OED also has a number of definitions that match the behaviors and mechanisms of ERM:

- Something which secures or makes safe …
- A protection or defense against, from, for something …
- Grounds for regarding something as secure, safe, or certain; an assurance, safeguard, guarantee
- … any checks and procedures intended to keep a person, place, or thing secure

The OED reference to "encryption … telecommunication or computer systems" addresses information security. The SANS Institute [12] defines information security as:

"… the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private, and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption …"

This definition is closely related to the well-known Confidentiality, Integrity, and Availability (CIA) model used for developing security policy.

In summary, information security is part of security, which is in turn part of ERM, and these domains encompass related goals. Figure 2 builds on Figure 1 to show the relationship between these domains.

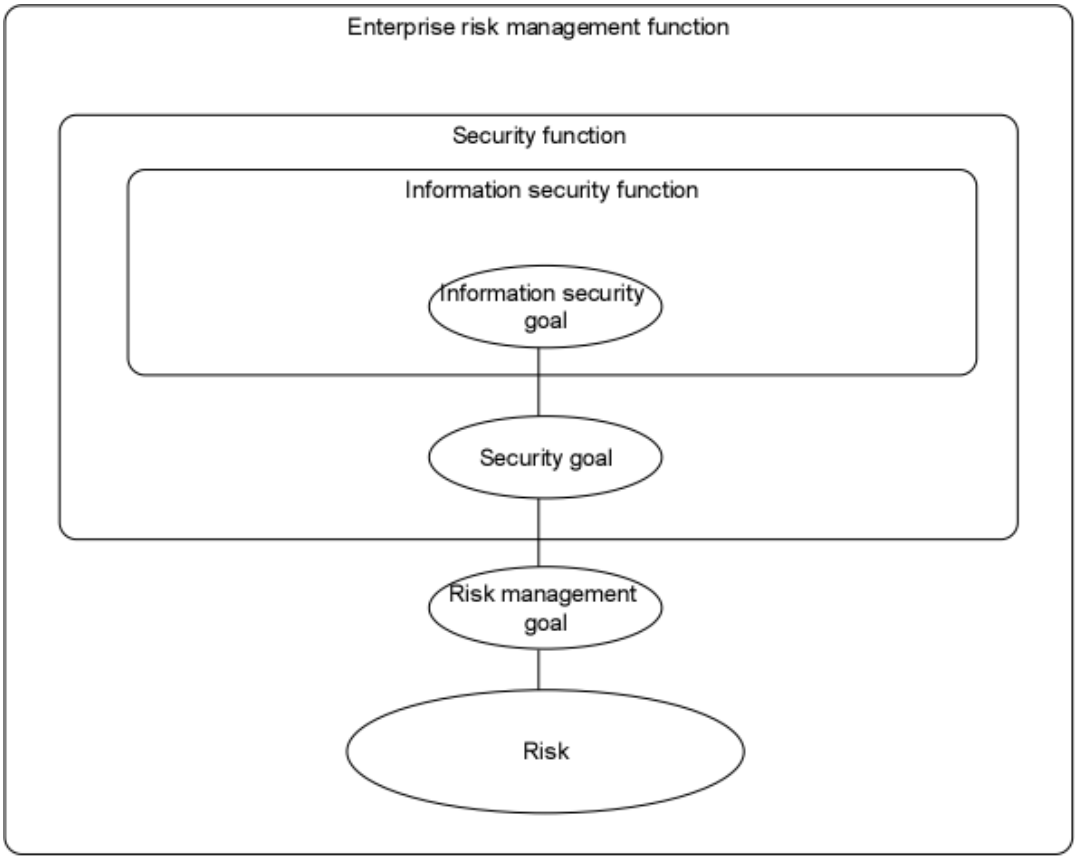

Figure 2: Security and Information Security as Specializations of ERM

COSO identifies four types of objectives for the continuous, enterprise-wide risk management activity that it specifies:

- Strategic objectives are high-level and aligned with the enterprise's mission.
- Operations objectives are concerned with effective and efficient use of resources.
- Reporting objectives are concerned with reliable reporting.
- Compliance objectives are concerned with applicable laws and regulations.

To specify and realize these activities, COSO defines seven types of activities:

- Objective Setting – Management must have a process in place to set objectives consistent with both the mission of the enterprise and its appetite for risk.
- Event Identification – Enterprises must identify both internal and external events, and distinguish between the risks and opportunities that they pose. Opportunities should be used for strategy development or objective setting.
- Risk Assessment – Enterprises must analyze and consider the likelihood and impact of risks, both

inherently and residually.

- Risk Response – Enterprises must determine how to respond to risks, which may be avoided, accepted, reduced, or shared, with actions based on organizational risk tolerance and appetite.
- Control – Policies and procedures must be established and implemented for effective responses to risk.
- Information and Communication – Timely identification, capture, and communication of relevant information across, up, and down organizations enables people to carry out their risk management responsibilities.

Figure 3 below models these activities as functions carried out by enterprises (entities, in COSO ERM parlance) to realize risk management objectivities.

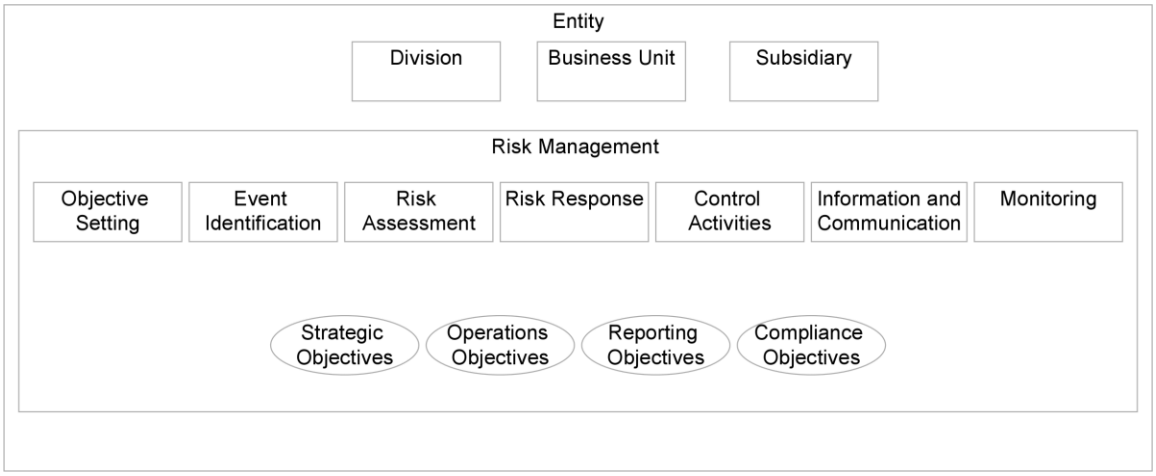

Figure 3: COSO ERM Model

Risk and Security Standards, Frameworks, and Concepts

This section identifies the risk and security concepts in the most common frameworks, including the Risk Taxonomy (O-RT) standard, the TOGAF security view risk classification, and the SABSA framework.

The breadth of ERM requires a structured approach to risk analysis along with a method of organizing the myriad risks facing every enterprise. The FAIR Risk Taxonomy defines and hierarchically classifies the elements of risk.

The Open Group Risk Taxonomy Standard/Open FAIR

This section summarizes The Open Group Risk Taxonomy (O-RT) standard, also known as the Open FAIR Risk Taxonomy (a part of the Open FAIR Body of Knowledge). This Open Group standard provides a definition and taxonomy for information security risk, as well as information regarding how to use the taxonomy. It describes the main factors that drive risk, their definitions, and relationships, so it provides a guideline for defining the basic terms for defining and measuring risk using a single logical and rational taxonomical framework. Although Open FAIR has its roots in information security risk, it can be applied to analyzing all kinds of risk.

The risk taxonomy overview is presented in Figure 4, which is taken from the O-RT standard.

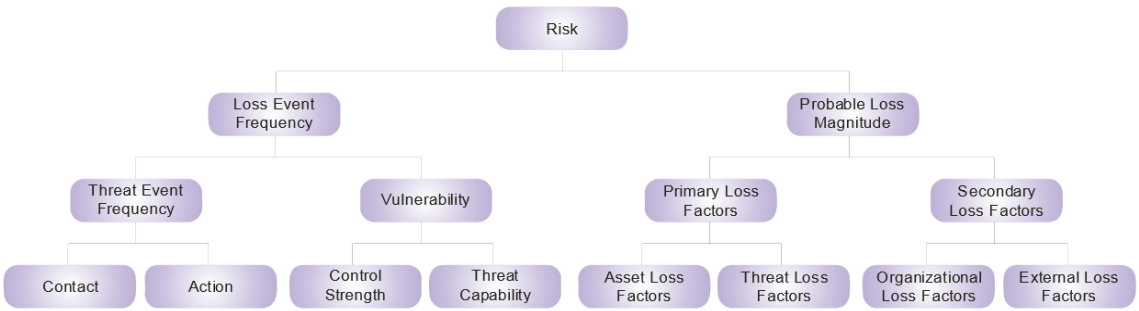

Figure 4: Open FAIR Risk Taxonomy [3]

In this taxonomy, "risk" is defined as the probable frequency and probable magnitude of future loss, which means that the risk definition is dependent on two factors: loss event frequency and probable loss magnitude. Then, recursively, each one of the rest of the factors is defined until the lower branches for the model are reached. For example, in the left branch of the model, the loss event frequency is dependent on threat event frequency and vulnerability.

All of the elements of the Open FAIR Risk Taxonomy refer to organizational assets that are being threatened by different environmental factors or agents that can be either internal or external to the organization. This risk exposure depends on the time interval in which the asset is being exposed and the vulnerability level that the asset might have. The right side of the model considers the risk impact, which depends on probable loss magnitude, which in turn depends on a hierarchy of loss factors.

Classifying Risks and Risk Assessments

While the Open FAIR Risk Taxonomy can be used to decompose and analyze a single risk, there are other risk taxonomies that seek to classify all risks within a particular domain. For example, the CAS ERM overview identifies four types of enterprise risk [10]:

- *Hazard Risks* include risks from fire and other property damage, windstorm and other natural perils, theft and other crime, personal injury, business interruption, disease and disability, as well as from liability claims.
- *Financial Risks* include risks from price, liquidity, credit, inflation and purchasing power, as well as from hedging and basis.
- *Operational Risks* include risks from business operations, empowerment mechanisms such as leadership and change readiness, information technology issues such as relevance and availability, as well as from problems with information and business reporting.
- *Strategic Risks* include risks from reputational damage, competition, customer wants, demographic and social and cultural trends, technological innovation and capital availability, as well as from regulatory and political trends.

Figure 5 represents the top two levels of this classification of enterprise risk.

Figure 5: CAS Classification of Enterprise Risk

Similarly, the American Society for Healthcare Risk Management (ASHRM) has developed an enterprise risk taxonomy for the healthcare domain [0], which is summarized in Figure 6 below.

Figure 6: ASHRM Common Healthcare Risk Domains

There could be several types of risks; some of them are more closely related with the EA development such as the operational, compliance, and security risks; however, other risk categories such as financial, project, organizational change, and system risk can also influence and be influenced by the EA practice.

Sherwood Applied Business Security Architecture (SABSA)

The SABSA matrix (framework) is a structure that is very similar to the Zachman framework, but specifically aimed at risk and security aspects. This matrix defines relevant viewpoints for risk and security modeling, in a systematic way. SABSA does not define specific modeling concepts, but the matrix does describe a wide variety of aspects that a modeler should be able to express. The exact content of each of the "cells" of the matrix is open to interpretation.

SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

© 1995 – 2009 SABSA Limited | info@sabsa.org

Figure 7: SABSA Framework [7,8]

In the context of this White Paper, mainly the upper three layers are relevant. The lower three layers are concerned with the detailed design of security controls. Some of the views are regular ArchiMate views that serve as the context for risk and security aspects, while others address specific security issues.

The table below summarizes the (new or specialized) concepts identified to populate the cells of the top three layers of the SABSA matrix. Concepts written in italics denote concepts that are already part of the ArchiMate language (core and extensions).

	Assets	Motivation	Process	People	Location	Time
Contextual Architecture	business asset; *goal*	opportunity; threat; risk; *stakeholder; driver, goal*	*business process*	*business actor, business role*	*location; network*	*plateau, requirement*
Conceptual Architecture	business attribute profile (business strategy; *business driver;* business asset; *goal; objective*)	business policy; control objective; (*goal; principle; requirement)*	security strategy	security entity (*business role; business actor; application component)*	(security domain); security element (security entity; security object); security policy	lifecycle
Logical Architecture	information asset	policy, policy statement (*requirement*); policy procedure (*process*); policy, guideline	*business process; business service*	trust; entity schema rule; object	network domain, *people/actor role* information resource *service; application component; application function; infrastructure service; network, infrastructure function;* information domain; application domain; people domain	*plateau,* program, *project*

Figure 8: Main Concepts in SABSA Framework Layers 1 to 3[1]

The SABSA approach toward risk factors considers both the risk of adverse occurrences as well as the prospect of beneficial events. The following ArchiMate model illustrates this approach, in which an asset at risk can be information, software, tangible organizational assets, human assets, and intangible assets. The two types of factors that can act against an asset are threats that have to be controlled and also opportunities that could become beneficial if exploited correctly.

[1] Concepts in italics more or less directly map to concepts in the ArchiMate 2.1 specification.

For a threat-based risk the following factors are important and are also mentioned in the Open FAIR Risk Taxonomy section of this White Paper:

- Threat
- Vulnerability
- Control

Threat management is not sufficient for organizations that want to innovate, enhance the value they deliver, and grow. Those organizations must also proactively identify events that present opportunities to increase the value of their assets and enhance their overall capabilities to deliver value to customers. The right side of Figure 9 depicts this approach, and differentiates it from the threat-centric approach to risk management.

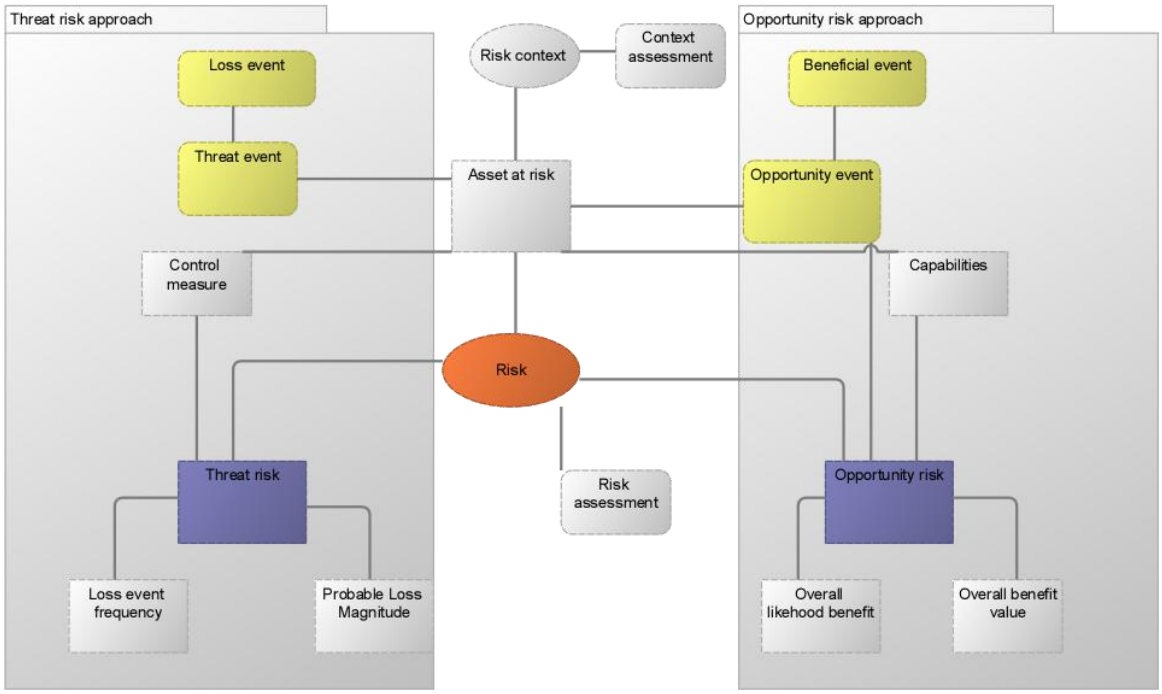

Figure 9: Comparison of Threat Risk and Opportunity Risk Approaches

Information System Security Risk Management (ISSRM) Domain Metamodel

In research performed at Tudor Research Centre, the different concepts of ISSRM and their relationships have been formalized as a domain metamodel (Figure 10); i.e., a conceptual model depicting the studied domain [15]. The ISSRM domain model has been established through the analysis of the related literature: risk management standards, security-related standards, security risk management standards and methods, and security requirements engineering frameworks (e.g., references [16,17,18]).

The ISSRM domain model is organized in three groups of concepts, as represented in Figure 10:

- Asset-related concepts describe assets and the goals which guarantee asset security.
- Risk-related concepts present how the risk itself is defined.

Risk treatment-related concepts describe what decisions, requirements, and controls should be defined and implemented in order to mitigate possible risks.

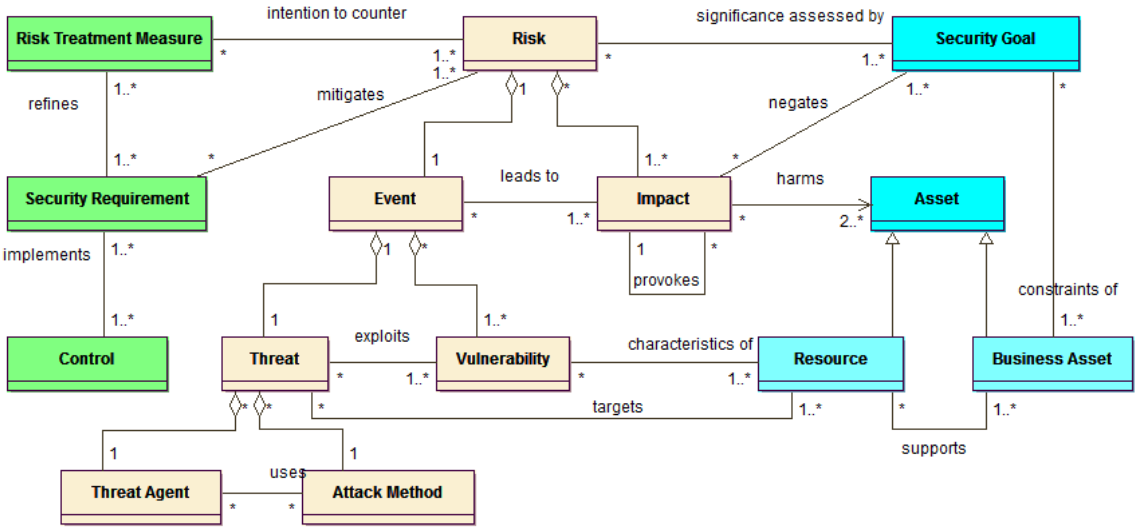

Figure 10: ISSRM Domain Model (Extracted from reference [15])

In this work, the concept of Security Goal merges the concepts of Security Criterion and Security Objective defined in an initial model. The description of the main concepts of the ISSRM domain model is summarized in the table below. An extension of the ArchiMate language with these concepts has been proposed in reference [20].

Concept	Description
Asset	Anything that has value to the organization and is necessary for achieving its objectives.
Business Asset	Describes information, processes, capabilities, and skills inherent to the business and core mission of the organization, having value for it.
IS Asset	A component of the IS supporting business assets like a database where information is stored.
Security Goal	A property or constraint on business assets describing their security needs, usually for confidentiality, integrity, and availability.
Risk	The combination of a threat with one or more vulnerabilities leading to a negative impact harming the assets.
Impact	The potential negative consequence of a risk that may harm assets of a system or an organization, when a threat (or the cause of a risk) is accomplished.
Vulnerability	A characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security.

Concept	Description
Threat	A potential attack or incident, which targets one or more IS assets and may lead to the assets being harmed.
Risk Treatment	An intentional decision to treat identified risks.
Security Requirement	The refinement of a treatment decision to mitigate the risk.
Control	Controls (countermeasures or safeguards) are designed to improve security, specified by a security requirement, and implemented to comply with it.

Introduction to the ArchiMate Standard

Core Concepts

ArchiMate [2], an Open Group standard, is an open and independent modeling language for EA that is supported by different tool vendors and consulting firms. It provides uniform representations for diagrams that describe EAs. Its core concepts (Figure 11) specify three main types of elements that are in turn often used to represent classes of real-world entities. These element types are:

- Active Structure Elements, which are entities capable of performing behavior
- Behavior Elements, which are units of activity performed by one or more Active Structure Elements
- Passive Structure Elements, upon which Active Structure Elements perform behavior

The ArchiMate language specializes two of these core element types to enable service-oriented architectural viewpoints:

- Behavior Elements, known as services, are units of functionality that systems expose to their environments. Services deliver value to their consumers while concealing the internal operations of the systems that expose them.
- Active Structure Elements, known as Interfaces, are points of access where systems expose one or more services to their environments.

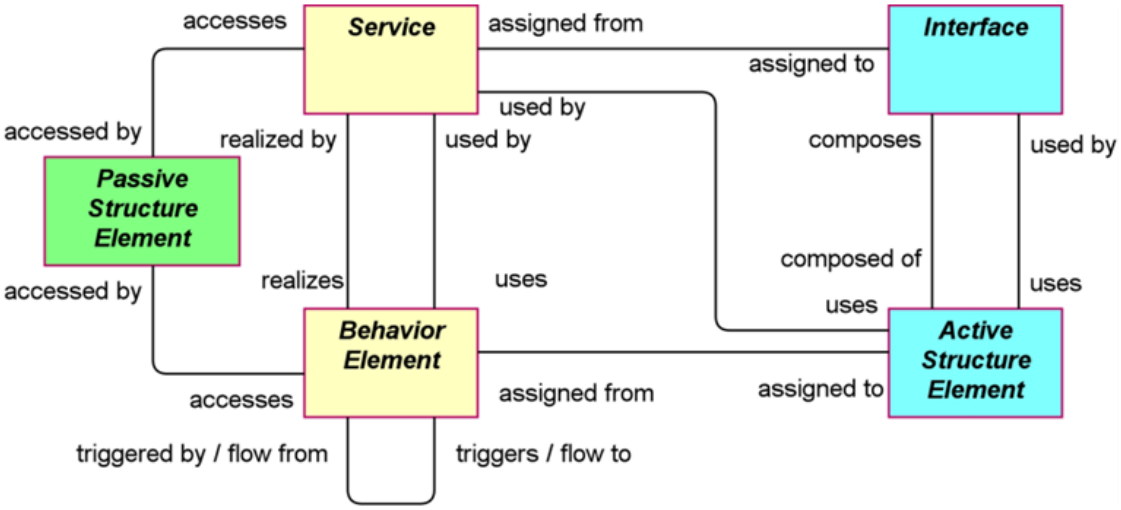

Figure 11: ArchiMate Core Concepts (Source [2])

Note that, in this diagram, relationships are red using the verb closest to the first element; e.g., an Active Structure Element uses an Interface, and a Service accesses a Passive Structure Element.

The ArchiMate language contains a core set of relationships that fall into three categories:

- Structural relationships model the structural coherence between structural or behavioral concepts of the

same or different types. They include association, access, used by, realization, assignment, aggregation, and composition.

- Dynamic relationships model dependencies between behavioral concepts. They include flow and triggering. In addition, the ArchiMate language enables the derivation of dynamic relationships between structural elements to which the behavioral functions are assigned. For example, modelers can depict a flow relationship between two application functions as a flow relationship between separate Application Components that perform those functions.
- Other relationships are neither structural nor dynamic. They include grouping, junction, and specialization.

The ArchiMate language defines three main layers based on specializations of its core concepts:

- The Business Layer models products and services available to external customers of the organization that is being described. These services are realized by business processes performed by business actors.
- The Application Layer provides the Business Layer with application services that are realized by software applications.
- The Technology Layer provides the infrastructure services such as data processing, storage, and communications necessary to run applications. These services are realized by hardware and system software.

The ArchiMate language combines its three layers with its three core element types for a nine-cell framework (Figure 12).

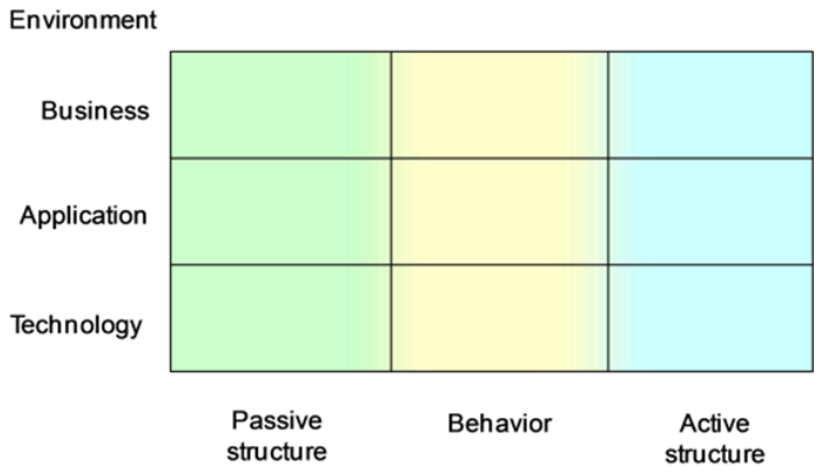

Figure 12: The ArchiMate Core Framework (Source [2])

Extensions

To its nine-cell core framework, the ArchiMate 2.1 standard adds two extensions:

- The Motivation extension models the elements that motivate enterprise design and operation. Its concepts include: stakeholder, driver, assessment, goal, requirement, and principle.

- The Implementation and Migration extension models the implementation of all aspects of EAs, as well as the migration between generations of implemented architectures. Its concepts include: work package, deliverable, plateau, and gap.

Viewpoints

The ArchiMate language also includes a set of architecture viewpoints and classifies them in two ways:

- Purpose, which may be designing a solution, deciding on a course of action, or informing employees, customers, or other stakeholders.
- Abstraction levels, which may embody the details needed by stakeholders such as software and process engineers, the systemic coherence needed by operational managers who must understand key relationships to solve problems and implement change, or the overview needed by executives, Enterprise Architects, and others who must make key decisions and manage change.

The ArchiMate Standard as a Modeling Language for the TOGAF Standard

The ArchiMate modeling language, together with its two extensions, can be used to model architectures developed using the TOGAF ADM. Figure 13 shows the correspondence between the activities of the ADM phases and the parts of the ArchiMate language.

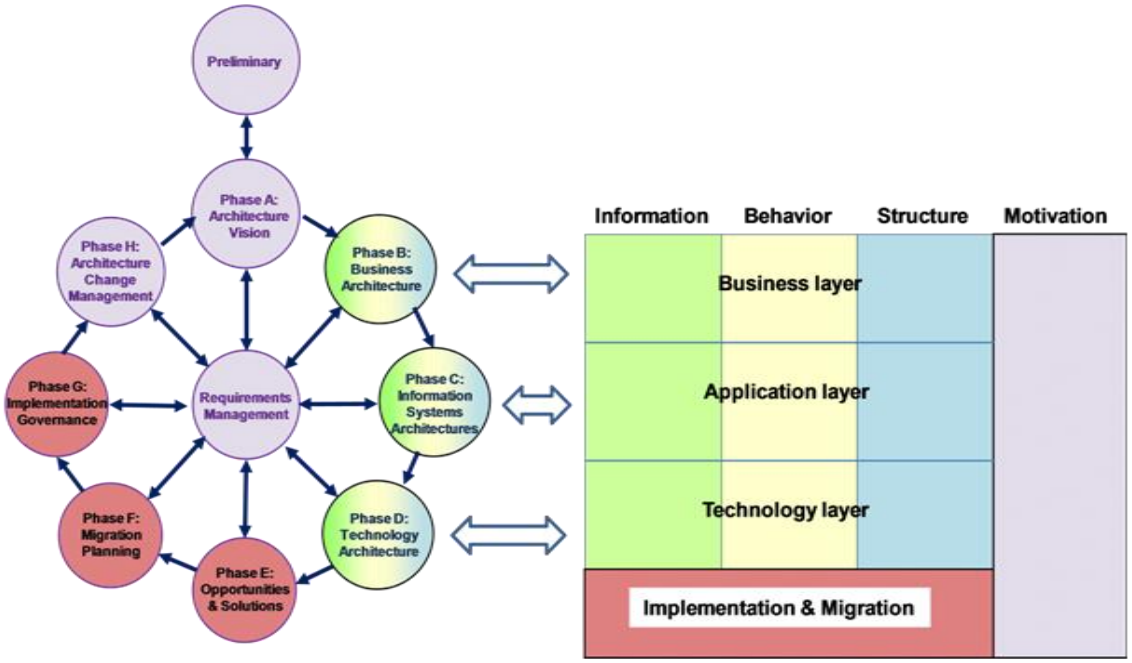

Figure 13: Correspondence between TOGAF ADM Phases and the ArchiMate Framework (Source [2])

Modeling Risk and Security Aspects with the ArchiMate Language

Business Value of Modeling ERM with the ArchiMate Language

The ArchiMate standard provides the modeling constructs to describe and interconnect the various architectural domains. Applying the ArchiMate language to represent risk and security concepts results in the ideal vehicle to consider these aspects in an integral way.

The ArchiMate language is a widely accepted open standard for modeling EA, with a large user base and a variety of modeling tools that support it. It fits well with other EA frameworks and standards, such as the TOGAF standard and the Zachman framework, as well as enterprise security management frameworks such as SABSA.

Through the Motivation extension, the ArchiMate language makes it possible to link control measures to security requirements, principles, and goals, as well as to the results of a risk analysis. On the other hand, ArchiMate models can be linked to design languages for business processes and IT solutions (e.g., BPMN and UML). In this way, full forward and backward traceability between architecture and design is achieved.

This traceability enables the definition of precise relationships between business and information technology entities, which facilitates cause and effect analysis. The ArchiMate language also allows modelers to define additional profile attributes for model elements. These attributes can be used to analyze architectures and determine the impact of architectural change on risk and security concerns. ArchiMate models are therefore suitable as a basis for both qualitative and quantitative risk and security analysis.

Consolidation of Risk and Security Concepts

This section identifies the common denominator of concepts for risk and security identified in our overview of standards and frameworks, and which are relevant in the context of EA models. It provides definitions for these concepts, as well as their main properties.

Risk

- The probable frequency and probable magnitude of future loss [3].
- The potential of loss (an undesirable outcome; however, not necessarily so) resulting from a given action, activity, and/or inaction, foreseen or unforeseen.
- A number of risk metrics are commonly applied, such as [3] loss event frequency and probable loss magnitude.
- Furthermore, a distinction may be made between:
    - Initial risk: before mitigation
    - Residual risk: after mitigation

Loss Event

Any circumstance that causes a loss or damage to an asset.

Threat

A possible danger that might exploit a vulnerability to breach security and thus cause possible harm. The term is ambiguous, as it can refer to a threatening circumstance, an entity capable of causing harm (threat entity), or the actual event that may cause harm (threat event). Therefore, we also introduce the more specific concepts:

- **Threat agent:** Anything – for example, an object, substance, individual, or group – that is capable of acting against an asset in a manner that can result in harm. This can be intentional; i.e., an attacker, but also unintentional; e.g., a well-intentioned, but inept, computer operator who trashes a daily batch job by typing the wrong command.
- **Threat event:** Event with the potential to adversely impact an asset. An *attack* is a specific type of threat event that is the result of an intentional malicious activity of an *attacker,* which is a specific type of threat agent.

Vulnerability

- The probability that an asset will be unable to resist the actions of a threat agent [3].
- A weakness which allows an attacker to threaten the value of an asset.

Domain

A set of related entities that share one or more characteristics and define the semantic of a specific field. This concept is essential to the next definition.

Risk Domain

A domain consisting of entities that share one or more characteristics relevant to risk management or security. A risk domain is also a context or set of conditions that affects a risk exposure level.

Risk Control, Treatment, Mitigation

- An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
- The deployment of a set of security services to protect against a security threat.

Control Requirement

A formalized need to be fulfilled by means of a control in order to face an identified threat.

Asset at Risk

- Anything tangible or intangible that is capable of being owned or controlled to produce value.
- Any data, device, or other component of the environment that supports information-related activities.

Policy

A set of rules which governs the behavior of a system:

- Exists at different levels: Strategy, Management, Design
- May be of different types: Operational, Structural, and Behavioral

Modeling Options

There are three different options for modeling risk and security aspects with the ArchiMate language:

1. The use of ArchiMate 2.1 concepts unmodified, as specified in the standard.
2. The use of the extension mechanisms as specified in the standard to define additional attributes or specializations of existing ArchiMate concepts.
3. The use of additional concepts that do not yet exist in the ArchiMate 2.1 standard and can be directly linked to existing concepts.

Of course, it is likely that a combination of these options will be used. If a combination of options 1 and 2 suffices, this would result in what could be called a "risk and security overlay" of the ArchiMate language, which may or may not be proposed for inclusion in the standard. If it turns out that option 3 is also required, this will result in proposing an actual risk and security extension for the standard.

Mapping of Consolidated Risk and Security Aspects to the ArchiMate Language

Although the TOGAF and ArchiMate standards, and various other standards and frameworks, deliver very valuable material that can help practitioners understand risk and security in the EA practice, they do not include specific guidelines and examples on how to model security and risk management. Therefore, in the remainder of this White Paper, this content is developed. Specific mappings will be suggested, and actual ArchiMate concepts and relations will be combined with profiling and specialization. Also, examples from case materials will be used to illustrate the use of these concepts.

The remainder of this section proposes a mapping between the consolidated risk and security concepts defined previously and components and concepts from the ArchiMate 2.1 specification.

Loss Event

A loss event can be mapped to the *business event* concept in ArchiMate, which may be triggered by a threat event. It may be useful to define a specific specialization of a business event to denote a loss event.

Threat

As indicated before, the term "threat" is ambiguous. The general notion of threat as a threatening circumstance can be modeled as a driver in the ArchiMate language. The mappings of the more specific concepts of "threat agent" and 'threat event' are given below.

- **Threat agent**: Different types of threat agent can be modeled as different kinds of active structure elements in the ArchiMate language; e.g., a business actor, business role, application component, node, system software, or device.
- **Threat event**: A threat event may map most naturally to a *business event* in the ArchiMate language. Because the concept of threat event plays an important role in risk management, it is advisable to introduce it as a specialization of a business event.

Risk

A risk is a quantification of a threat, and as such it maps most naturally to an *assessment* in the ArchiMate language. Because of the central role of this concept in ERM, the proposal is to define the risk concept as a specialization of an assessment.

Risk Metrics

As well as the different types of risks (e.g., initial and residual), may be defined as attributes in a risk profile of an assessment.

Vulnerability

A vulnerability is the result of analyzing the weaknesses of elements in the architecture considering all the environmental factors that could affect the system. An example of a vulnerability is a non-encrypted communication channel over the public Internet, which means that confidential messages may be intercepted. For explicitly modeling a vulnerability, it most naturally maps to an *assessment* in the ArchiMate language. In that case, the proposal is to model a vulnerability as a specialization of an assessment. Alternatively, it may be specified as an attribute of an asset at risk or a risk domain.

Domain

The ArchiMate language does not yet define a general *domain* concept. The *location* concept represents a specific kind of domain (i.e., a geographic domain). The *grouping* relation can also be used to group elements that belong to a certain domain, but has some limitations (e.g., it is not possible to link a group to other elements with a relation). For an example of the use of the domain concept, see Use of the Risk Domain Concept.

Risk Control, Treatment, and Mitigation

Depending on the kind of control, almost any core concept or combination of core concepts can be used to model the implementation of the control. A control may also be realized by a grouping of a number of core concepts, which is something that cannot properly be modeled in the ArchiMate language (see Domain).

Control Requirement

In a risk analysis process, a specification of an action or set of actions that have to be performed or that should be implemented as part of the control, treatment, and mitigation of a particular risk. A control requirement is realized by core entities used for mitigation, treatment, and control.

Asset at Risk

Almost any core concept or combination of concepts can be an asset to the organization. A specific *asset* profile can be assigned to these concepts to specify specific attributes of assets; e.g., their value. Alternatively, the concept can be associated with the ArchiMate *value* concept.

Policy

At the design level, a policy may map to a *principle* from the ArchiMate Motivation extension. The ArchiMate language does not yet have the concept of *operational* policy. This is a candidate concept that could be considered for a future version of the ArchiMate standard. Note that the concept of *policy* can be used in a generic way, with risk policy and security policy as possible specializations.

Figure 14summarizes the main mapping of the concepts.

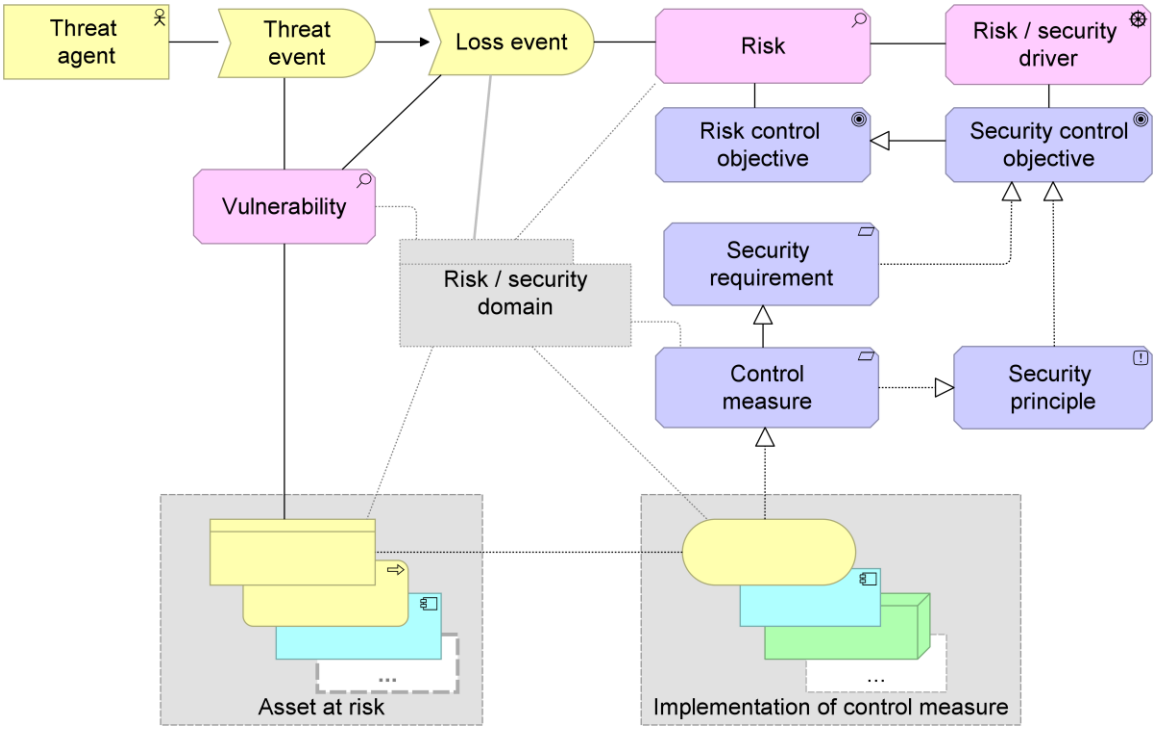

Figure 14: Mapping of Risk and Security Concepts to the ArchiMate Language

Case Studies and Examples

This section further explores the risk domain concept and uses the ArchiMate 2.1 language together with additional risk domain notations to depict four scenarios. The first is an original scenario involving security at aircraft maintenance facilities, and the next three are elaborations of the Coldhard Steel scenario [9]. This scenario, part of the CAS ERM Overview, describes the risks faced by a US-based manufacturer of steel products, such as roller and ball bearings, used in industrial machinery. The final scenarios in this section illustrate a vulnerability assessment of technical infrastructure.

Use of the Risk Domain Concept

In Mapping of Consolidated Risk and Security Aspects to the ArchiMate Language, this White Paper has defined a risk domain as "consisting of entities that share one or more characteristics relevant to risk management or security". Table 1 details these common characteristics and provides examples of domains that share them. The entries describing common characteristics are numbered for reference in examples later in the text.

Table 1: Common Characteristics Shared by Entities within a Risk Domain

Common Characteristic	Example Risk Domains
Exposure to a threat or risk	Registered users of an e-commerce website from which credit card information has been stolen, and are therefore particularly vulnerable to fraudulent charges, or residences that do not have smoke alarms, and are therefore particularly vulnerable to fire.
Possession of a vulnerability	Individuals who record their passwords on paper near their computer workstations, or instances of an operating system that are missing a critical security patch.
Possession of a control requirement	Individuals recently released from prison who must report regularly to a parole officer, or wireless devices that access a corporate network that transmits sensitive information, and must therefore be authenticated, authorized, and monitored whenever they are connected.
Participation in a control, treatment, or mitigation	Individuals who use password managers to generate and store complex, random passwords for the websites they access, or firewalls that control access to a government network.
Participation in a threat agent	Individuals with criminal records who possess unlicensed handguns or flammable material stored in a warehouse.
Relevance, authority, or influence of a control, treatment, or mitigation	Individuals subject to the laws of a particular jurisdiction, or all neighborhoods in a city subject to extra police patrols due to high crime rates.
Inclusion in a classification for the purpose or assessing or mitigating risk	All computers that are connected to the same corporate network and running a particular operating system, for which a patch assessment or patching cycle could be developed, or all individuals living in a neighborhood that has been exposed to toxic industrial chemicals, for which a set of health checks or precautionary recommendations could be developed.

ArchiMate modelers can use the grouping relationship to identify domains and describe their contents. The grouping concept is uniquely suited for this purpose, since it is the only relationship within the language in which any number of elements representing any combination of concepts can participate. This flexibility is critical to representing domains, since instances, classifications, and assessments of vulnerabilities, risks, threats, controls, and related risk concepts frequently aggregate diverse elements.

For example, a software component may possess an internal vulnerability that could be exploited by an attacker, but if the software component is used within a cardkey system to control physical access to an aircraft maintenance facility operated by an airline, its vulnerability may put the functioning of the aircraft, the lives of passengers and crew, and the financial health of the airline at risk. A comprehensive approach to mitigating the overall risk of access control software malfunction could require:

- Technical controls such as software patches and code restructuring instituted by the software vendor
- Administrative controls such as:
    - Enhanced quality assurance procedures instituted by the software developer
    - Revisions in the contract between the airline and the software vendor
    - Audits of the software vendor by the airline or a trusted agent
    - Enhanced patching procedures instituted by the airline's IT organization
- Physical controls such as placing the onsite access control server appliance in a locked closet

In addition, different domains might require different controls to mitigate the risk (Table 1, entry 6). If the airline uses two aircraft maintenance facilities at different airports with separate instances of the same cardkey system, but outsources the operations of one to a service provider, then mitigating the risk at the second facility could also require:

- Administrative controls such as:
    - Enhanced patching procedures instituted by the outsourcer's IT organizations
    - Revisions in the contract between the airline and the outsourcer
    - Audits of the outsourcer by the airline or a trusted agent

The ArchiMate grouping relationship can be used for this scenario to organize both the elements of risk, and the measures taken to mitigate risk. However, in order to express the mitigation relationship between the risk of software attack and different combinations of measures required to mitigate that risk at the two aircraft maintenance facilities, ArchiMate modelers must be able to combine diverse elements into risk domains that can participate in explicit mitigation relationships (Table 1, entry 1).

Figure 15 illustrates the use of the ArchiMate 2.1 language, and the opportunities for expression of domains and mitigation relationships. The diagram expresses domains as ellipses with dashed borders, and mitigation relationships as thick grey lines with long dashes, and hollow-point arrows pointing from the mitigating domain to the domain exposed to the risk. The two facility domains share exposures to the same risks (Table 1, entries 4 and 6) which are expressed as drivers. The shared risk of unauthorized access positively influences the risk of aircraft malfunction, which has enterprise-wide implications. Per the scenario, some mitigation requirements are specific to one of the two facilities, and some are shared. Each of the three

mitigation domains (Table 1, entry 4) contain requirements that mitigate the risks of software attack and unauthorized access.

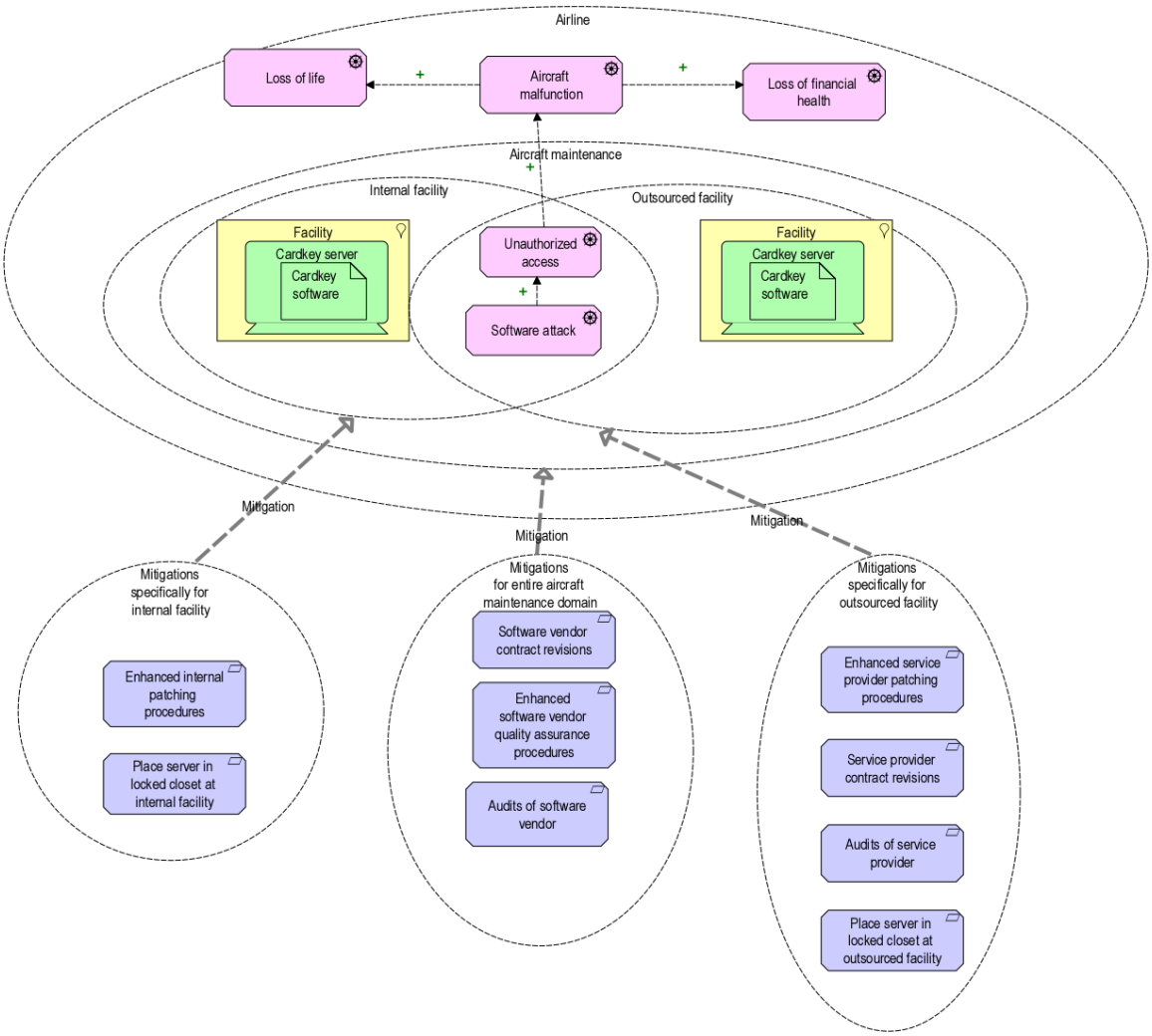

Figure 15: Aircraft Maintenance Scenario with Risk Domains

Figure 18 and Figure 19 illustrate a risk mitigation approach – continuous improvement of machine reliability – which applies across the entire Coldhard Steel risk domain (Table 1, entry 1). However, the Gary and Chicago factory risk domain have different vulnerabilities (Table 1, entry 2), and therefore the local implementation of the enterprise risk mitigation strategy constitutes two very different domains (Table 1, entry 4).

Coldhard Steel

This section uses the Coldhard Steel company case from reference [9] to illustrate the stereotyping of ArchiMate Motivation extension concepts as risk concepts. Coldhard Steel manufactures products such as roller and ball bearings that are used in other industrial machinery. Coldhard Steel operates in the Midwest

region of the United States, is family-owned, and has a unionized labor force. The Coldhard Steel case has been selected because it is a well-accepted example case in the risk and security field.

Figure 16 illustrates such use of stereotyped ArchiMate 2.1 concepts to model risk and security concepts. Coldhard steel experiences a threat that machines may fail due to inadequate power supply. This threat is mapped onto the concept of driver. This threat leads to a risk that once a year the power supply is inadequate, and with an effect that the production loss is $100.000, an assessment is stereotyped to risk. A control objective is added to mitigate the risk. The control objective is to increase peak capacity of the power supplies. The concept goal is stereotyped to control objective. A control measure, replace factory power supplies, is used to realize the control objective. A requirement is stereotyped to control measure to model this.

A threat can also lead to a loss event, in the case of Coldhard Steel a power supply failure. A business event is stereotyped to express this. A vulnerability of an asset can lead to a loss event. In the case of Coldhard Steel, the power supply cannot handle large power fluctuations. An assessment is stereotyped to express this. ArchiMate Core elements are stereotyped to assets. In this example the asset realizes the control measure, to illustrate that the control measure is implemented.

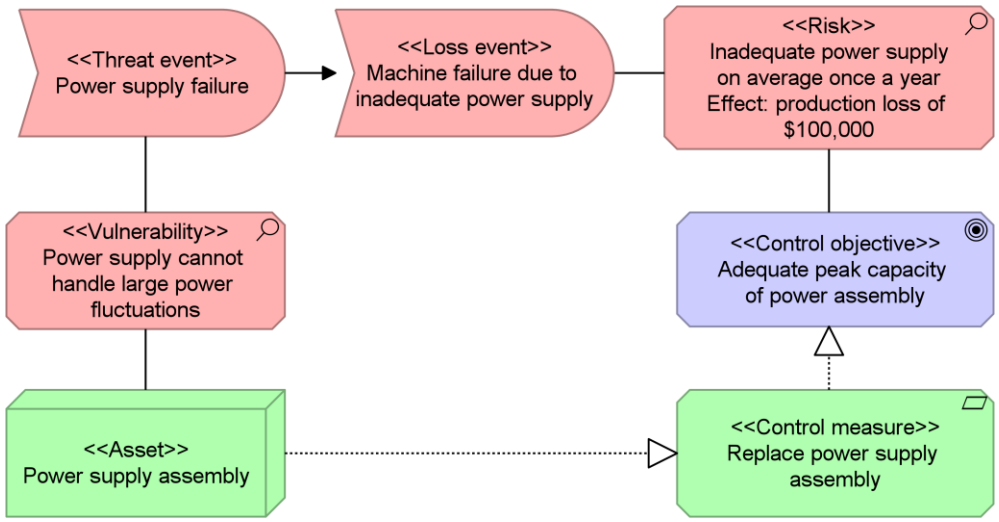

Figure 16: Coldhard Steel, Example 1

Figure 17 illustrates two other examples. The left figure can be read as follows. There is a threat that an employee submits a compensation claim for work-related injuries. This leads to the risk that the compensation claims for injuries are unacceptable. A control objective is stated to reduce the exposure to compensation claims. The control measure is to implement safety procedures. The threat can lead to the loss event work-related safety incident. This loss event is possible through the vulnerability of inadequate safety procedures.

The right part of the figure illustrates yet another kind of risk example. Coldhard steel is situated in an area where there is a threat of tornados. These tornados can cause damage to plant and equipment. This leads to the risk that there are unacceptable costs to repair the damage. This leads to the control objective to reduce exposure to tornado damage and the control measure to improve the structural integrity of the building.

The threat can lead to the loss event that the tornado hits the factory. The vulnerability that the equipment is not resistant to tornados leads to the loss event and the risk.

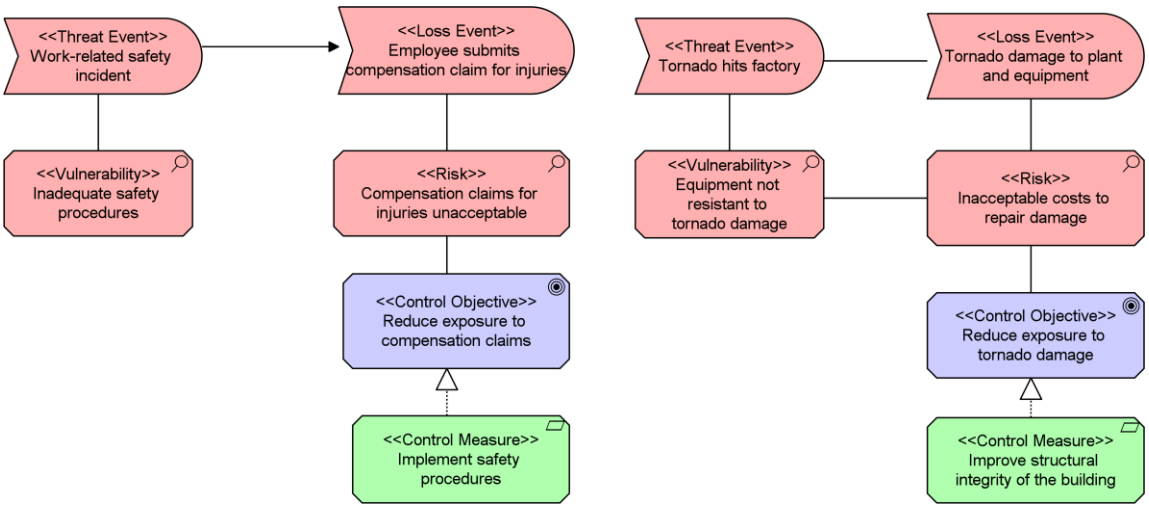

Figure 17: Coldhard Steel, Examples 2 and 3

As another example of the use of the domain concept, as explained in the previous subsection, Figure 18 and Figure 19 illustrate a risk mitigation approach – continuous improvement of machine reliability – which applies across the entire Coldhard Steel risk domain (Table 1, entry 1). However, the Gary (Figure 18) and Chicago (Figure 19) factory risk domains have different vulnerabilities (Table 1, entry 2), and therefore the local implementation of the enterprise risk mitigation strategy constitutes two very different domains (Table 1, entry 4).

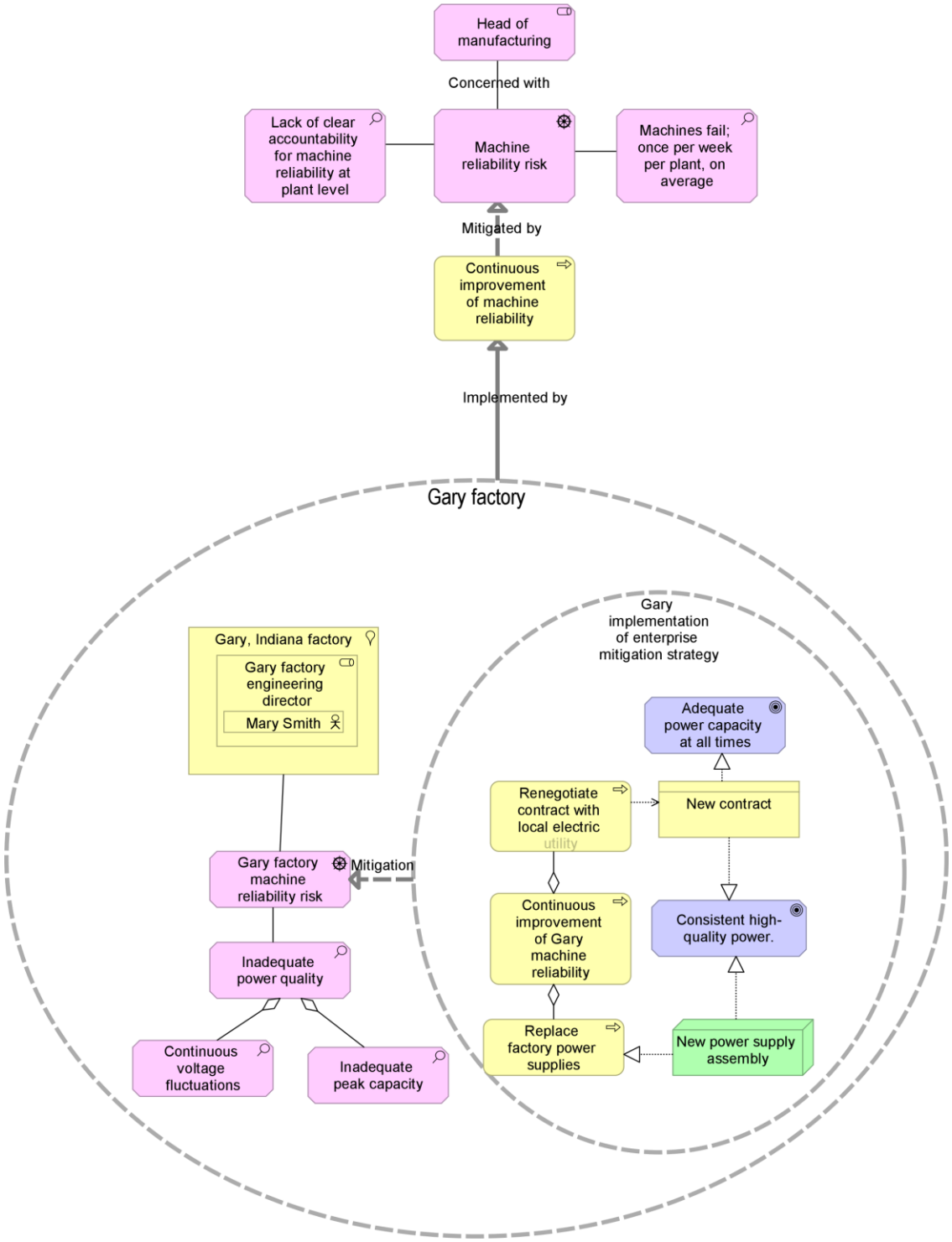

Figure 18 Mitigation of Machine Failure Risk at Coldhard Steel *Gary* Factory

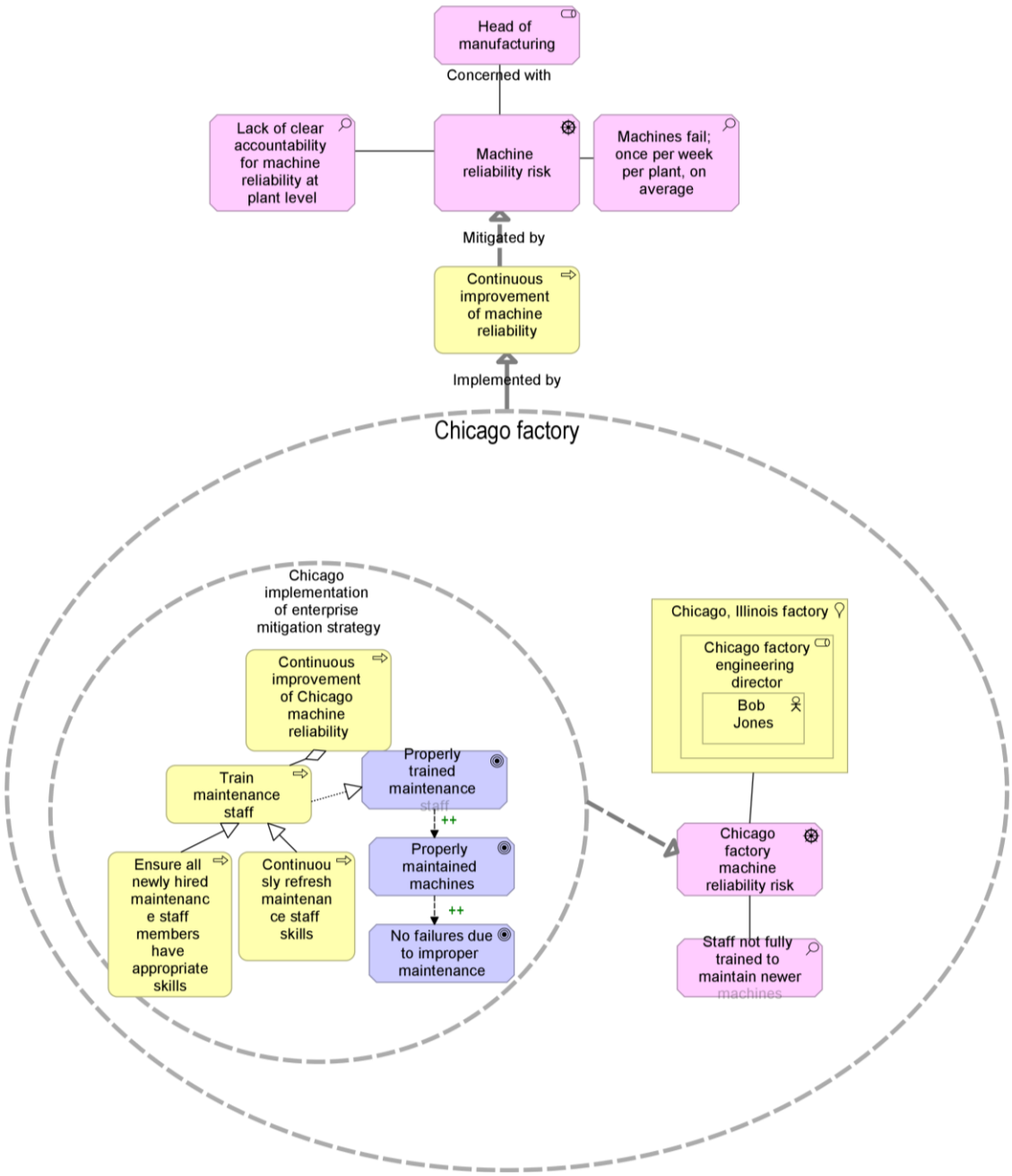

Figure 19: Mitigation of Machine Failure Risk at Coldhard Steel *Chicago* Factory

Vulnerability Assessment of a Technical Infrastructure

A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a computer network or system. A vulnerability assessment may include the use of a penetration test (pen test); i.e., an attack on a computer network or system with the intention of finding security weaknesses, potentially gaining access to it, its functionality, and data. This process may be supported by one of the many available commercial or open source automated vulnerability scanners, which produce a report of the vulnerabilities found in a computer network, host, or set of hosts.

Figure 20 below shows an example of the results of a vulnerability scan of a single application server. Five vulnerabilities are found, with varying levels of risk (risk factors), related to different ports. The overall security of the server is determined by the weakest link; i.e., the maximum of the risk factors of the relevant vulnerabilities.

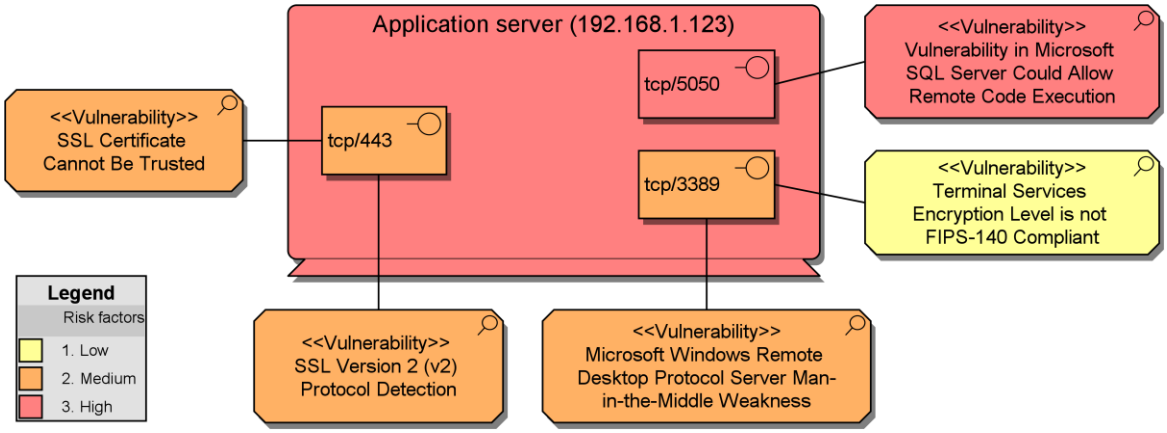

Figure 20: Results of a Vulnerability Scan

Figure 21 shows the context of one of these vulnerabilities. The vulnerability is present on three different hosts in the network. Also, a known control measure that can be used to mitigate the risk associated with vulnerability is shown in the model.

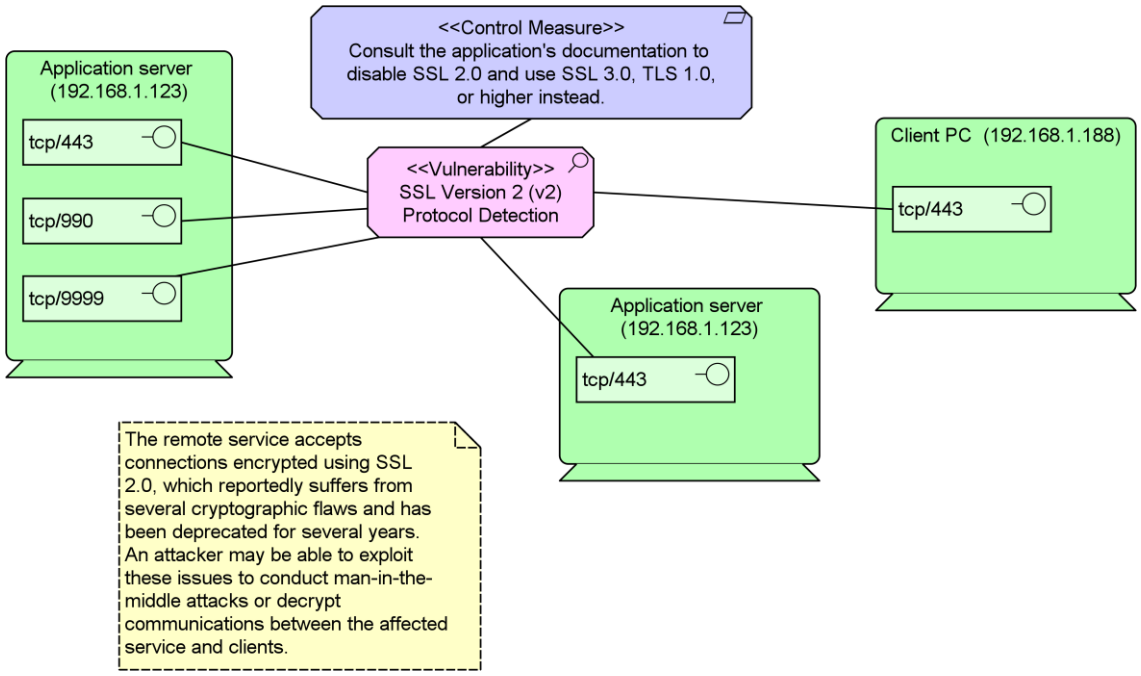

Figure 21: Vulnerability Context

Although a vulnerability assessment provides an overview of vulnerabilities at the technology level, this is not sufficient for a well-informed assessment of the risks at the business level. An EA model can help to analyze the business impact of the technical vulnerabilities, as illustrated in the example in Figure 22. Based on the results of this analysis, the (intermediate or final) results of which may be captured as profile elements attached to ArchiMate concepts, a decision can be made as to whether a control measure should be implemented to mitigate the risk.

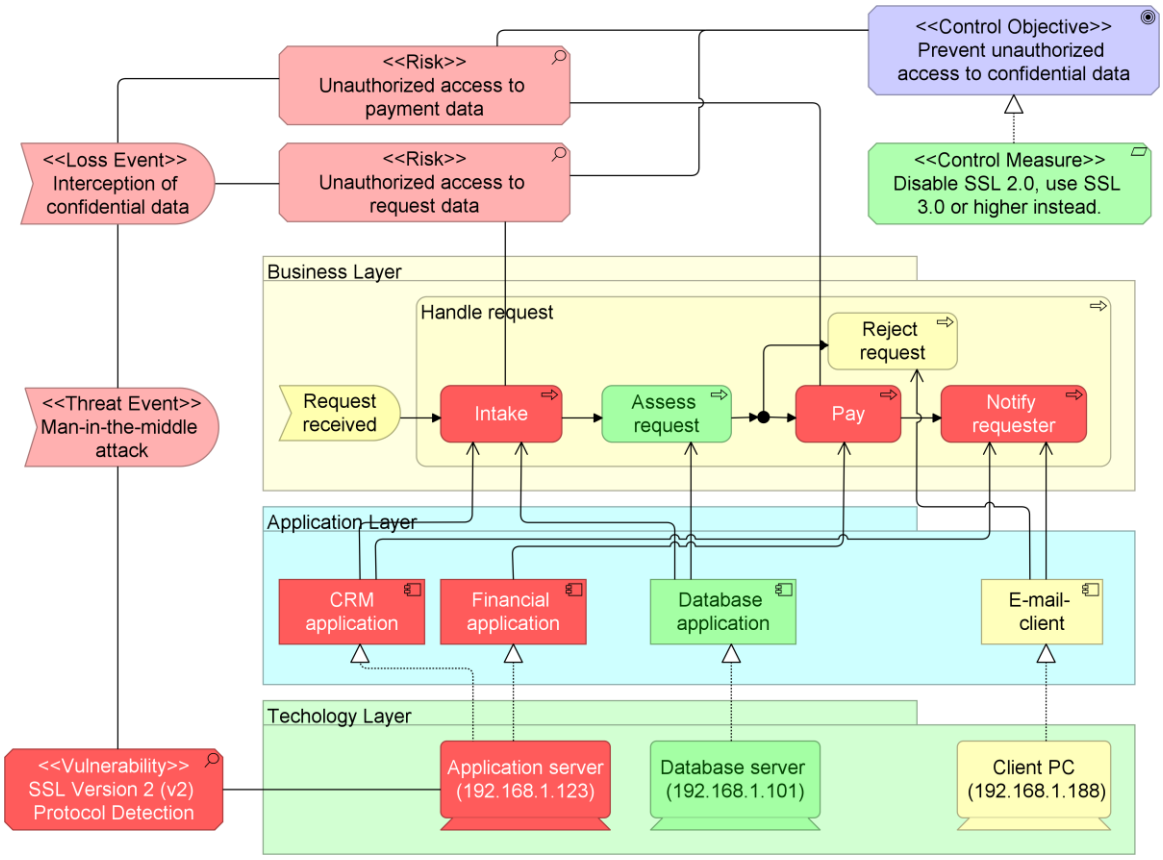

Figure 22: Business Impact of a Technical Vulnerability

Summary and Conclusions

ERM and security are closely interlinked with EA, including the design of organizations and the IT applications and infrastructure that support them. Therefore, this White Paper proposes how ERM and security can be expressed in the ArchiMate language for EA modeling.

In order to identify the relevant concepts, this White Paper examines a wide variety of standards and frameworks for ERM and security deployment, including those employed in the risk and security-related activities of The Open Group. Based on this, the paper establishes a common set of risk and security concepts, and demonstrates a mapping of these concepts to the ArchiMate language. Example cases illustrate these concepts.

The mapping and examples show that most of the risk and security concepts can be mapped to existing concepts in the ArchiMate language (Core and Motivation extension). However, to improve understanding, it is helpful to make explicit which of the risk or security concepts they represent. Specialization, one of the language extension mechanisms described in the ArchiMate standard, is primarily used for this. Two elements used in some of the examples are not in the standard language: the domain concept, a grouping that can have relationships with other concepts; and the mitigation relationship.

This White Paper also illustrates that the security and risk concepts and relationships can be added to a wide range of ArchiMate viewpoints. Any of the viewpoints described in the current ArchiMate 2.1 standard can be overlaid with risk and security concepts, and organizations may adopt these to assess risks. In a similar way, these concepts can also be used to express risk and security aspects in several TOGAF diagrams. In addition, modelers may add a number of additional viewpoints; e.g., a risk mitigation domain viewpoint (see the examples in Use of the Risk Domain Concept) or a risk analysis viewpoint (see the examples in the Coldhard Steel section).

References

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

[1] R.E. Giachetti: Design of Enterprise Systems, Theory, Architecture, and Methods, CRC Press, Boca Raton, FL, 2010 (p.4).

[2] ArchiMate® 2.1 Specification, Open Group Standard (C13L), December 2013, published by The Open Group; available at: www.opengroup.org/bookstore/catalog/c13l.htm.

[3] Risk Taxonomy (O-RT), Version 2.0, Open Group Standard (C13K), October 2013, published by The Open Group (as part of the Open FAIR Body of Knowledge); available at: www.opengroup.org/bookstore/catalog/c13k.htm.

[4] Institute of Risk Management: A Risk Management Standard, 2002; refer to: www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf.

[5] Oxford English Dictionary; refer to: www.oed.com (consulted December 2013).

[6] D. Ionita: Current Established Risk Assessments Methodologies and Tools, MSc Thesis, University of Twente, Enschede, the Netherlands, July 2013.

[7] J. Sherwood, A. Clark, D. Lynas: Enterprise Security Architecture: A Business-driven Approach, CMP Books, 2005.

[8] J. Sherwood, A. Clark, D. Lynas: Enterprise Security Architecture, White Paper, SABSA Institute, 2009.

[9] Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management – Integrated Framework, 2004; refer to: www.coso.org/documents/coso_erm_executivesummary.pdf.

[10] Casualty Actuary Society (CAS) Overview of Enterprise Risk Management, 2003; refer to: http://www.casact.org/area/erm/overview.pdf.

[11] Risk Management Handbook for Healthcare Organizations, Sixth Edition, Volume 1, American Society for Healthcare Risk Management (ASHRM), 2011.

[12] SANS Institute; refer to: www.sans.org/information_security.php (consulted December 2013).

[13] 44 United States Code (USC) 3542 – Definitions; refer to: www.law.cornell.edu/uscode/text/44/3542 (consulted December 2013).

[14] Chad Perrin: The CIA Triad; refer to: www.techrepublic.com/blog/it-security/the-cia-triad/488 (consulted December 2013).

[15] E. Dubois, P. Heymans, N. Mayer, R. Matulevičius: A Systematic Approach to Define the Domain of Information System Security Risk Management (ISSRM), in Intentional Perspectives on Information Systems Engineering, S. Nurcan, C. Salinesi, C. Souveyet, J. Ralyté, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010 (pp.289–306).

[16] AS/NZS 4360: Risk Management, SAI Global, 2004.

[17] ISO/IEC Guide 73: Risk Management – Vocabulary – Guidelines for Use in Standards, Geneva: International Organization for Standardization, 2002.

[18] ISO/IEC 13335-1: Information Technology – Security Techniques – Management of Information and Communications Technology Security – Part 1: Concepts and Models for Information and Communications Technology Security Management, Geneva: International Organization for Standardization, 2004.

[19] E. Grandry, C. Feltus, E. Dubois: Conceptual Integration of Enterprise Architecture Management and Security Risk Management, The Fifth Workshop on Service-Oriented Enterprise Architecture for Enterprise Engineering (SoEA4EE'2013), Vancouver, BC, Canada.

[20] TOGAF® Version 9.1, Enterprise Edition, Open Group Standard (G116), December 2011, published by The Open Group; available at www.opengroup.org/bookstore/catalog/g116.htm.

About the Authors

Iver Band is a practicing Enterprise Architect and a developer and communicator of Enterprise Architecture standards and methods. Recently, he joined Cambia Health Solutions, where he shapes solutions that promote accountability, quality, and efficiency in healthcare delivery. For the previous six years at The Standard, a diversified financial services company, he focused on business solutions and governance, and prior to that, infrastructure. He guided contact center and CRM implementations, claims system modernization, end-user computing, and trading workflow automation. In his infrastructure role, Iver developed data center, computing platform, and resilience strategies. Prior to his work at The Standard, Iver had a lengthy career at Hewlett-Packard with roles ranging from IT Director for a global business to HP Labs Visiting Technologist. At HP Labs, he researched security topics such as role engineering, and led the development of a patented approach to network security management.

Iver also serves as Director of Enterprise and Solution Architecture for EA Principals, a training and consulting firm, for which he works with clients, develops curriculum materials, and edits the Enterprise Architecture Professional Journal and EAPJ.org. Iver represents EA Principals in The Open Group, where he is the elected Vice Chair of The ArchiMate Forum. As Vice Chair, Iver has led development of a number of Open Group White Papers.

Iver is TOGAF 9 Certfied, ArchiMate 2 Certified, a Certified Information Systems Security Professional (CISSP), a Certified Information Professional (CIP), and a Prosci Certified Change Consultant.

Wilco Engelsman is a research consultant at BiZZdesign, specialized in the areas of enterprise architecture, business requirements management and enterprise risk management. He was one of the main contributors to the development of the Motivation extension of the ArchiMate standard. He is also pursuing a PhD in Computer Science at the University of Twente.

Christophe Feltus graduated as an Electromechanics Engineer from the Institut Supérieur Industriel des Art et Métiers Pierrard (Belgium) and Doctor of Science (Computer Science) from the University of Namur (Belgium). He worked for several years in private companies as: Production Head at Pfizer SA in Jette, Project Coordinator at Nizet Entreprise in Louvain-la-Neuve, and Assessor for the Civil Belgium Aviation Administration in Brussels, Belgium. Than he joined the Public Research Centre Henri Tudor in the Grand-Duchy of Luxembourg in 1999 to work in the field of Service Science and Innovation. There he has taken part in projects related to IT security, IT governance, business IT/alignment, and enterprise architecture modeling. In 2015, the Public Research Centre Gabriel Lippmann and the Public Research Centre Henri Tudor merged to become the Luxembourg Institute of Science and Technology.

Sonia Gonzalez is a Senior Consultant at Dux Diligens. Sonia provides consulting and training services in the areas of business innovation, business process modeling, and Enterprise Architecture. In this position she is involved in the development of new products and services that the company is offering to its customers in Latin America and Spain. She is also TOGAF® 9 Certified and ArchiMate® 2 Certified, and is a trainer for an accredited training course provider and has developed workshops and EA consultancy projects using the TOGAF standard as a reference framework and the ArchiMate standard as a modeling language. As a representative of an Open Group member organization, she is participating in several projects in the Architecture and ArchiMate Forums.

Jim Hietala, CISSP, GSEC, is Vice President, Security for The Open Group, where he manages all security and risk management programs and standards activities, including the Security Forum. He has participated in the development of several industry standards including O-ISM3, O-ESA, Risk Taxonomy, and O-ACEML. He also led the development of compliance and audit guidance for the Cloud Security Alliance v2 publication.

Jim is a frequent speaker at industry conferences. He has participated in the SANS Analyst/Expert program, having written several research white papers and participated in several webcasts for SANS. He has also published numerous articles on information security, risk management, and compliance topics in publications including CSO, The ISSA Journal, Bank Accounting & Finance, Risk Factor, SC Magazine, and others.

An IT security industry veteran, he has held leadership roles at several IT security vendors. Jim holds a BS in Marketing from Southern Illinois University.

Henk Jonkers is a senior research consultant, involved in BiZZdesign's innovations in the areas of Enterprise Architecture and engineering. He participates in multi-party research projects, contributes to training courses, and performs consultancy assignments. Previously, as a member of scientific staff at an applied IT research institute, he was involved in research projects on business process modeling and analysis, EA, SOA, and model-driven development. He was one of the main developers of the ArchiMate language and an author of the ArchiMate 1.0 and 2.0 Specifications, and is actively involved in the activities of The Open Group ArchiMate Forum.

Sébastien Massart is a senior consultant at Arismore and is responsible for the first ArchiMate training center in France. He manages the ArchiMate Work Group at The Open Group France, providing methodology and assessing competencies to elect new trainers. He works across a variety of sectors, with a particular focus on Telecommunications and Industries. His current mission is a project which bridges the gap between business and IS/IT through the Entreprise Architecture Taskforce. Prior to his current role, he was a Technical Architect on a range of complex infrastructures.

About The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 400 member organizations, The Open Group has a diverse membership that spans all sectors of the IT community – customers, systems and solutions suppliers, tool vendors, integrators, and consultants, as well as academics and researchers – to:

- Capture, understand, and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

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