



Information Systems for the Compliance of Service Systems

Prof. Dr. Eric Dubois
(Service Science & Innovation department)

tudor

Copyright Tudor Center - Eric Dubois

PUBLIC RESEARCH CENTRE HENRI TUDOR

The content of the contribution in a nutshell

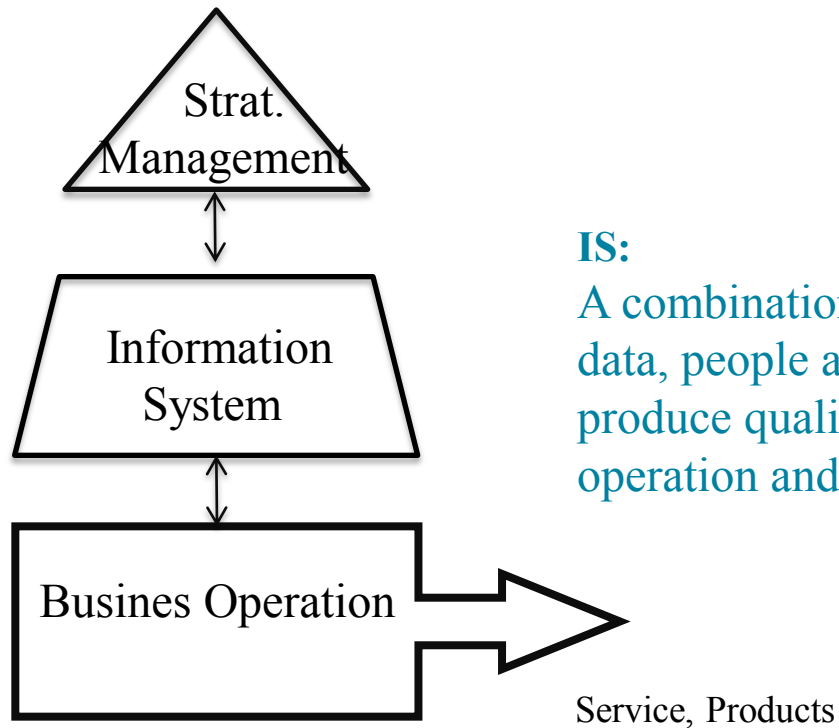
We have eco-systems of service-oriented companies where services are combined/bundled together

These services have to be compliant to regulations, compliance has to be considered at the level of the company as well as at the level of eco-system

Implementing and demonstrating compliance has an important cost. This has to be considered at the local and systemic levels

- *Proposal of reference frameworks and of the role of Information System for supporting the implementation and the demonstration of the compliance*
- *Illustration with an application in the context of security risk management*

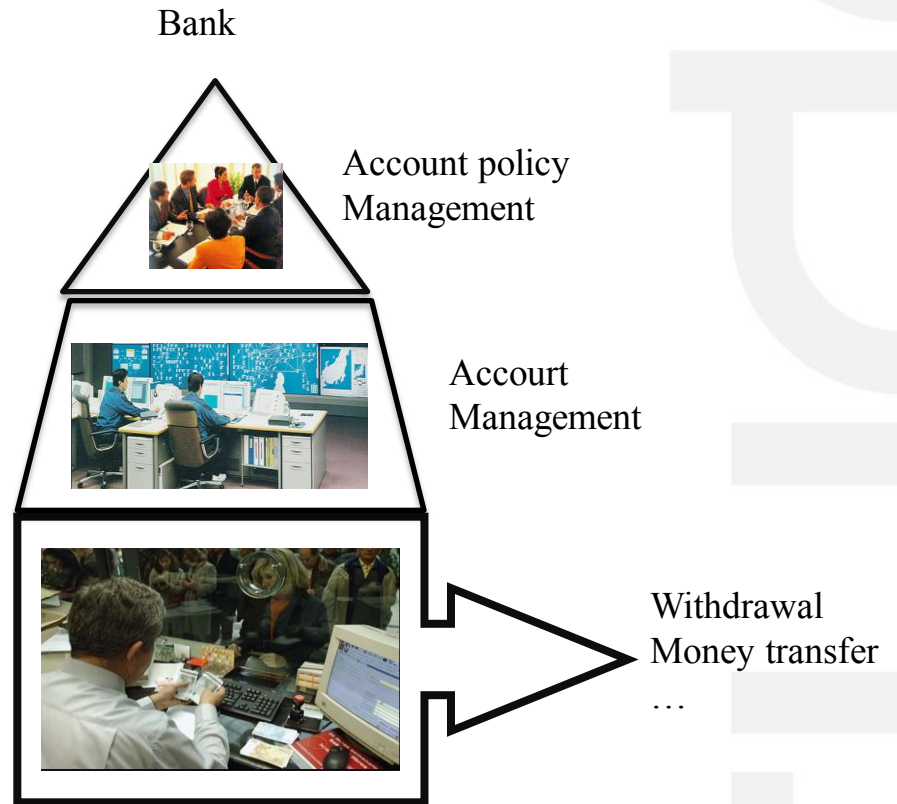
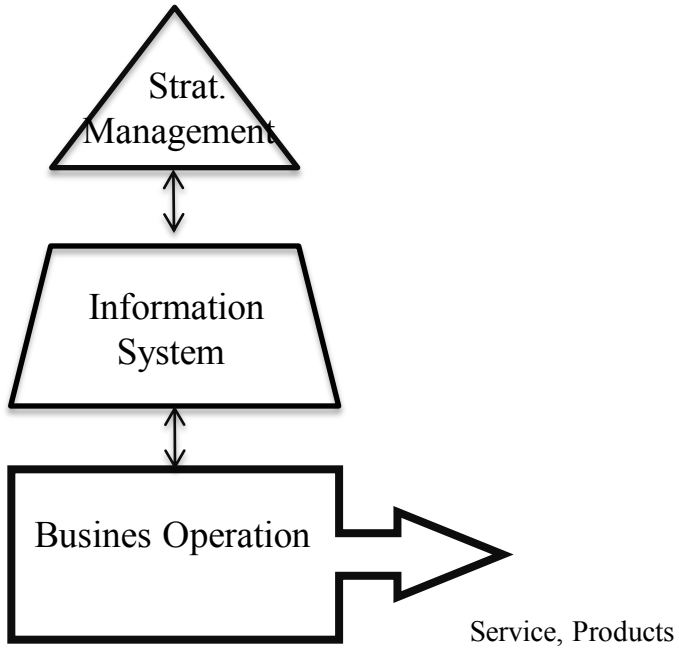
The Compliance Context and Challenges

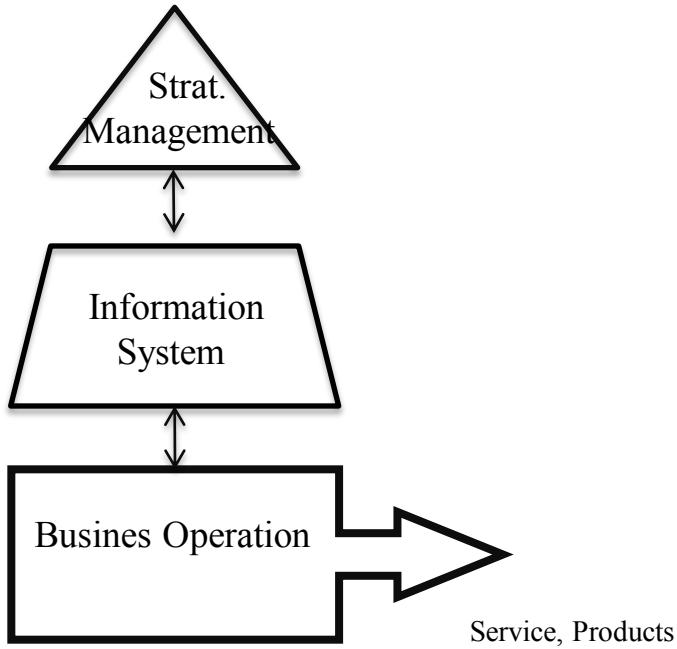


IS:

A combination of hardware, software, infrastructure data, people and procedures that work together to produce quality information supporting business operation and decision making in an organization

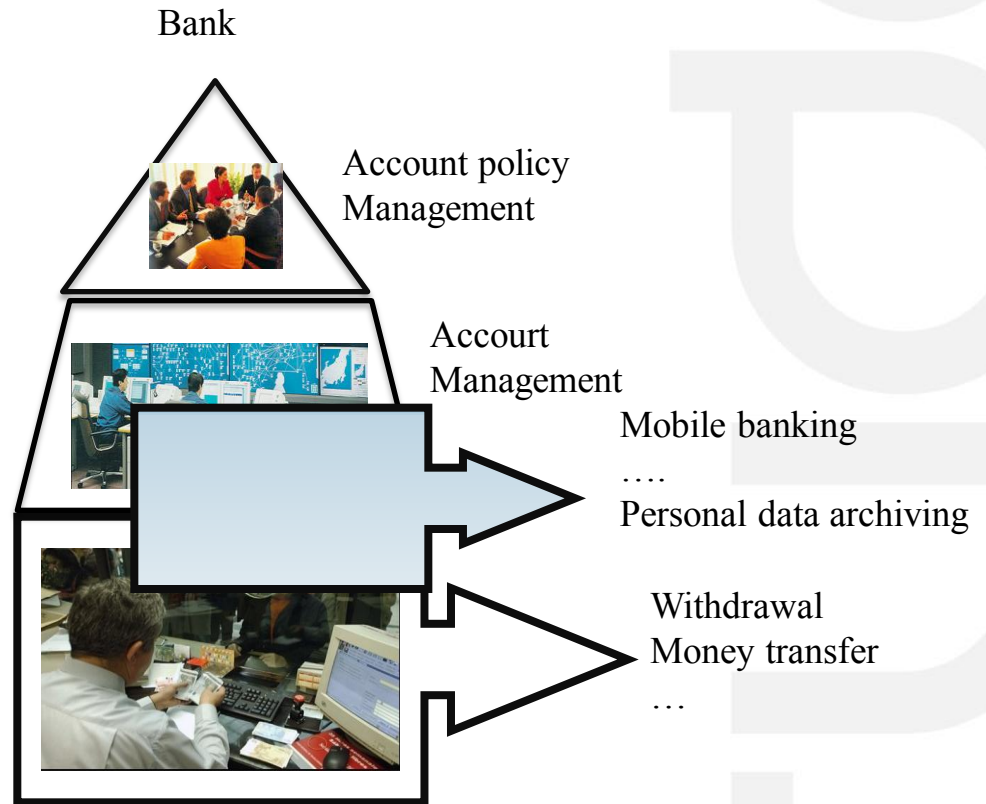
from [Lemoigne, 1977]

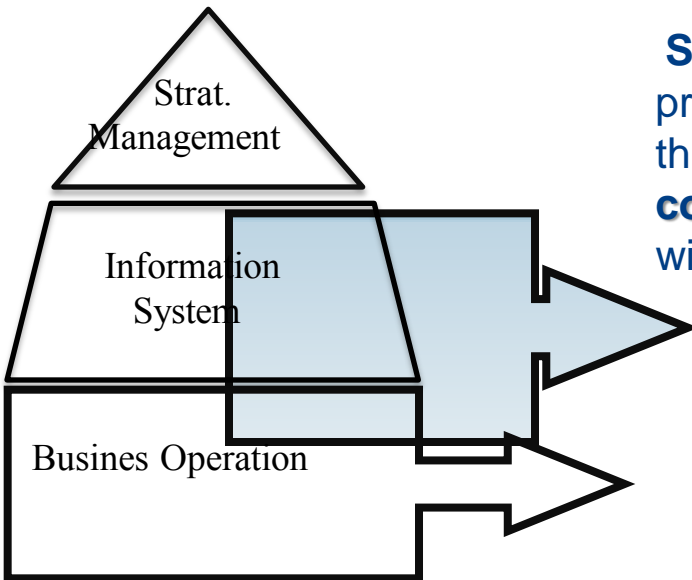




IS, from a center of costs

... to a center of profit

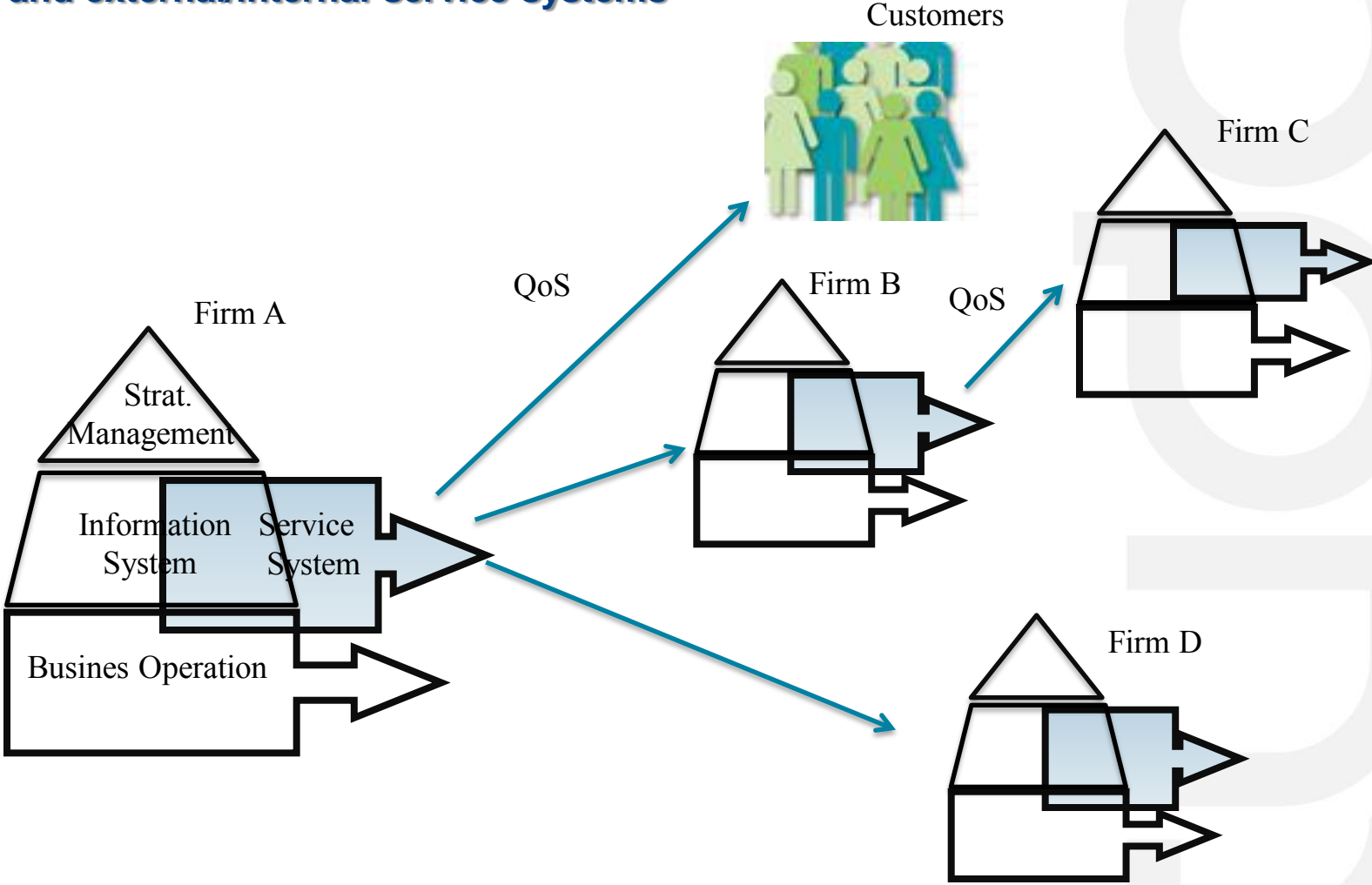


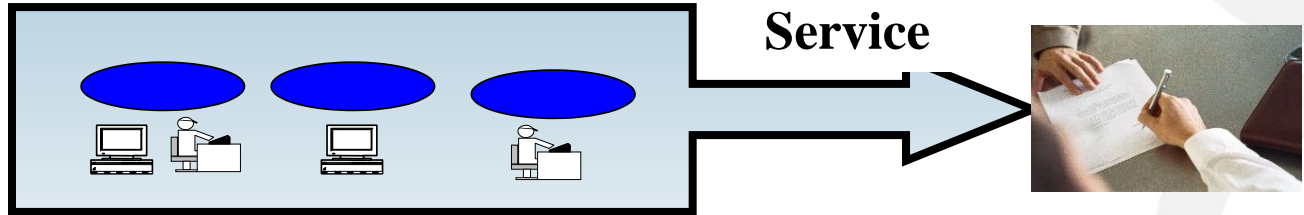
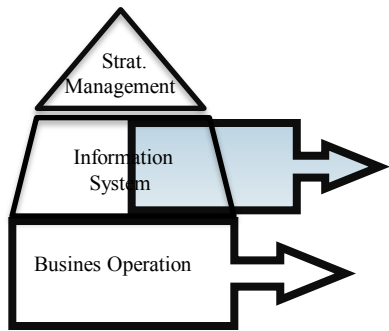


Service system is defined as a configuration of people, processes, technology and shared information connected through **a value proposition** with the aim of **a dynamic co-creation of value** through the participation in the exchanges with customers and external/internal service systems

from [Spohrer, Maglio, 2007]

Service system is defined as a configuration of people, processes, technology and shared information connected through a value proposition with the aim of a dynamic co-creation of value **through the participation in the exchanges with customers and external/internal service systems**





Quality of services (QoS) is an essential aspect of service contract / SLA

QoS

- Service availability, performance,
- Usability, users experience, etc.

QoS Issues

- Which confidence ?
- Which metrics ?
- Which evidences ?

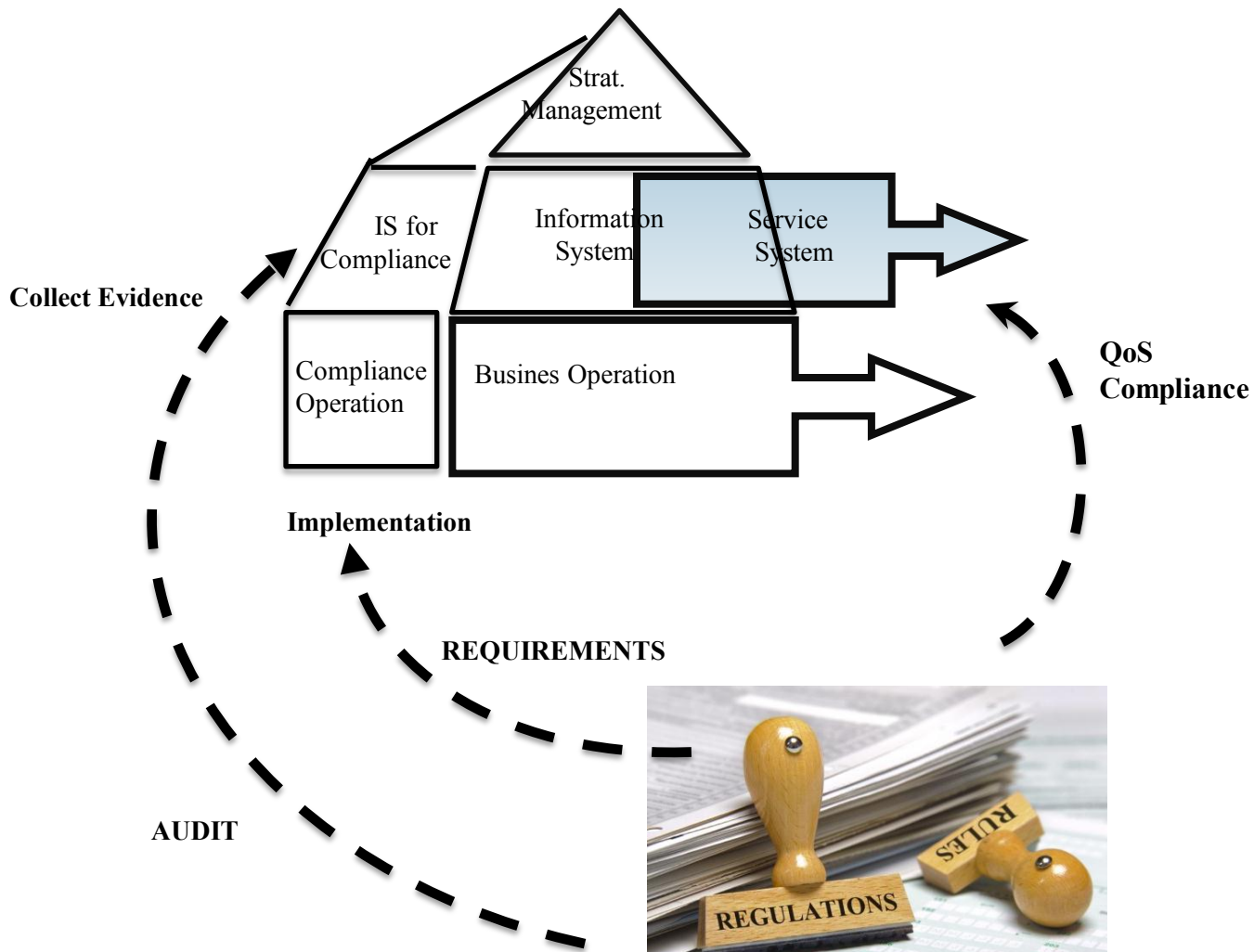
Compliance issues related to services

Regulations like Basel III, SoX, KYC, etc
 Norms IT Service Management (ISO 20000, ISO 27000),
 Best Practices (like ITIL)

Which level of assurance associated with the delivery of a compliant Service ?

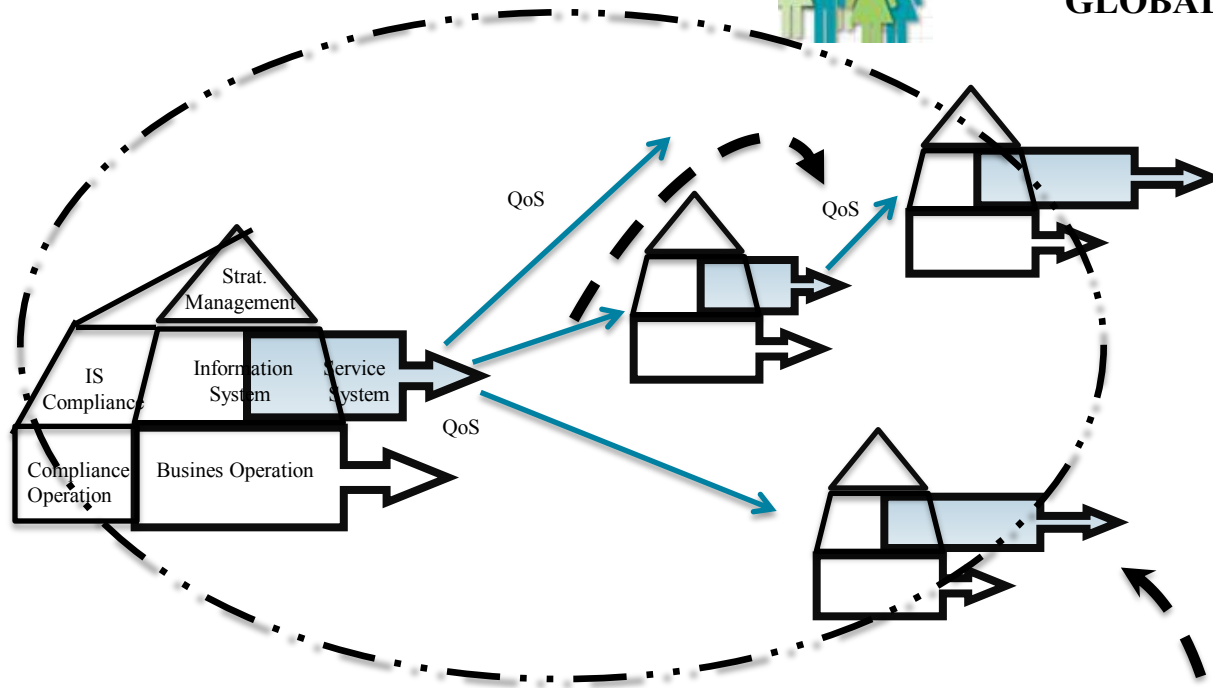


**Non prescriptive regulations, such as principle-based, risk-based regulations, goal-based regulations
 but also norms, standards and best practices**





GLOBAL LEVEL OF CONFIDENCE



Intteroperability between

- the local compliance operation implementations
- the local collection of evidences

QoS
Compliance
at systemic
level



Concrete Case and Research Questions

The Finance Service System in Luxembourg

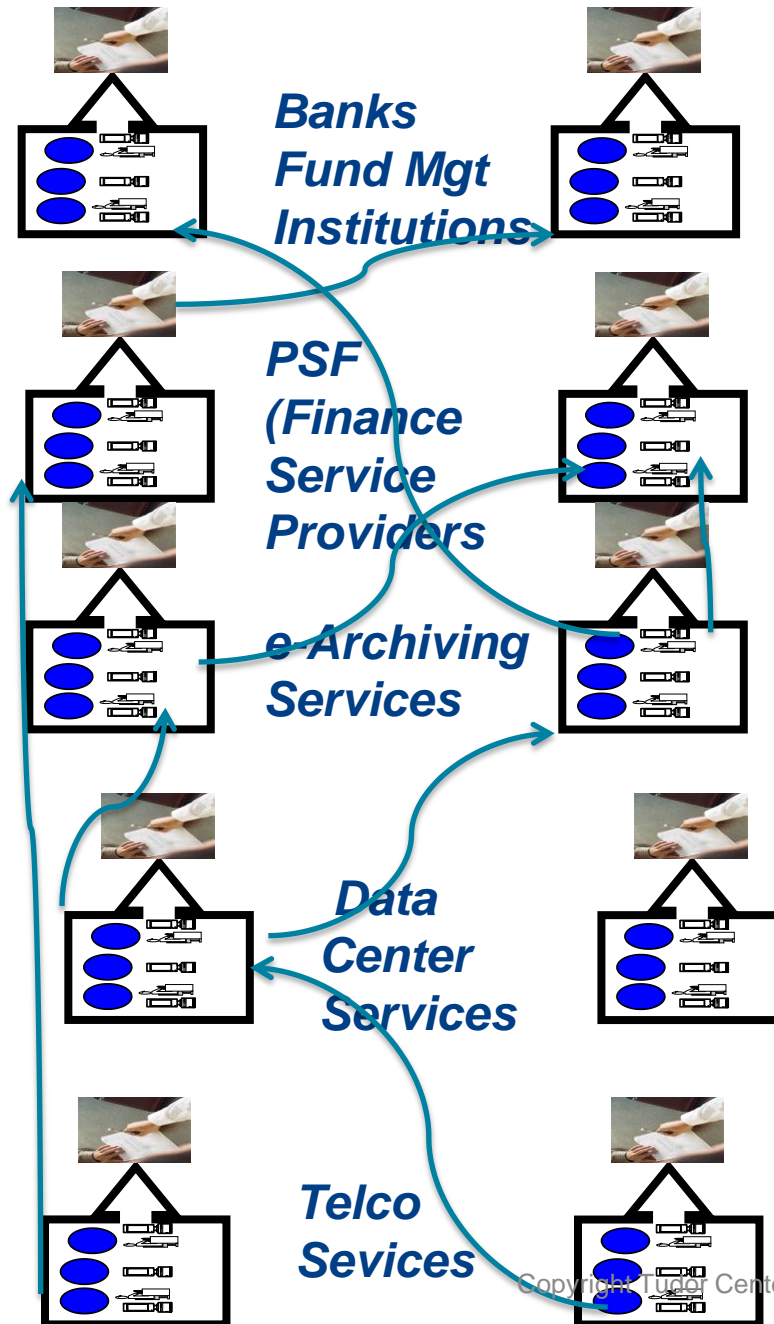
Regulators

CSSF: supervision of the finance sector

ILNAS: Luxembourg Law on e-Archiving

CNPD/EU: data protection

ILR/EU: quality of service



The Finance Service System in Luxembourg

Regulators

CSSF: supervision of the finance sector

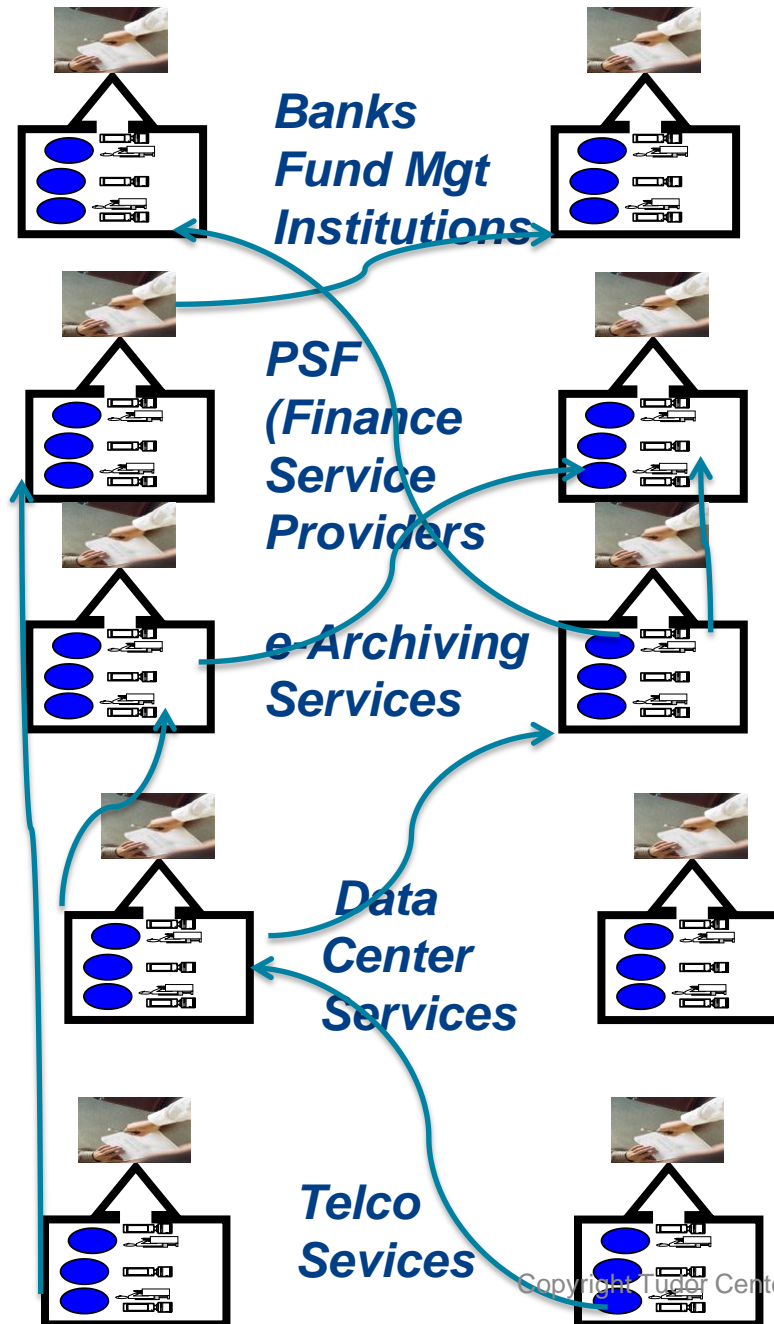
security risks (as part of operational risks – Basel III)
ISO15405

ILNAS: Luxembourg Law on e-Archiving

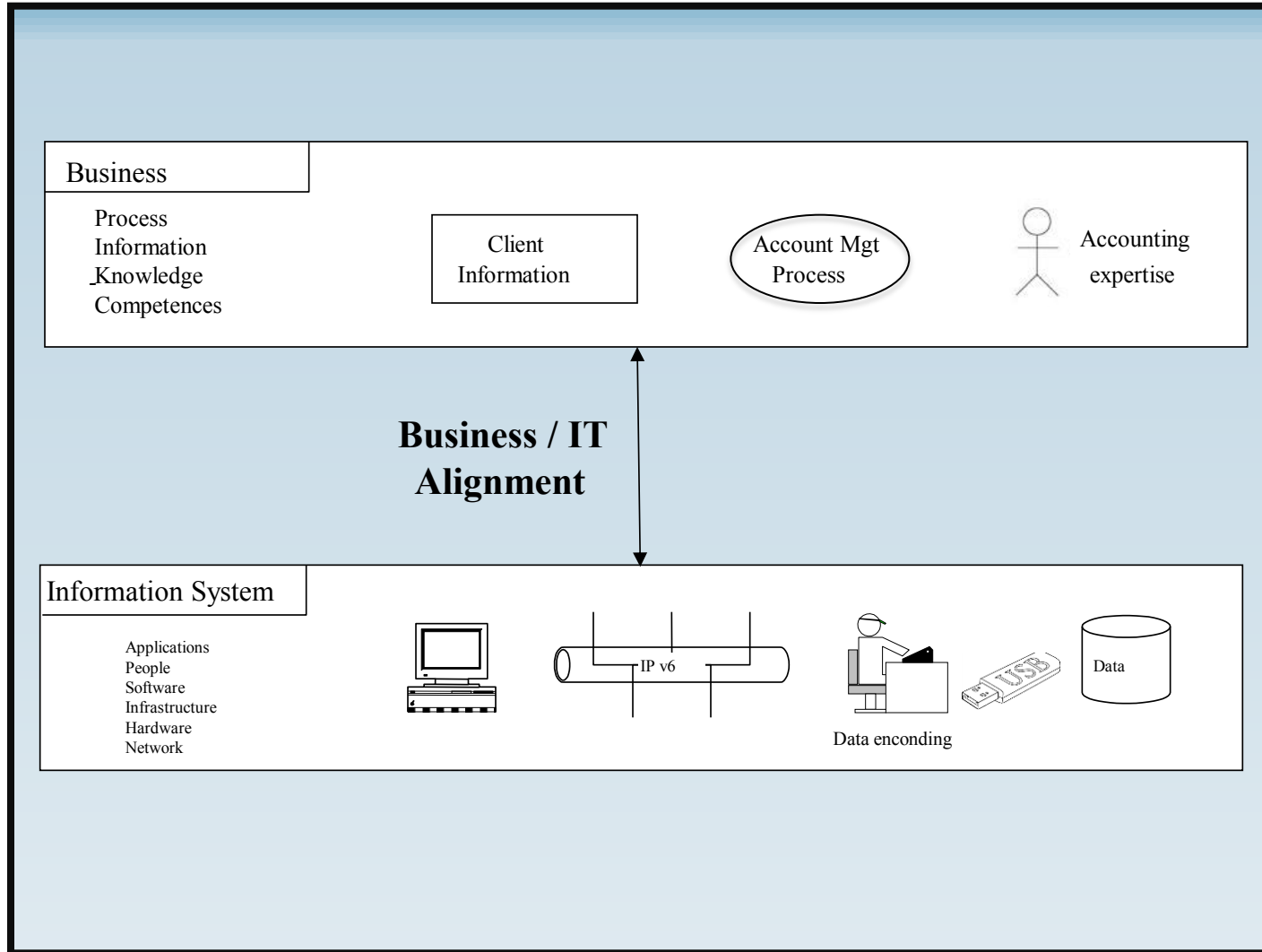
security risk management (ISO 27001 – ISO 27005)

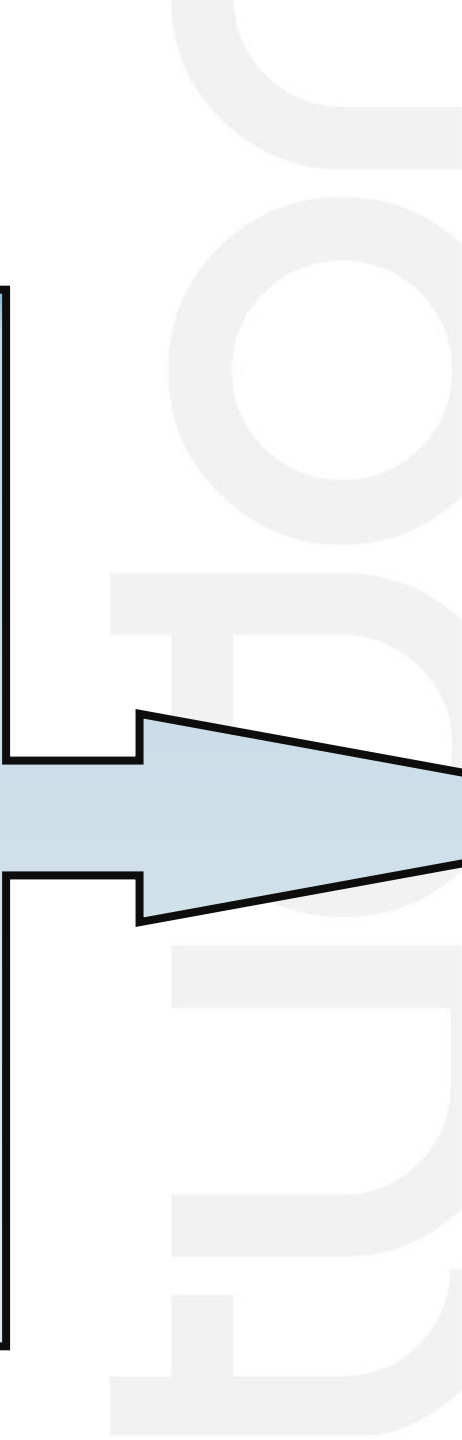
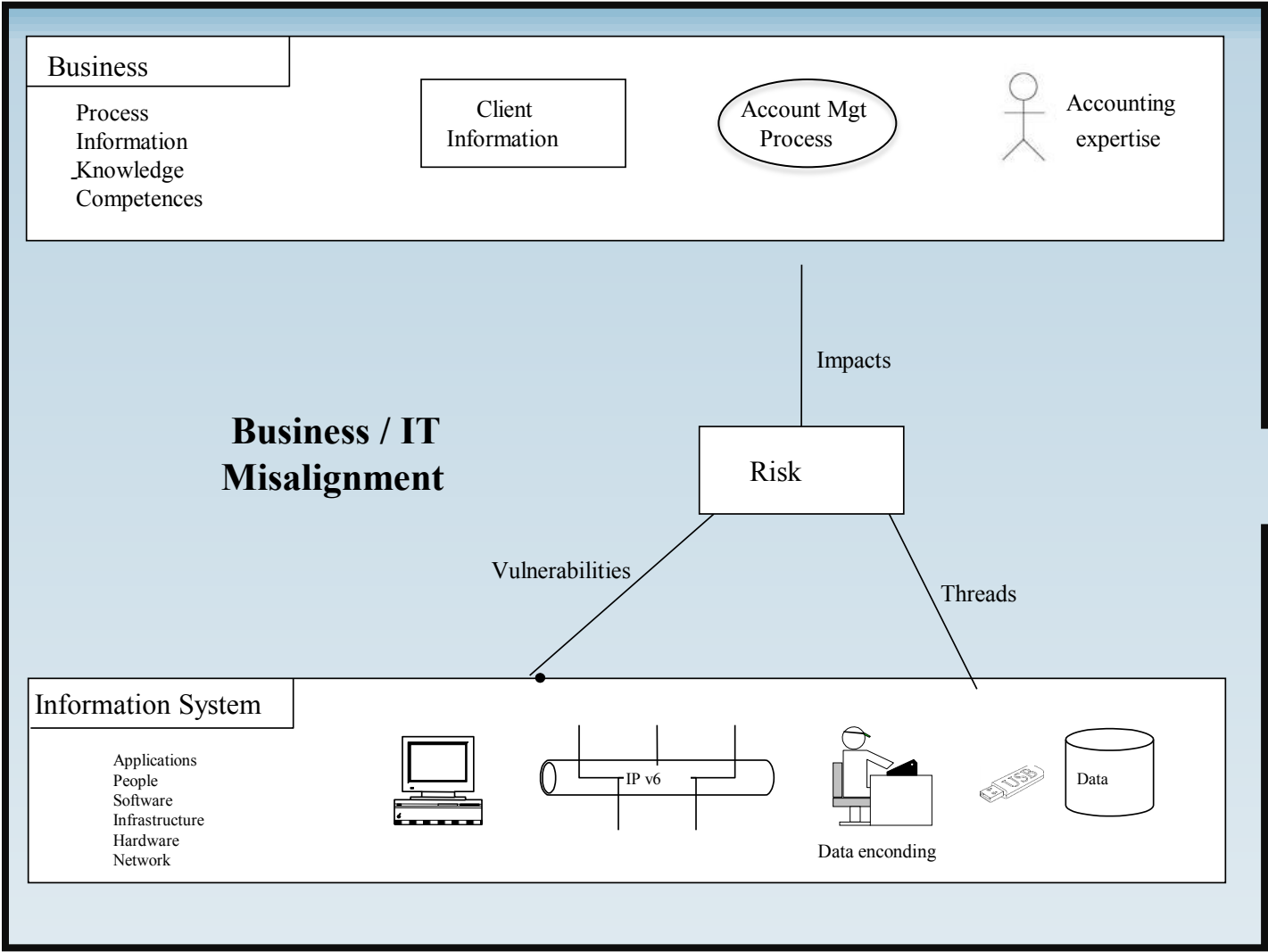
ILR/EU: quality of service

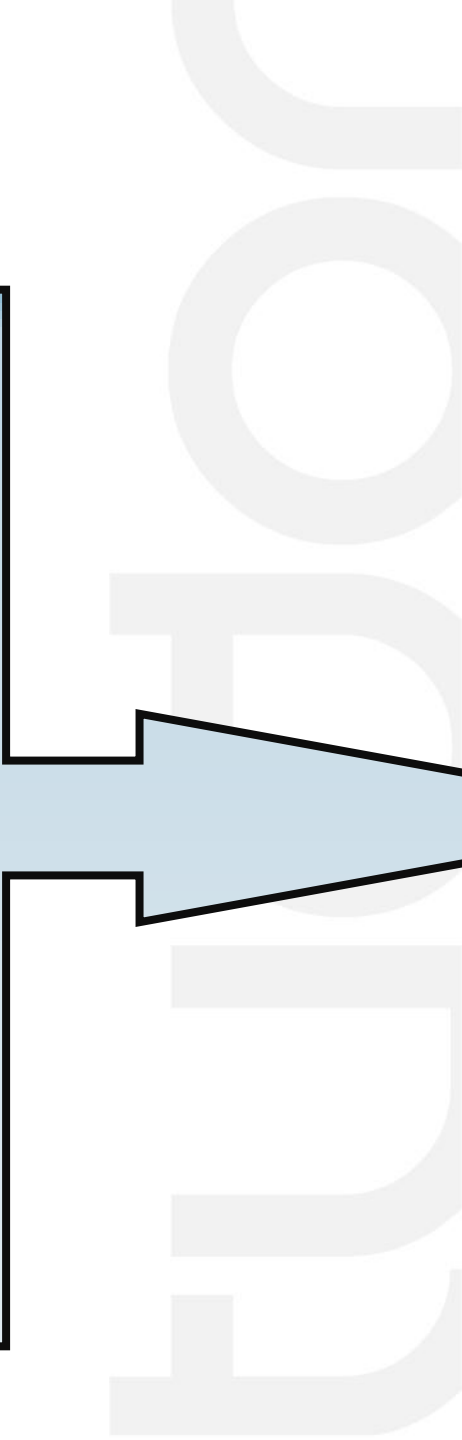
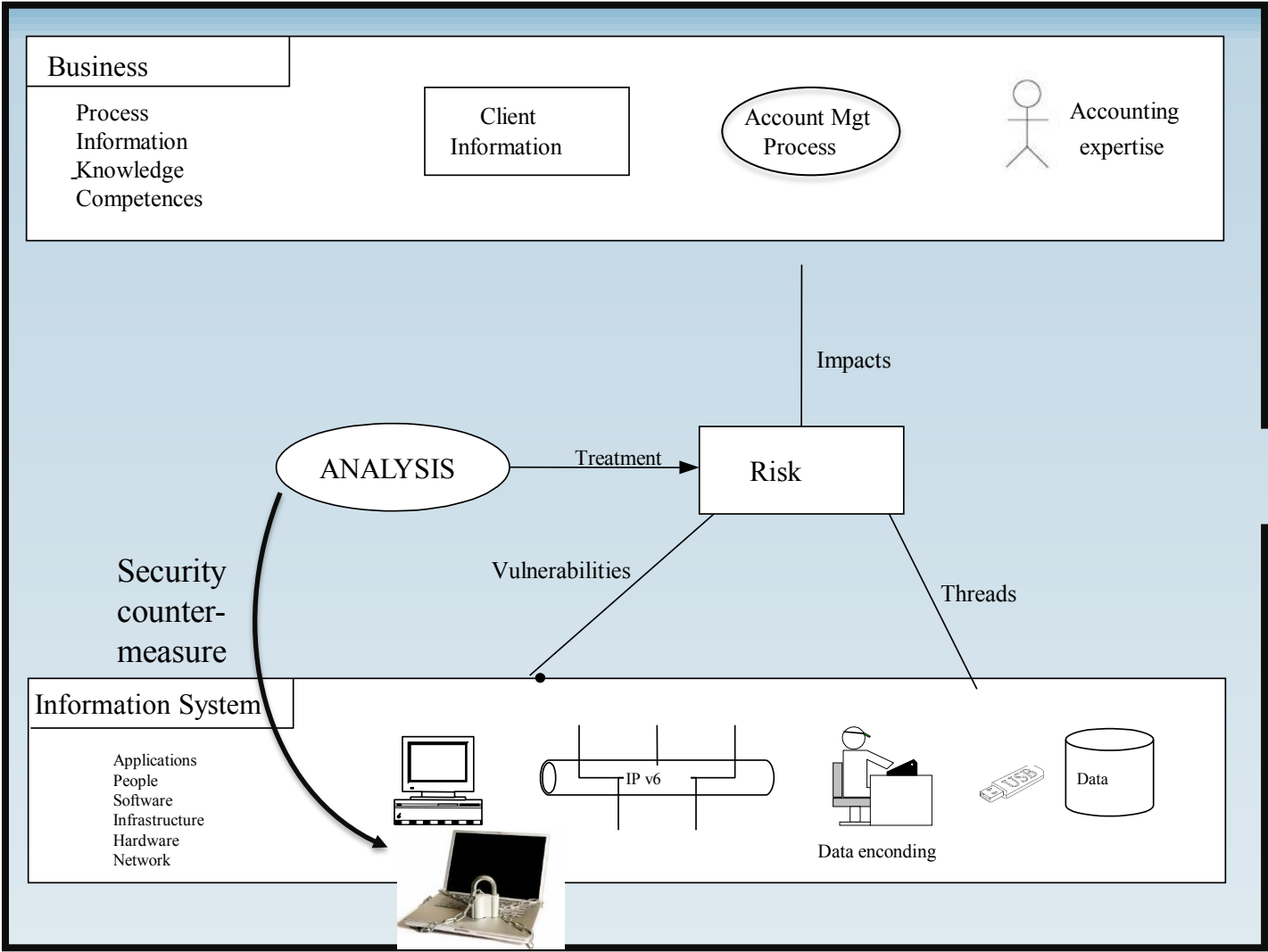
security and availability risks (ENISA)



What is security risk management ?







There exists a lot of security risk management regulations, norms, standards and best practices.

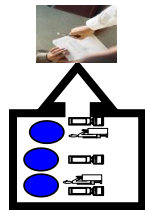


IPAA Security Rule Standard Implementation Specification	Implementation	Requirement Description
Security Management Process	Required	Policies and procedures to manage s violations
Risk Analysis	Required	Conduct vulnerability assessment
Risk Management	Required	Implement security measures to red security breaches
Sanction Policy	Required	Worker sanction for policies and pro violations
Information System Activity Review	Required	Procedures to review system activity
Assigned Security Responsibility	Required	Identify security official responsible fo procedures
Workforce Security	Required	Implement policies and procedures to appropriate PHI access
Authorization and/or Supervision	Addressable	Authorization/supervision for PHI acc
Workforce Clearance Procedure	Addressable	Procedures to ensure appropriate PH
Termination Procedures	Addressable	Procedures to terminate PHI access document management
Information Access Management	Required	Policies and procedures to authorize
Isolation Health Clearinghouse	Required	Policies and procedures to separate operations
Access Authorization	Addressable	Policies and procedures to authorize
Access Establishment and	Addressable	Policies and procedures to grant acc
Verification	Addressable	Policies and procedures to grant acc
Security Awareness Training	Required	Training program for workers and ma

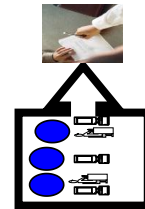
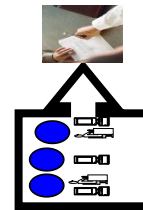
ambiguities, inconsistencies, terminology problems, etc.

Research Question # 1

Support the implementation of regulations, norms and standards in terms of an objective and measurable assurance reference model ?



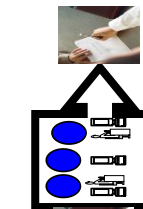
**Banks
Fund Mgt
Institutions**



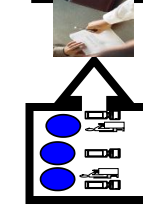
**PSF
(Finance
Service
Providers**



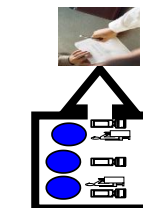
**e-Archiving
Services**



**Data
Center
Services**



**Telco
Services**



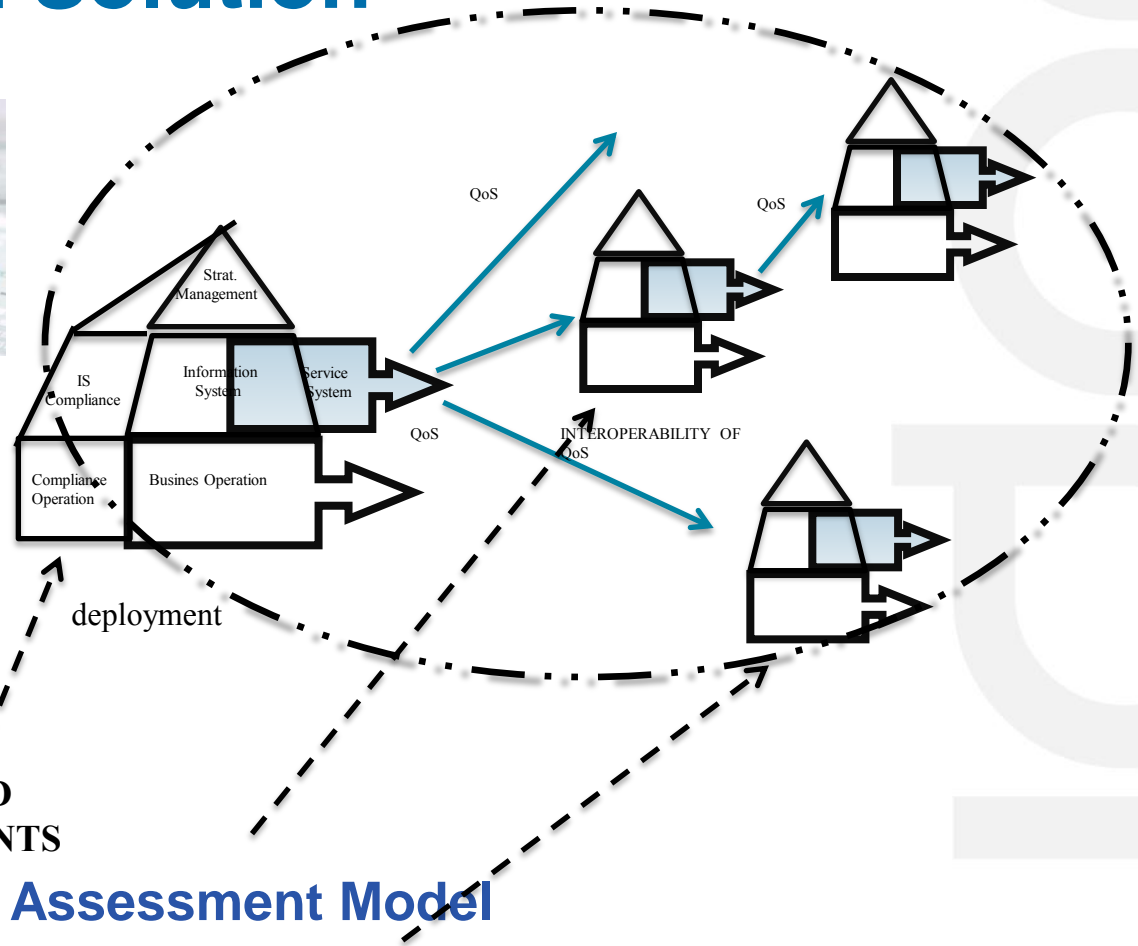
Research Question # 2

Support the compliance reporting in terms of an interoperable model associated with the collected evidences

The proposed approach (1): Process Reference and Assessment Model

The Proposed Solution

- Regulation
- Laws
- Standards
- Norms
- Best Practices

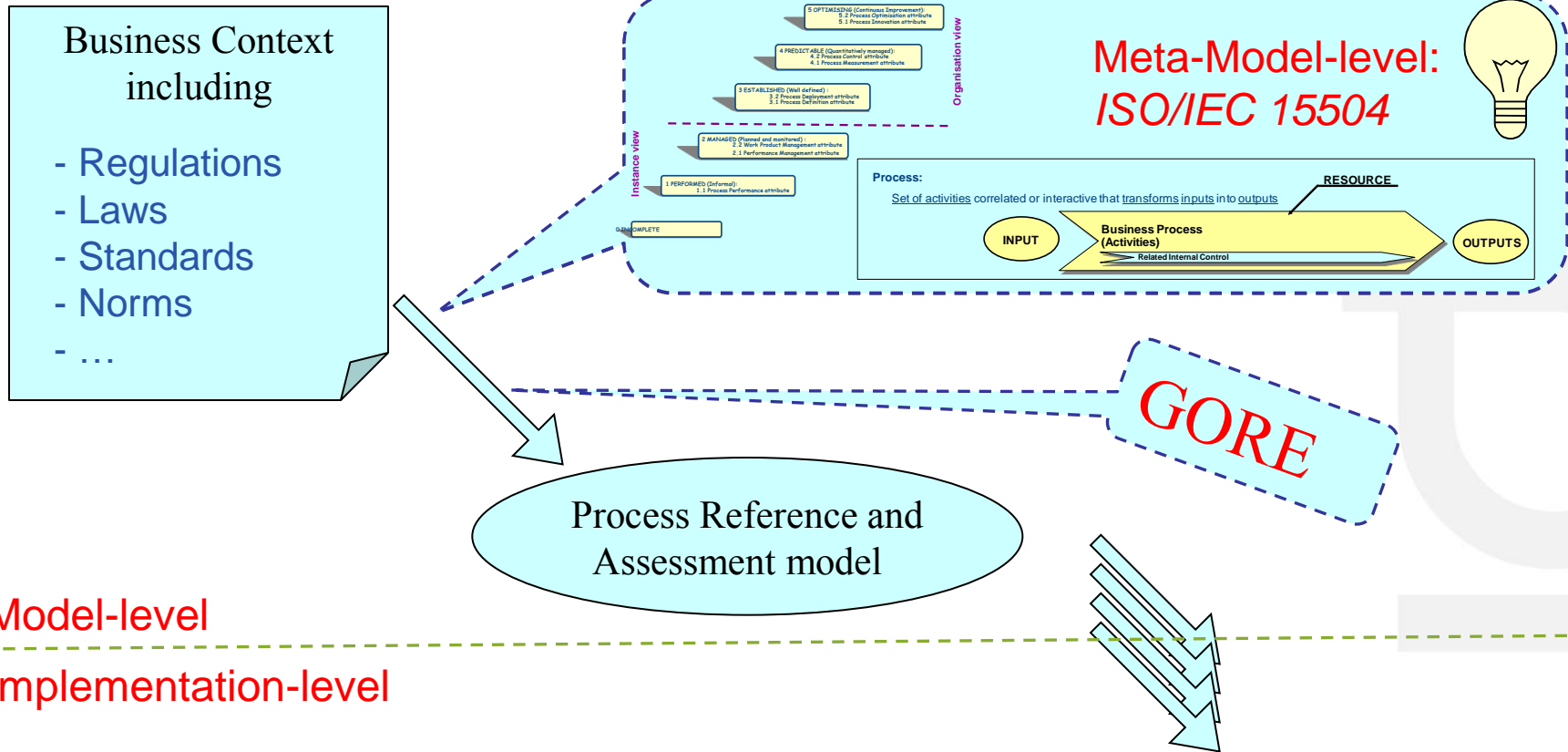


Process Reference and Assessment Model

for supporting the

- Definition of a compliant organisation at design time
- Audit the organisation at run time by measuring the level of assurance

The Gist of the Approach



Process Model based on ISO 15504

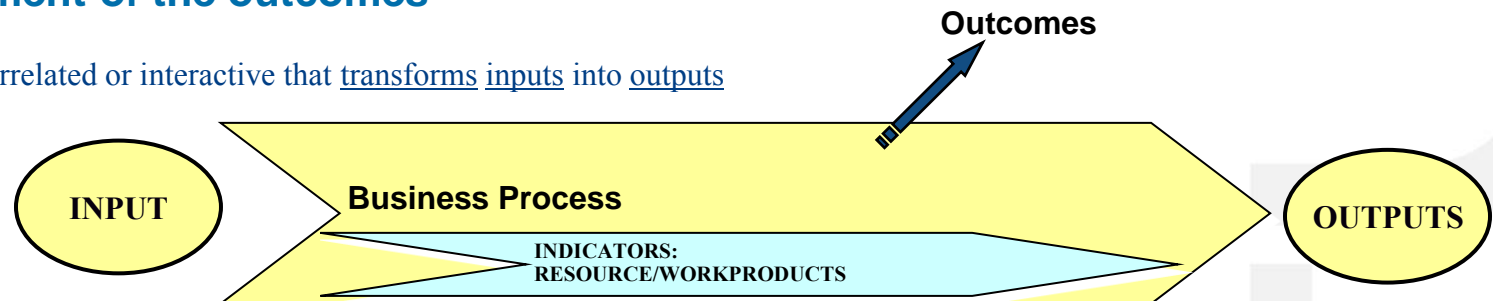
Principles for building a Process Reference and Assessment Model

For each process

- **A Purpose**
 - The high-level objectives of performing the process
- **Outcomes**
 - Observable and measurable results/best practices associated with the process
 - Necessary and sufficient to demonstrate successful achievement of the process purpose
- **Workproducts, practices, and resources are the indicators associated with the measurement of the outcomes**

Process:

Set of activities correlated or interactive that transforms inputs into outputs



Assurance Aspects – 5 Levels

Higher levels may give greater confidence that an organization's business goals will be met

5 OPTIMISING (Continuous Improvement):
5.2 Process Optimisation attribute
5.1 Process Innovation attribute

The process is continuously improved to meet business goals

4 PREDICTABLE (Quantitatively managed):
4.2 Process Control attribute
4.1 Process Measurement attribute

Quantitative objectives, Measures
Analysis of variation

3 ESTABLISHED (Well defined) :
3.2 Process Deployment attribute
3.1 Process Definition attribute

A standard process is defined at the entity level and is effectively deployed
Personnel is appropriately trained
Defined methods for assessing process effectiveness

2 MANAGED (Planned and monitored) :
2.2 Work Product Management attribute
2.1 Performance Management attribute

The process is planned, monitored & adjusted (supervised)
Responsibilities & Authorities are defined
Work products are defined, controlled & adjusted

1 PERFORMED (Informal):
1.1 Process Performance attribute

The process achieves its purpose but is not really monitored and repeatable
The results of the process often depend on "heroes"

0 INCOMPLETE

The process is not implemented or fails to achieve its purpose

Instance view

Organisation view

15504 Guidelines for extracting assurance indicators

- 5.2 *Changes to the definition, management and performance of the process result in effective impact that achieves the relevant process improvement objectives.*

- 5.1 *Changes to the process are identified from analysis of common causes of variation in performance, and from investigations of innovative approaches to the definition and deployment of the process.*

- 4.2 *The process is quantitatively managed to produce a process that is stable, capable, and predictable within defined limits.*

- 4.1 *The standard process is effectively deployed as a defined process to achieve its process outcomes.*

- 3.2 *A standard process is maintained to support the deployment of the defined process.*

- 3.1 *Measurement results are used to ensure that performance of the process supports the achievement of relevant process performance objectives in support of defined business goals.*

- 2.2 *Work products produced by the process are appropriately managed.*

- 2.1 *Performance of the process is managed.*

- 1. *Process purpose is achieved.*

<i>Indicators</i>	<p><u>Practices:</u> <i>Dependencies between work products are identified and understood. Requirements for the approval of work products to be controlled are defined. ...</i></p> <hr/> <p><u>Workproducts:</u> <i>Plan. (Expresses selected policy or strategy to manage work products. Describes requirements to develop, distribute, and maintain the work products. ...)</i></p> <hr/> <p><u>Resources:</u> <i>Document identification and control procedure; Work product review methods and experiences; Review management method / toolset; Intranets, extranets and/or other communication mechanisms; ...</i></p>
<i>Outcomes</i>	<p><i>a) requirements for the work products of the process are defined;</i></p> <hr/> <p><i>b) requirements for documentation and control of the work products are defined;</i></p> <hr/> <p><i>c) work products are appropriately identified, documented, and controlled;</i></p> <hr/> <p><i>d) work products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.</i></p>

The main issues identified when creating Process Reference & Assessment Models

Issue1: Difficulties when translating norms and standards in ISO 15504 compliant model

- Lack of a systematic rules for building compliant models

Issue2: Lack of requirements on the indicators

- How to derive them in a systematic way ?

→ ***Proposition of a requirements engineering (RE) method for building ISO 15504 Process Reference & Assessment Models***

Proposition of a RE method based on i^*

(a GORE -Goal Oriented Requirements Engineering- notation)

For each process

- **A Purpose**
 - The high-level objectives of performing the process
- **Outcomes**
 - Observable and measurable results of process
 - Necessary and sufficient to demonstrate successful achievement of the process purpose
- **Workproducts, Practices and Resources are the indicators associated with the measurement of the outcomes**

i^* Soft-Goals

i^* Goals

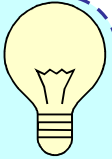
i^*
decomposition link

i^* Resource
Task, Agents

[Yu, Mylopoulos, 1993]

[Publications 2,3,5]

Meta-Model-level: ISO/IEC 15504



V. Operational Risk

A. Definition of operational risk

644. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk,¹⁴⁴ but excludes strategic and reputational risk.

B. The measurement methodologies

645. The framework outlined below presents three methods for calculating operational risk capital charges in a continuum of increasing sophistication and risk sensitivity. (i) the Basic Indicator Approach, (ii) the Standardised Approach, and (iii) Advanced Measurement Approaches (AMA).

646. Banks are encouraged to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices. Qualifying criteria for the Standardised Approach and AMA are presented below.

647. Internationally active banks and banks with significant operational risk exposures (for example, specialised processing banks) are expected to use an approach that is more sophisticated than the Basic Indicator Approach and that is appropriate for the risk profile of the institution.¹⁴⁵ A bank will be permitted to use the Basic Indicator or Standardised Approach for some parts of its operations and an AMA for others provided certain minimum criteria are met, see paragraphs 650 to 653.

648. A bank will not be allowed to choose to revert to a simpler approach once it has been approved for a more advanced approach without supervisory approval. However, if a supervisor determines that a bank using a more advanced approach no longer meets the qualifying criteria for this approach, it may require the bank to revert to a simpler approach for some or all of its operations, until it meets the conditions specified by the supervisor for returning to a more advanced approach.

1. The Basic Indicator Approach

649. Banks using the Basic Indicator Approach must hold capital for operational risk equal to the average over the previous three years of a fixed percentage (denoted alpha) of positive annual gross income. Figures for any year in which annual gross income is negative or zero should be excluded from both the numerator and denominator when calculating the average.¹⁴⁶ The charge may be expressed as follows:

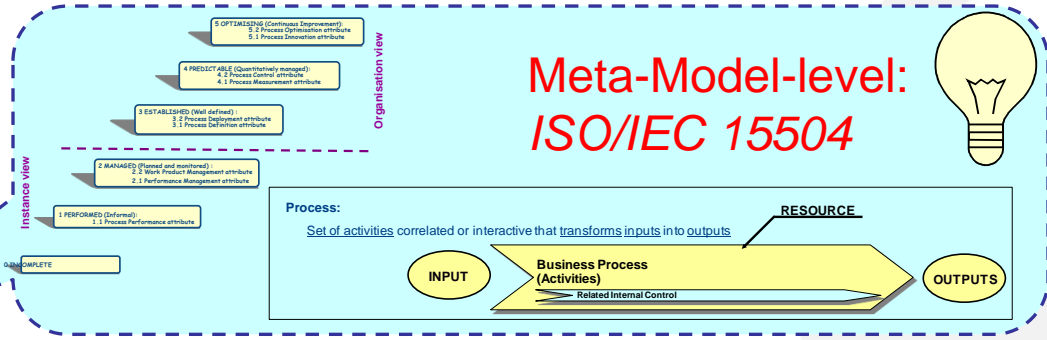
$$K_{\text{BIA}} = \left[\frac{\sum_{i=1}^n (G_{i,t} + \alpha)}{n} \right] \alpha$$

¹⁴⁴ Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

¹⁴⁵ Supervisors will review the capital requirement produced by the operational risk approach used by a bank (either the Basic Indicator Approach, Standardised Approach or AMA) for general credibility, supervisory in relation to a firm's peers. In the event that credibility is lacking, appropriate supervisory action under Pillar 2 will be considered.

¹⁴⁶ If negative gross income distorts a bank's Pillar 1 capital charge, supervisors will consider appropriate supervisory action under Pillar 2.

144



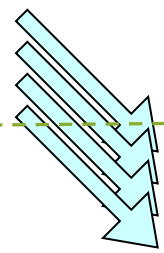
Process Reference and Assessment model

GORE

[Publications 4,6,7]

Model-level

Implementation-level



Meta-Model-level: ISO/IEC 15504



V. Operational Risk

A. Definition of operational risk

644. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk,¹ but excludes strategic and reputational risk.

B. The measurement methodologies

645. The framework outlined below presents three methods for calculating operational risk capital charges in a continuum of increasing sophistication and risk sensitivity. (i) the Basic Indicator Approach, (ii) the Standardised Approach, and (iii) Advanced Measurement Approaches (AMA).

646. Banks are encouraged to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices. Qualifying criteria for the Standardised Approach and AMA are presented below.

647. Internationally active banks and banks with significant operational risk exposures (for example, specialised processing banks) are expected to use an approach that is more sophisticated than the Basic Indicator Approach and that is appropriate for the risk profile of the institution.² A bank will be permitted to use the Basic Indicator or Standardised Approach for some parts of its operations and an AMA for others provided certain minimum criteria are met, see paragraphs 650 to 653.

648. A bank will not be allowed to choose to revert to a simpler approach once it has been approved for a more advanced approach without supervisory approval. However, if a supervisor determines that a bank using a more advanced approach no longer meets the qualifying criteria for this approach, it may require the bank to revert to a simpler approach for some or all of its operations, until it meets the conditions specified by the supervisor for returning to a more advanced approach.

1. The Basic Indicator Approach

649. Banks using the Basic Indicator Approach must hold capital for operational risk equal to the average over the previous three years of a fixed percentage (denoted alpha) of positive annual gross income. Figures for any year in which annual gross income is negative or zero should be excluded from both the numerator and denominator when calculating average.³ The charge may be expressed as follows:

$$R_{\text{Basic}} = [\sum (\alpha I_{i,t}) / n]^{1.6}$$

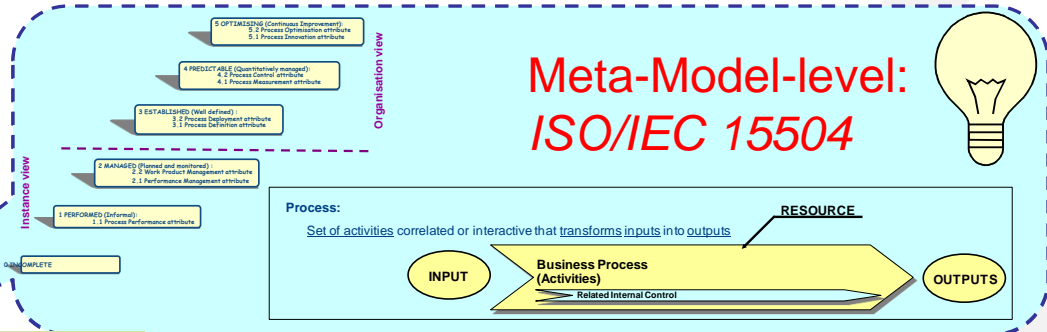
¹ Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

² Supervisors will review the capital requirement produced by the operational risk approach used by a bank under the Basic Indicator Approach, Standardised Approach or AMA, for general suitability, against relation to a firm's peers. In the event that credibility is lacking, appropriate supervisory action under Pill 1 will be considered.

³ If negative gross income causes a bank's Pillar 1 capital charge, supervisors will consider appropriate supervisory action under Pillar 2.

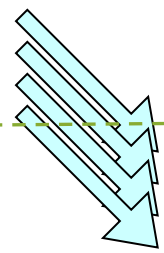
Model-level

Implementation-level

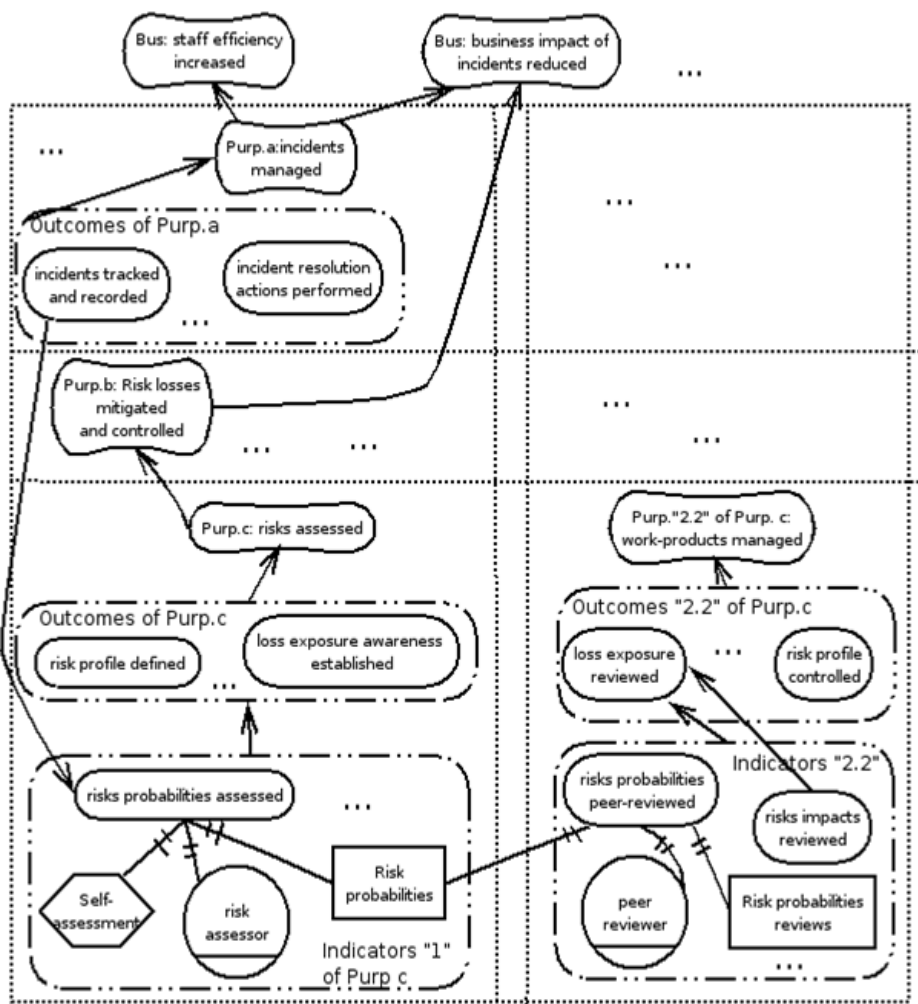


Op. Risk Assess.	1	2.1	2.2	...
Purpose	Identified operational risks are qualitatively assessed. [Source: 140, 652, ..., 859]
Outcomes	<ul style="list-style-type: none"> a) an operational risk assessment strategy is developed, including the principles of how operation risk is to be assessed, according to the size, the sophistication, the nature and the complexity of the bank's activity; [Source: 1, 357] b) bank is aware of the loss exposure (qualitatively) of each identified risk on its business; [Source: 139, ..., 248] c) identified risks are organized (7 loss event types in Basel II); or [Source: 139, 455] d) bank's risk profile is determined [Source: 140] 	<ul style="list-style-type: none"> Bus. staff efficiency increased Bus. business impact of incidents reduced ... 	<ul style="list-style-type: none"> Purp. a: incidents managed ... Outcomes of Purp. a: incidents tracked and recorded, incident resolution actions performed ... Purp. b: Risk losses mitigated and controlled ... Purp. c: risks assessed Outcomes of Purp. c: risk profile defined, loss exposure awareness established ... risks probabilities assessed Self-assessment, risk assessor, Risk probabilities Indicators "1" of Purp. c 	<ul style="list-style-type: none"> Purp. "2.2" of Purp. c: work-products managed Outcomes "2.2" of Purp. c: loss exposure reviewed, risk profile controlled ... risks probabilities peer-reviewed peer reviewer, Risk probabilities reviews Indicators "2.2" risks impacts reviewed
Indicators	<p>Practices: Risk probabilities are self-assessed</p> <p>WorkProducts: Risk probabilities with defined probabilities categories</p> <p>Resources: Risk assessor has knowledge in risks and self-assessment techniques used.</p>

GORE



Bank D
Bank C
Bank B
Bank A



Op. Risk Assess.	1	2.1	2.2	...
Purpose	Identified operational risks are qualitatively assessed. [Source: 141, ..., 662, ..., 859]	...	The loss exposure, the risk profile, ... are appropriately managed.	...
Outcomes	<p>a) an operational risk assessment strategy is developed, including the principles of how operational risk is to be assessed, according to the size, the sophistication, the nature and the complexity of the bank's activity; [Source: 1, ..., 357]</p> <p>b) bank is aware of the loss exposure (qualitatively) of each identified risk on its business; [Source: 139, ..., 248]</p> <p>c) identified risks are organized (7 loss event types in Basel II); and [Source: 139, 455]</p> <p>d) bank's risk profile is determined. [Source: 140]</p>	...	<p>a) WP Req.: The risk profile must defined for each of the 7 loss event type;</p> <p>b) Control Req.: risk probabilities must be consistent across months;</p> <p>c) Control. Req.: Historical differences of loss exposures must be documented;</p> <p>d) Loss exposures must be reviewed once a month by peers under supervision of operational risk management department</p> <p>e) ...</p>	...
Indicators	<p><u>Practices:</u> Risk probabilities are self-assessed.</p> <p><u>WorkProducts:</u> Risk probabilities with defined probabilities categories</p> <p><u>Resources:</u> Risk assessor has knowledge in risks and self-assessment techniques used.</p>	...	<p><u>Practices:</u> Peer-review of risk probabilities</p> <p><u>WorkProducts:</u> Peer-review report of risk probabilities</p> <p><u>Resources:</u> Peer reviewer has knowledge in risks and peer-review technique</p>	...

A fragment of the security risk management model

Process Name	Risk Assessment
Process Purpose	The purpose of the process is to assess risks faced by the assets which are in the scope of the identified business
Process Expected Results	As a result of successful implementation of the Risk Assessment process: <ol style="list-style-type: none">1. Criteria for accepting risks are developed;2. Criteria for accepting risks are approved by the management;3. Assets and their owners are identified.4. Risks are identified in terms of vulnerabilities and threads5. Identified risks are analyzed and evaluated in terms of their impact
Base Practices	RA.BP1: Context and Assets Identification Identification of the perimeter of the company for which the security risk assessment will apply. Identification of the primary business assets and of the supporting resources (secondary assets) RA.BP2: Determination of security criteria Identification of security criteria (like confidentiality, availability and integrity) applicable to the protection of business assets

A fragment of security risk management process

	RA.BP3 Risk analysis and assessment Identification of each risk component (thread, vulnerability and impact). Qualitative/quantitative ranking of risks
--	--



Output Work Product		
ID	Name	Expected results and related BPs
06_02	List of assets	[RA.BP1]
05_06	List of security criteria	[RA.BP 2]
06_06	Ranked list of risks	[RA.BP 3]2, 3]

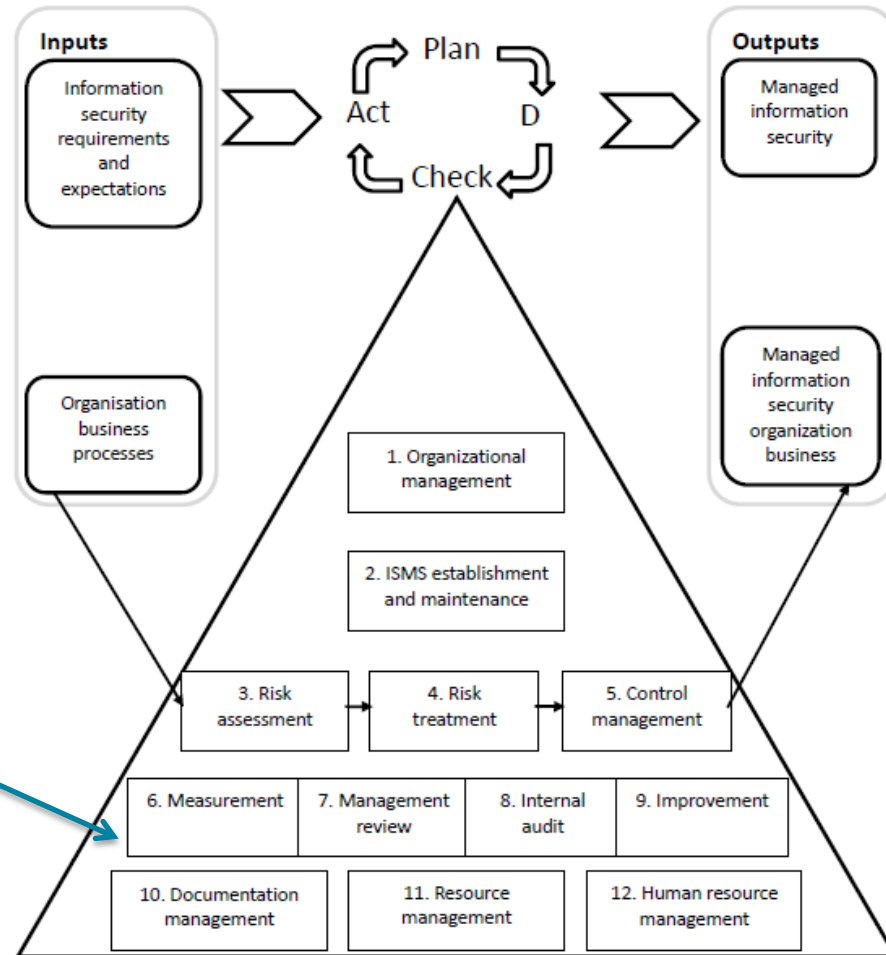
Indicators Level 2.2

The contents and structure of the work products are defined. They are standardized at the level of the organisation

Dependencies between work products are identified and understood.

The monitoring of changes to workproducts is supported

The complete security risk management reference model

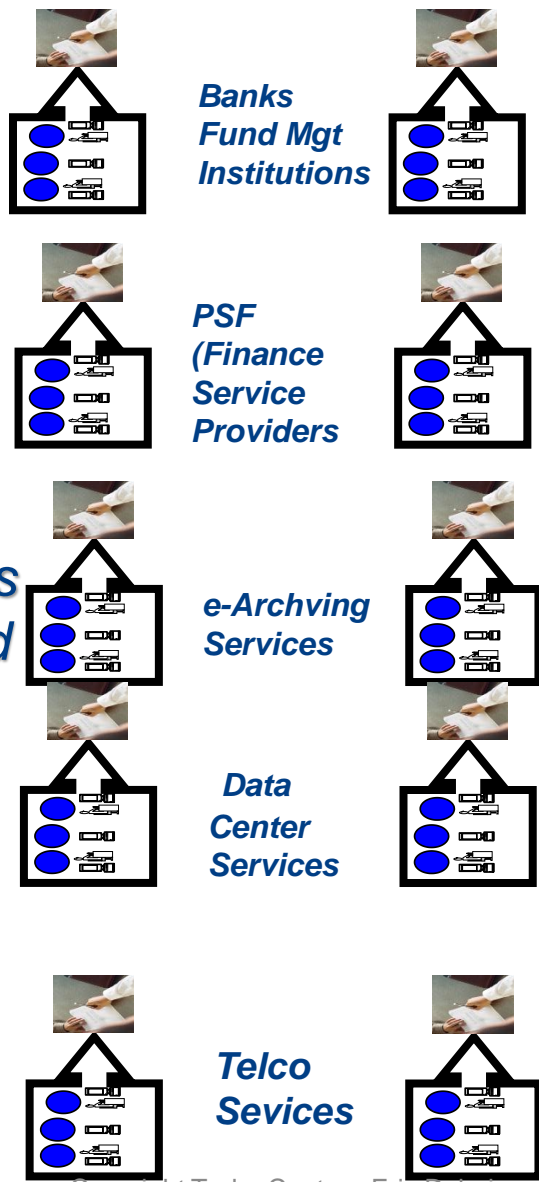


Process Name	Risk Assessment
Process Purpose	The purpose of the process is to assess risks faced by the assets which are in the scope of the identified business.
Process	As a result of successful implementation of the Risk Assessment process:
Expected Results	<ol style="list-style-type: none"> 1. Criteria for accepting risks are developed; 2. Criteria for accepting risks are approved by the management; 3. Assets and their owners are identified; 4. Risks are identified in terms of vulnerabilities and threats; 5. Identified risks are analyzed and evaluated in terms of their impact.
Base Practices	<p>RA.BP1: Context and Assets Identification Identification of the perimeter of the company for which the security risk assessment will apply, identification of the primary business assets and of the supporting resources (secondary assets).</p> <p>RA.BP2: Determination of security criteria Identification of security criteria (like confidentiality, availability and integrity) applicable to the protection of business assets.</p>

Regulators/ Standards

Research Question

Support the compliance reporting in terms of an interoperable model associated with the collected evidences



Research Question

Support the implementation of regulations and standards in terms of an objective and measurable assurance models

The Research Question (2)

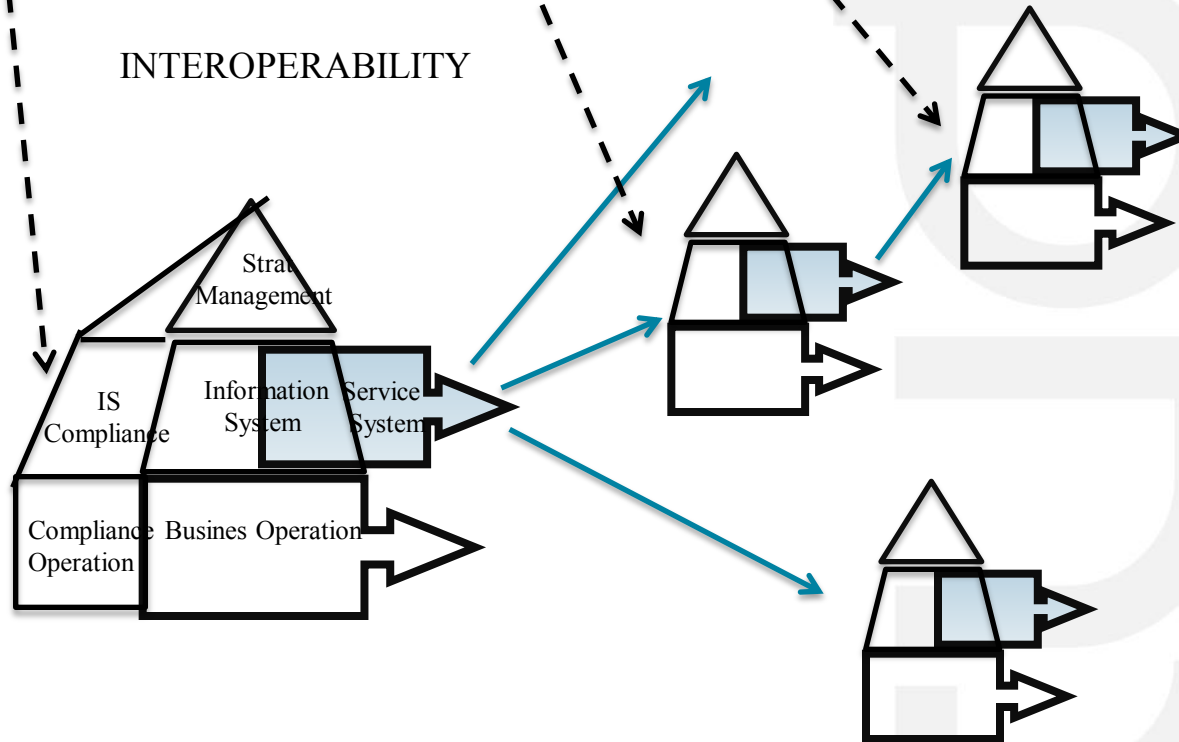
- Regulations
- Laws
- Standards
- Norms
- Best Practices

Interoperable Reporting Compliance Model for documenting evidences associated with compliance operations

INTEROPERABILITY

Process Name	Risk Assessment
Process Purpose	The purpose of the process is to assess risks faced by the assets which are in the scope of the identified business.
Process Expected Results	As a result of successful implementation of the Risk Assessment process: <ol style="list-style-type: none"> 1. Criteria for accepting risks are developed; 2. Criteria for accepting risks are approved by the management; 3. Assets and their owners are identified; 4. Risks are identified in terms of vulnerabilities and threats; 5. Identified risks are analyzed and evaluated in terms of their impact.
Best Practices	<p>RA.BP1: Context and Assets Identification Identification of the business of the company for which the security risk assessment will apply, identification of the primary business assets and of the supporting resources (secondary assets).</p> <p>RA.BP2: Determination of security criteria Identification of security criteria (like confidentiality, availability and integrity) applicable to the protection of business assets.</p>

Process Reference and Assessment Model



The proposed approach (2):

Using Enterprise Architecture models as the conceptual models for documenting compliance evidences

Why Enterprise Architecture ?

Enterprise Architecture is used as an instrument for governing the management and the transformation of enterprises in order to support their:

Control: Implementing a system of controls over the creation and monitoring of all architectural components and activities, to ensure the effective introduction, implementation, and evolution of architectures within the organization

Compliance: Implementing a system to ensure compliance with internal and external standards and regulatory obligations

Management: Establishing processes that support effective management of the above processes within agreed parameters

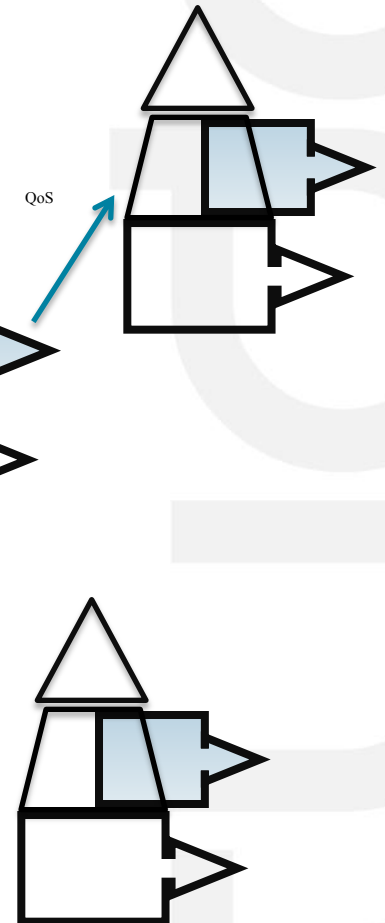
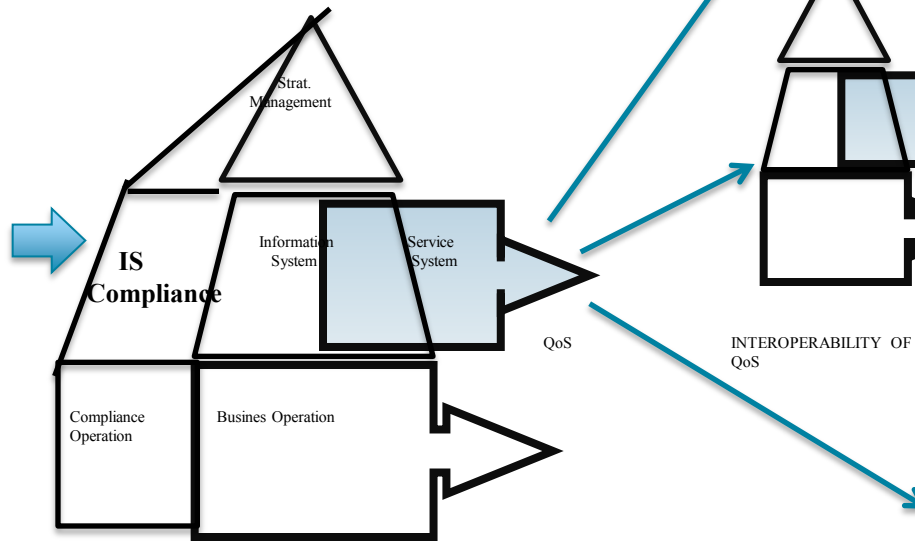
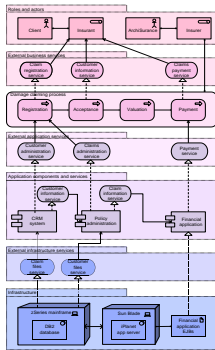
Accountability: Developing practices that ensure accountability to a clearly identified stakeholder community, both inside and outside the organization

.....

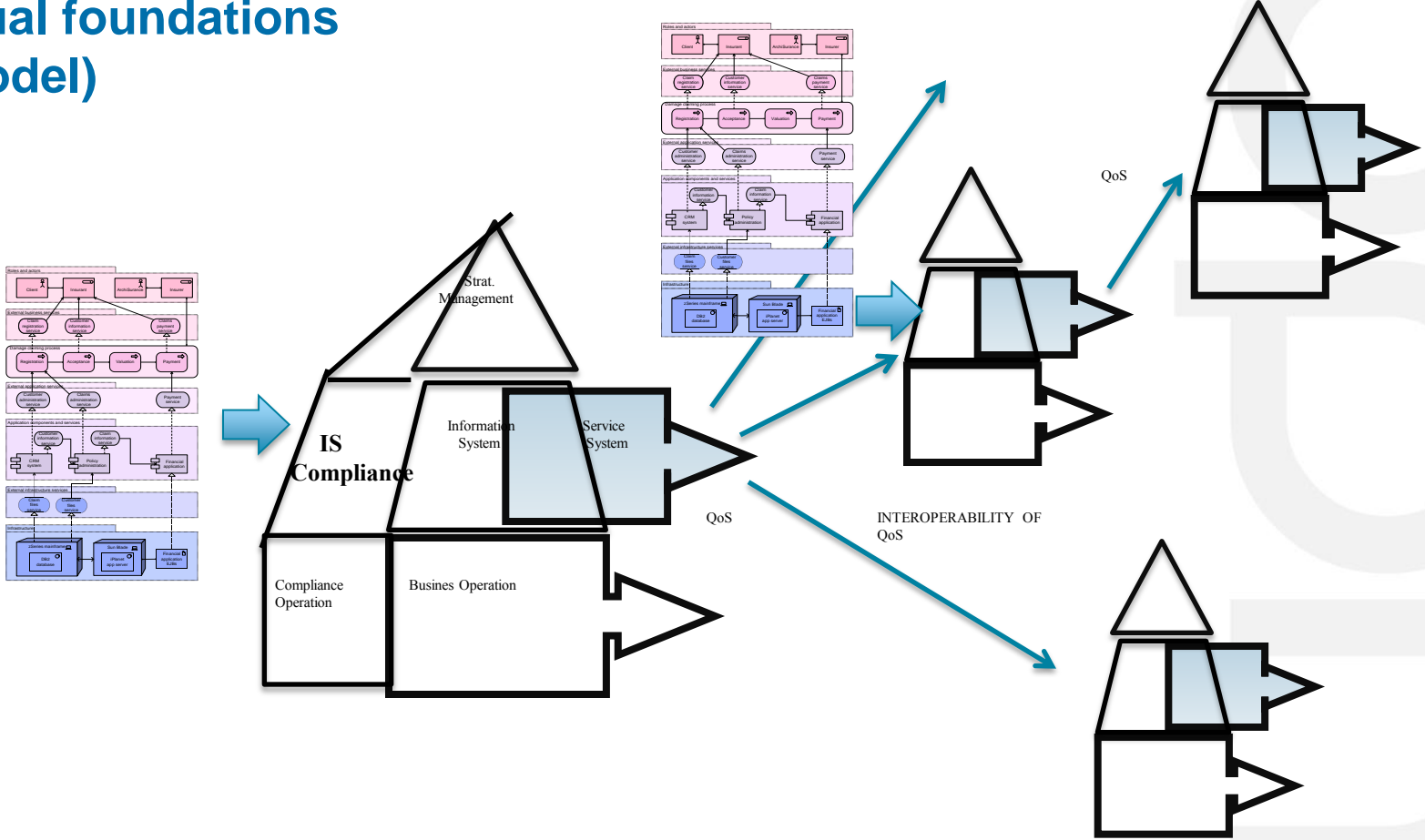
•

from [TOGAF, Open Group]

Enterprise Architecture (EA) conceptual models as IS reference models documenting compliance evidence

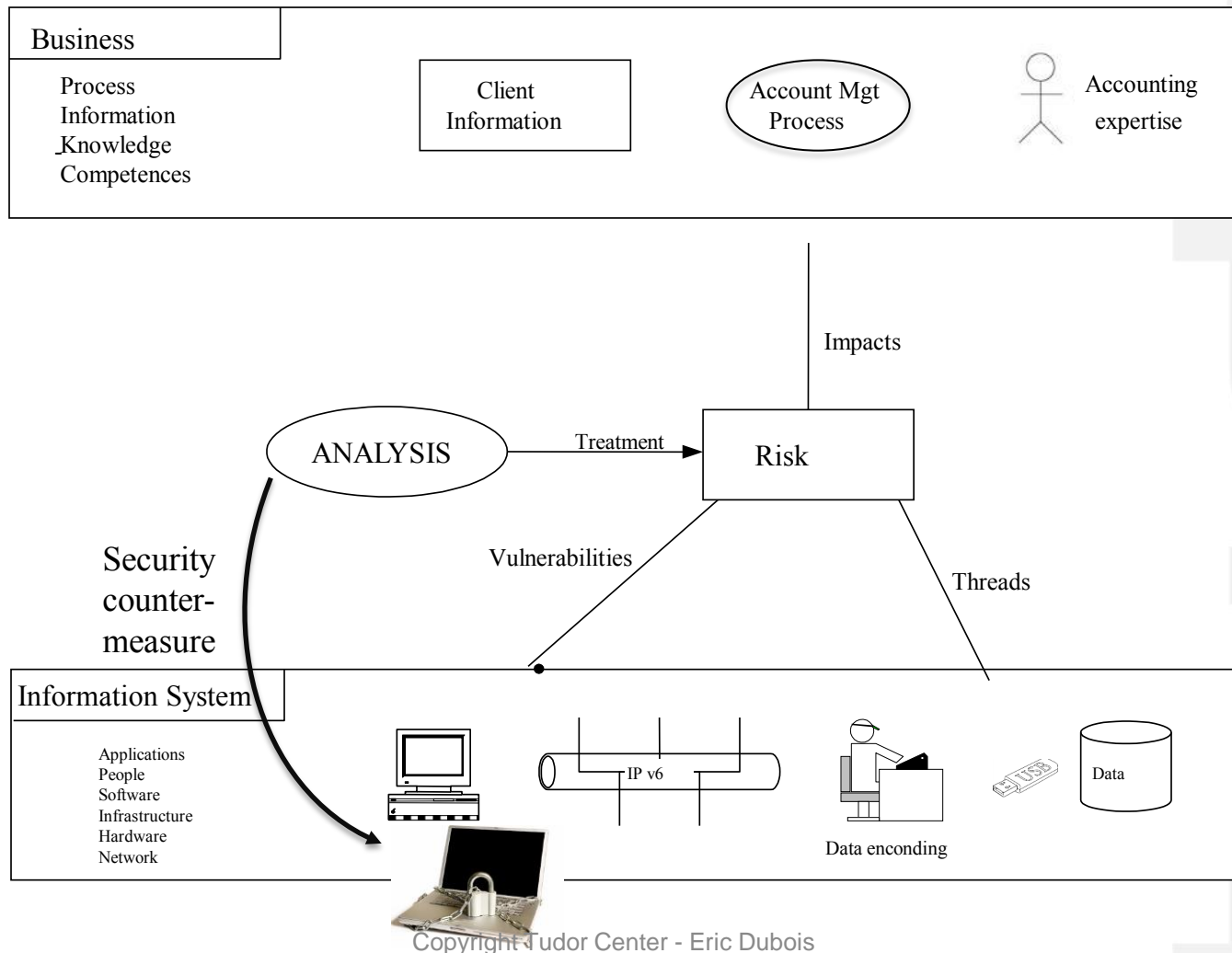


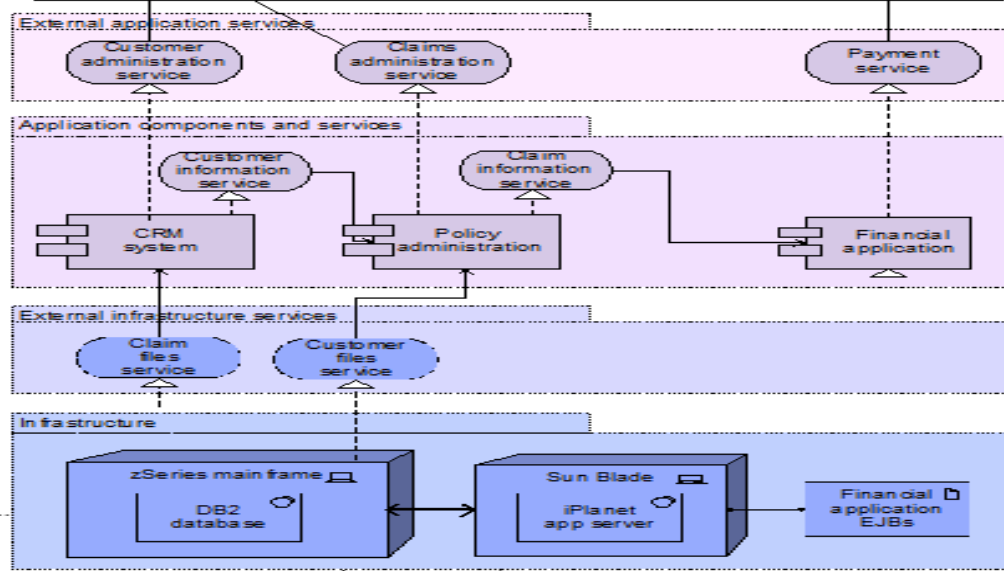
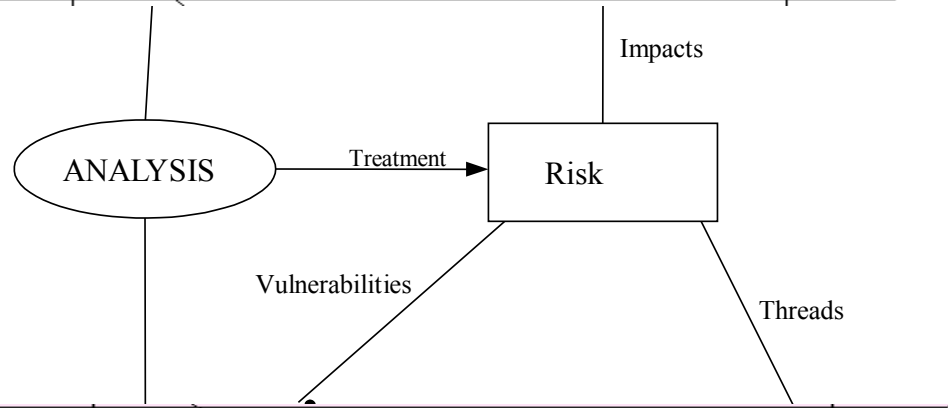
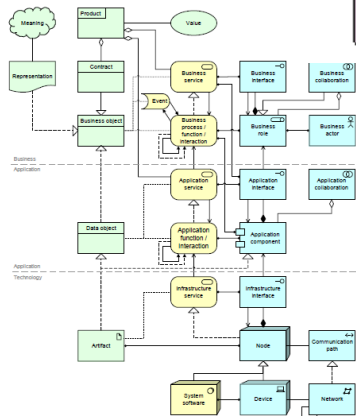
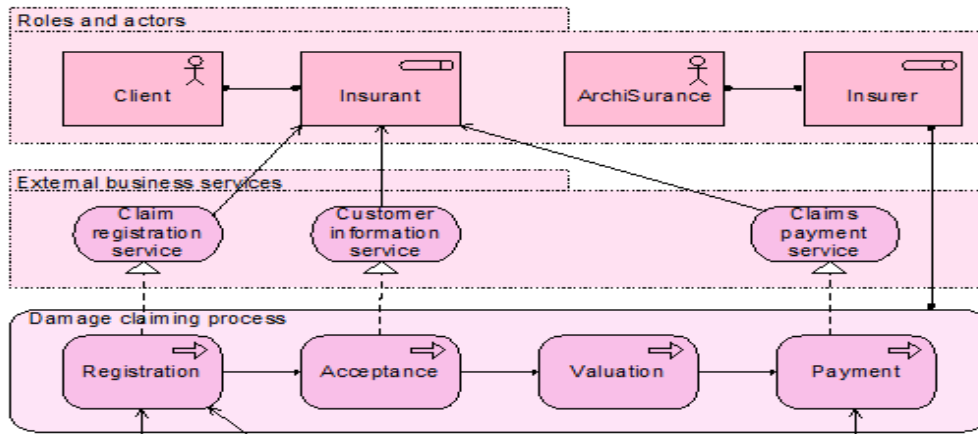
Interoperability guaranteed by the use of the same EA conceptual foundations (meta-model)



Research Question: Enhance the EA meta-model for capturing compliance evidences

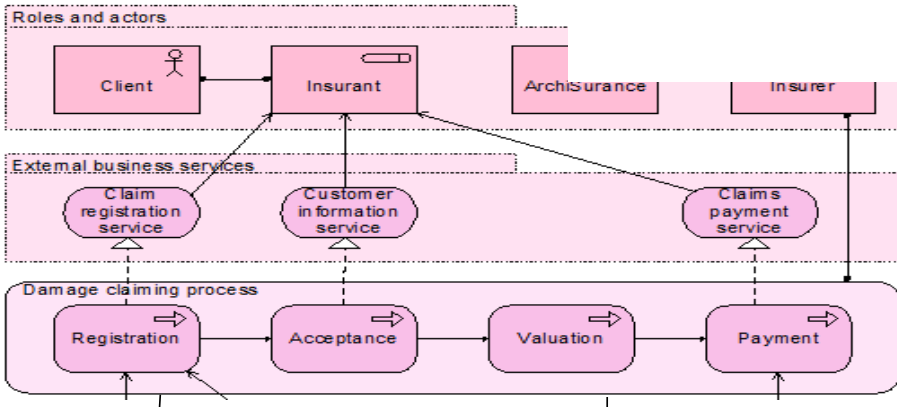
Application: ArchiMate and Security Risk Management





ArchiMate
Meta-model

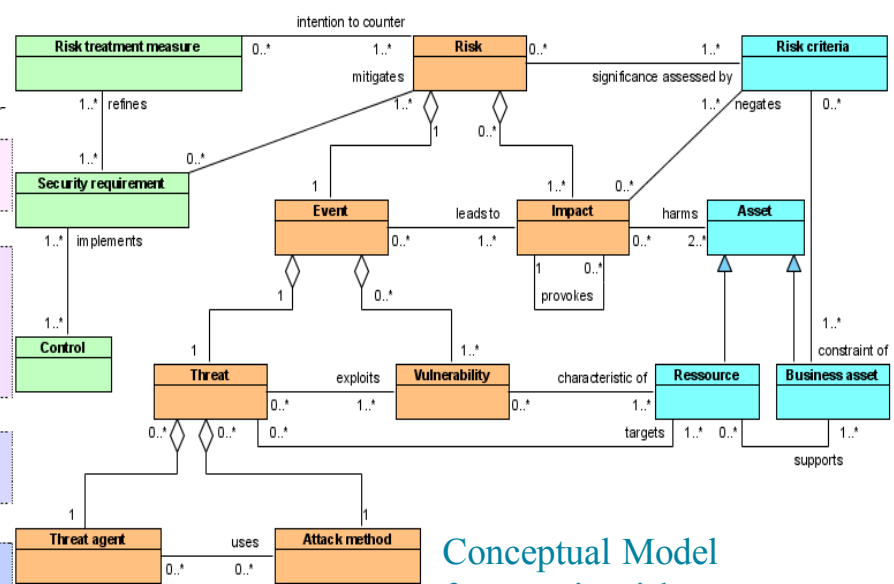
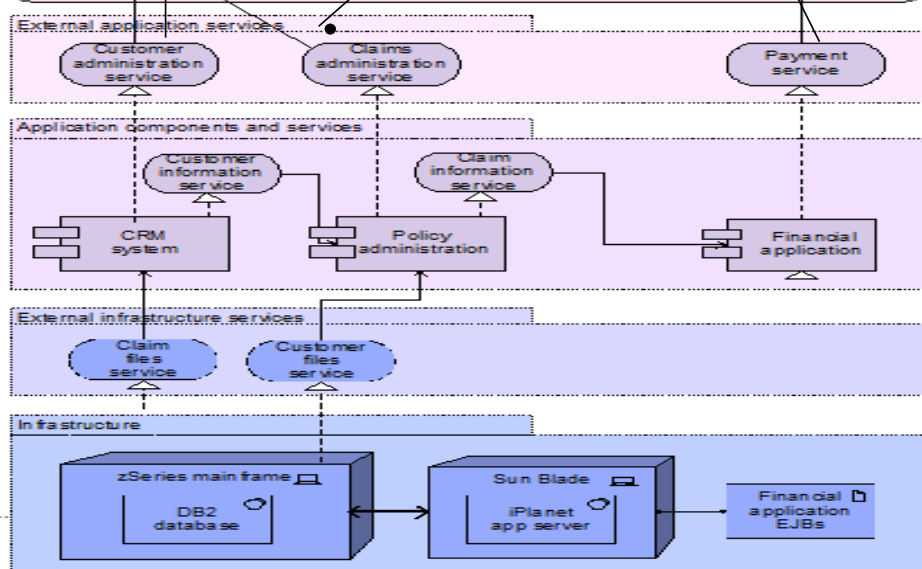
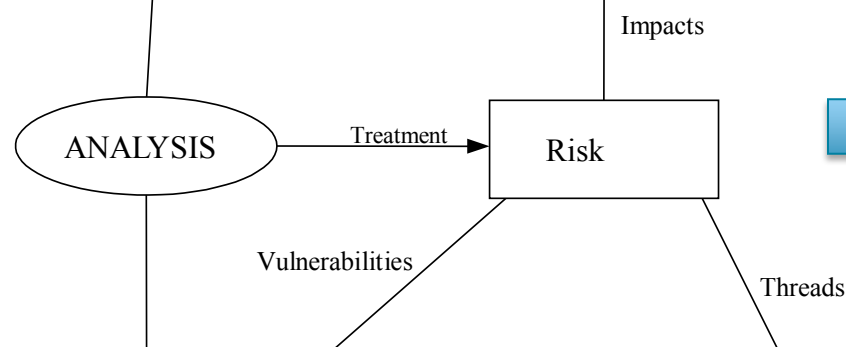
Information System



Process Name	Risk Assessment
Process Purpose	The purpose of the process is to assess risks faced by the assets which are in the scope of the identified business
Process Expected Results	As a result of successful implementation of the Risk Assessment process: 1. Criteria for accepting risks are developed; 2. Criteria for accepting risks are approved by the management; 3. Assets and their owners are identified. 4. Risks are identified in terms of vulnerabilities and threads 5. Identified risks are analyzed and evaluated in terms of their impact
Base Practices	RA.BP1: Context and Assets Identification Identification of the perimeter of the company for which the security risk assessment will apply. Identification of the primary business assets and of the supporting resources (secondary assets) RA.BP2: Determination of security criteria Identification of security criteria (like confidentiality, availability and integrity) applicable to the protection of business assets RA.BP3: Risk analysis and assessment Identification of each risk component (thread, vulnerability and impact). Qualitative/quantitative ranking of risks

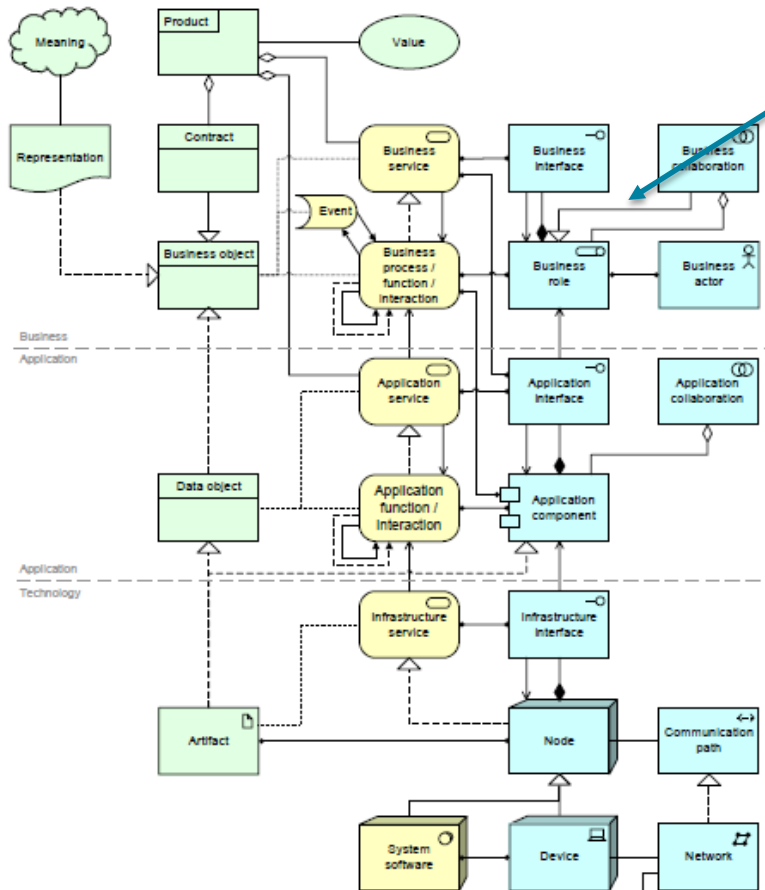
Output Work Product		
ID	Name	Expected results and related BPs
06_02	List of assets	[RA.BP1]
05_06	List of security criteria	[RA.BP 2]
06_06	Ranked list of risks	[RA.BP 3], [3]

Indicators Level 2.2
 The contents and structure of the work products are defined. They are standardized at the level of 1 between work products are identified and understood. of changes to workproducts is supported

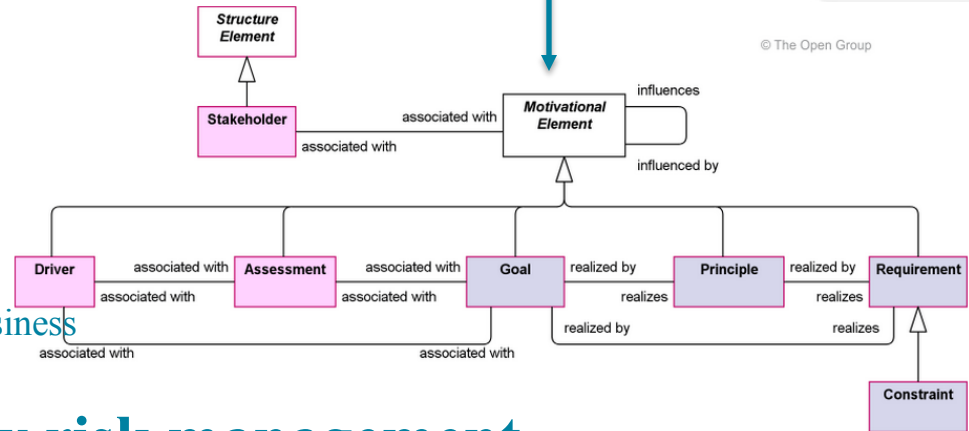
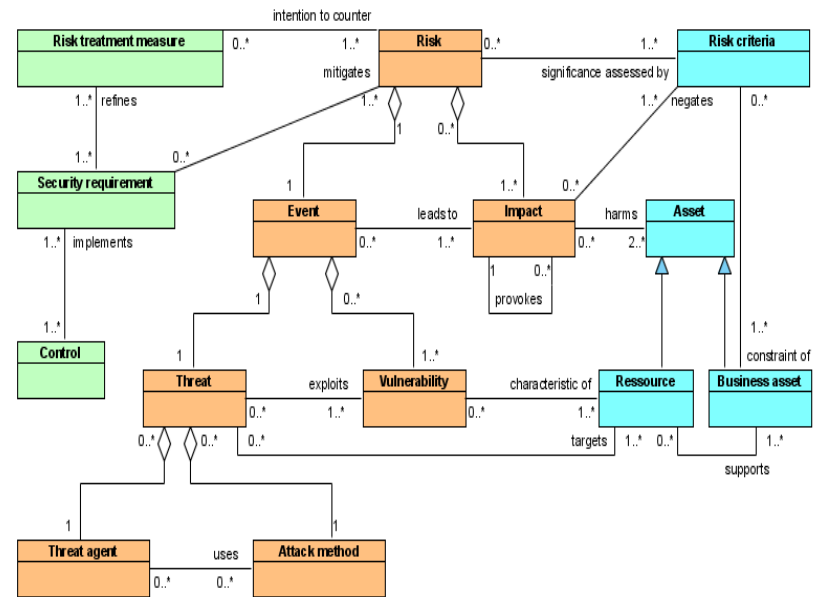


Conceptual Model for security risk management

ArchiMate meta-model integration reported in [8]



ArchiMate Meta-model 2.0 including the Business Motivation Model

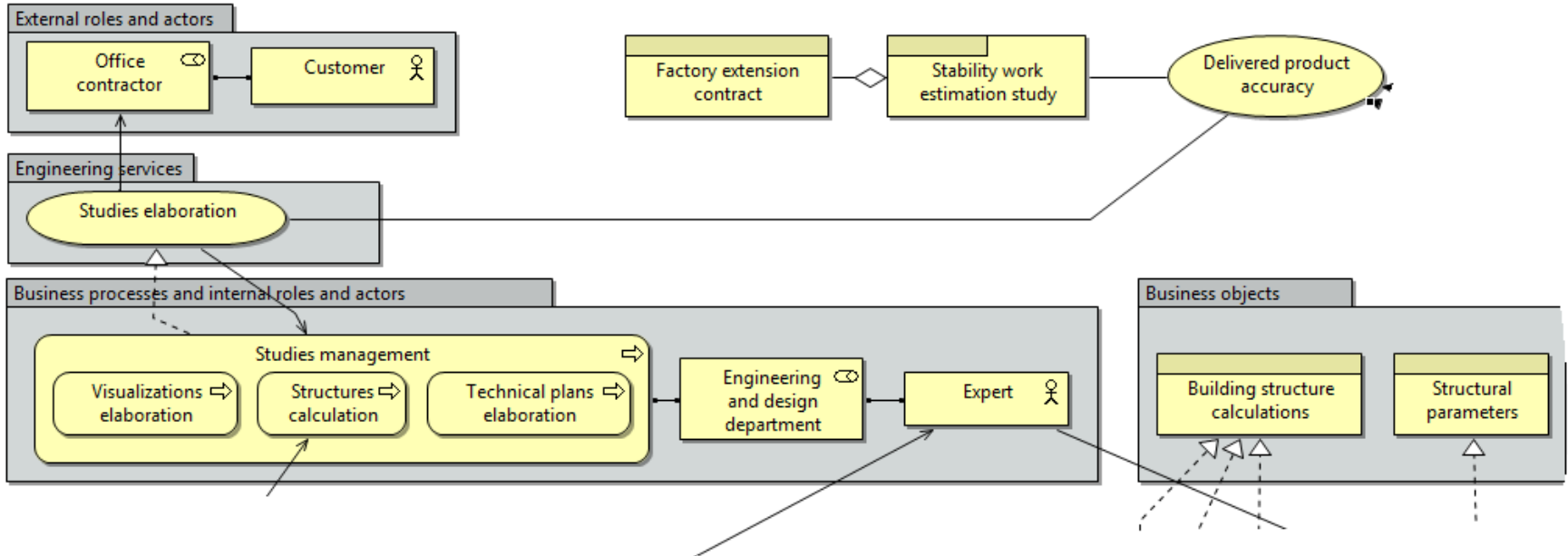


© The Open Group

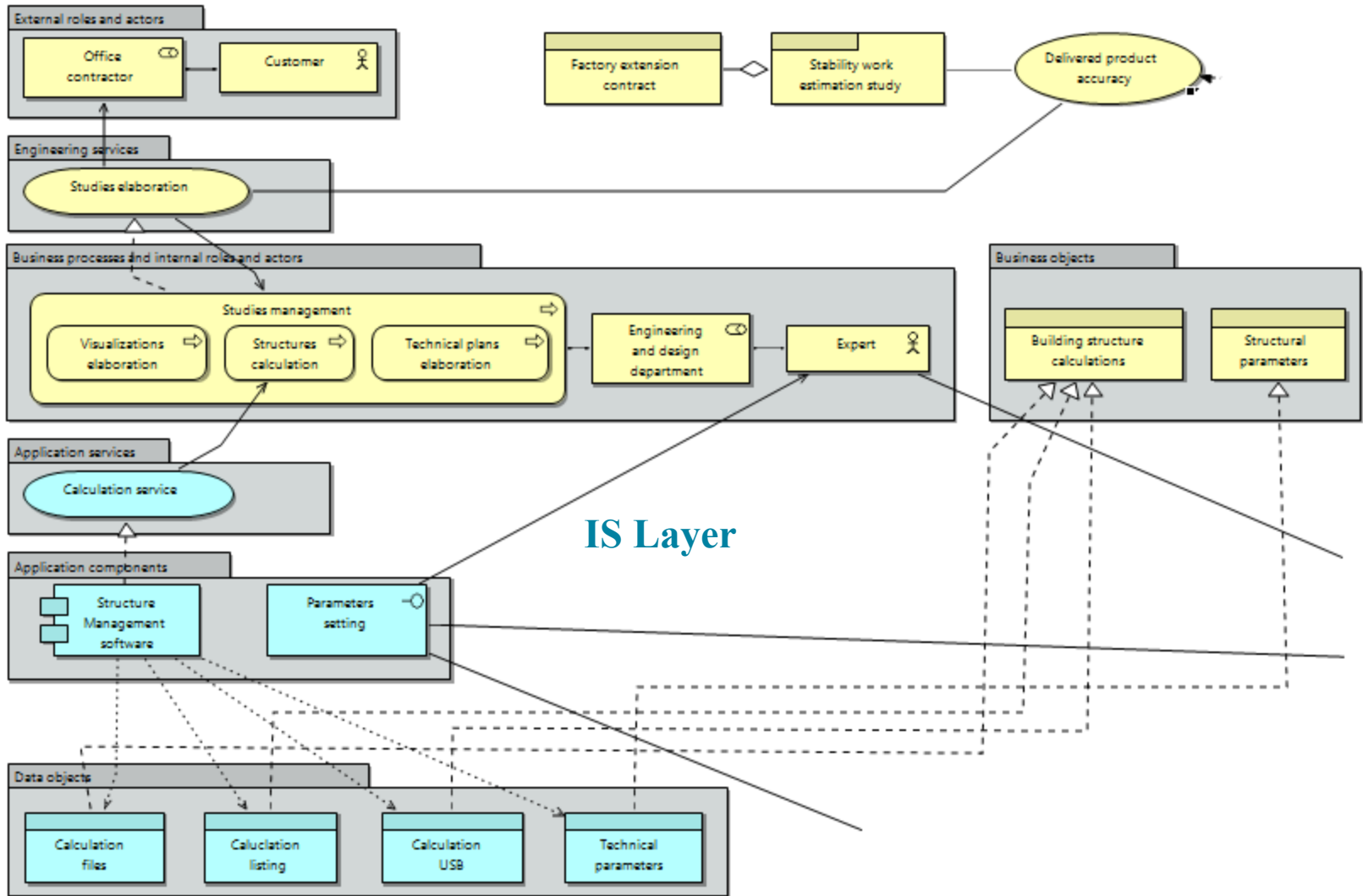
a ArchiMate profile for security risk management (contribution to the Open Group RfP)

Copyright Tudor Center - Eric Dubois

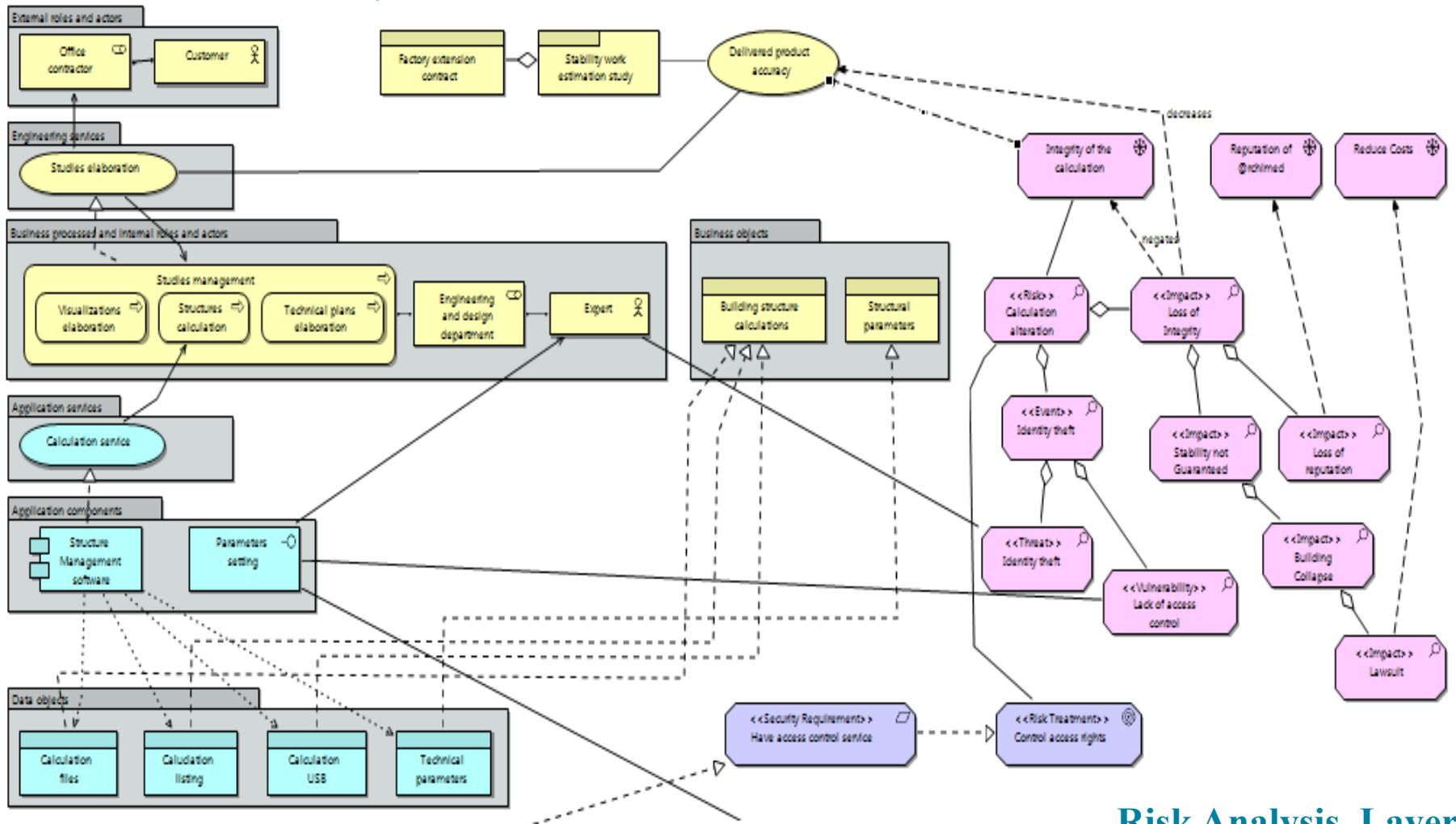
Business Layer



Business Layer



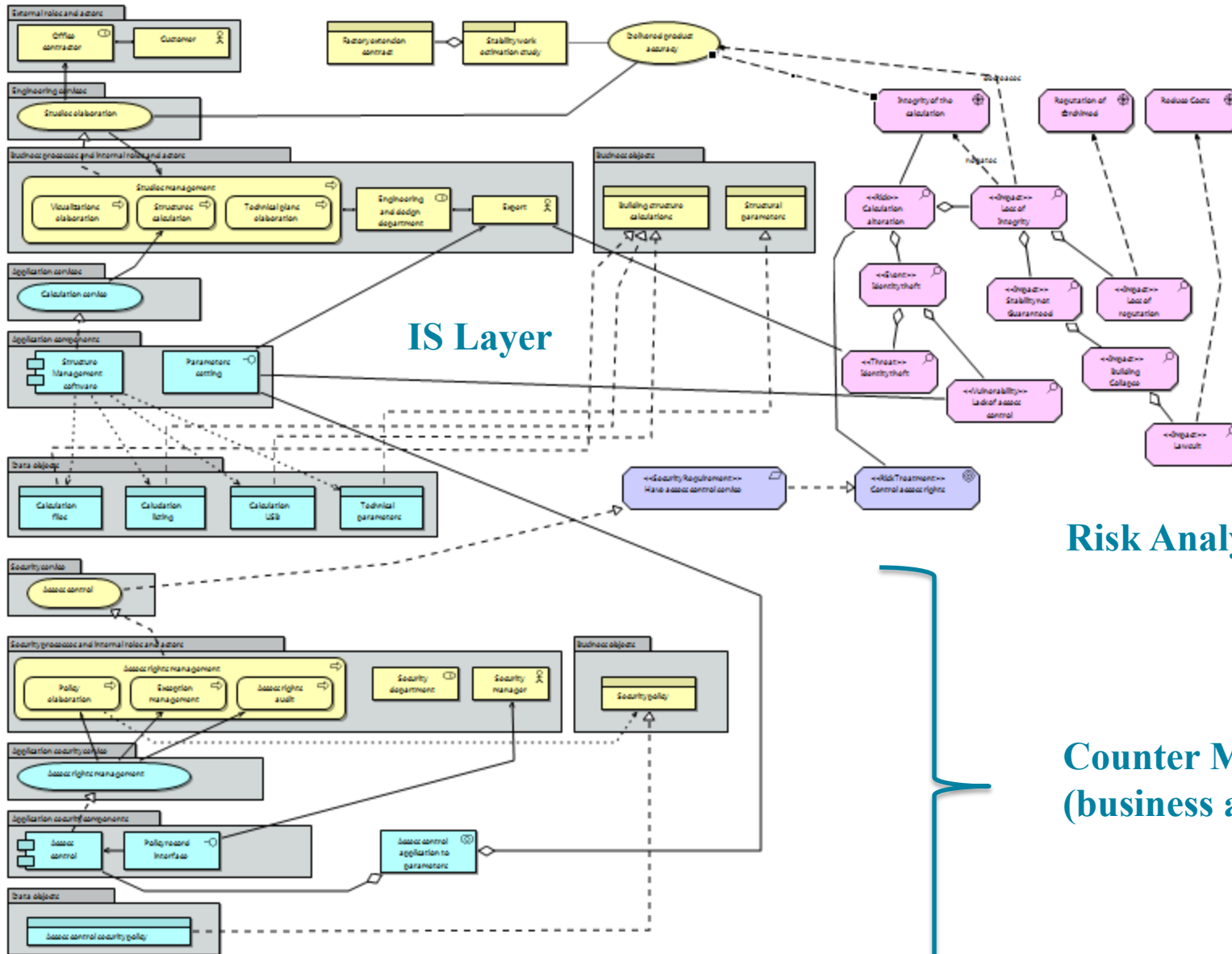
Business Layer



IS Layer

Risk Analysis Layer

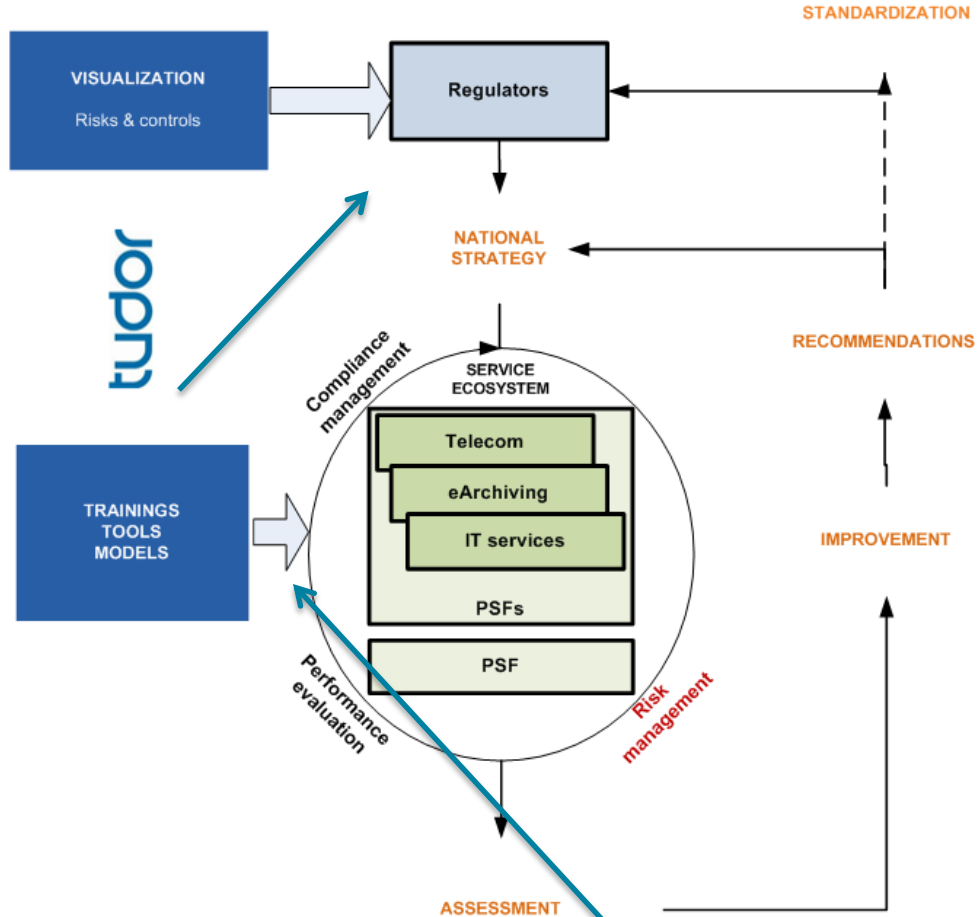
Business Layer



Risk Analysis Layer

Counter Measure (business and IS layers)

Conclusion



innofinance[®]
 an initiative of CRP Henri Tudor

A PPP devoted to the development of REFERENCE MODELS for the finance service supply chain helping in managing compliance, confidence and trust issues and of their deployment through PROCESS ASSURANCE MODELS and ENTERPRISE ENGINEERING

Transfer and Dissemination of Results

- Regulations
- Laws
- Standards
- Norms
- Best Practices

- ...



UNSTRUCTURED
REQUIREMENTS

**Process Reference and
Assessment Model**



Transfer and Dissemination of Results



•Co-editor of ISO 20000/4



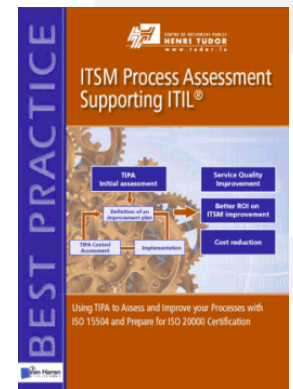
JTC1 / SC7

Software & System Engineering

•Training provided by IT Preneurs

- Approx. 170 TIPA certified Assessors
- 24 countries: Japan, USA, Canada, Denmark, Australia ..

UNSTRUCTURED
REQUIREMENTS



**TIPA® - Tudor ITSM Process
Assessment**
www.tipaonline.org



References

- [1] Eric Dubois, Anne Rousseau, “Service Science: A Service System Design Science Research Method? “ , Exploring Services Science - 4th International Conference, IESS 2013, Porto, Portugal, February 7-8, 2013. Proceedings. Springer Lecture Notes in Business Information Processing, 2013
- [2] Béatrix Barafort, [Anne Rousseau](#): Sustainable Service Innovation Model: A Standardized IT Service Management Process Assessment Framework. [EuroSPI 2009](#): 69-80
- [3] [Michel Picard](#), Alain Renault, [Stéphane Cortina](#): How to Improve Process Models for Better ISO/IEC 15504 Process Assessment. [EuroSPI 2010](#): 130-141
- [4] André Rifaut, [Eric Dubois](#): Using Goal-Oriented Requirements Engineering for Improving the Quality of ISO/IEC 15504 based Compliance Assessment Frameworks. [RE 2008](#): 33-42
- [5] [Olivier Mangin](#), Béatrix Barafort, [Patrick Heymans](#), [Eric Dubois](#): Designing a Process Reference Model for Information Security Management Systems. [SPICE 2012](#): 129-140
- [6] André Rifaut, [Sepideh Ghanavati](#): Measurement-oriented comparison of multiple regulations with GRL. [RELAW 2012](#): 7-16
- [7] Sepideh Ghanavati, Daniel Amyot, André Rifaut, and Eric Dubois, Goal-Oriented Compliance with Multiple Regulations, RE 2014,, to appear
- [8] Eric Grandry, [Christophe Feltus](#), [Eric Dubois](#): Conceptual Integration of Enterprise Architecture Management and Security Risk Management. [EDOC Workshops 2013](#): 114-123
- [9] [Nicolas Mayer](#), [Jocelyn Aubert](#), [Hervé Cholez](#), Eric Grandry: Sector-Based Improvement of the Information Security Risk Management Process in the Context of Telecommunications Regulation. [EuroSPI 2013](#): 13-24

Thanks for your attention

Livrables

