

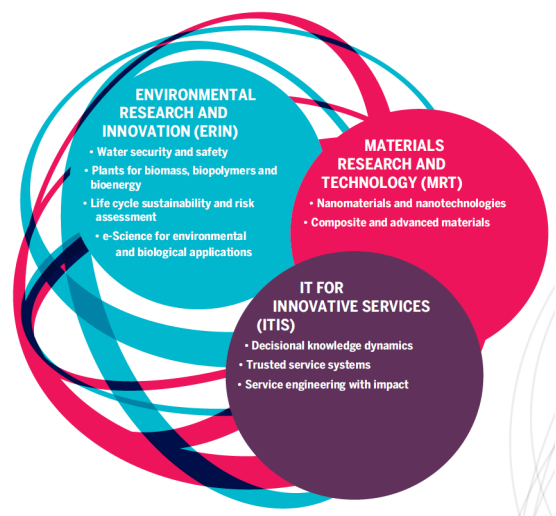
A Risk Management Framework for Compliance of Regulated Services

Nicolas MAYER
Luxembourg Institute of Science and Technology



Nicolas Mayer

- Since 2012: **Senior R&T Associate** at the Luxembourg Institute of Science and Technology
 - Management of projects in the domain of information security
- 2010 to 2012: **Project manager** for the Economic Interest Group supporting the National Standards Body of Luxembourg
 - in charge of the development and follow-up for ILNAS of the IT standardization field
- 2009 to 2010: **Product Manager** at Centre de Recherche Public Henri Tudor
 - in charge of the business line Security & Continuity Management
- 2009: **PhD in Computer science** at University of Namur, Belgium
 - Title: Model-based Management of Information System Security Risk



OUTLINE

- **PART 1: Development of a risk management framework covering the entire regulation cycle: the Telco case**
 - Development of a sector-specific risk management approach and tool
 - Development of a NRA data platform
- **PART 2: Risk management enhanced by the use of enterprise architectures**
 - Context and challenges
 - Background work: the ISSRM domain model
 - EAM-ISSRM integrated model design
 - Evaluation of the RSO of ArchiMate to represent the EAM-ISSRM conceptual model
- Conclusions and future work

PART 1: Development of a risk management framework covering the entire regulation cycle, the Telco case

—
Development of a sector-specific risk management approach and tool

LEGAL CONTEXT

EU Directive 2009/140/EC, Article 13a

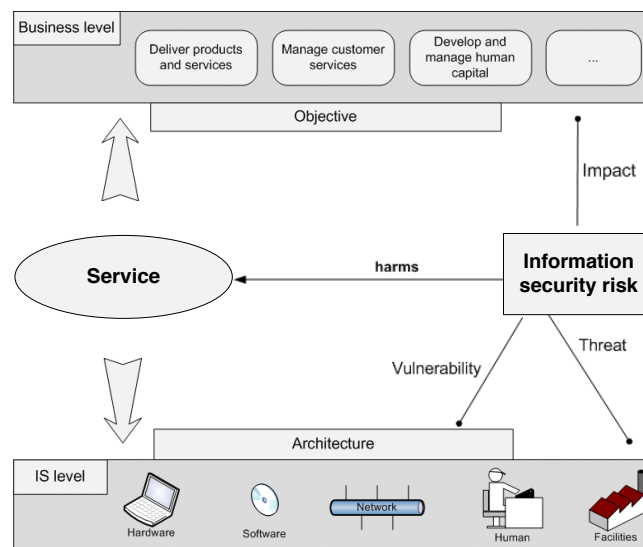
- **Article 13a** states that Member States shall ensure that providers of public communications networks “take appropriate technical and organizational measures to **appropriately manage the risks posed to security of networks and services**”. In addition, the article points out that “these measures shall ensure **a level of security appropriate to the risk presented**”

=> A **supervision of the Telecommunications Service Provider (TSP)** is thus required and operated by the National Regulatory Authority (NRA) of the different countries.

- **Adoption at the national level**
 - *Loi du 27 février 2011 sur les réseaux et les services de communications électroniques, Art. 45 et 46 sur la sécurité et intégrité des réseaux et services*
 - *Règlement 15/200/ILR du 18 décembre 2015*

5

INFORMATION SECURITY RISK AND THE TELECOMMUNICATIONS SECTOR



6

INSTITUT LUXEMBOURGEOIS DE RÉGULATION

Our partner: the National Regulatory Authority

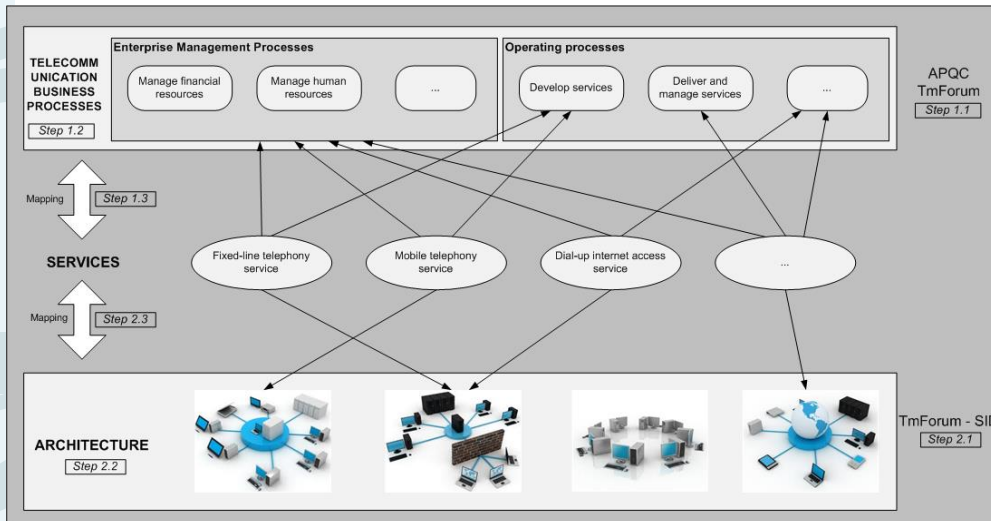
- In charge of the **supervision of the Telecommunications sector** (among others)
- In charge of the **supervision of the OSE (Operators of Essential Services) and DSP (Digital Service Providers) [NIS Directive] since July 2019**
- ILR's objectives:
 - Provide a **support to Telecommunications Service Providers (TSPs)** in Luxembourg for Article 13a compliance purpose
 - Suggest a **homogeneous, standard and easy-to-compare and to analyse** risk assessment process
 - **Sector-specific knowledge bases** integrated and **first level of risk identification** already performed (typical services and assets, main threats...) to ease the process and have a **fine-tuned tool adapted to TSPs**



OUR APPROACH

- **Context:** TSPs in Luxembourg have a **very different level of expertise** in security risk management
- **Goal:** **Adaptation of Information Security Risk Management process and practices** to the telecommunications sector and its context
 1. Modelling of the telecommunications services through **business processes**
 2. Modelling of the telecommunications services through **information system architecture**
 3. Definition of the service-related **knowledge base of risks**
 4. Integration of the results in a **software tool** and experimentation
- User-centered design approach
 - ILR
 - TSPs

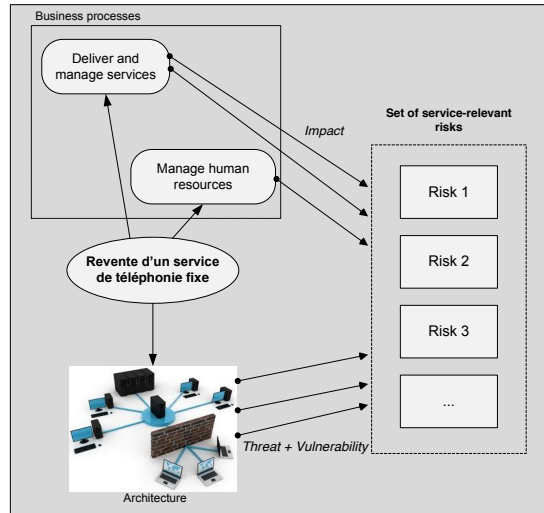
MODELLING OF THE TELECOMMUNICATIONS SERVICES THROUGH BUSINESS PROCESSES AND AN INFORMATION SYSTEM ARCHITECTURE



MODELLING OF THE TELECOMMUNICATIONS SERVICES THROUGH BUSINESS PROCESSES AND AN INFORMATION SYSTEM ARCHITECTURE

- Literature review:
 - Business processes
 - Business Process Framework (eTOM) of TMForum
 - Telecommunications Process Classification Framework of IBM and APQC
 - Architecture
 - Open Group
 - Information Framework (SID) of TMForum
- Co-design
 - Workshops with a representative panel of TSPs covering all services, infrastructures and telecommunications media (e.g. optical fibre, satellite, etc.)
 - Defining and refining meaningful elements for TSPs

DEFINITION OF THE SERVICE-RELATED KNOWLEDGE BASE OF RISKS



DEFINITION OF THE SERVICE-RELATED KNOWLEDGE BASE OF RISKS

- **Inventory of standards and references proposing knowledge bases of threats**
 - Generic ISRM
 - Telecommunications-related
- **Selection of a relevant subset of threats**
 - Focusing essentially on those harming availability and integrity
 - Grouping threats when applicable
 - Specifying relevant threats
- **22 (mandatory) threats selected**
- **Inventory of standards and references proposing knowledge bases of vulnerabilities**
 - Generic ISRM
 - Telecommunications-related
- **Selection of a relevant subset of vulnerabilities**
 - Only potentially exploitable by selected threats
 - Specifying relevant vulnerabilities
- **90+ vulnerabilities selected**

Impact criteria

	% of affected customers
1	Less than 1%
2	Between 1% and 2%
3	Between 2% and 5%
4	Between 5% and 10%
5	More than 10%

	Expected unavailability
1	Less than 30 minutes
2	Between 30 minutes and 1 hour
3	Between 1 hour and 2 hours
4	Between 2 hours and 3 hours
5	More than 3 hours

		Combined impact				
		% of affected customers				
		1	2	3	4	5
Availability	1	Low	Low	Low	Medium	High
	2	Low	Low	Medium	Medium	High

Risk evaluation criteria

Threat

Level	Description
1	Very unlikely, regarding statistics, cost or skills needed
2	Can happen occasionally
3	Very likely, easy to do, no particular investment or skill needed

Vulnerability

Level	Description
0	Very low: controls are implemented and effective against the threat
1	Medium: not enough controls, not effective enough or improvement opportunities identified
2	High: no effective control implemented
3	Very high: lack of control, obsolete control or not implemented

Risk level calculation

Risk level = func(impact, (threat+vulnerability-1))

		Threat + vulnerability - 1					
		0	1	2	3	4	5
Impact	Low	0	1	2	3	4	5
	Medium	0	2	4	6	8	10
	High	0	3	6	9	12	15
	Very high	0	4	8	12	16	20

Risk acceptance under: 8

Risks assessment		Define additional threats for a group	Define an additional threat for groups	Define affected asset(s)	IMPACT			Vulnerabilities by group
SERVICE	GROUP	THREAT	AFFECTED ASSET(S)	THREAT LEVEL	% OF AFFECTED CUSTOMERS	EXPECTED UNAVAILABILITY	IMPACT LEVEL	
Mobile voice	General (INTERNATIONAL)	Equipment failure	28 affected assets	2	4	2	Medium	Lack of continuity plans Lack of business continuity
		Equipment malfunction	28 affected assets	1	3	2	Medium	Single point of failure Badly configured network
		Software malfunction	2 affected assets	1	2	1	Low	Outdated software patches Inadequate service maint
		Breach of information system maintainability	8 affected assets	2	5	1	High	Insufficient maintenance/ Lack of change control pro Lack or insufficient Service
		Unauthorised use of computers, data, services and applications	30 affected assets	3	2	3	Medium	Failure to produce manage Lack of policies for the cor and messaging
		Corruption of data	3 affected assets	2	2	2	Low	Lack of procedures for repi Lack of regular managemen Unprotected public netwo
		Error in use	28 affected assets	1	2	4	Medium	Applying application progr Lack of formal procedure f Lack of formal procedure f Widely-distributed softwa Complicated user interfac Incorrect dates Incorrect parameter set up Incorrect use of software t Insufficient security traini Lack control Lack of documentation Lack of e-mail usage polic Lack of information securi Lack of procedures for clas

PART 1: Development of a risk management framework covering the entire regulation cycle

Development of a NRA data platform

LEGAL CONTEXT

EU Directive 2009/140/EC , Article 13a – National adoption

- TSPs are required, on an annual basis, to send a **security risk management report** + their so-called **level of sophistication for the 26 security objectives** (SOs) introduced by the Technical Guideline on Security Measures published by ENISA.

SO 3: Security roles and responsibilities

Establish and maintain an appropriate structure of security roles and responsibilities.

	Security measures	Evidence
1	a) Assign security roles and responsibilities to personnel. b) Make sure the security roles are reachable in case of security incidents.	<ul style="list-style-type: none"> List of security roles (CISO, DPO, business continuity manager, etc), who occupies them and contact information.
2	c) Personnel is formally appointed in security roles. d) Make personnel aware of the security roles in your organisation and when they should be contacted.	<ul style="list-style-type: none"> List of appointments (CISO, DPO, etc), and description of responsibilities and tasks for security roles (CISO, DPO, etc). Awareness/dissemination material for personnel explaining security roles and when/how they should be contacted.
3	e) Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents.	<ul style="list-style-type: none"> Up-to-date documentation of the structure of security role assignments and responsibilities Documentation of review process, taking into account changes and past incidents.

PROJECT OBJECTIVE

- **Objective:** to establish a framework to **analyse risk-related data** collected by the National Regulatory Authority (NRA) through the standard approach they recommend to the Telecommunications Service Providers (TSPs)
- **Framework:** **a set of measurements depicting the trust the NRA can have in the security of telecommunications companies**, as well as in the whole telecommunications sector
- The measurement framework shall
 - be in line with state of the art practices of the domain (industry standards and methods)
 - take into account the specificity of the regulatory context
 - take into account the local constraints of the NRA.
- **Outcome for the NRA:** to depict the **trust** the NRA can have in the **security of telecommunications companies**, as well as in the **whole telecommunications sector**

CONSTRAINTS COMING FROM THE NRA

To be taken into account when developing the measurements

- **Resources** allocated by the NRA to the data collection and analysis are limited. It is thus necessary to limit the number of measurements and their management complexity.
- **Information available** to feed the measurements is limited to the risk management reports and the sophistication levels defined for each SO (i.e., what is required by the tool promoted by the NRA)
- In order to assess the trust the NRA can have individually in each TSP, as well as the trust it can have in the whole sector, **two classes of measurements are expected:** measurements related to the individual analysis of each TSP and measurements related to the sector.

STATE OF THE ART

Existing IS measurement standards and approaches

- **ISO/IEC 27004**: Information security management -- Measurement
- **NIST SP 800-55**: Performance Measurement Guide for Information Security
- **Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** guide and example of application for building information security dashboard
- **ENISA technical report**: overview of existing approaches about measurement frameworks and metrics for resilient networks and services

STATE OF THE ART

Existing IS measurement standards and approaches

- **Measurement templates** proposed in the different references studied are generally of high interest with regard to our objectives.
- => Our measurement template will be inspired by these different proposals, especially the one from ISO/IEC 27004, which has the most detailed model.
- However, regarding the **set of measurements** proposed as examples in the studied references, they are generally not relevant to our context.
 - Focused on an organization's information security

MEASUREMENT TAXONOMY

- **Compliance:** measuring the compliance with regard to requirements imposed by legislation;
- **Performance:** measuring the effectiveness in terms of IS security.

Scope	TSP			Sector				
Type	Compliance	Performance		Compliance	Performance			
Category		Risk	Maturity	Gap		Risk	Maturity	Gap

- **Performance-Risk:** measuring the risk management effectiveness;
- **Performance-Maturity:** measuring the information security maturity, relying on the sophistication levels proposed by ENISA;
- **Performance-Gap:** comparing Performance-Risk with Performance-Maturity, in order to assess the consistency of the risk management activities compared to the maturity stated.

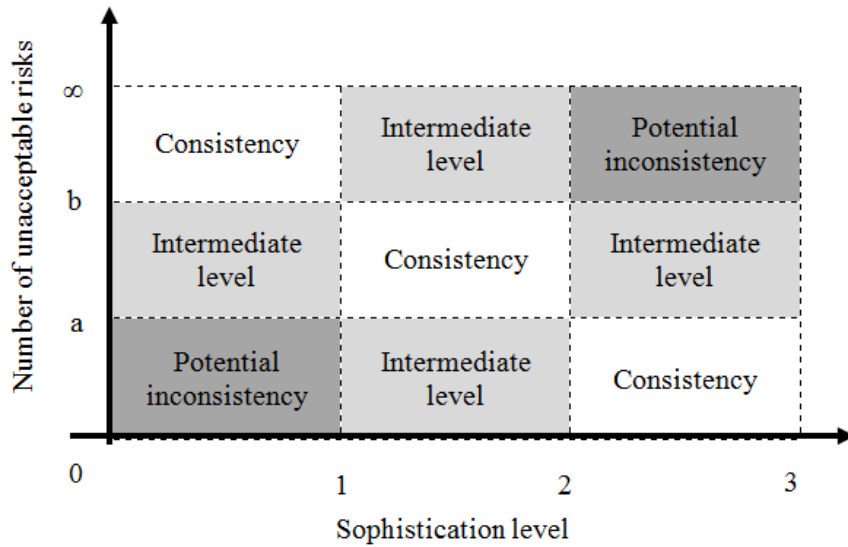
PERFORMANCE-GAP MEASUREMENT

Categories

- Three different Performance-Gap measurements, corresponding to risk categories:
 - **Physical/Environmental risk** (e.g., water damage, fire etc.)
 - **Technological risk** (e.g., equipment failure, loss of essential services, or similar)
 - **Human risk** (e.g., breach of staff availability, theft of equipment etc.)
- Risk categories have been mapped with the different SOs defined by ENISA (e.g., a SO dedicated to the security of buildings is mapped with the physical/environmental family of risks)
- SOs that are generic (i.e. helping to deal with risks from all three categories) are intentionally set aside (e.g., Information security policy, Business continuity management, etc.).

PERFORMANCE-GAP MEASUREMENT

Analytical model & interpretation




23

EXAMPLE OF MEASUREMENT (1)

Field	Description
<i>Identification</i>	
Name / ID	Unacceptable risk rate
Type & target measurement	Compliance: <input type="checkbox"/> Performance: <input checked="" type="checkbox"/> Risk <input checked="" type="checkbox"/> TSP: <input checked="" type="checkbox"/> Maturity <input type="checkbox"/> Sector: <input type="checkbox"/> Gap <input type="checkbox"/>
Measurable objective	To know the number of unacceptable risks compared to the total number of risks
<i>Measurement construct</i>	
Objet	Tab "Risk Assessment" (TISRIM)
Attribute	Column "Risk" (TISRIM)
Measurement method	X = total number of risks resulting from the risk assessment Y = number of unacceptable risks identified during the risk assessment R = number of unacceptable risks compared to the total of risks, expressed as a percentage: $R = \frac{Y}{X} * 100$

24

EXAMPLE OF MEASUREMENT (2)

<i>Measurement specification</i>	
Analytical model & interpretation	Target value: 0% Thresholds value: If $R \geq 20\%$ then "unsatisfactory" If $9\% \leq R \leq 19\%$ then "room for improvement" If $R \leq 8\%$ then "satisfactory"
Decision criteria	If "satisfactory" then do nothing If "room for improvement" then a review is nice to have If "unsatisfactory" then a review is mandatory
<i>Measurement result</i>	
Reporting format	The result is represented in the form of a "traffic light" as follows: <ul style="list-style-type: none"> - Red = unsatisfactory - Orange = room for improvement - Green = satisfactory 

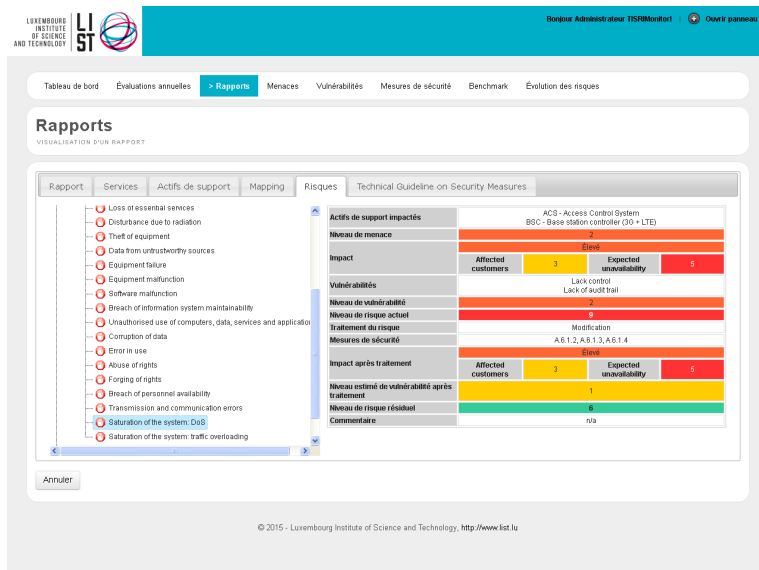
SET OF MEASUREMENTS ESTABLISHED

For TSPs and for the telecommunications sector

	Measurement name	Type
TSP	Risk management performed annually for each regulated service	Compliance
	Unacceptable risk rate for each regulated service	Performance-Risk
	Unacceptable risk rate compared to the total number of risks	Performance-Risk
	Average level of all risks	Performance-Risk
	Sophistication level for each Security Objective	Performance-Maturity
	Sophistication level for each Domain	Performance-Maturity
	Average level of sophistication for a TSP	Performance-Maturity
	Consistency in terms of governance in the field of physical and environmental threats	Performance-Gap
	Consistency in terms of governance in the field of technological threats	Performance-Gap
	Consistency in terms of governance in the field of human threats	Performance-Gap
Telecommunications sector	Risk management rate performed once a year in time	Compliance
	Unacceptable risk rate for each regulated service	Performance-Risk
	Unacceptable risk rate compared to the total number of risks	Performance-Risk
	Average level of all risks	Performance-Risk
	Top 5 threats causing the highest risks for each regulated service	Performance-Risk
	Top 5 threats causing the highest risks for the sector	Performance-Risk
	Most sensitive assets by regulated service	Performance-Risk
	Most sensitive assets for the sector	Performance-Risk
	Sophistication level for each Security Objective	Performance-Maturity
	Sophistication level for each Domain	Performance-Maturity
	Average level of sophistication for the sector	Performance-Maturity

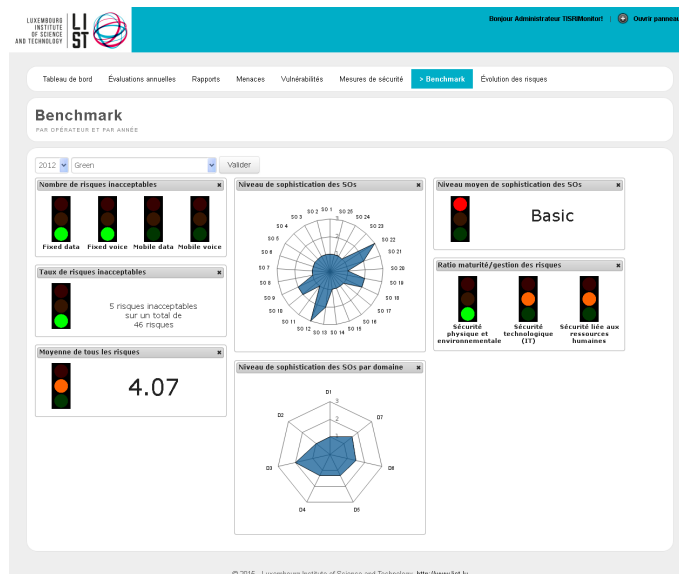
DASHBOARD OF MEASUREMENTS (1) Implementation of the measurements!

TISRIMonitor

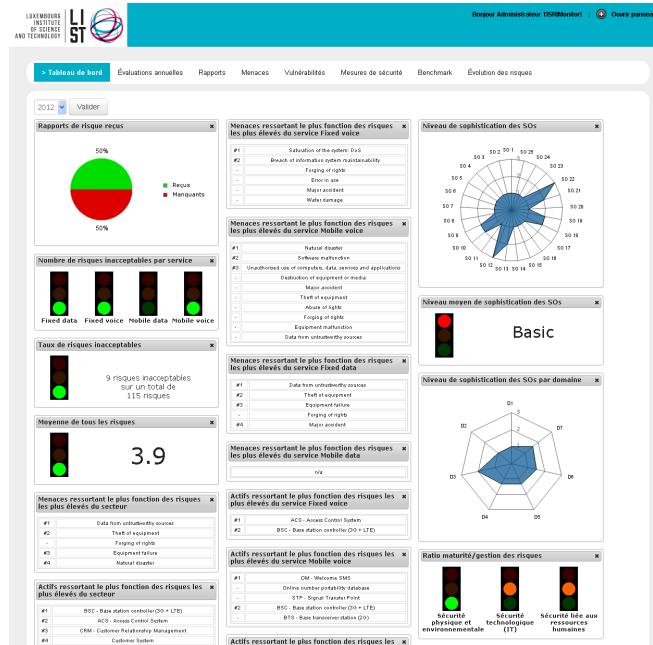


DASHBOARD OF MEASUREMENTS (2) Implementation of the measurements!

TISRIMonitor



DASHBOARD OF MEASUREMENTS (3) Implementation of the measurements! TISRIMonitor

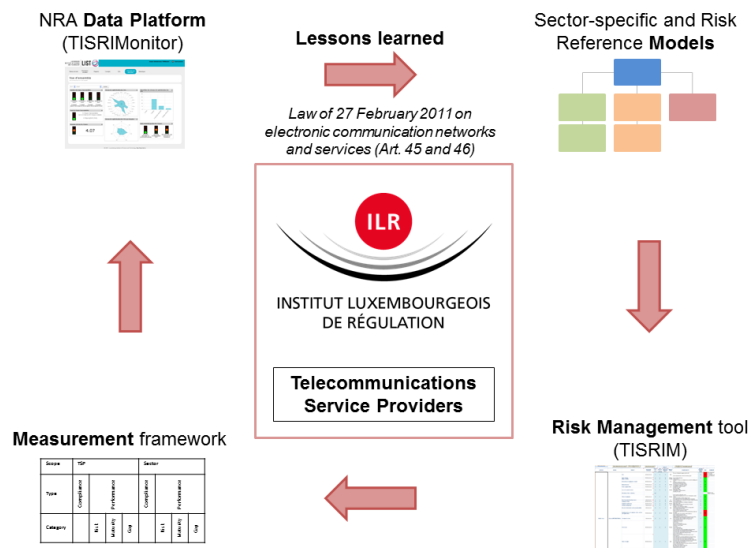


DEVELOPMENT OF A NRA DATA PLATFORM

Benefits

- Generation of:
 - A **global risk profile for each TSP** based on their individual risk assessment;
 - A **risk profile for the whole sector** either for all the telecommunications services or for each individual telecommunications service;
 - **Benchmarks between two or more distinct TSP**, either for a specific service or globally;
 - **Individual reports** for regulated entities.
- Results used for lessons learned:
 - **Consolidated lists of the concepts used by the TSP** in their risk assessment, in particular threats, vulnerabilities, supporting assets and controls. These data are particularly relevant for the update and improvement of the knowledge bases included in TISRIM tool;
 - **Statistical data** of the yearly risk assessment results for the whole sector including a ranking of the highest risks, a summary of the risk levels, a ranking of the most sensitive assets, a list of the most implemented security measures, etc.;
 - **Evolution of the risk assessments' results** over the years both at TSP and sector level.

REGULATION CYCLE



31

EMERGING CHALLENGES

- **Three regulatory cycles** performed from **12.2015 to 07.2018** and followed by the gathering of data by ILR:
 - December 2015 => July 2016
 - August 2016 => July 2017
 - (August 2017 => July 2018)
- **Limitations** identified after the two first regulatory cycles:
 - Opportunities for improvement (in terms of completeness and/or usability) of the **compliance models and reference architectures** supporting TSP's regulations
 - Risk management **carried out at the individual level** by each operator, with no link between the risks of different operators with regard to the dependencies between entities
 - Opportunities for improvement of the regulatory authority's **data analysis framework** and lack of data analysis capabilities on the regulated entities side

32

PART 2: Risk Management Enhanced by the Use of Enterprise Architectures

—
Opportunities for improvement (in terms of completeness and/or usability) of the compliance models and reference architectures supporting TSP's regulations

ILLUSTRATIVE EXAMPLE

POST Telecom



- **ISO/IEC 27001 certified**
 - Information security risk management, compliant with the requirements of the standard.
- **Telecommunications Service Provider**
 - EU Directive 2009/140/EC, Article 13a on security and integrity of networks and services: providers of public communication networks shall manage the security risks of networks and services.
- **IT service provider for the financial sector**
 - *Circulaire CSSF 12/544* is a national regulation requiring that each financial service provider uses a “risk-based approach” in order to identify the operational risks the financial institutions are taking when using their services.

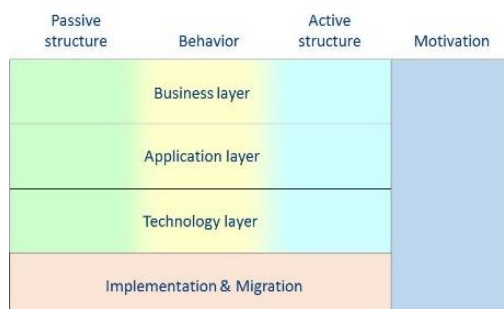
CONTEXT AND CHALLENGE

- Current Information Systems (IS) are more and more **complex** and subject to an increasing number of threats to manage
 - Today, and particularly in **regulations** at our national level, a strong emphasis is put on the security of IS and on the management of security risks
 - It is difficult to have a clear and manageable **documentation** for IS Security Risk Management (ISSRM) activities
- => Classical ISSRM methods are thus **no more suitable** to deal with the complexity of organizations and associated risks in such a context of compliance and governance**
- **Enterprise Architecture Management (EAM)** has appeared to be relevant to face these challenges

35

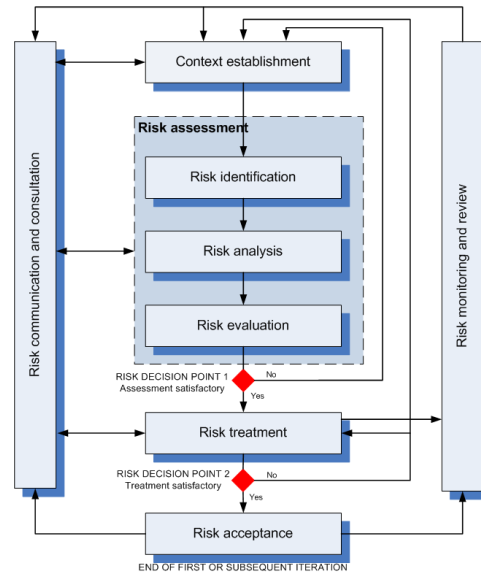
ENTERPRISE ARCHITECTURE MANAGEMENT

- **Enterprise Architecture Management (EAM)**
 - has shown to be a valuable and engaging instrument to face **enterprise complexity** and the necessary enterprise transformation (Saha, 2013; Zachman, 1987)
 - offers means to **govern enterprises** and make informed decisions
 - describing Enterprise Architecture (EA) with a suited **language** (i.e. EA modelling) is considered as a key activity (Lankhorst, 2005)



36

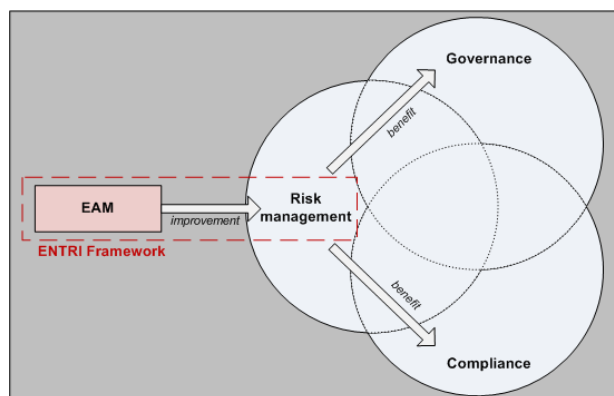
SECURITY RISK MANAGEMENT PROCESS



RESEARCH GOAL

Design problem

- **Improve ISSRM** by defining a **framework** (modelling language, method, tool) that **uses the results from EAM research for compliance and governance purpose**

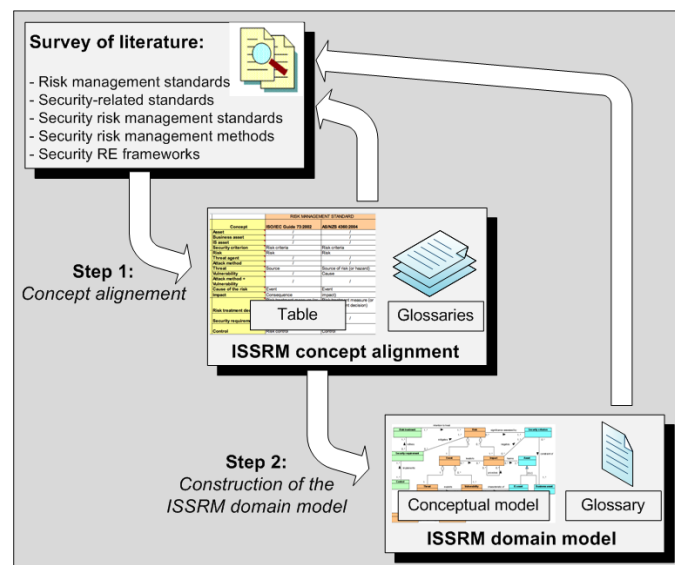


OBJECTIVES OF THE PROJECT

1. To assess and integrate the **conceptual models** of EAM and ISSRM domains
2. To assess and improve the ArchiMate **modelling language** to support the integrated conceptual model of EAM and ISSRM
3. *To analyse the processes supporting both ISSRM and EAM, and to define relevant **method fragments/chunks** allowing to link both domains at the methodological level*
4. *To analyse and position the integrated EAM-ISSRM framework (conceptual model, modelling language and method chunks/fragments), called “ENTRI framework”, with regards to **GRC models***
5. *To implement the designed artefacts on a **technological platform***

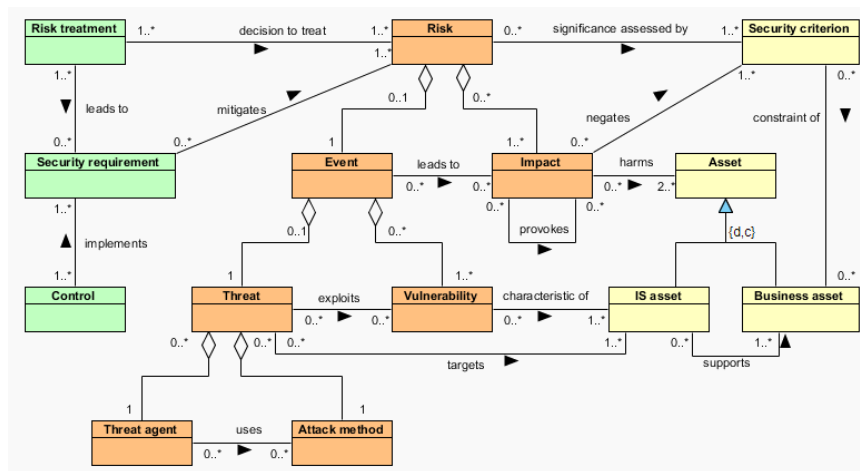
BACKGROUND WORK

What are the concepts that should be present in a modelling language supporting ISSRM?



BACKGROUND WORK

ISSRM domain model



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

ENTRI FRAMEWORK MODEL DESIGN

EAM-ISSRM Model Development

1) Selection of relevant conceptual references for EAM

Focus on industry used conceptual references (i.e. contemporary and widely used) to insure a high acceptance level of our extension by practitioners

2) Conceptual alignment between concepts used to model an EA and concepts of the ISSRM domain model

3) Design of the EAM-ISSRM integrated conceptual model

4) Validation of the EAM-ISSRM integrated conceptual model

- First cycle (1=>3) with TOGAF as conceptual reference
- Second design cycle (1=>3) including all of the selected conceptual references => ArchiMate, DoDAF (standardized in UPDM), IAF

SELECTION OF RELEVANT CONCEPTUAL REFERENCES FOR EAM

- The objective of our integrated conceptual model is **to describe the concepts used when defining an EA**. More in particular, the following criteria have been established in order to consider an approach as relevant in our context:
 - a) The approach shall provide information for designing **architecture descriptions**, i.e. the work product used to express an architecture.
 - b) The approach shall **clearly describe** the concepts at stake for architectural description, in order to enable a conceptual alignment. Methods that are insufficiently precise at the conceptual level must be set aside. Explicit definitions of the concepts used to describe architectures are required.
 - c) The approach shall allow us to deal with the **architecture of systems** that may consist of hardware, software, data, people, business processes, procedures, facilities, materials, or naturally occurring entities. It shall not be restricted to specific kinds of systems (e.g., software products).
- Of the approaches listed by existing reviews about EAM [31] or recommended by experts, the following satisfy these criteria: **TOGAF, ArchiMate, DoDAF, IAF**

CONCEPTUAL ALIGNMENT




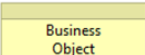
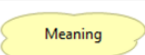
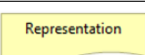
Semantic mapping types [Zivkovic *et al.*]

- **Equivalence**: *concept A* is semantically equivalent to *concept B*;
- **Generalisation**: *concept A* is a generalisation of *concept B*, i.e. *concept B* is a specific class of *concept A*;
- **Specialisation**: *concept A* is a specialisation of *concept B*, i.e. *concept B* is a generic class of *concept A*;
- **Aggregation**: *concept A* is composed of *concept B*, i.e. *concept B* is a part of *concept A*;
- **Composition**: *concept A* is composed of *concept B* (with strong ownership), i.e. *concept B* is a part of *concept A* and does only exist as part of *concept A*;
- **Association**: *concept A* is linked to *concept B*.

ALIGNMENT TABLE (TOGAF)

TOGAF 9.1	ISSRM domain model	Semantic mapping type	Running example
Business Architecture			
Organization Unit	IS asset Asset	Specialisation Association	“Biomedical laboratory”
Actor	IS asset	Specialisation	N/A
Function	Business asset	Specialisation	“Biomedical pre-analysis”
...
Process	Business asset	Specialisation	N/A
Data architecture			
Data Entity	IS asset	Specialisation	“Clinical information”
Physical Data Component	IS asset	Specialisation	N/A
...

ALIGNMENT TABLE (ARCHIMATE)

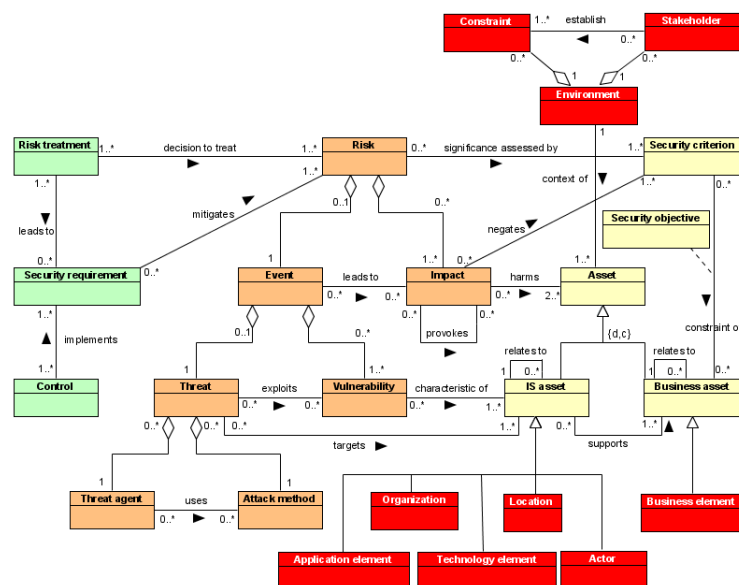
ArchiMate 2.1	ISSRM domain model	Semantic mapping type [20]	Running example
Business Layer			
 Value	Business asset: value	<i>equivalence</i>	“Home care”
 Product	Business asset	<i>specialisation</i>	“Home Blood Analysis”
 Contract	Business asset	<i>specialisation</i>	“Contract”
 Business Object	Asset	<i>specialisation</i>	“Biomedical Analysis Prescription”
 Meaning	Business asset	<i>specialisation</i>	“Prescribed Analyses”
 Representation	IS asset	<i>specialisation</i>	“Biomedical Paper Prescription”

KEY CONCLUSIONS

- Although the mapping is complex, EAM brings a more fine grained representation of (business and IS) assets.
=> **refinement of business and IS assets**
- EAM considers concepts that are part of the environment of assets. This is not the case of the ISSRM domain model.
=> **introduction of the environment of the assets**

ENTRI FRAMEWORK MODEL DESIGN

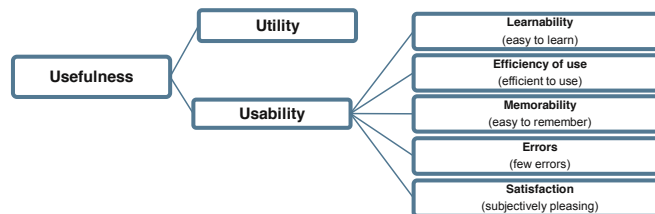
EAM-ISSRM Model Development



VALIDATION

EAM-ISSRM integrated model

- Objective = to test the **utility and usability** of the **EAM-ISSRM integrated model** as the **conceptual foundation to design a framework** (modelling language, method, and tool) to perform ISSRM



VALIDATION OF THE EAM-ISSRM INTEGRATED MODEL

Meeting attendance

#	Sector	Position	Experience (years)
1	Telecommunications	Information Security Officer	1
2	Data centres, Cloud services	Chief Information Security Officer	15
3	Data centres, Cloud services	Security consultant & Deputy Chief Information Security Officer	8
4	Public research centre	System administrator	15
5	Telecommunications	Information Security Officer	8
6	European and international institutions	Chief Information Security Officer & Data Protection Officer	23
7	Public research centre	Network engineer	19
8	Archiving, Cloud services, Data centre	Information Security and Risk Manager	3
9	Corporate services	IT Manager & Chief Information Security Officer	10

VALIDATION OF THE EAM-ISSRM INTEGRATED MODEL

Experiment structure

- a) **Introduction**: General introduction to the topic and the objectives of the meeting. Reminder about the concepts of the ISSRM domain model. (40 min.)
- b) Pre-test survey (see Appendix 1): **Open question** about the strengths and the weaknesses in performing ISSRM based on TISRIM and the ISSRM domain model. (20 min.)
- c) Execution: After having exposed the EAM extension for the ISSRM domain model (30 min.), the participants need to perform two **exercises** and fill one **questionnaire** (see Appendix 2):
 - **Exercise 1**: Based on the description of a case, members of the validation group need to identify an instance of each concept of the EAM-ISSRM integrated model [specifically helps to assess learnability and errors]. (40 min.)
 - **Exercise 2**: Based on the requirements provided in ISO/IEC 27001 [6], members of the validation group need to identify if, by instantiating the EAM-ISSRM integrated model, and more specifically its extension, some requirements are satisfied and which ones [specifically helps to assess utility and errors]. (20 min.)
 - **SUS questionnaire** about usability of the EAM-ISSRM integrated model. (10 min.)
- d) Post-test survey (Appendix 3): Ask people to **recap about the concepts that are part of the EAM extension** of the ISSRM domain model [specifically helps to assess memorability]. (15 min.)
- e) Closure: Ask people about their **general feedback** about the potential felt that the EAM-ISSRM integrated model is suitable as the conceptual foundation to design a framework to perform ISSRM [specifically helps to assess utility and satisfaction]. (30 min.)

VALIDATION OF THE EAM-ISSRM INTEGRATED MODEL

Conclusions

- Based on the results obtained, we conclude that the participants **found the model useful**:
 - a greater degree of contextualization,
 - a better understanding of the scope,
 - an easier maintainability of the risk management results over time,
 - a better compliance thanks to a broader scope of study
- But they highlighted **some necessary improvements**:
 - **Better definition of Actor and Organization**, making especially clear the relation and difference between the two concepts (see *Utility* and *Errors*)
 - **Better definition of Environment**, making clear its relation with the other related concepts (see *Memorability* and *Errors*)
 - **Further explanation on Business element, Application element and Technology element** to facilitate their adoption by users (see *Memorability*)
- We applied these improvements to the current version of the integrated model.

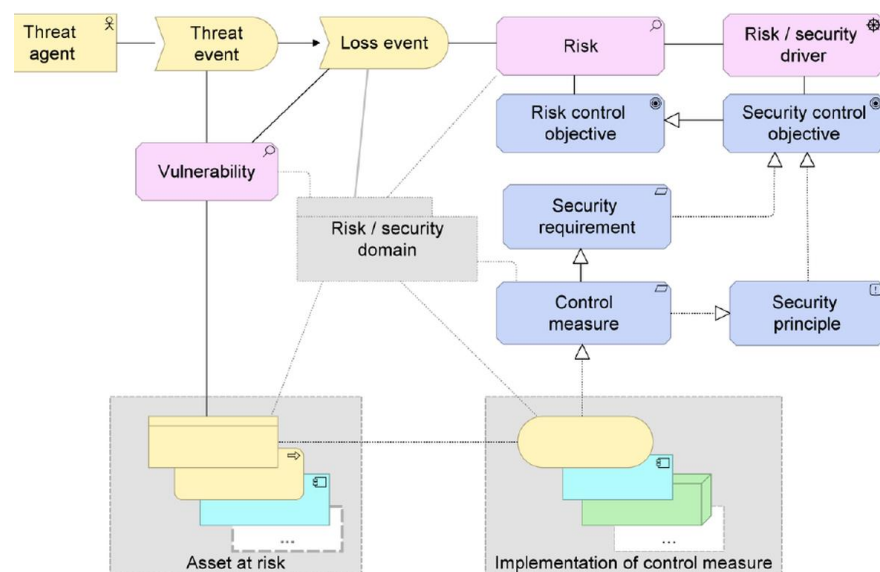
Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., Wieringa, R.: An Integrated Conceptual Model for Information System Security Risk Management supported by Enterprise Architecture Management. Accepted for publication in the *International Journal on Software and Systems Modeling (SoSyM)*.

A MODELLING LANGUAGE FOR EAM-ISSRM

- **Step 1:** Integration of ISSRM concepts with EAM concepts in a model called the “EAM-ISSRM integrated model”
- **Step 2:** Definition of a **modelling language** (i.e. a graphical notation) to support this “EAM-ISSRM integrated model”
 - Such a language will be used by practitioners to document the different steps of ISSRM and enhance decision-making all along this process
 - A graphical notation is considered as more expressive and maintainable than the traditional table-based approach of ISSRM
- **Research approach:** instead of starting defining a new modelling language, we first want to **assess existing one(s)** in the literature
 - The “**Risk and Security Overlay**” (RSO) of the ArchiMate language is a natural candidate

VISUAL NOTATION FOR THE EAM-ISSRM MODEL

Evaluation of the Risk and Security Overlay (RSO) of ArchiMate



VISUAL NOTATION FOR THE EAM-ISSRM MODEL

Evaluation of the RSO of ArchiMate

1. **Completeness** of the notation

- Does the RSO provide a complete coverage of the EAM-ISSRM integrated model?
=> Assessment of the conceptual coverage of the RSO with regards to the EAM-ISSRM integrated model

2. **Cognitive effectiveness** of the notation.

- Is the RSO cognitive effective to support the users in their ISSRM activities?
=> Assessment of the cognitive effectiveness of the RSO based on the work of Moody: “The Physics of Notations”
- Nine principles for designing “cognitive effective visual notations”
- Semiotic clarity, perceptual discriminability, semantic transparency, complexity management, cognitive integration, visual expressiveness, dual coding, graphic economy, cognitive fit

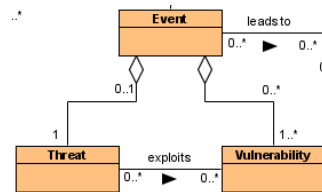
ALIGNMENT OF THE EAM-ISSRM CONCEPTS WITH THE CONSTRUCTS OF ARCHIMATE SUGGESTED IN THE RSO

EAM-ISSRM integrated model		Risk and Security Overlay of the ArchiMate language [14]	Constructs from ArchiMate 2.1 [13]
Asset-related concepts	Asset	Asset at Risk	Any core concept or combination of concepts
	Business Asset		
	IS Asset		
	Security criterion	Risk / security driver	Driver
	Security objective	Security control objective	Goal
	Organization	N/A	Any core concept from the application layer, technology layer, or combination of them
Location	N/A	Location	
Risk-related concepts	Risk	Risk	(Specialization of an) Assessment
	Impact	Loss Event	(Specialization of a) Business event
	Event	N/A	N/A
	Threat	Threat	Driver
	Vulnerability	Vulnerability	(Specialization of an) Assessment Attribute of an asset at risk or a risk domain
	Threat agent	Threat agent	Active structure elements (e.g., business actor, business role, application component, node, system software, or device)
	Attack method	Threat event	(Specialization of a) Business event

ALIGNMENT EAM-ISSRM CONCEPTS - RSO

Conclusion

- The coverage of the EAM-ISSRM integrated model by the RSO is **complete** apart from “Event”, concept not included in the RSO
- However, we consider this **lack as negligible** because an event is defined in the EAM-ISSRM integrated model as being (only) the composition of threat and vulnerability.
 - Thus, modeling a threat (i.e. a threat agent performing a threat event) and its associated vulnerability(ies) is strictly equivalent as modelling an event.



57

COGNITIVE EFFECTIVENESS OF THE RSO AS A NOTATION FOR THE EAM-ISSRM MODEL

- **Semiotic clarity:** There should be a 1:1 correspondence between semantic constructs and graphical symbols
- **Perceptual discriminability:** Different symbols should be clearly distinguishable from each other. (e.g., shape, size, color, position, etc.)
- **Semantic transparency:** Visual representations whose appearance suggests their meaning should be used.
- **Complexity management:** Explicit mechanisms for dealing with complexity should be included, such as modularization or hierarchy.
- **Cognitive interaction:** Explicit mechanisms to support integration of information from different diagrams should be included.
- **Visual expressiveness:** The full range and capacities of visual variables should be used (shape, size, color, brightness, orientation, and texture for retinal variables, and horizontal and vertical position for planar variables).
- **Dual coding:** Text should be used to complement graphics
- **Graphic economy:** The number of different graphical symbols should be cognitively manageable (i.e. number of legend entries).
- **Cognitive fit:** Different visual dialects should be used for different tasks and audiences

D. Moody, "The 'Physics' of Notations: Toward a Scientific Basis for Constructing Visual Notations in Software Engineering," *IEEE Trans. Softw. Eng.*, vol. 35, no. 6, pp. 756–779, Nov. 2009

58

COGNITIVE EFFECTIVENESS OF THE RSO AS A NOTATION FOR THE EAM-ISSRM MODEL

Principle of semantic transparency

- **Definition:** Visual representations whose appearance suggests their meaning should be used. In other words, the meaning of a symbol should be understood by looking at its representation.
- **ArchiMate:** In ArchiMate, only one iconic shape (i.e. symbol which perceptually resemble the object it represents) is provided: the alternative representation of a business actor that is a stickman [18]. Other constructs are represented using “neutral” shapes or even confusing ones, like, e.g., the cylinder shape that represents *Business role* but which is usually associated to a database. ArchiMate uses spatial enclosure but the latter may have different meanings (e.g., inheritance, assignment, aggregation, etc.) and, as a result, loses its value.
- **RSO:** In the RSO, no iconic shape is introduced. Existing “neutral” shapes of ArchiMate are reused.

D. L. Moody, “Review of ArchiMate: The Road to International Standardisation,” ArchiMate Foundation and BiZZDesign B.V., Technical Report, 2007.

CONCLUSIONS ON THE COGNITIVE EFFECTIVENESS ASSESSMENT

- The RSO is **better than ArchiMate** on one principle: dual coding. Indeed, specific and detailed labels are used as well as stereotypes, used to specify ArchiMate concepts in a risk and security context.
- The RSO is **strictly equivalent to ArchiMate** on four principles: semantic transparency, cognitive integration, visual expressiveness, and cognitive fit. Modelling with the RSO does not add or modify anything in relation to these principles with regards to the proper use of ArchiMate.
- The RSO has a **negative impact on four principles**: semiotic clarity, perceptual discriminability, complexity management, and graphic economy. For these principles, the RSO basically inherits from the negative aspects of ArchiMate and aggravates them by adding new concepts coming with the same weaknesses.

=> Although no quantitative analysis has been performed to objectify this conclusion, **the RSO can decently not be considered as an appropriate notation from a cognitive effectiveness point of view** and there is room to propose a notation better on this aspect.

CONCLUDING REMARKS

- Regarding **completeness**, we can consider the RSO as an **appropriate notation** to support the EAM-ISSRM integrated model
- Regarding **cognitive effectiveness** that appeared as a key concern during the validation focus group discussions, **many gaps** have been identified.
=> the RSO can decently not be considered as an appropriate notation from a cognitive effectiveness point of view and there is room to propose a notation better on this aspect

THREATS TO VALIDITY

1. The analysis performed for the RSO is **subjective**, because **performed (only) by researchers from LIST**.
2. The analysis performed for the RSO is **subjective**, because it relies only on **qualitative statements** and not on any quantitative analysis that would be best suited to provide clear-cut conclusions on the cognitive effectiveness level of the RSO.
3. The analysis performed is based on **ArchiMate 2.1**, the RSO being built on top of ArchiMate 2.1, and not on ArchiMate 3.0 that is the last published and up-to-date version of the ArchiMate standard.

Ref.: N. Mayer and C. Feltus, "Evaluation of the Risk and Security Overlay of ArchiMate to model Information System Security Risks", 9th International Workshop on Vocabularies, Ontologies and Rules for the Enterprise, in conjunction with the 21th IEEE International EDOC Conference – The Enterprise Computing Conference, Québec-City, Canada, October 2017.

FUTURE WORK

- **Evaluation of the current framework** with an industrial partner (modelling language and method)
- **Improvement of the visual notation** to reach a cognitive effective notation for the target group of users, i.e. information security risk managers
- **Implementation of the results** as a module of a risk management tool (in discussion for a partnership)

THANKS FOR YOUR ATTENTION

QUESTIONS?



Supported by the National Research Fund, Luxembourg, and financed by the RegTech4ILR project (PUBLIC2-17/IS/11816300).

Survey of literature used for the establishment of the ISSRM domain model

- **RM standards**
 - ISO/IEC Guide 73
 - AS/NZS 4360
- **Security-related standards**
 - ISO/IEC 13335-1
 - Common Criteria
- **Security RM standards**
 - ISO/IEC 27001
 - ISO/IEC 27005
 - NIST 800-27 / NIST 800-30
 - The IT-Grundschutz
- **Security RM methods**
 - EBIOS
 - MEHARI
 - OCTAVE
 - CRAMM
 - CORAS
- **Security frameworks**
 - Firesmith
 - Haley *et al.*
 - The DITSCAP framework

65

DEVELOPMENT OF A NRA DATA PLATFORM

Measurements

- **Objective:** Platform to **manage the reports** received annually by the NRA and to **analyse efficiently their contents**
- Based on a **set of measurements** depicting the trust the NRA can have in the security of telecommunications companies, as well as in the whole telecommunications sector
 - **compliance measurements**, measuring the compliance to requirements imposed by legislation,
 - **performance measurements**, measuring the effectiveness of the security
 - **Performance-Risk:** measuring the security risk management effectiveness;
 - **Performance-Maturity:** measuring the information security maturity, relying on the sophistication levels reported for the security controls;
 - **Performance-Gap:** comparing Performance-Risk with Performance-Maturity, in order to assess the consistency of the risk management activities compared to the maturity stated.
- 10 measurements defined for TSP and 11 measurements defined for the whole telecommunications sector

66

MAIN RESULTS EXPECTED FOR THE PROJECT

- Reference **enterprise architecture models** for TSPs [Objective 1];
- **Extension of the security risk management model** to integrate related aspects (i.e. incident notification and data protection) [Objective 1];
- **Systemic security risk management framework** (conceptual model, dedicated measurements and methodological aspects) [Objective 2];
- Set of **measurements** for both individual TSPs and the whole sector [Objective 3];
- An **industrial technological platform** developed and operated by an industrial partner [Objective 4]

- **Cooperation with IBPT, the Belgian regulatory authority**, that aims to adopt our approach and tools