Holistic approach for IT security

A Language for Multi-Perspective Modelling of IT Security: Objectives and Analysis of Requirements

Anat Goldstein
Ulrich Frank

Information Systems and Enterprise Modelling

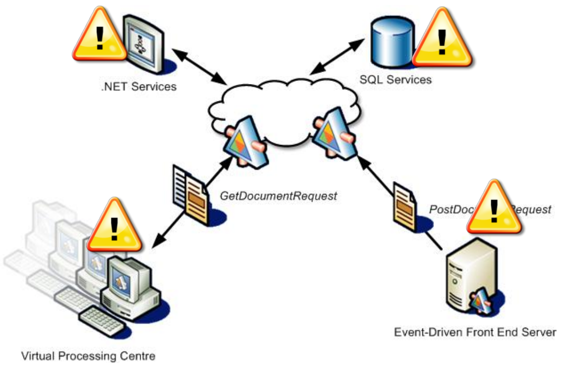
ICB Institute for Computer Science and Business Information Systems

Institut für Informatik und Wirtschaftsinformatik (ICB)

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Protecting IT– New Challenges

Technical complexities: Computing and Data resources are more distributed



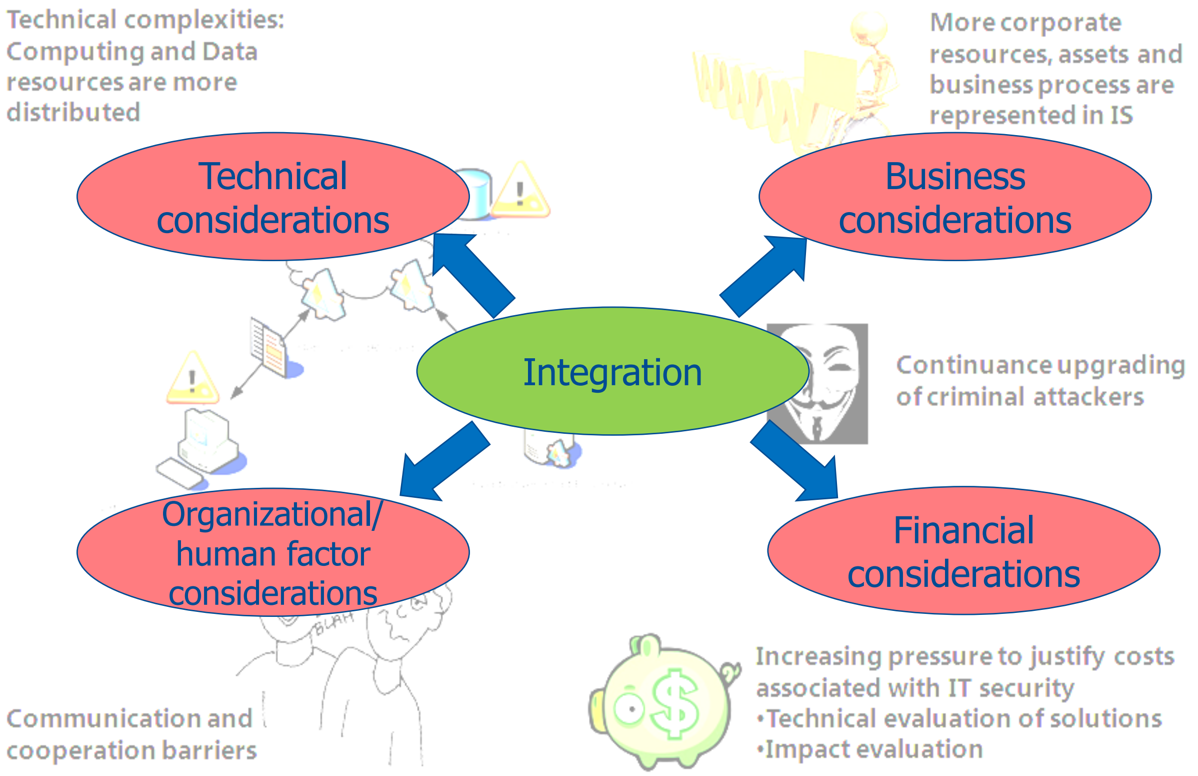
More corporate resources, assets and business process are represented in IS

Continuance upgrading of criminal attackers

Communication and cooperation barriers

Increasing pressure to justify costs associated with IT security
- Technical evaluation of solutions
- Impact evaluation

Protecting IT– Areas of Relevance



Technical complexities: Computing and Data resources are more distributed

Technical considerations

More corporate resources, assets and business process are represented in IS

Business considerations

Integration

Continuance upgrading of criminal attackers

Organizational/ human factor considerations

Financial considerations

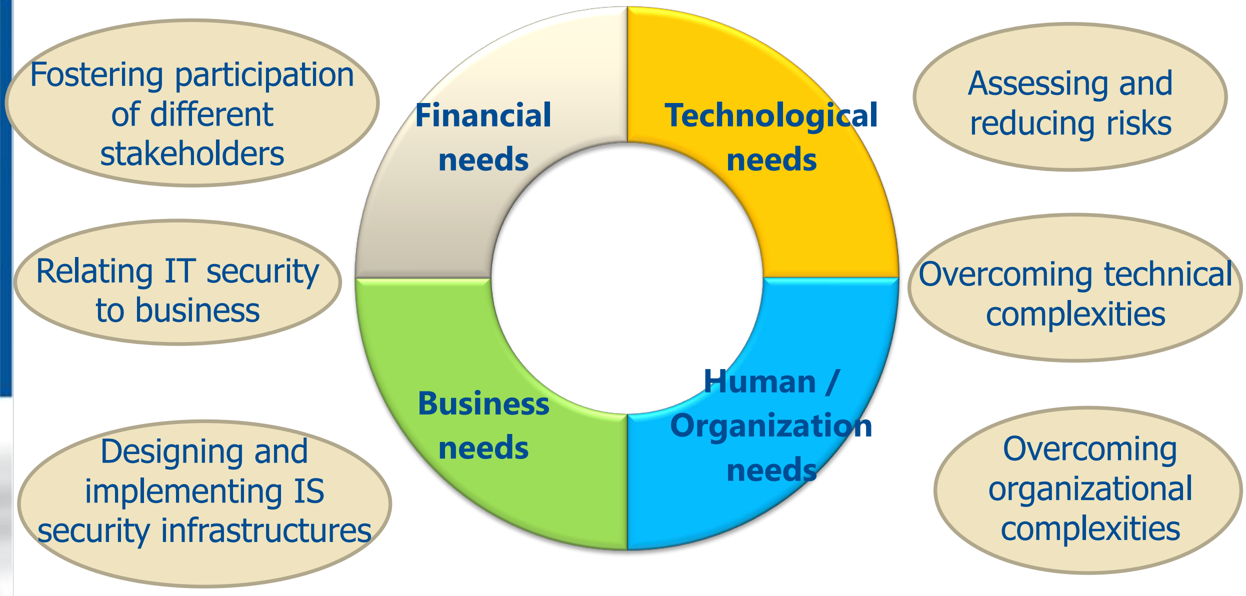
Communication and cooperation barriers

Increasing pressure to justify costs associated with IT security

- Technical evaluation of solutions
- Impact evaluation

The Goal

Develop a comprehensive IT security solution



Fostering participation of different stakeholders

Relating IT security to business

Designing and implementing IS security infrastructures

Financial needs

Technological needs

Business needs

Human / Organization needs

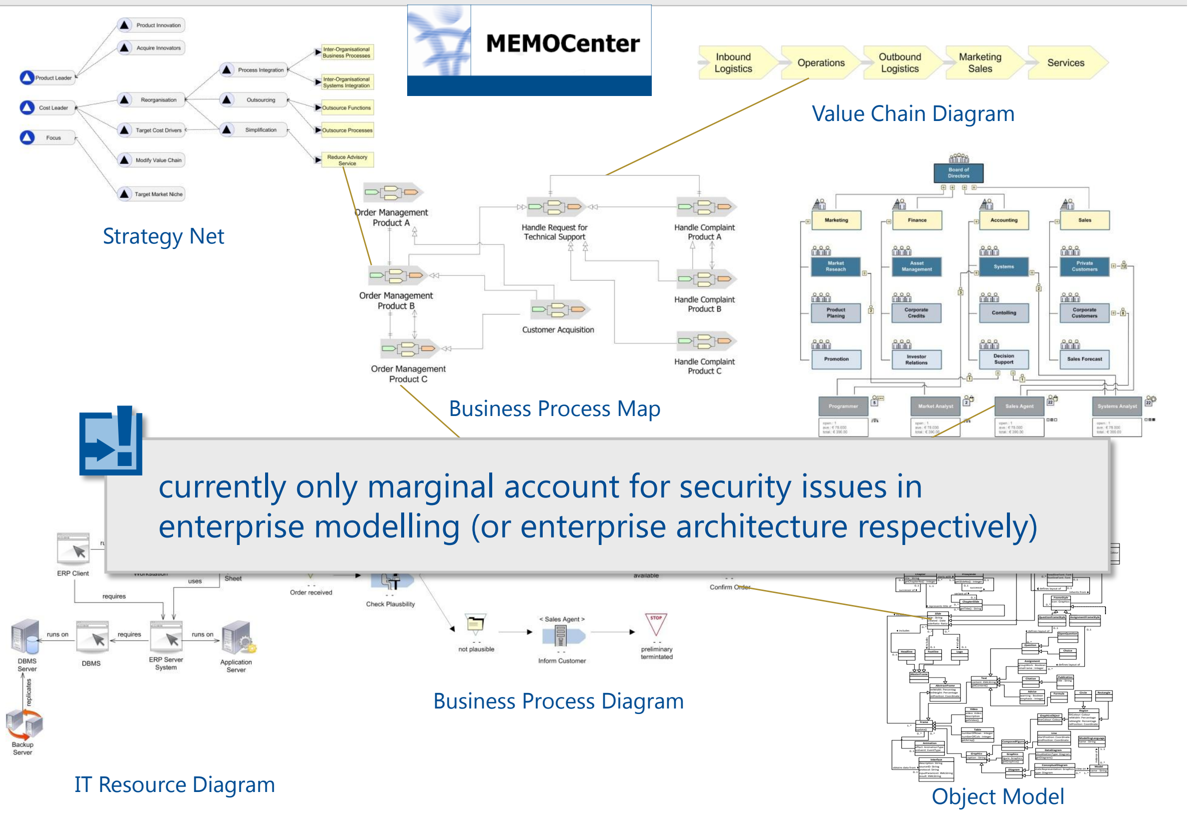
Assessing and reducing risks

Overcoming technical complexities

Overcoming organizational complexities

Requires a common conceptual framework → Enterprise Modelling (EM)

In a Nutshell: Enriching EM with IT Security Concepts



currently only marginal account for security issues in enterprise modelling (or enterprise architecture respectively)

Developing a new DSML - Challenges

The first step towards developing a new DSML is **requirements analysis**

Available Sources:

- Literature
- Ask prospective users about their needs and expectation from the targeted DSML
- use scenario development approach (Frank, 2010)

→**Our Method for Requirements Analysis**

- Theoretical basis → General requirements
- Use Scenario approach → Specific requirements
- Validating with practitioners

General Requirements

The method (language) should:

- **include concepts to describe IT security aspects from various perspectives**: technical, human, organizational, business and financial [e.g., Von Solms, 2001; Zuccati, 2007; Kokolakis 2000]. → integration with other MEMO DSMLs
- **support various phases of the enterprise's system development lifecycles**: initial stages of system requirement analysis, the design phase, derivation of security related code fragments. [e.g., Rodriguez et al, 2006; Nakamura et al 2005; Premkumar and Stubblebine, 2000]
- **facilitate communication and support of different stakeholders**: supporting different levels of abstraction and representation of multiple perspectives for the different stakeholders of the IT security design and management. [e.g., Braber et al, 2007; Giorgini et al, 2003; Nakamura et al, 2005]

Analyzing Use Scenarios

Augmented Process Map

Which business process types are affected by a new security regulation?

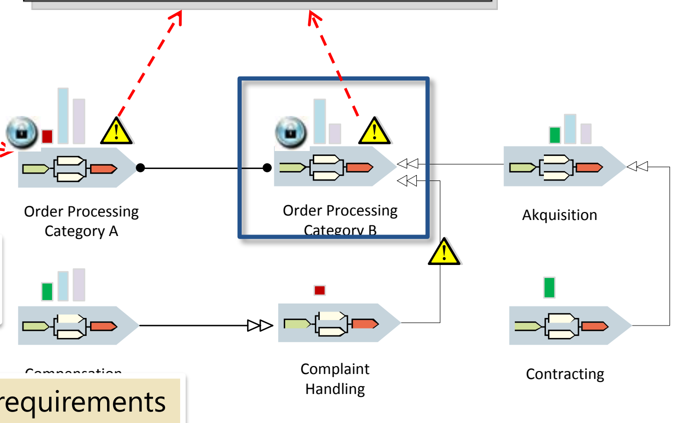
Which business process types are exposed to a threat?

Which business process types are confidential?

Security Requirement	security breach notification
Security Goal	Confidentiality
Measure	IDS
regulation	California security law

What is the total cost of protecting a BP type?

Average Costs per month	90.000 €
Average IT Security Costs/month	15.000 €
Average IT Costs per instance*	25 €



Does a BP have security implications on another BP?

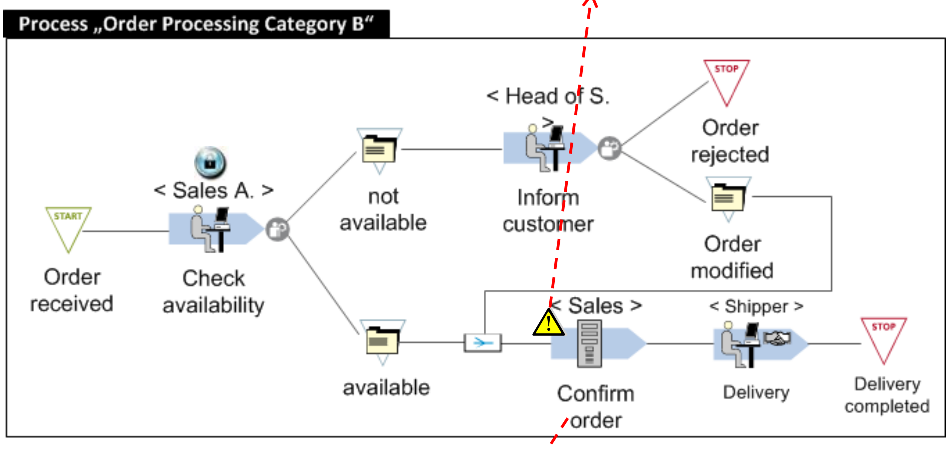
Is there a conflict between security requirements of BPs (e.g., 2 BPs, which share information, comply with different security regulations)?

© Prof. Dr. Ulrich Frank | SecuMod project

Augmented Process Diagram

Security Requirement	ensure customer privacy
Security Goal	Confidentiality
Measure	encryption
regulation	SD4856

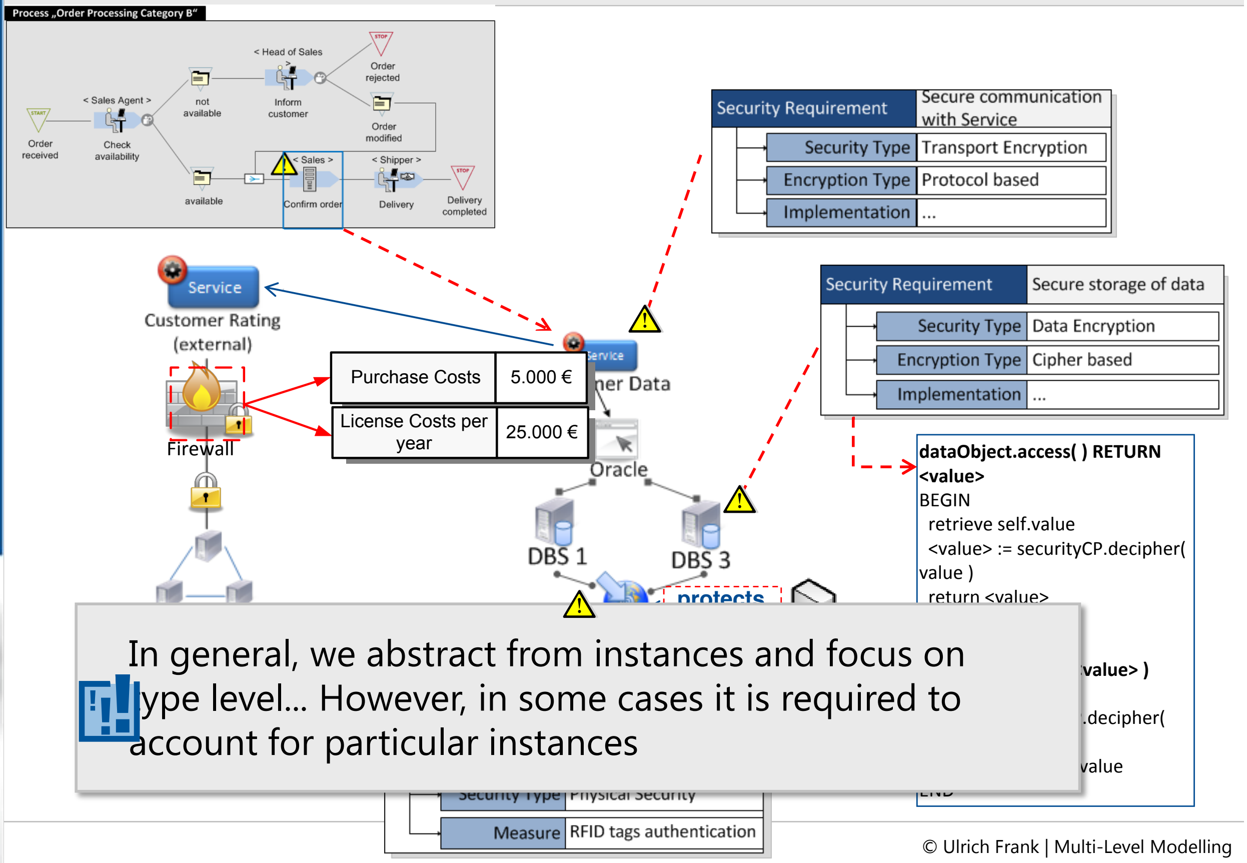
Process „Order Processing Category B“



Average Costs per month	50.000 €
Average IT Security Costs/month	15.000 €
Average IT Costs per instance*	15 €

© Ulrich Frank | Multi-Level Modelling

Augmented IT Resource Diagram



Purchase Costs	5.000 €
License Costs per year	25.000 €

Security Requirement	Secure communication with Service
Security Type	Transport Encryption
Encryption Type	Protocol based
Implementation	...

Security Requirement	Secure storage of data
Security Type	Data Encryption
Encryption Type	Cipher based
Implementation	...

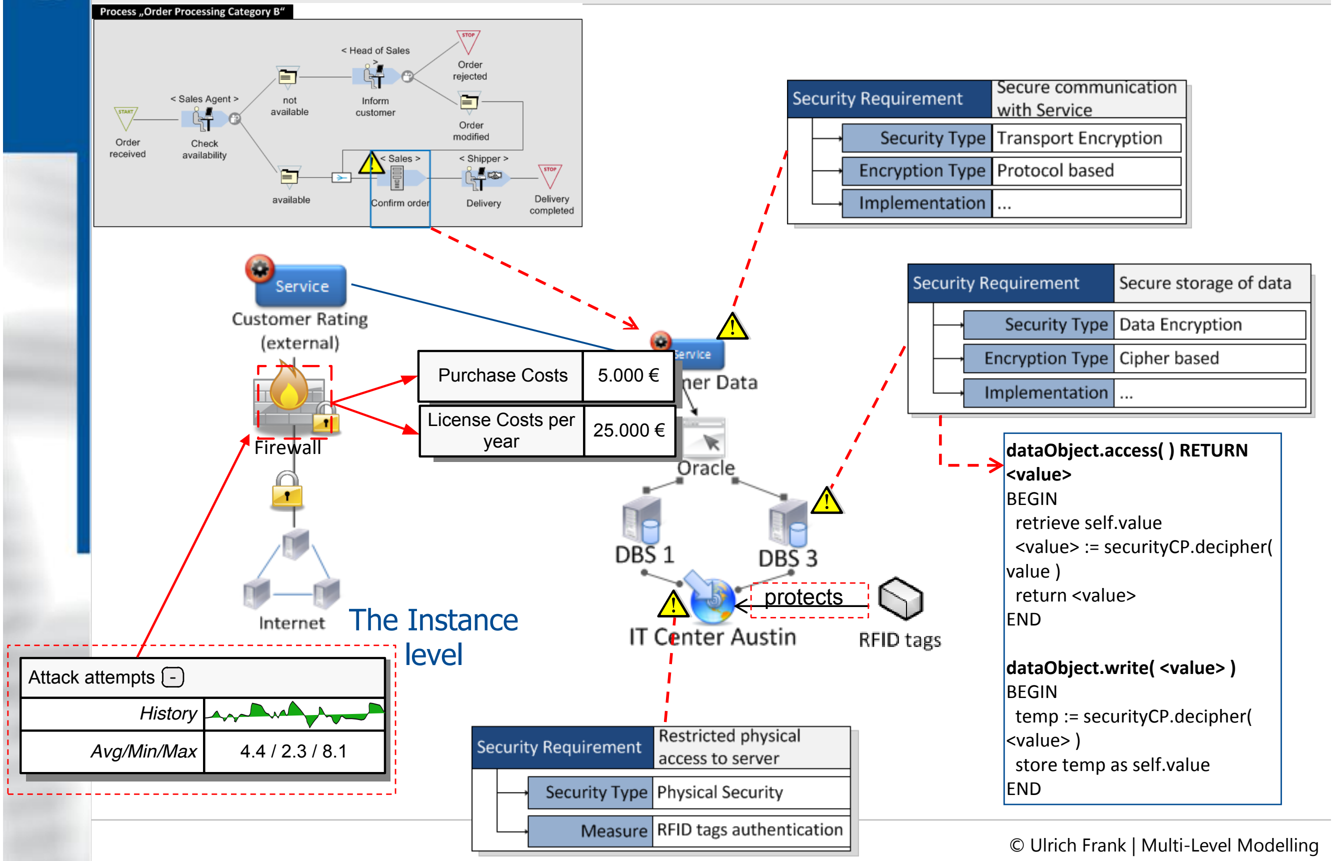
```
dataObject.access( ) RETURN
<value>
BEGIN
  retrieve self.value
  <value> := securityCP.decipher(
value )
  return <value>
```

```
value> )
.decipher(
value
END
```

Security Type	Physical Security
Measure	RFID tags authentication

In general, we abstract from instances and focus on type level... However, in some cases it is required to account for particular instances

Augmented IT Resource Diagram



The Instance level

Purchase Costs	5.000 €
License Costs per year	25.000 €

Attack attempts -	
History	
Avg/Min/Max	4.4 / 2.3 / 8.1

Security Requirement	Secure communication with Service
Security Type	Transport Encryption
Encryption Type	Protocol based
Implementation	...

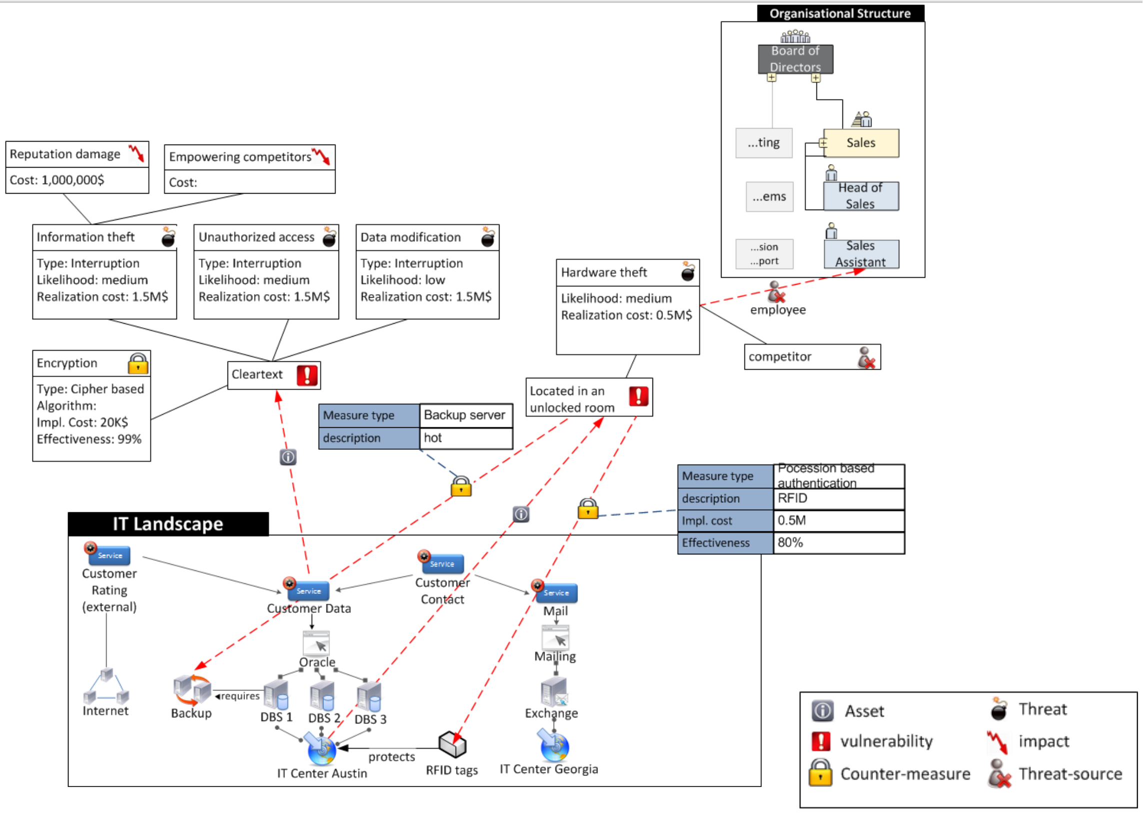
Security Requirement	Secure storage of data
Security Type	Data Encryption
Encryption Type	Cipher based
Implementation	...

```
dataObject.access( ) RETURN
<value>
BEGIN
  retrieve self.value
  <value> := securityCP.decipher(
value )
  return <value>
END

dataObject.write( <value> )
BEGIN
  temp := securityCP.decipher(
<value> )
  store temp as self.value
END
```

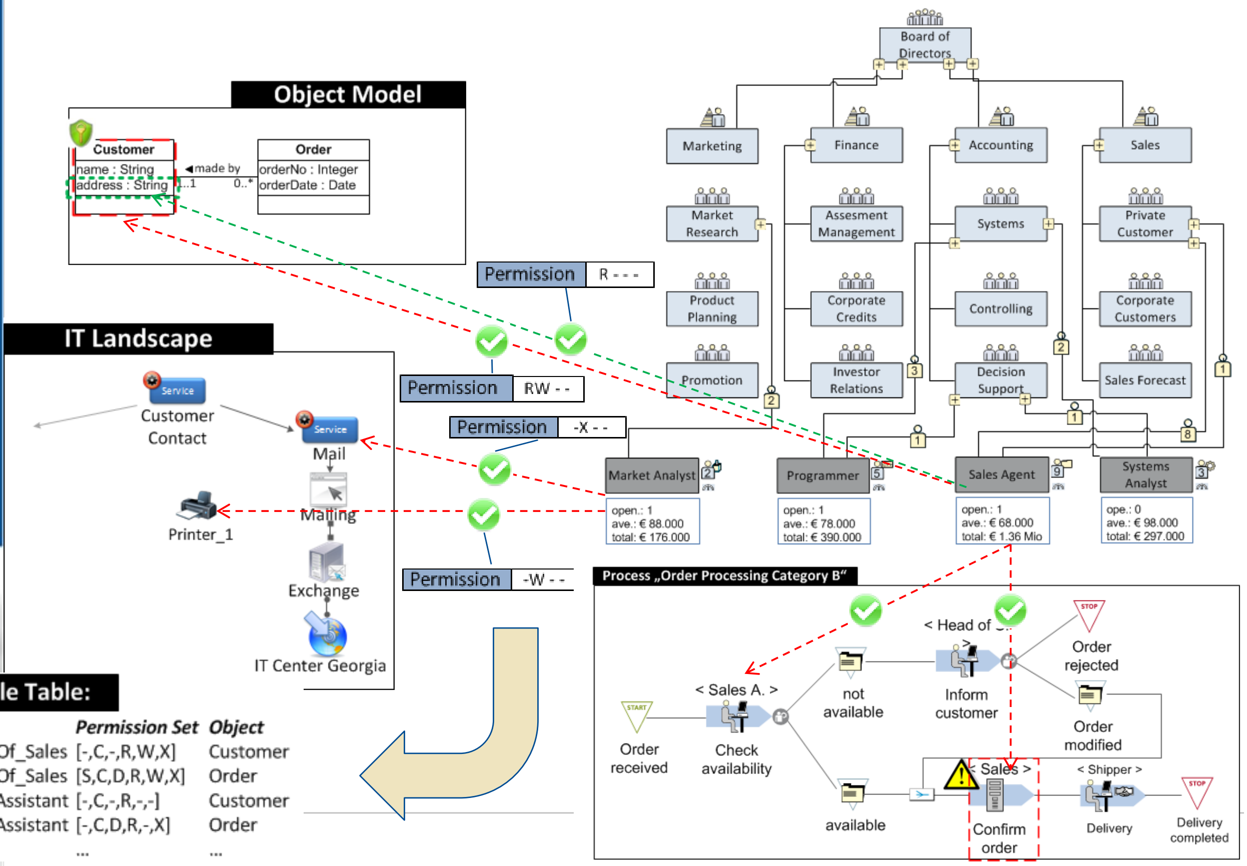
Security Requirement	Restricted physical access to server
Security Type	Physical Security
Measure	RFID tags authentication

Risk Management Diagram



© Ulrich Frank | Multi-Level Modelling

Augmented Organizational Chart



Role Table:

Role	*Permission Set*	*Object*
Head_Of_Sales	[-,C,-,R,W,X]	Customer
Head_Of_Sales	[S,C,D,R,W,X]	Order
Sales_Assistant	[-,C,-,R,-,-]	Customer
Sales_Assistant	[-,C,D,R,-,X]	Order
...	...	...

Specific Requirements

It should be possible to:

- indicate that a process type has security requirements. It should also be possible to analyze these security requirements in more details
- analyze the aggregated cost of process types: the total cost of protecting activities of a process or the financial impact of the realization of security risks within the process.
- indicate that an association between two process types has security implications.
- The modelling language should provide concepts that enable a detailed description of the security needs in order to allow filtering and representation of different types of security requirements.
- Integrate between the business process perspective and the IT perspective: associate an activity with its vulnerable assets (IT resources) and with selected (IT) counter-measures. These associations should allow for cost and impact analysis of the damage/implementation.
- To allow linking process activities with threats and vulnerabilities. Thus, the ML should be integrated with concepts from the business process diagram (i.e. activities), provided by MEMO OrgML.
- To link activities with users who: 1. are authorized to perform them ; 2. might interfere with their execution.
- define security requirements for IT resources and to describe the security measures used in detail. This implies that a protection association is required. This association can be used to indicate that one IT resource is intended to protect another IT resource.
- support cost-benefit analyses of security measures: effectiveness, implementation costs, justification…
- support different levels of abstraction of security requirements, ranging from high-level, definition of security controls to low-level definition of technical details of encryption methods, cipher settings, communication protocols and access control policies → Support code generation.
- define for each IT resource who is allowed to access it and their permissions (read, write, execute, delete).
- support activities like risk analysis, risk mitigation and evaluation: assign vulnerabilities to assets, define threat-sources and the vulnerabilities they can exploit , assign probabilities to threats and the impact they have, match counter-measures to vulnerabilities, and to analyze their costs.
- be integrated with the ITML. This will enable connecting security concepts with IT resources for example, connecting a vulnerability to an IT resource or connecting a counter-measure to the IT resource which is used to resolve a vulnerability.
- support the comparison of different counter-measures against threats and for cost-benefit analysis.
- allow gathering information about attack history, i.e. statistics on the occurrence of threats (instance level).
- allow access rights definitions for the different positions, roles and business units with respect to data resources.
- The formal definition of permission sets allows the automatic derivation of access control policies, such as RBAC, which is supported by many software platforms.
- allow defining that entity objects should be encrypted or that a specific attribute should be encrypted
- allow the definition of access rights to entities and to their attributes

Conclusions and Future Steps

- 23 requirements were derived
- Are the requirements exhaustive?
- …Validating with practitioners
- Future steps:
  - Continue validating the requirements
  - Developing the Security modeling method
    - Extension or creation?
  - Validating the method empirically.

QUESTIONS & ANSWERS