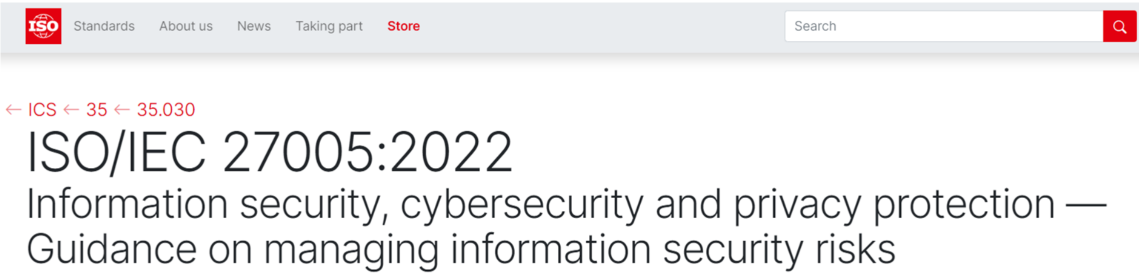
# EA and Risk Management

# EA supporting asset identification

Information security risk management

# Need to describe the assets

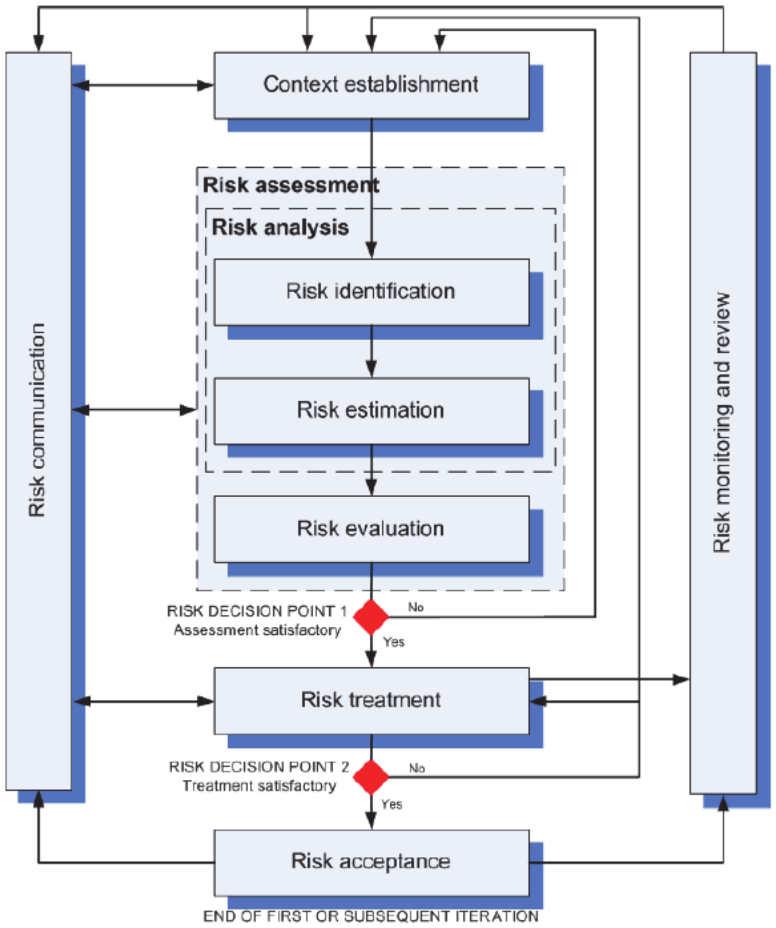


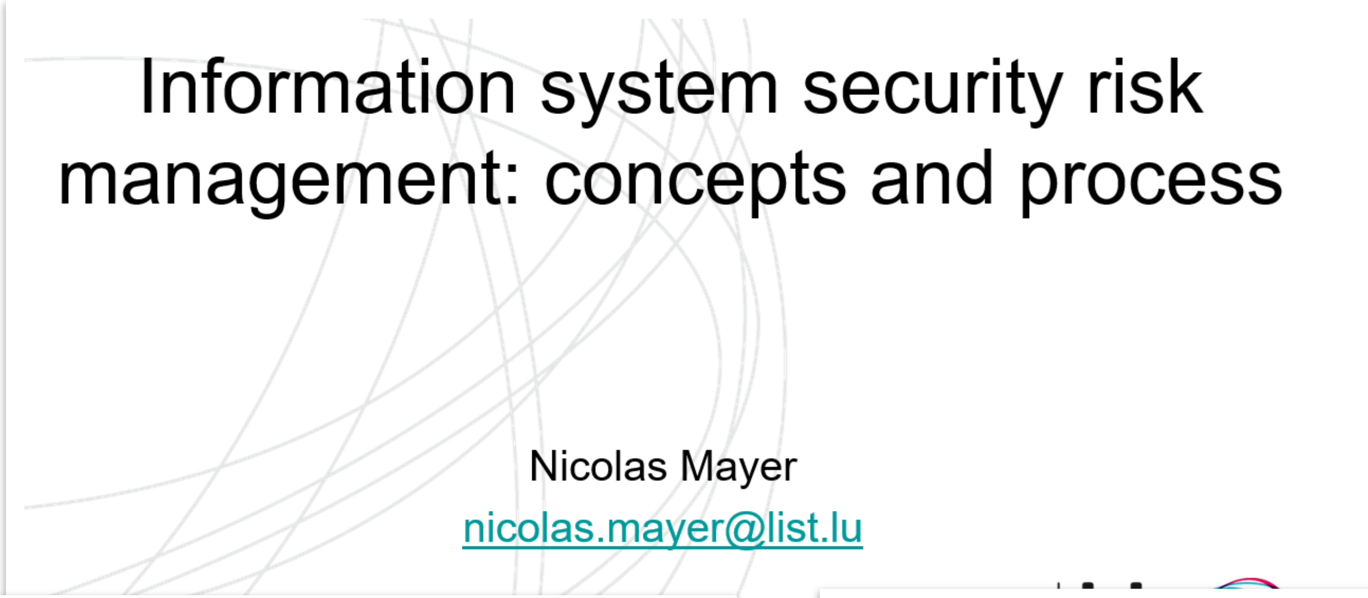
← ICS ← 35 ← 35.030

ISO/IEC 27005:2022

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

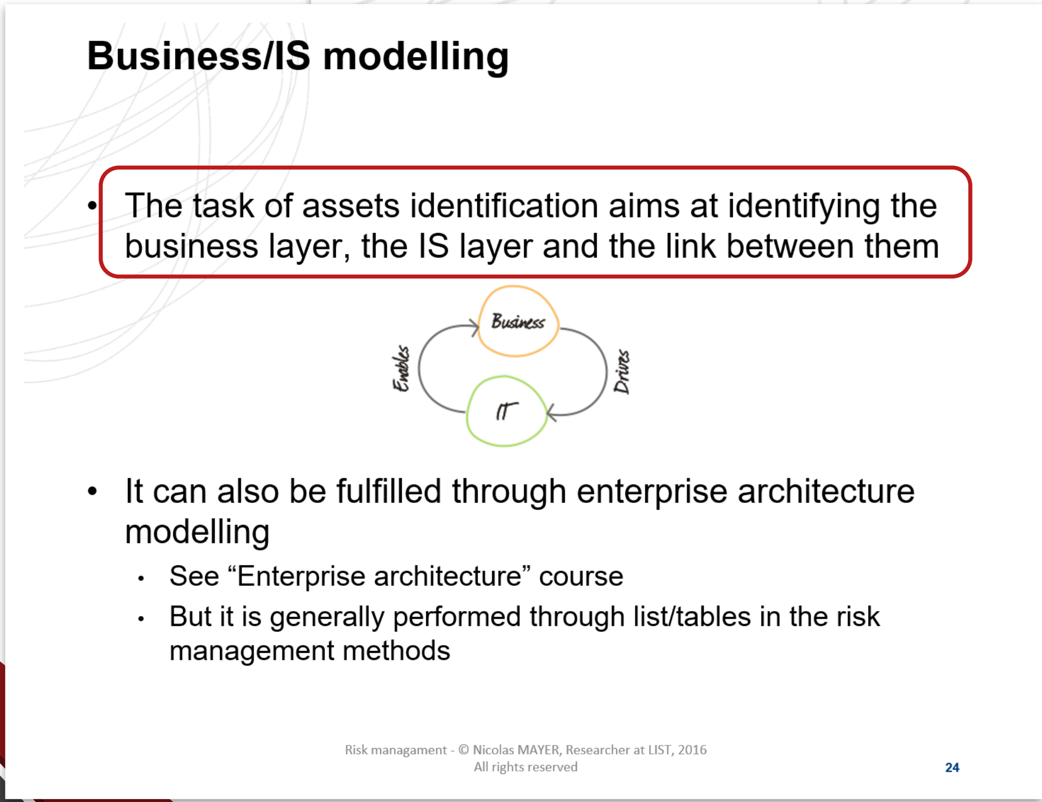
- Context establishment
  - Define the scope of the analysis
- Risk assessment
  - Identify the assets
  - Identify the impacts on business
- Risk treatment
  - Define the controls





# Information system security risk management: concepts and process

Nicolas Mayer
nicolas.mayer@list.lu

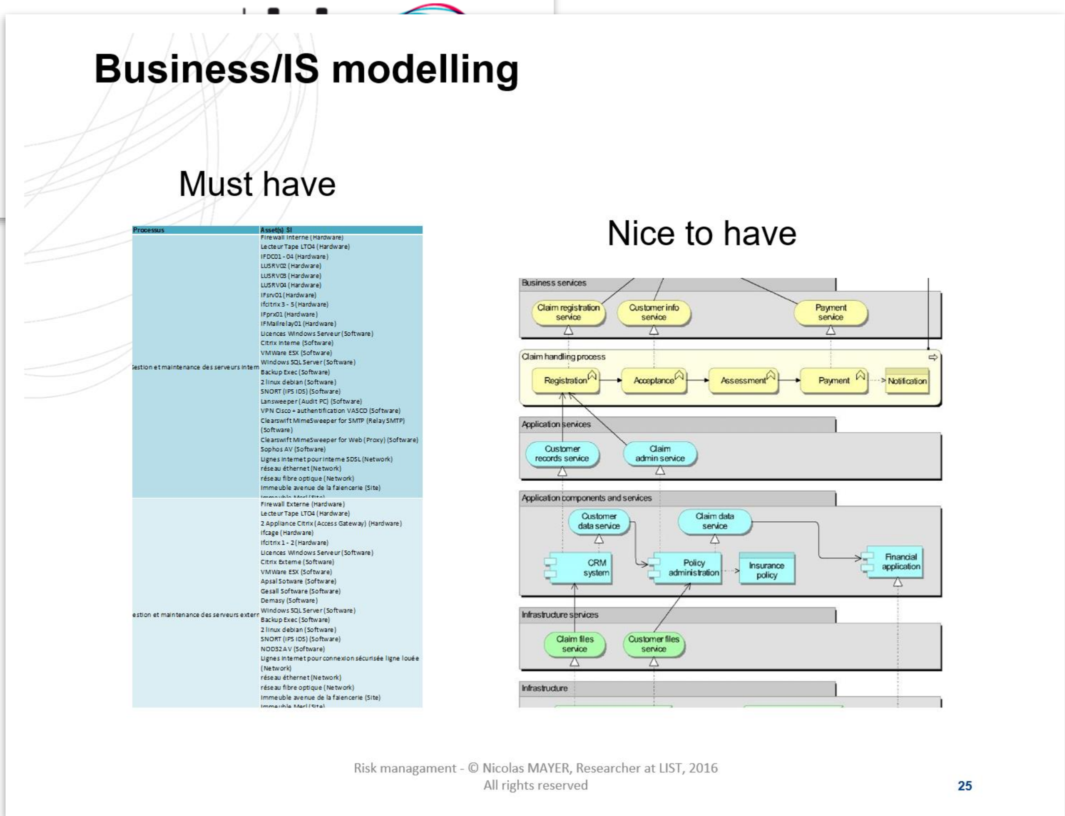


## Business/IS modelling

- The task of assets identification aims at identifying the business layer, the IS layer and the link between them

Business
Enables
Drives
IT

- It can also be fulfilled through enterprise architecture modelling
  - See "Enterprise architecture" course
  - But it is generally performed through list/tables in the risk management methods



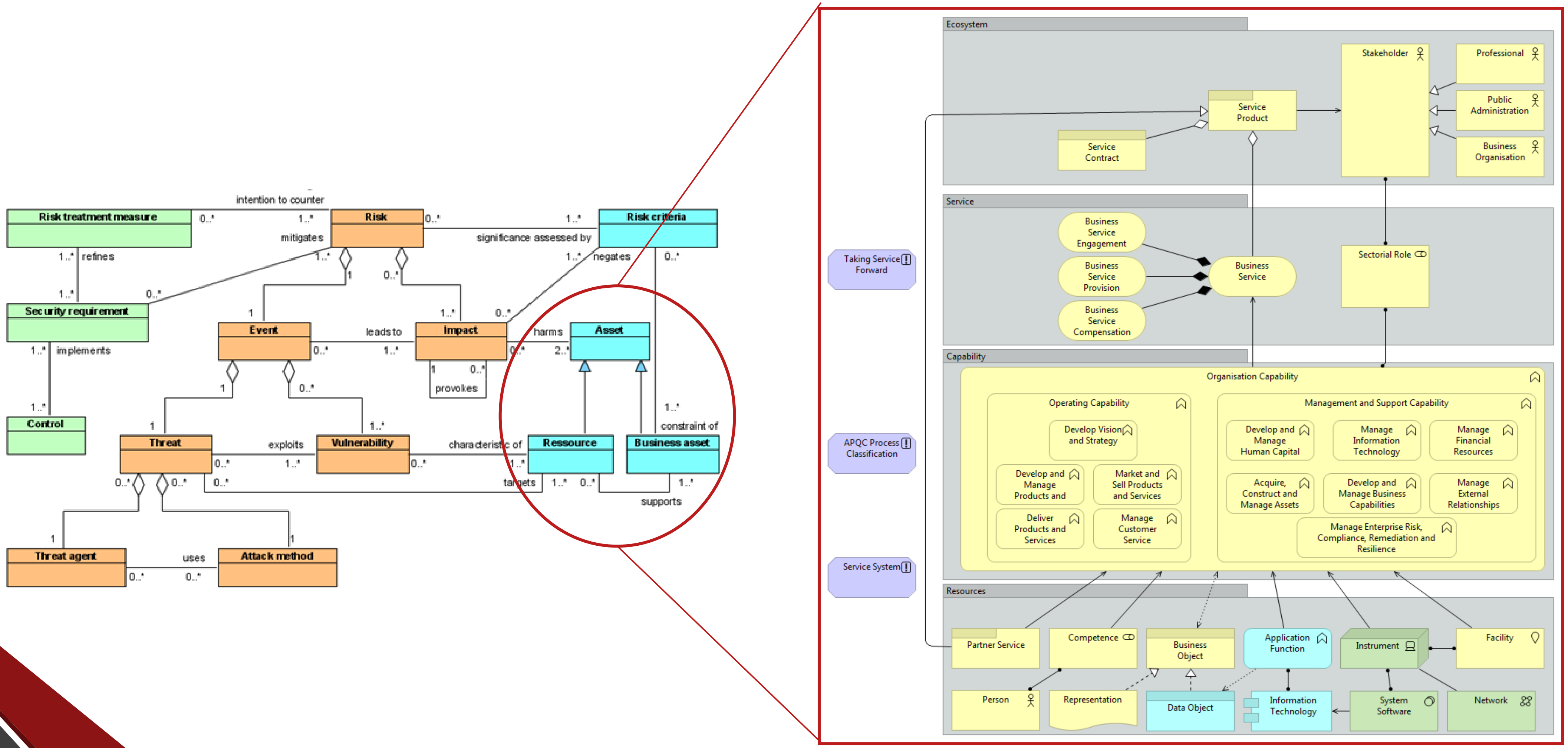
## Business/IS modelling

Must have

| Processus | Asset(s) SI |
|---|---|
| Gestion et maintenance des serveurs intern | Firewall Interne (Hardware)<br>Lecteur Tape LTO4 (Hardware)<br>IFDC01 - 04 (Hardware)<br>LUSRV02 (Hardware)<br>LUSRV03 (Hardware)<br>LUSRV04 (Hardware)<br>IFsrv01 (Hardware)<br>Ifcitrix 3 - 5 (Hardware)<br>IFprx01 (Hardware)<br>IFMailrelay01 (Hardware)<br>Licences Windows Serveur (Software)<br>Citrix Interne (Software)<br>VMWare ESX (Software)<br>Windows SQL Server (Software)<br>Backup Exec (Software)<br>2 linux debian (Software)<br>SNORT (IPS IDS) (Software)<br>Lansweeper (Audit PC) (Software)<br>VPN Cisco + authentification VASCO (Software)<br>Clearswift MimeSweeper for SMTP (Relay SMTP) (Software)<br>Clearswift MimeSweeper for Web (Proxy) (Software)<br>Sophos AV (Software)<br>Lignes internet pour interne SDSL (Network)<br>réseau éthernet (Network)<br>réseau fibre optique (Network)<br>Immeuble avenue de la faiencerie (Site)<br>Immeuble Merl (Site) |
| estion et maintenance des serveurs extern | Firewall Externe (Hardware)<br>Lecteur Tape LTO4 (Hardware)<br>2 Appliance Citrix (Access Gateway) (Hardware)<br>Ifcage (Hardware)<br>Ifcitrix 1 - 2 (Hardware)<br>Licences Windows Serveur (Software)<br>Citrix Externe (Software)<br>VMWare ESX (Software)<br>Apsal Sotware (Software)<br>Gesall Software (Software)<br>Demasy (Software)<br>Windows SQL Server (Software)<br>Backup Exec (Software)<br>2 linux debian (Software)<br>SNORT (IPS IDS) (Software)<br>NOD32 AV (Software)<br>Lignes internet pour connexion sécurisée ligne louée (Network)<br>réseau éthernet (Network)<br>réseau fibre optique (Network)<br>Immeuble avenue de la faiencerie (Site)<br>Immeuble Merl (Site) |

Nice to have

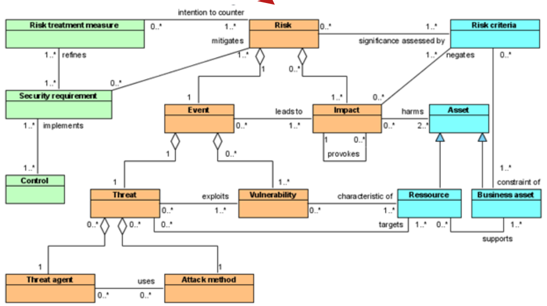
# ISSRM Assets and EA

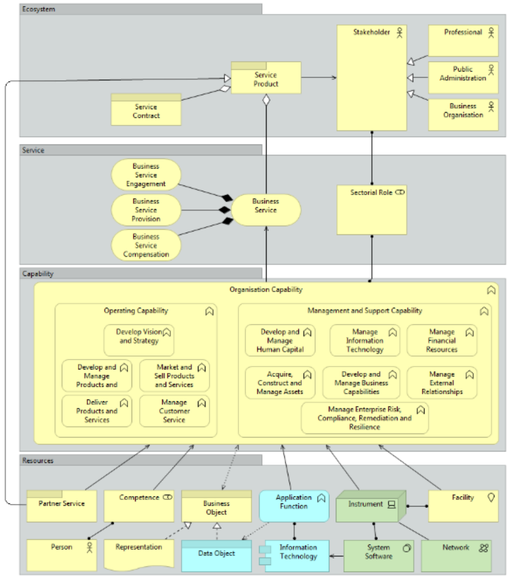


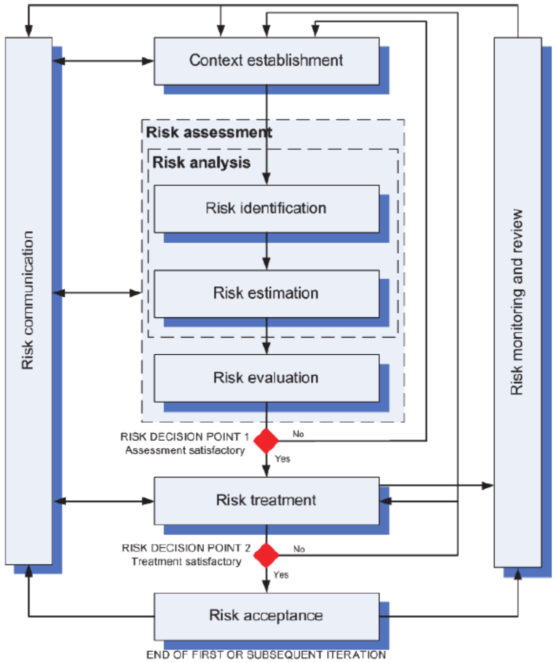
# 1. Context establishment

a. Scoping by modelling business boundaries

b. Define risk criterias



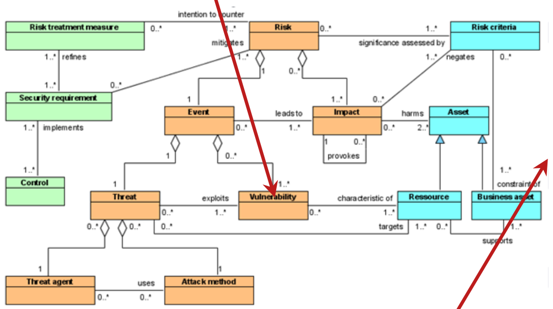

Ecosystem
Stakeholder
Professional
Service Product
Public Administration
Service Contract
Business Organisation
Service
Business Service Engagement
Business Service Provision
Business Service
Sectorial Role
Business Service Compensation
Capability
Organisation Capability
Operating Capability
Management and Support Capability
Develop Vision and Strategy
Develop and Manage Human Capital
Manage Information Technology
Manage Financial Resources
Develop and Manage Products and
Market and Sell Products and Services
Acquire, Construct and Manage Assets
Develop and Manage Business Capabilities
Manage External Relationships
Deliver Products and Services
Manage Customer Service
Manage Enterprise Risk, Compliance, Remediation and Resilience
Resources
Partner Service
Competence
Business Object
Application Function
Instrument
Facility
Person
Representation
Data Object
Information Technology
System Software
Network

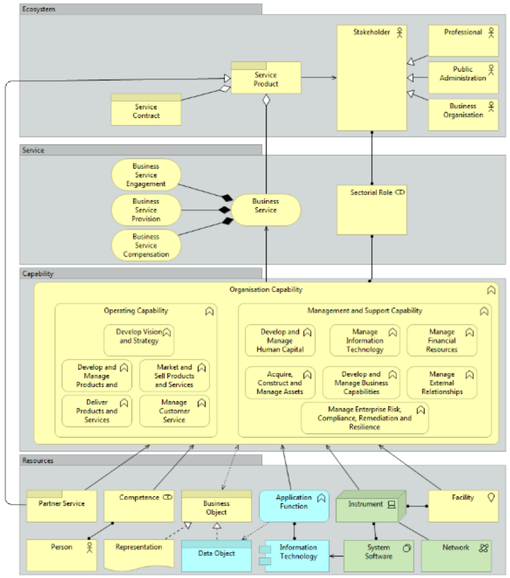


# 2. Risk Assessment

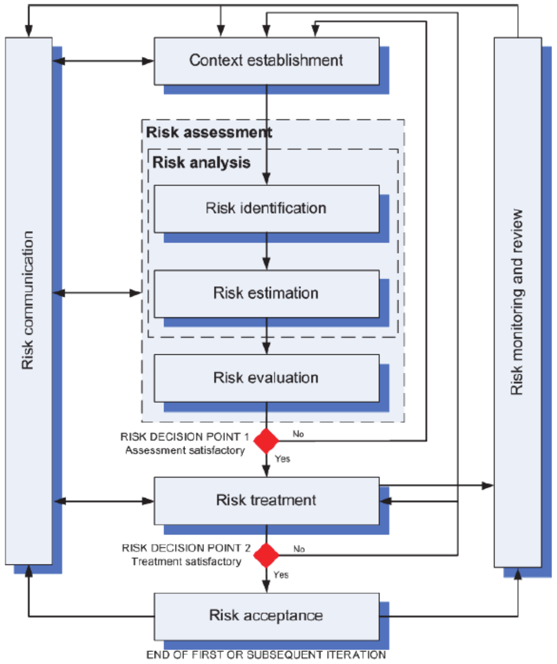
a. Assets modelling (business and IS)

b. Identify threats and vulnerabilities





Ecosystem
Stakeholder
Professional
Service Product
Public Administration
Service Contract
Business Organisation
Service
Business Service Engagement
Business Service Provision
Business Service
Sectorial Role
Business Service Compensation
Capability
Organisation Capability
Operating Capability
Management and Support Capability
Develop Vision and Strategy
Develop and Manage Human Capital
Manage Information Technology
Manage Financial Resources
Develop and Manage Products and
Market and Sell Products and Services
Acquire, Construct and Manage Assets
Develop and Manage Business Capabilities
Manage External Relationships
Deliver Products and Services
Manage Customer Service
Manage Enterprise Risk, Compliance, Remediation and Resilience
Resources
Partner Service
Competence
Business Object
Application Function
Instrument
Facility
Person
Representation
Data Object
Information Technology
System Software
Network

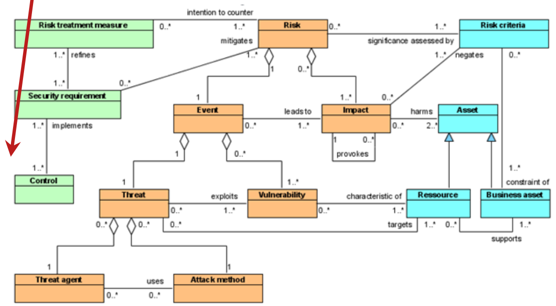


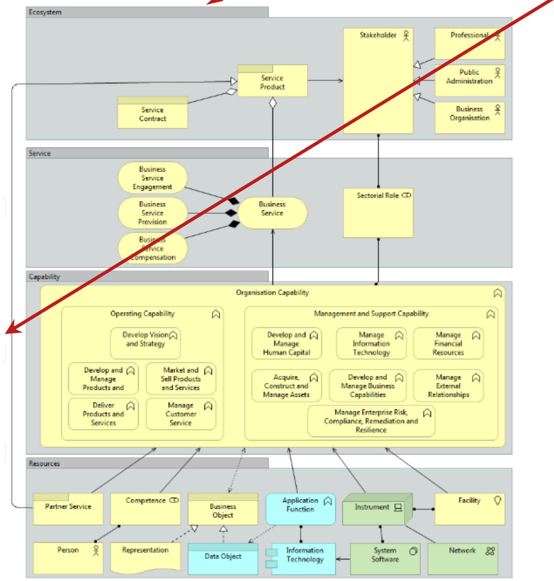
c. Estimate impact on business

# 3. Risk Treatment

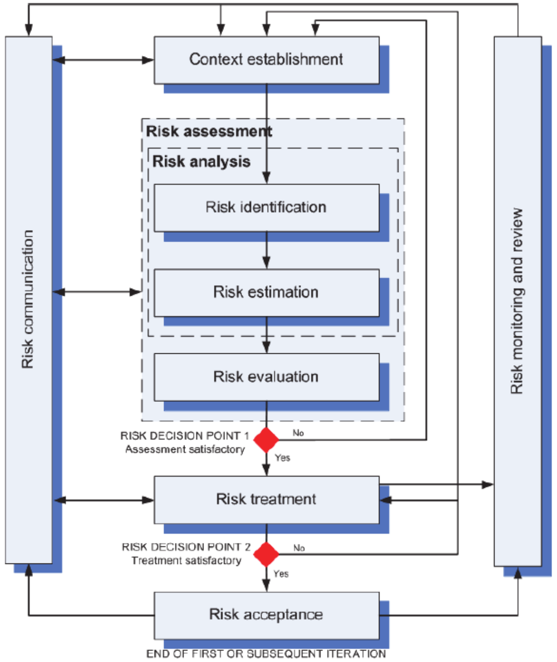
a. Specify controls

c. Compute residual risk





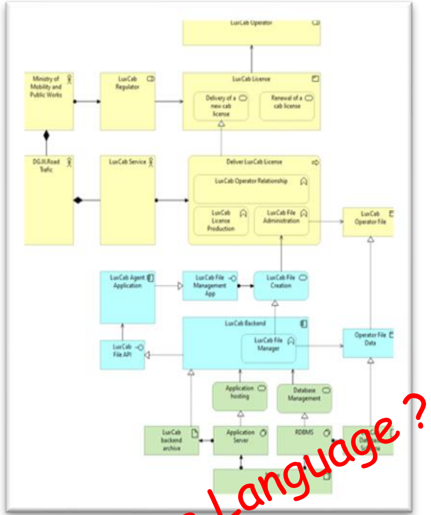
Ecosystem
Stakeholder
Professional
Service Product
Public Administration
Service Contract
Business Organisation
Service
Business Service Engagement
Business Service Provision
Business Service
Sectorial Role
Business Service Compensation
Capability
Organisation Capability
Operating Capability
Management and Support Capability
Develop Vision and Strategy
Develop and Manage Human Capital
Manage Information Technology
Manage Financial Resources
Develop and Manage Products and
Market and Sell Products and Services
Acquire, Construct and Manage Assets
Develop and Manage Business Capabilities
Manage External Relationships
Deliver Products and Services
Manage Customer Service
Manage Enterprise Risk, Compliance, Remediation and Resilience
Resources
Partner Service
Competence
Business Object
Application Function
Instrument
Facility
Person
Representation
Data Object
Information Technology
System Software
Network



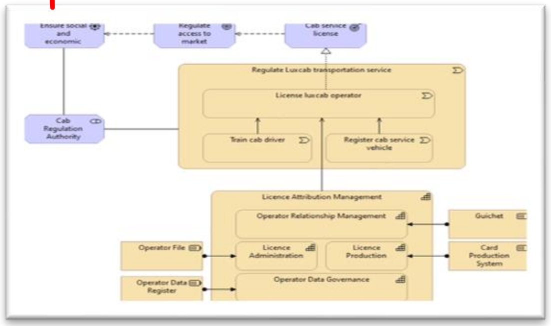
b. Estimate new vulnerability level

# 4. Risk Communication

- Addressing business stakeholders
  - Business services and processes
- Addressing technical stakeholders
  - Application components and nodes
- Addressing C-Level stakeholders
  - Strategy, Capability and Resources



ArchiMate Language ?



# EA supporting Threat Analysis

Another way to identify risks

# Master Thesis 2025

Master in Information System Security Management (MISSM)
University of Luxembourg

Academic Year 2024-2025

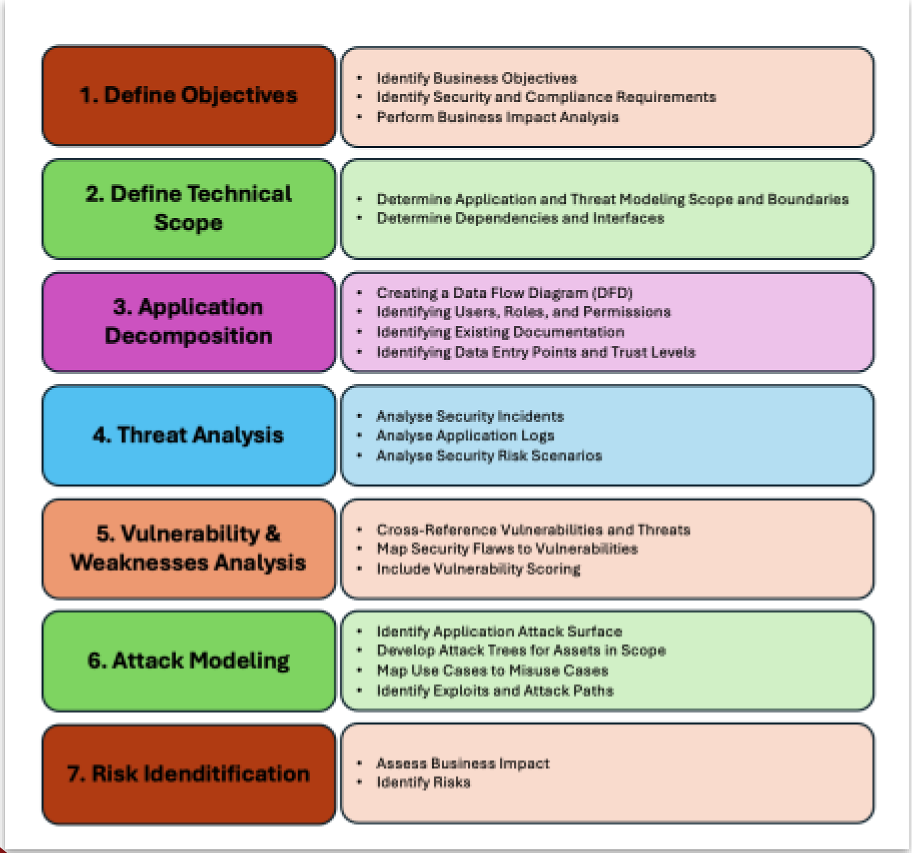
MASTER THESIS

COMBINING THREAT MODELLING AND ENTERPRISE ARCHITECTURE MANAGEMENT TO ASSIST IN INFORMATION SECURITY RISK IDENTIFICATION

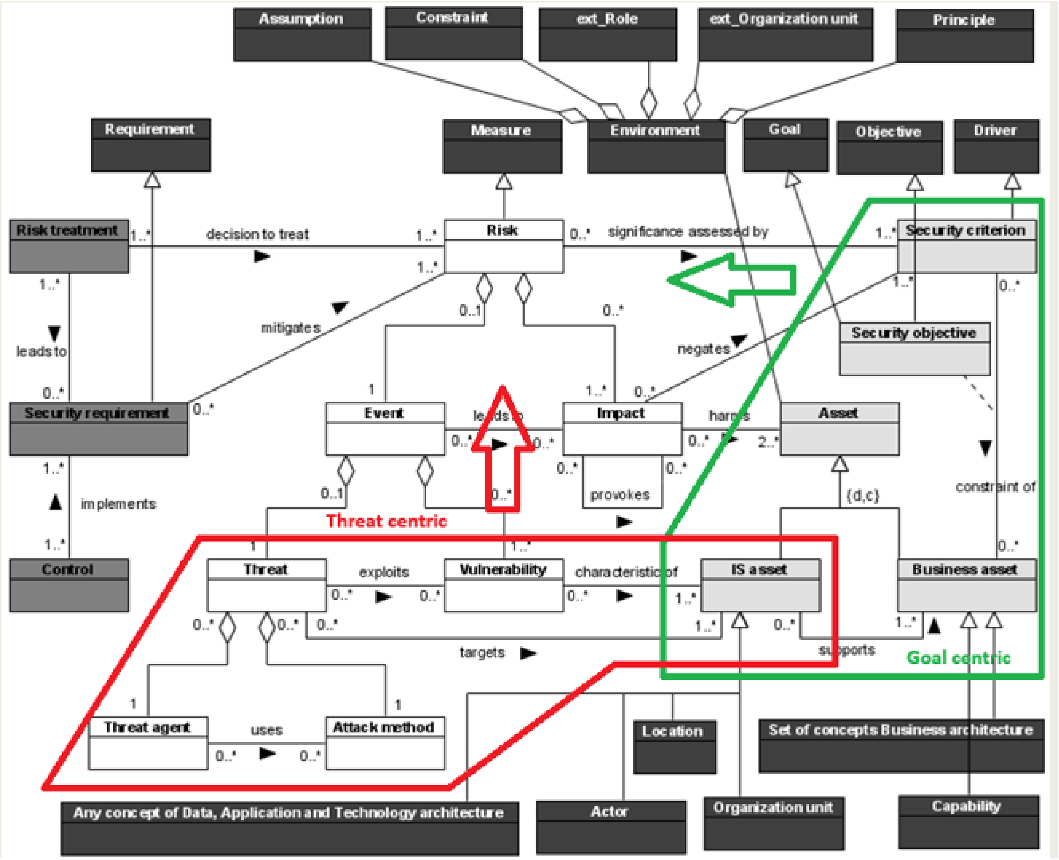
STUDENT: Mr. Geoffrey MARIËN (geoffrey.marien@gmail.com)
ACADEMIC SUPERVISOR: Mr. Eric Grandry

- Integration of Enterprise Architecture (EA) with Threat Modelling to address gaps in traditional information security risk management approaches
  - lack of an attacker-centric perspective
  - weakness in addressing contemporary threats effectively
- Combining the structured, layered approach of EA with the analytical power of Threat Modelling
  - method to identify, analyse, and link security risks directly to enterprise systems and processes

# PASTA* and ISSRM

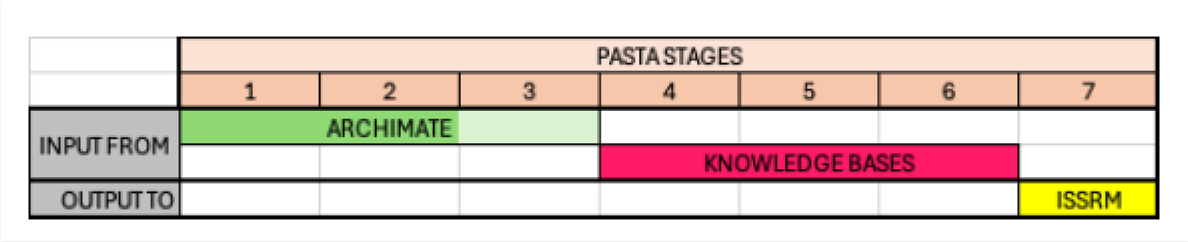


| | |
|---|---|
| 1. Define Objectives | • Identify Business Objectives<br>• Identify Security and Compliance Requirements<br>• Perform Business Impact Analysis |
| 2. Define Technical Scope | • Determine Application and Threat Modeling Scope and Boundaries<br>• Determine Dependencies and Interfaces |
| 3. Application Decomposition | • Creating a Data Flow Diagram (DFD)<br>• Identifying Users, Roles, and Permissions<br>• Identifying Existing Documentation<br>• Identifying Data Entry Points and Trust Levels |
| 4. Threat Analysis | • Analyse Security Incidents<br>• Analyse Application Logs<br>• Analyse Security Risk Scenarios |
| 5. Vulnerability & Weaknesses Analysis | • Cross-Reference Vulnerabilities and Threats<br>• Map Security Flaws to Vulnerabilities<br>• Include Vulnerability Scoring |
| 6. Attack Modeling | • Identify Application Attack Surface<br>• Develop Attack Trees for Assets in Scope<br>• Map Use Cases to Misuse Cases<br>• Identify Exploits and Attack Paths |
| 7. Risk Idenditification | • Assess Business Impact<br>• Identify Risks |



*Process for Attack Simulation and Threat Analysis – see https://threat-modeling.com/pasta-threat-modeling/

# PASTA and EA



| | PASTA STAGES | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| INPUT FROM | ARCHIMATE | | | | | | |
| | | | | KNOWLEDGE BASES | | | |
| OUTPUT TO | | | | | | | ISSRM |

- EA plays a central role in the initial stages, providing structured insights into business and technical requirements, even though the integration is expected to be limited at stage 3.
- Threat Knowledge bases are used to assess vulnerabilities and identify potential attack vectors in the middle stages.
- ISSRM is introduced to conduct risk and impact analysis, providing a formal risk management framework.

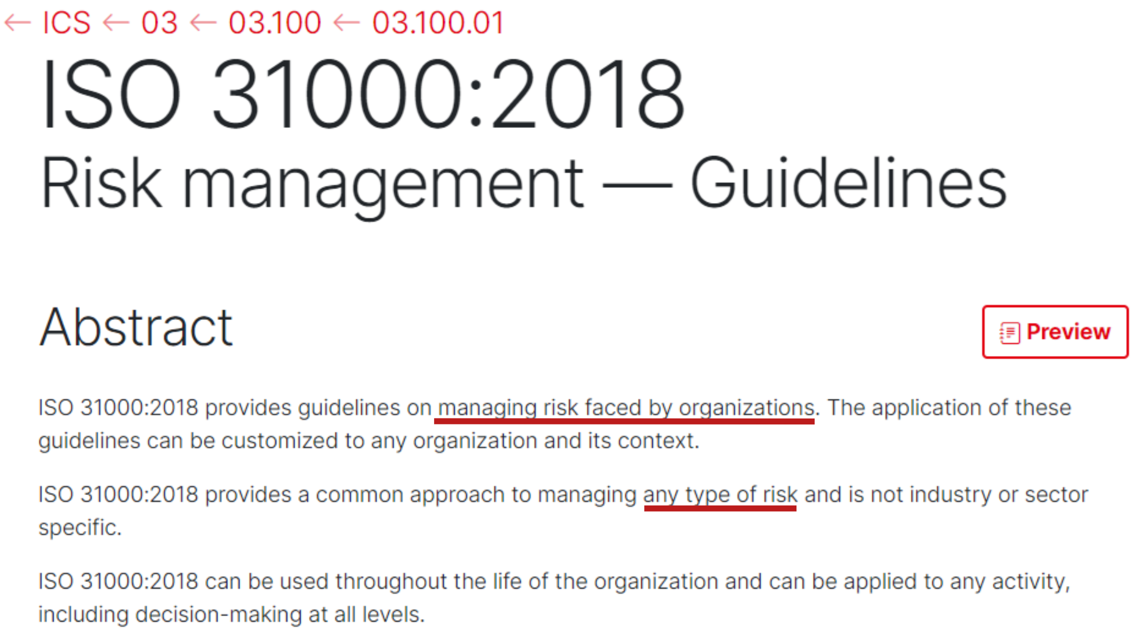
## Opportunities

- Specify ArchiMate required information to be captured in early stages will ease stages 4 to 6
- Automation is possible, integrating Archi with open source threat modelling tool
- Way to Secure-by-Design

# From ISRM to ERM

And the need to describe the enterprise

# From information security to enterprise risk



← ICS ← 03 ← 03.100 ← 03.100.01

## ISO 31000:2018

### Risk management — Guidelines

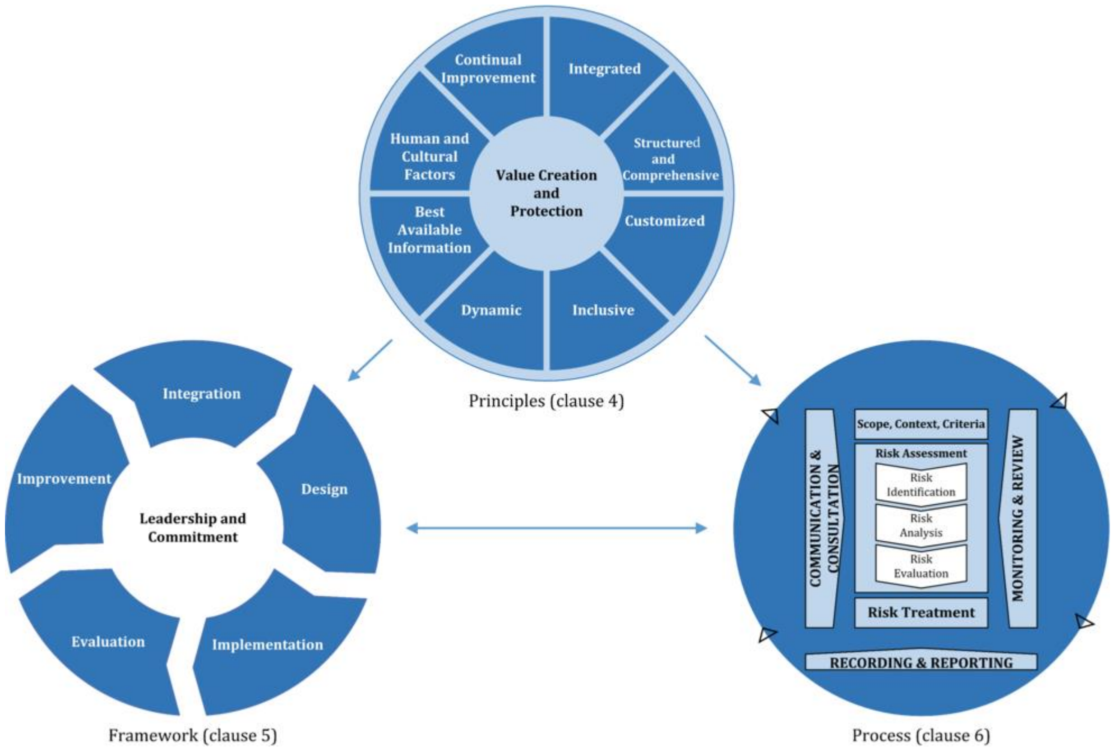
### Abstract

Preview

ISO 31000:2018 provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context.

ISO 31000:2018 provides a common approach to managing any type of risk and is not industry or sector specific.

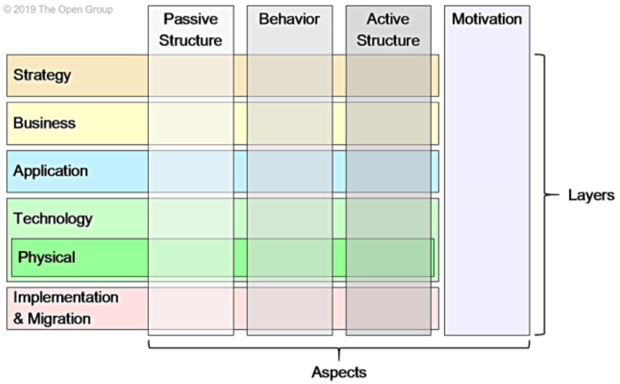
ISO 31000:2018 can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.

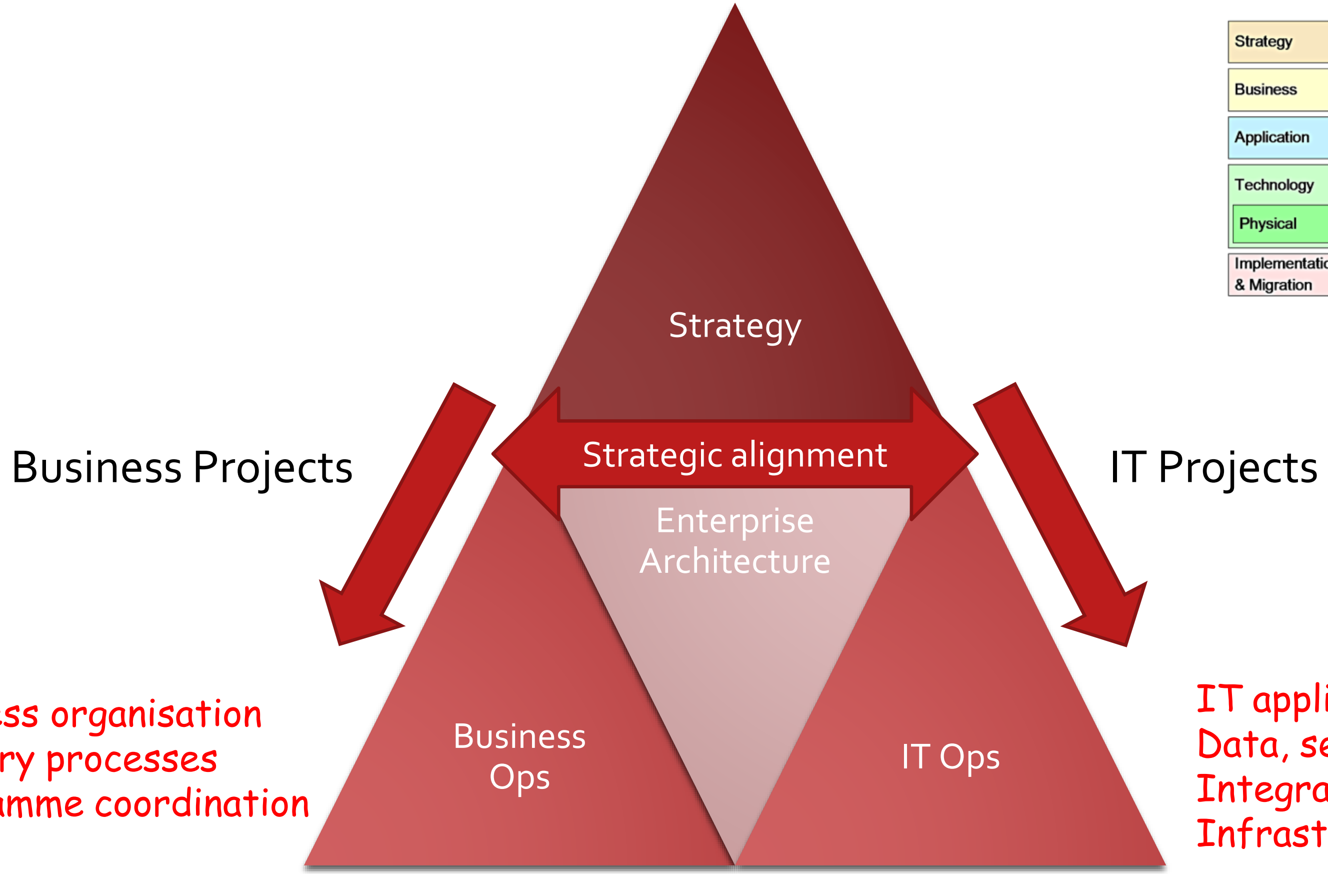


# Requirements on enterprise description

- Describe the assets of the enterprise
  - Business assets
  - IT Resources, and any other resource
- Establish the relation between IT and business
  - IT (and any resource) supports business
  - IT (and any resource) is vulnerable
- Understand the protection level of business
  - Security criteria
  - Any other criteria

# EA description ?





Business organisation
Delivery processes
Programme coordination

IT applications specs
Data, service specs
Integration requirements
Infrastructure

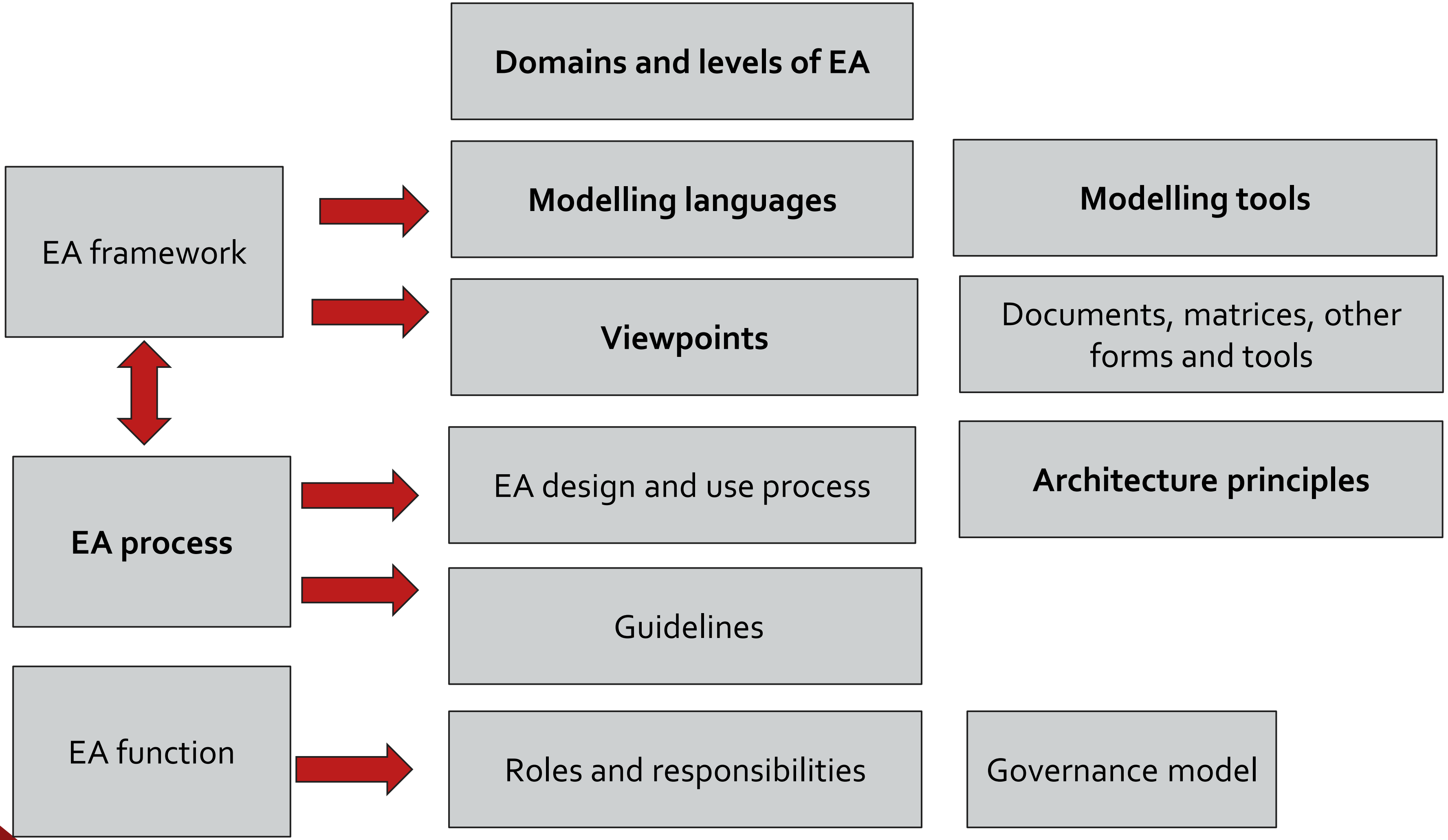
# Security-by-Design

and the role of EA

# Different roles of EA models/knowledge

- Descriptive
  - Represents EA as they are, using adequate frameworks/languages/models
  - Can be specific to an enterprise, general to a class of problems (e.g. reference architecture for industry/sector)
- Prescriptive/normative
  - **Rules, constraints, desired patterns/practices** for enterprise design (including IS assets and business assets) which essentially restricts the freedom of design choices available to individual projects
  - This allows to formalise and include in security-related best practices and enforce

# EA - Blueprint type of thinking about enterprise



Domains and levels of EA

EA framework

Modelling languages

Modelling tools

Viewpoints

Documents, matrices, other forms and tools

EA process

EA design and use process

Architecture principles

Guidelines

EA function

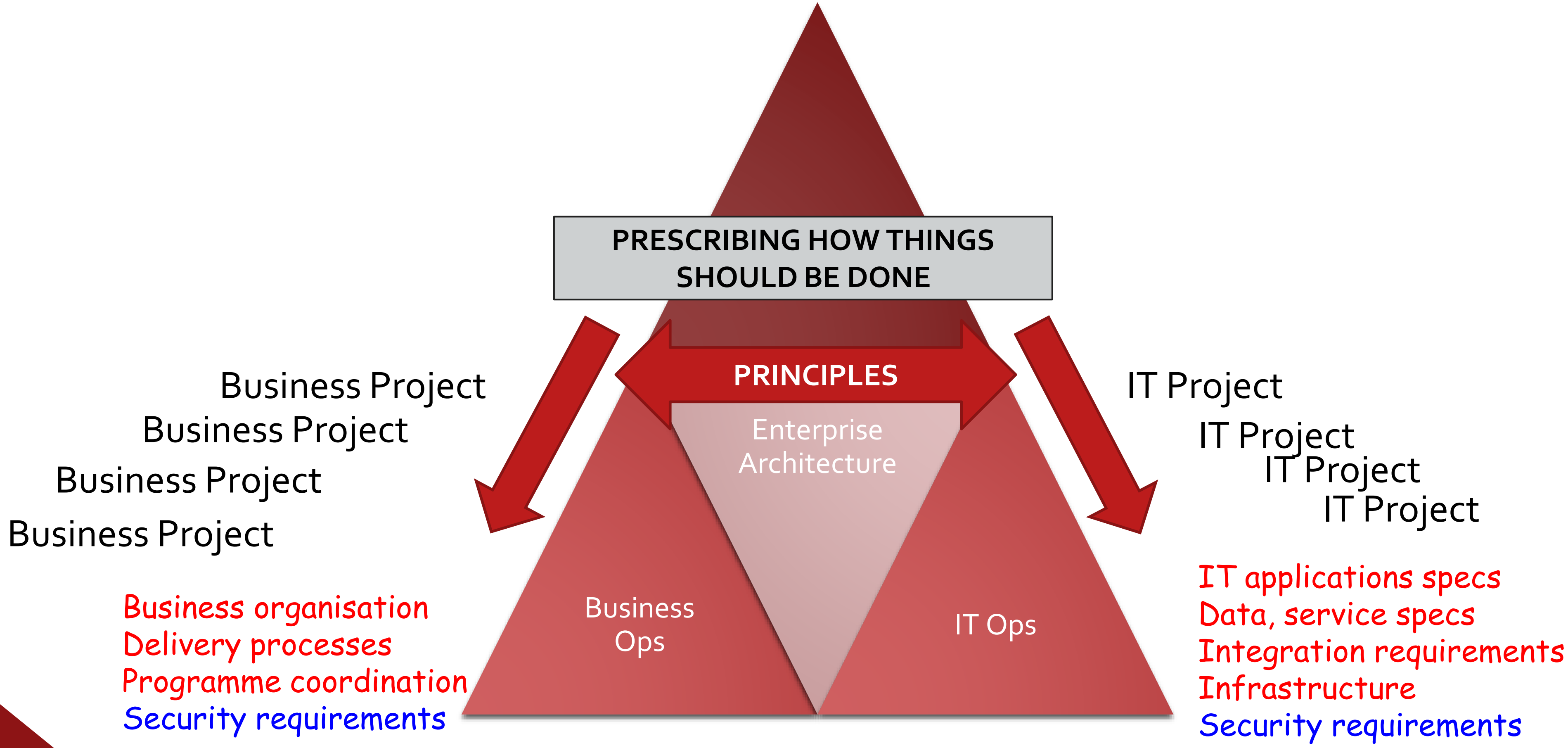
Roles and responsibilities

Governance model

# EA in a normative/prescriptive role

- Architectural knowledge can be formalised in terms of general rules and guidelines for design and evolution of EA (**architecture principles**)
- Architecture principles
  - Intended as enduring and seldom amended
  - Prescriptive/normative in nature
  - Clear, specific, measurable and achievable
  - Motivated by
    - Strategic objectives, values, **risks**, constraints, etc.
    - Bridge from strategy to design

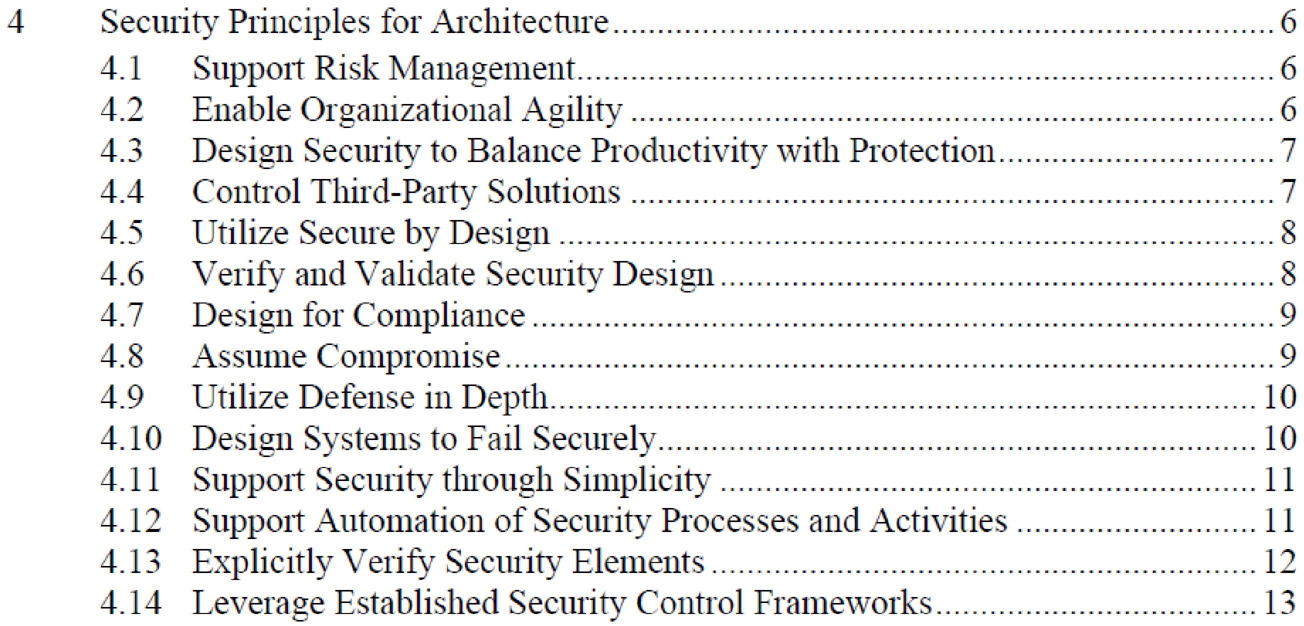
# EA in a normative/prescriptive role



Business organisation
Delivery processes
Programme coordination
Security requirements

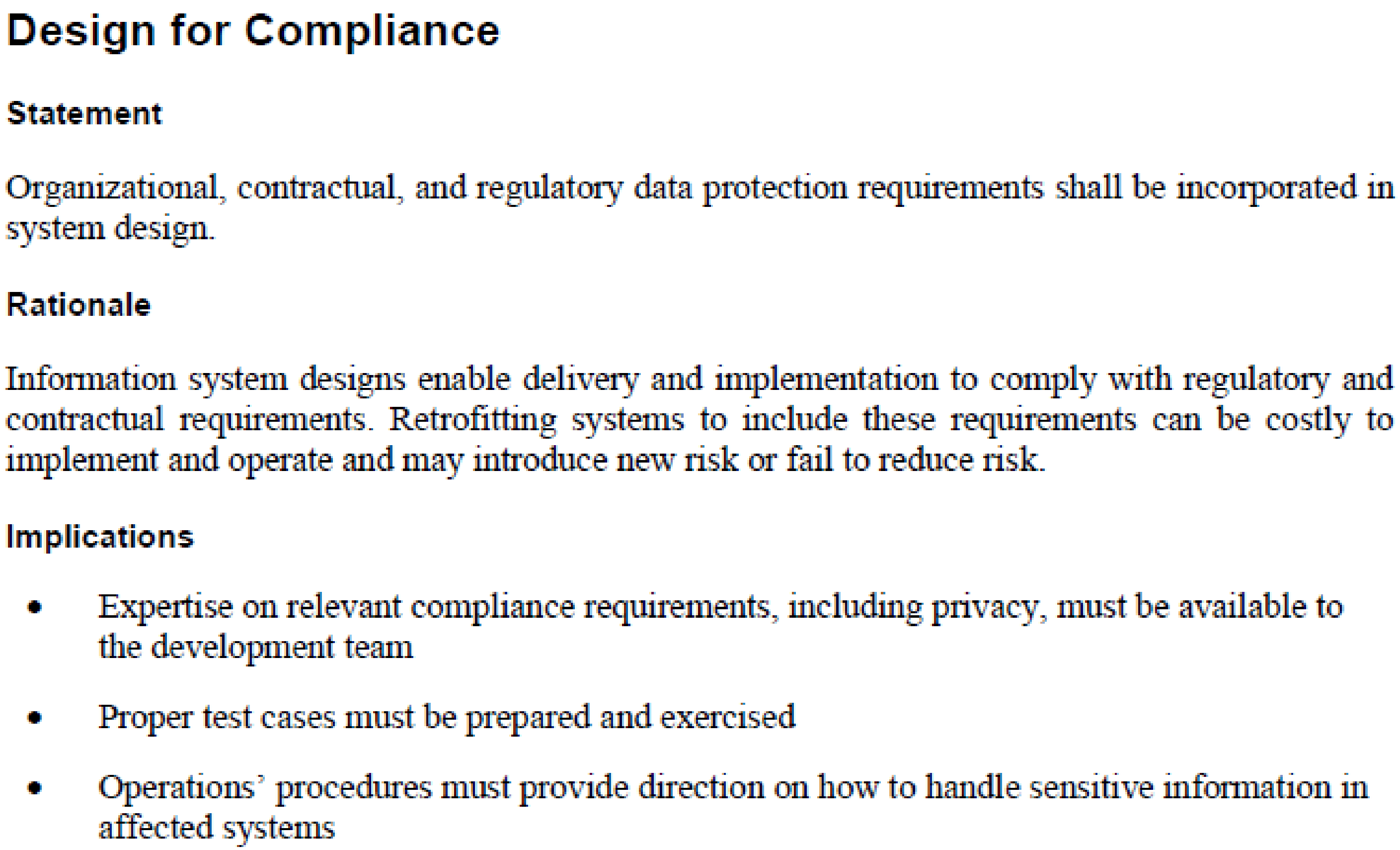
IT applications specs
Data, service specs
Integration requirements
Infrastructure
Security requirements

# Security principles for architecture



https://www.opengroup.org/forum/security/architecture

# Security principles for architecture



## Design for Compliance

### Statement

Organizational, contractual, and regulatory data protection requirements shall be incorporated in system design.

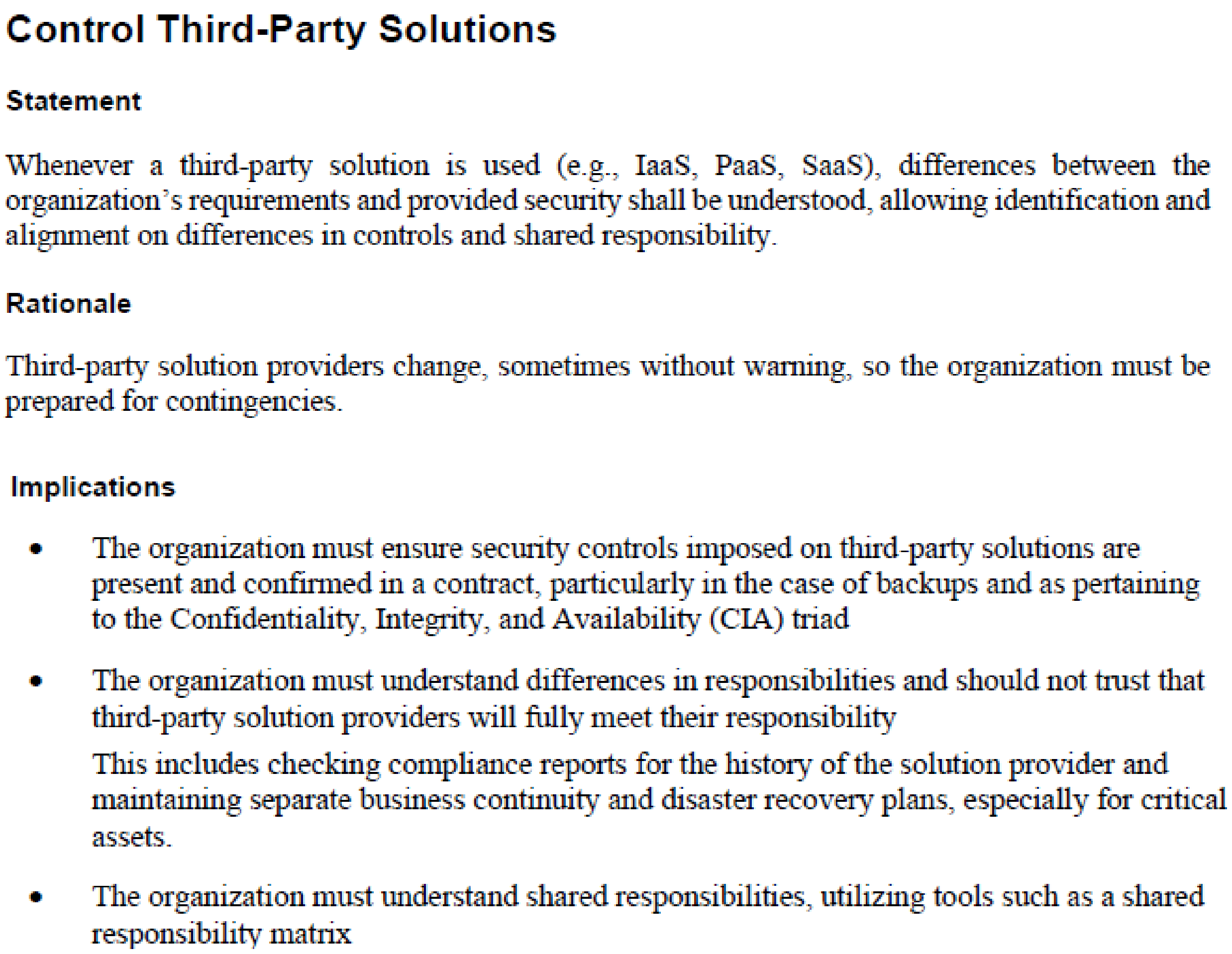
### Rationale

Information system designs enable delivery and implementation to comply with regulatory and contractual requirements. Retrofitting systems to include these requirements can be costly to implement and operate and may introduce new risk or fail to reduce risk.

### Implications

- Expertise on relevant compliance requirements, including privacy, must be available to the development team
- Proper test cases must be prepared and exercised
- Operations' procedures must provide direction on how to handle sensitive information in affected systems

# Security principles for architecture



## Control Third-Party Solutions

### Statement

Whenever a third-party solution is used (e.g., IaaS, PaaS, SaaS), differences between the organization's requirements and provided security shall be understood, allowing identification and alignment on differences in controls and shared responsibility.

### Rationale

Third-party solution providers change, sometimes without warning, so the organization must be prepared for contingencies.

### Implications

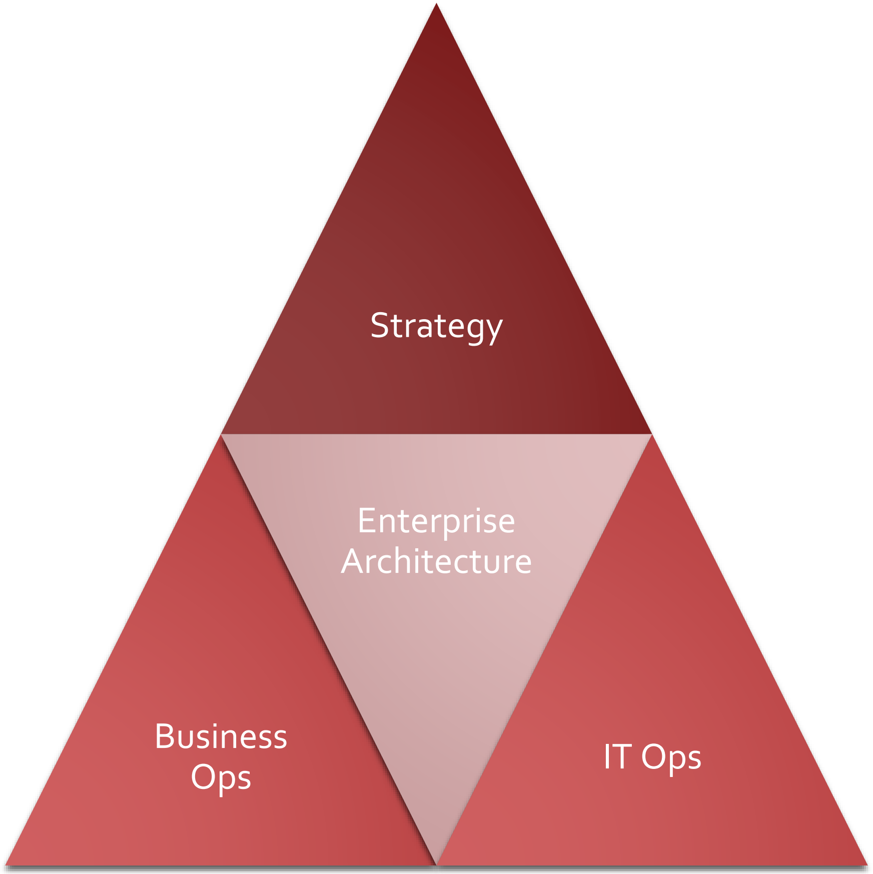
- The organization must ensure security controls imposed on third-party solutions are present and confirmed in a contract, particularly in the case of backups and as pertaining to the Confidentiality, Integrity, and Availability (CIA) triad
- The organization must understand differences in responsibilities and should not trust that third-party solution providers will fully meet their responsibility

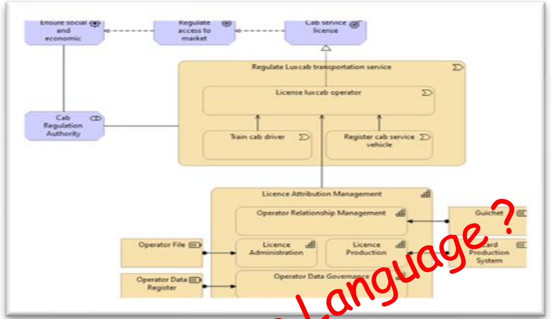
  This includes checking compliance reports for the history of the solution provider and maintaining separate business continuity and disaster recovery plans, especially for critical assets.
- The organization must understand shared responsibilities, utilizing tools such as a shared responsibility matrix

# Communication concerns

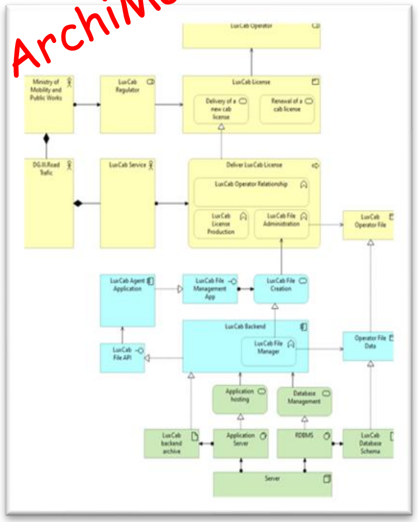
And the modeling value stream

# Variety of stakeholders





ArchiMate Language ?



Survey Sourcer

prometa

ARIS Platform

ARIS Sourcer

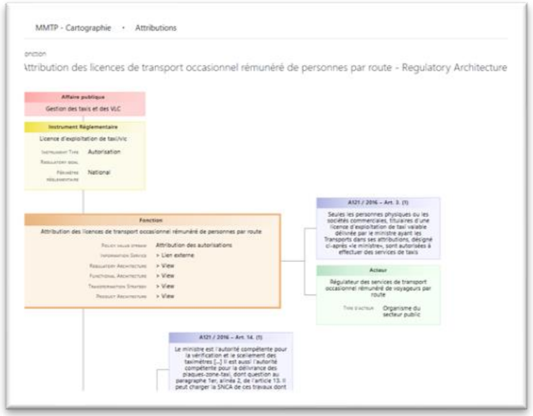
Data Sourcer

Model and Formalize Enterprise Knowledge

Archi
archimate modelling

Model Repository

Web Diffuser



MMTP - Cartographie • Attributions

onction

ttribution des licences de transport occasionnel rémunéré de personnes par route - Regulatory Architecture

**Affaire publique**

Gestion des taxis et des VLC

**Instrument Réglementaire**

Licence d'exploitation de taxi/vlc

| | |
|---|---|
| Instrument Type | Autorisation |
| Regulatory goal | |
| Périmètre réglementaire | National |

**Fonction**

Attribution des licences de transport occasionnel rémunéré de personnes par route

| | |
|---|---|
| Policy value stream | Attribution des autorisations |
| Information Service | > Lien externe |
| Regulatory Architecture | > View |
| Functional Architecture | > View |
| Transformation Strategy | > View |
| Product Architecture | > View |

**A121 / 2016 – Art. 3. (1)**

Seules les personnes physiques ou les sociétés commerciales, titulaires d'une licence d'exploitation de taxi valable délivrée par le ministre ayant les Transports dans ses attributions, désigné ci-après «le ministre», sont autorisées à effectuer des services de taxis

**Acteur**

Régulateur des services de transport occasionnel rémunéré de voyageurs par route

| | |
|---|---|
| Type d'acteur | Organisme du secteur public |

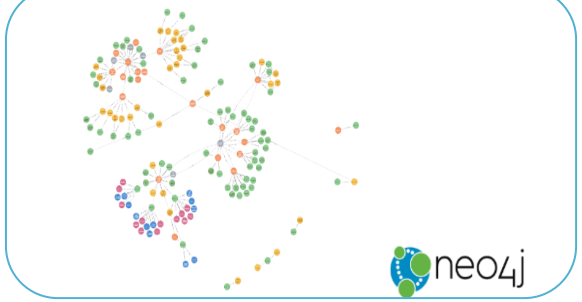
**A121 / 2016 – Art. 14. (1)**

Le ministre est l'autorité compétente pour la vérification et le scellement des taximètres [...] Il est aussi l'autorité compétente pour la délivrance des plaques-zone-taxi, dont question au paragraphe 1er, alinéa 2, de l'article 13. Il peut charger la SNCA de ces travaux dont

RDBMS Diffuser

Business Intelligence

Graph Diffuser



neo4j

**Model Sourcing**

**Model Design & Transformation**

**Model Diffusion**

***Modelling Value Stream***