Efficient and reliable business impact analysis using SABSA and DEMO

20 years experience in delivery of IT applications

Executive master Enterprise IT Architecture (MEITA) 2019-2021

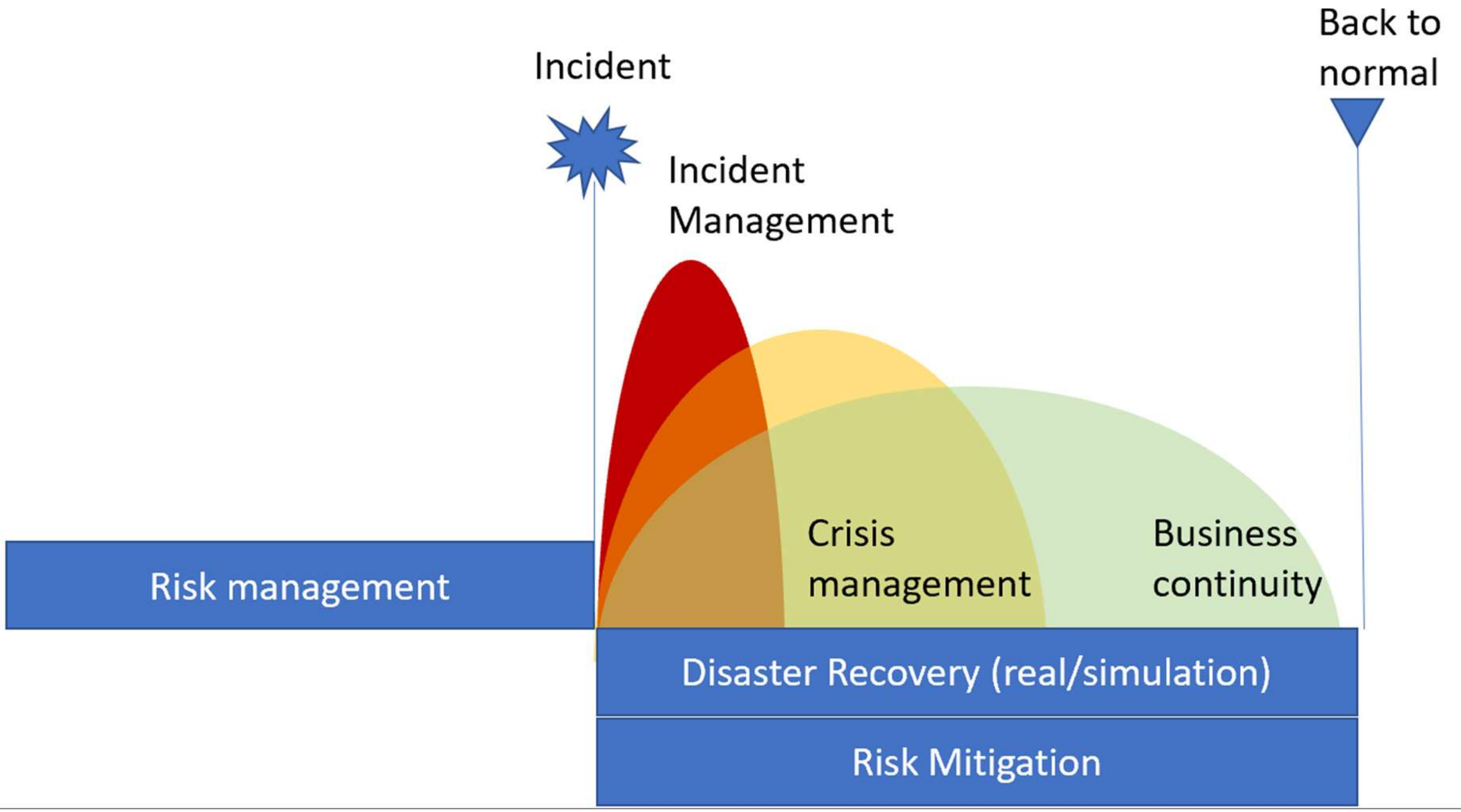
at Antwerp Management School

Geert Boelens

geert@boelens-ict.be

+32 496 465 732

Business continuity plan (BCP)



Based on: control risks

Business impact analysis (BIA)

Top-down analysis to prioritize business capabilities.

Process

Identify capabilities

Identify minimum acceptable levels

Identify the resources on which capabilities depend

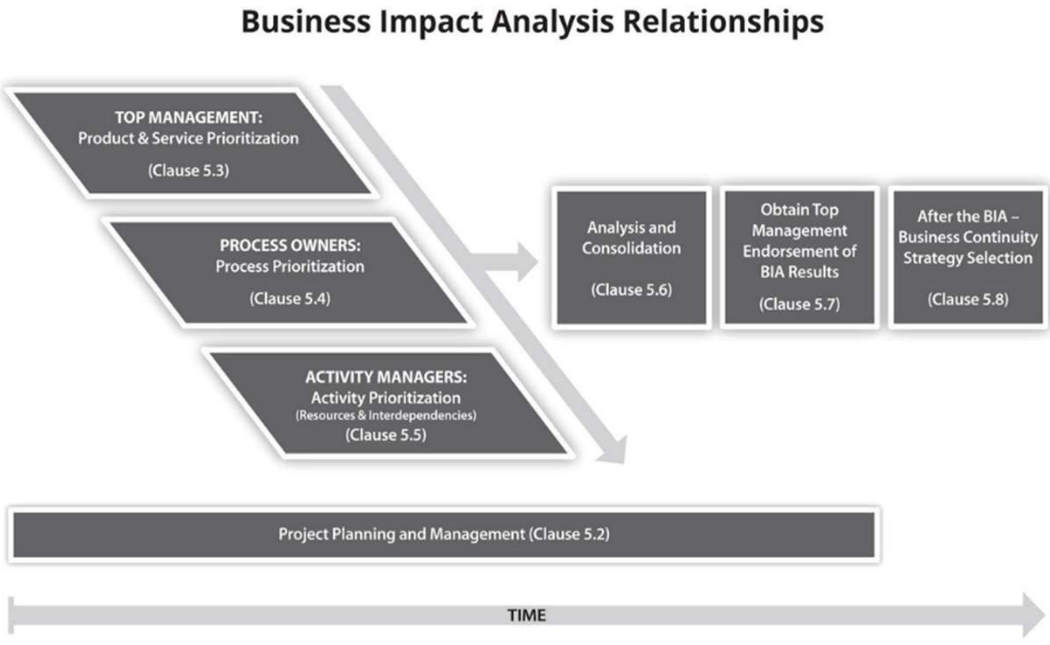
Agree on timeline to assess downtime impacts

Agree on acceptable risk or impact

Agree on implementing measures

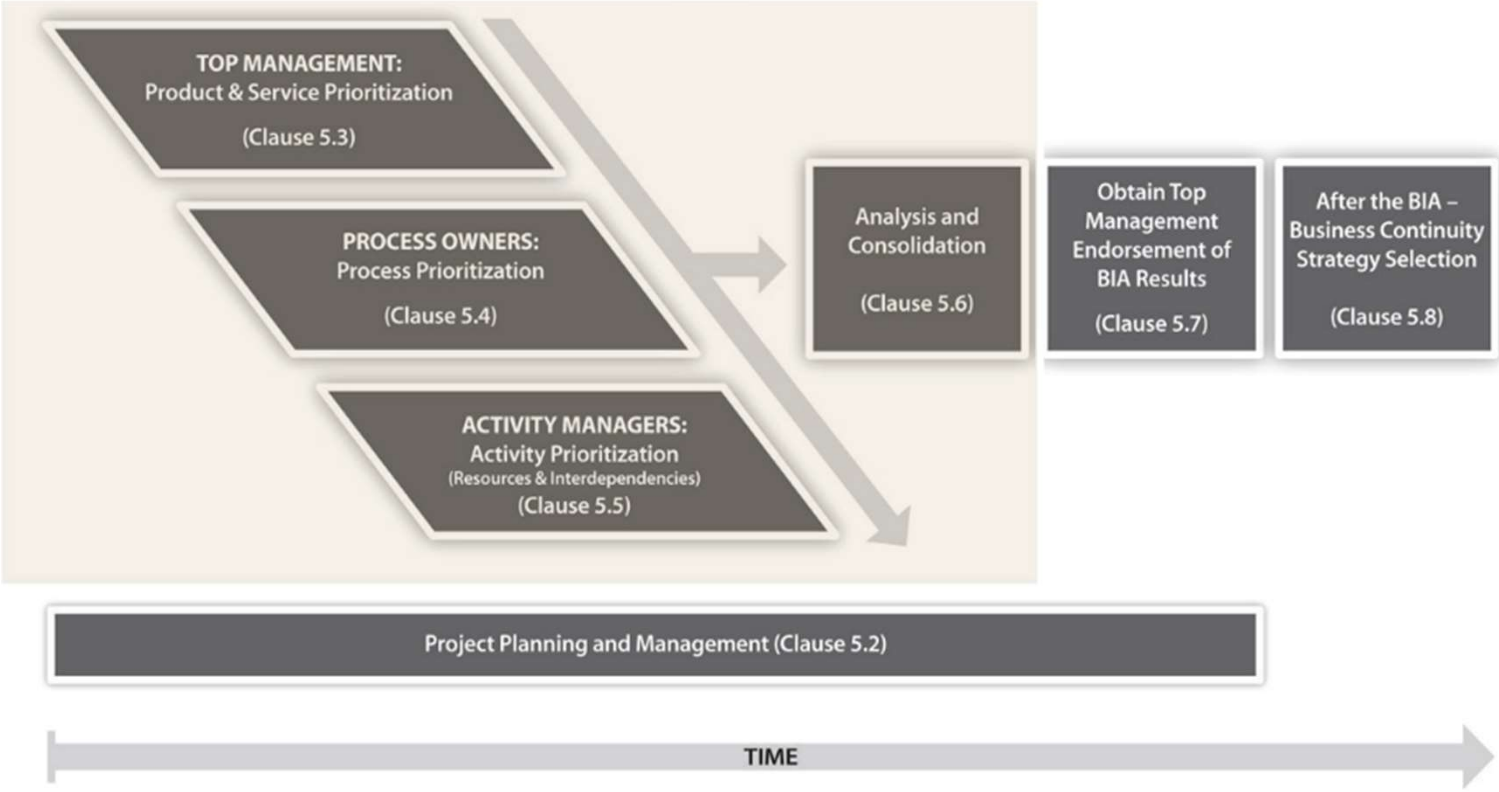
Calculate theoretical impact of downtime for the agreed timeline

Analysis of impacts over time should result in MTPD.


Business Impact Analysis Relationships
TOP MANAGEMENT: Product & Service Prioritization (Clause 5.3)
PROCESS OWNERS: Process Prioritization (Clause 5.4)
ACTIVITY MANAGERS: Activity Prioritization (Resources & Interdependencies) (Clause 5.5)
Analysis and Consolidation (Clause 5.6)
Obtain Top Management Endorsement of BIA Results (Clause 5.7)
After the BIA – Business Continuity Strategy Selection (Clause 5.8)
Project Planning and Management (Clause 5.2)
TIME

Business impact analysis relationships, source: ISO22317:2015, page 5

The importance of an accurate BIA


TOP MANAGEMENT:
Product & Service Prioritization
(Clause 5.3)
PROCESS OWNERS:
Process Prioritization
(Clause 5.4)
ACTIVITY MANAGERS:
Activity Prioritization
(Resources & Interdependencies)
(Clause 5.5)
Analysis and Consolidation
(Clause 5.6)
Obtain Top Management Endorsement of BIA Results
(Clause 5.7)
After the BIA – Business Continuity Strategy Selection
(Clause 5.8)
Project Planning and Management (Clause 5.2)
TIME

Business impact analysis relationships, source: ISO22317:2015, page 5

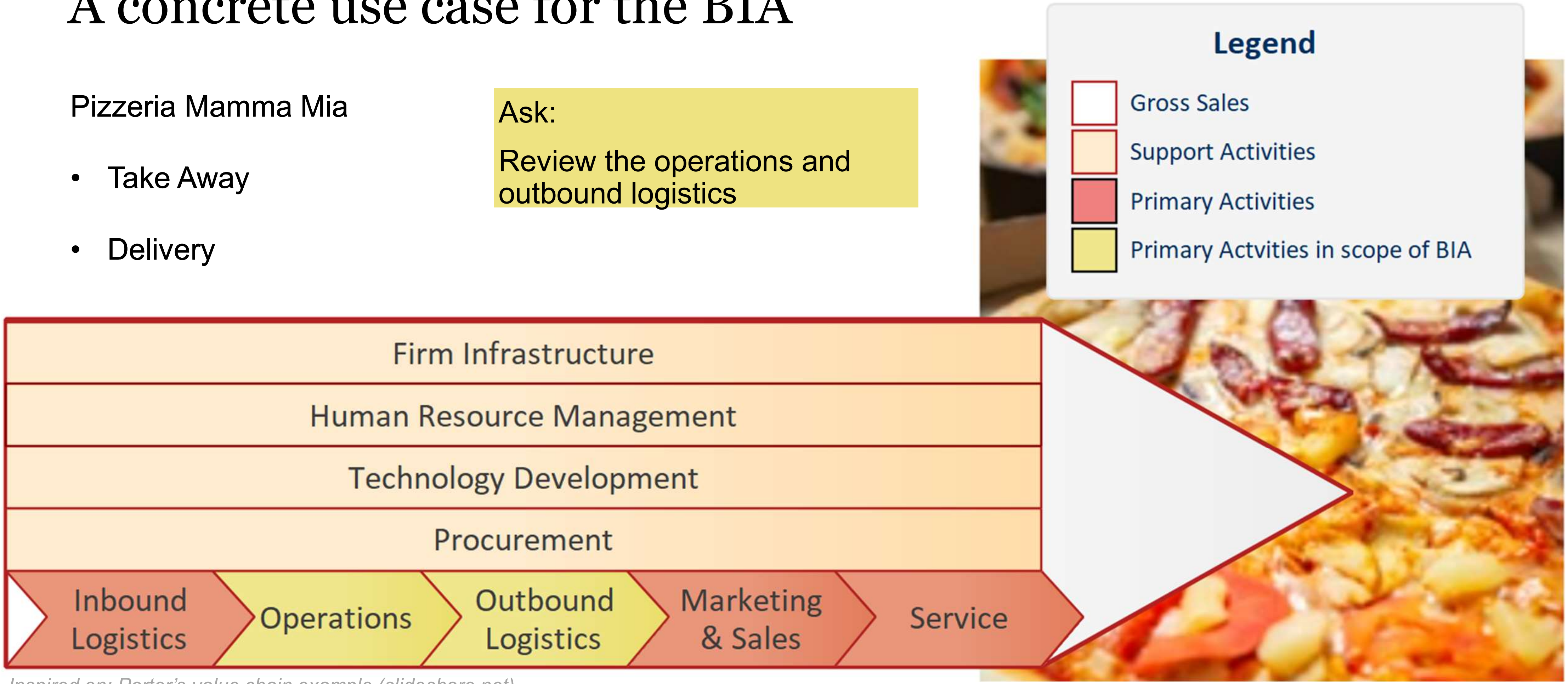
A concrete use case for the BIA

Pizzeria Mamma Mia

- Take Away
- Delivery

Ask:

Review the operations and outbound logistics



Legend

- □ Gross Sales
- 🟧 Support Activities
- 🟥 Primary Activities
- 🟨 Primary Actvities in scope of BIA

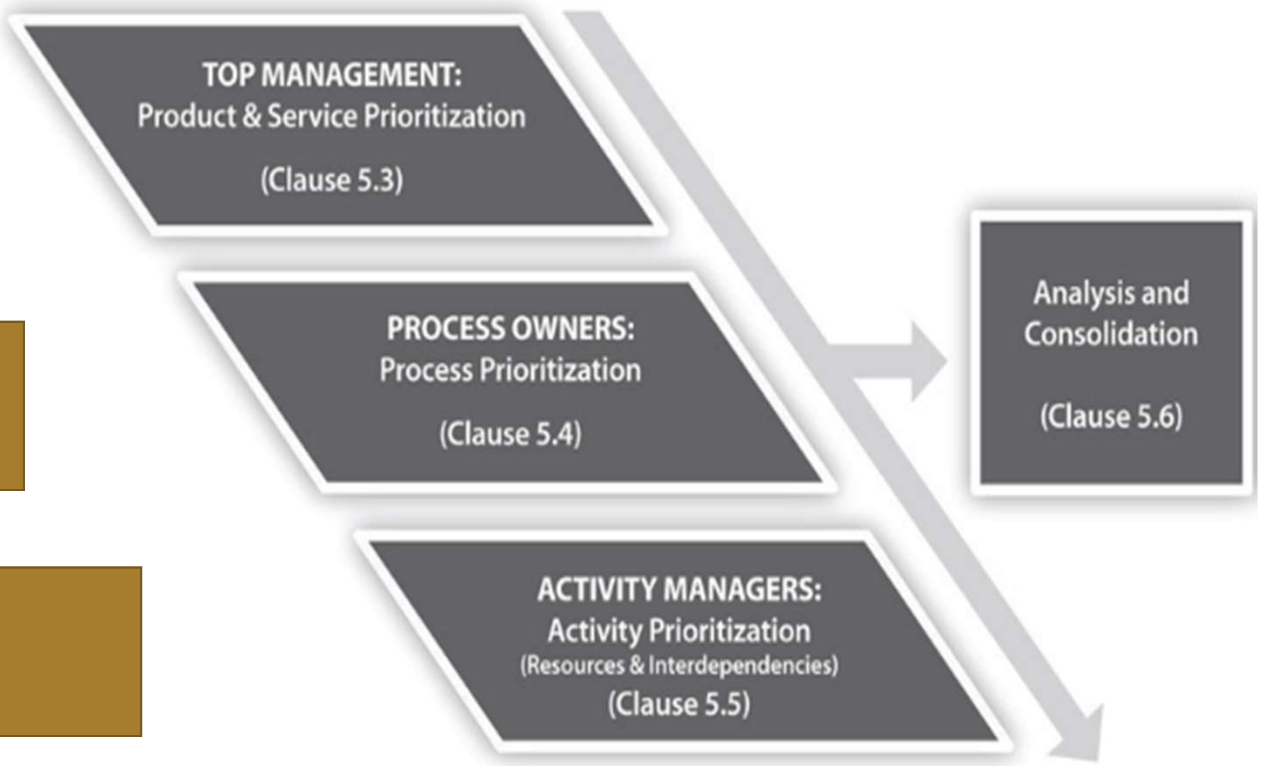
Inspired on: Porter's value chain example (slideshare.net)

The outcomes per prioritization step

- Requirements (Risk)
- Identification of processes
- Prioritization

- Dependencies
- Priorities
- Activities in the process

- Dependencies
- Resources
- Impacts



TOP MANAGEMENT:
Product & Service Prioritization
(Clause 5.3)

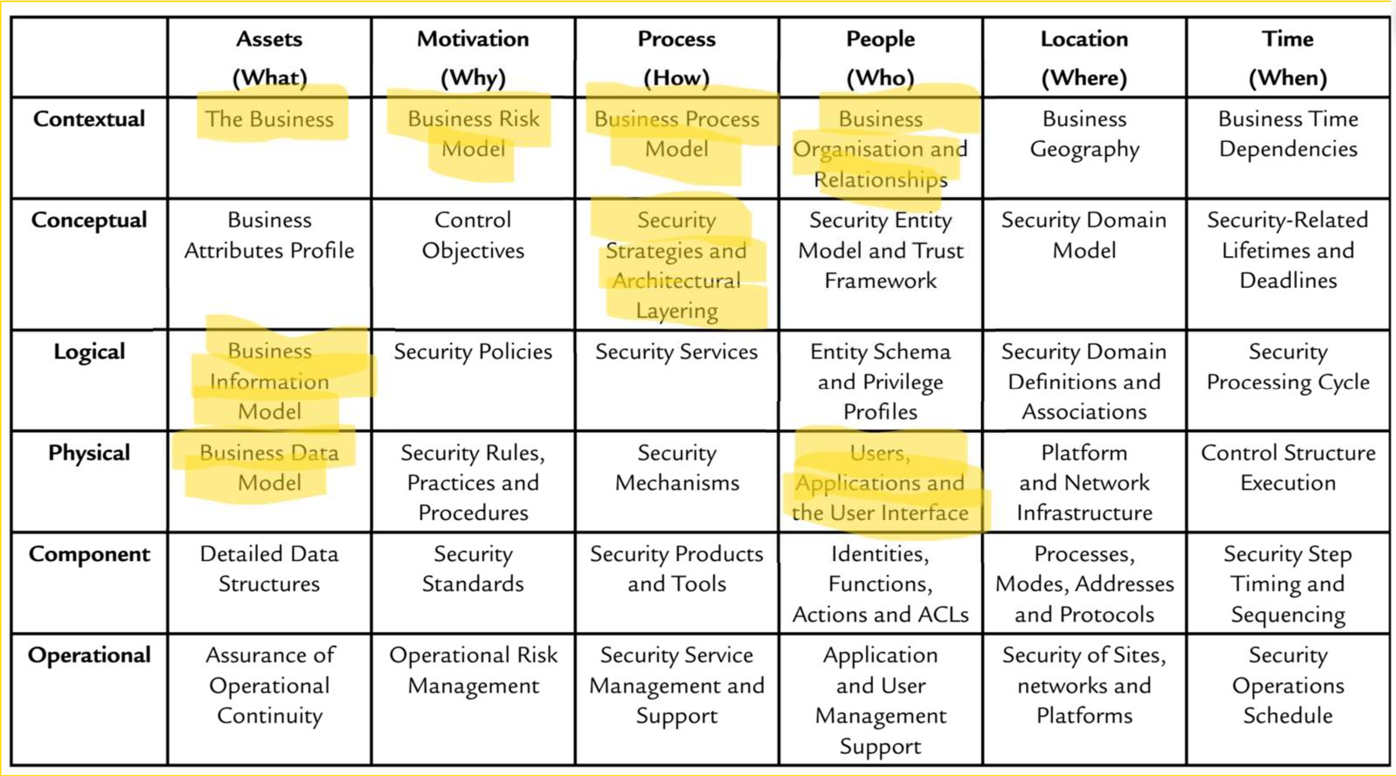
PROCESS OWNERS:
Process Prioritization
(Clause 5.4)

ACTIVITY MANAGERS:
Activity Prioritization
(Resources & Interdependencies)
(Clause 5.5)

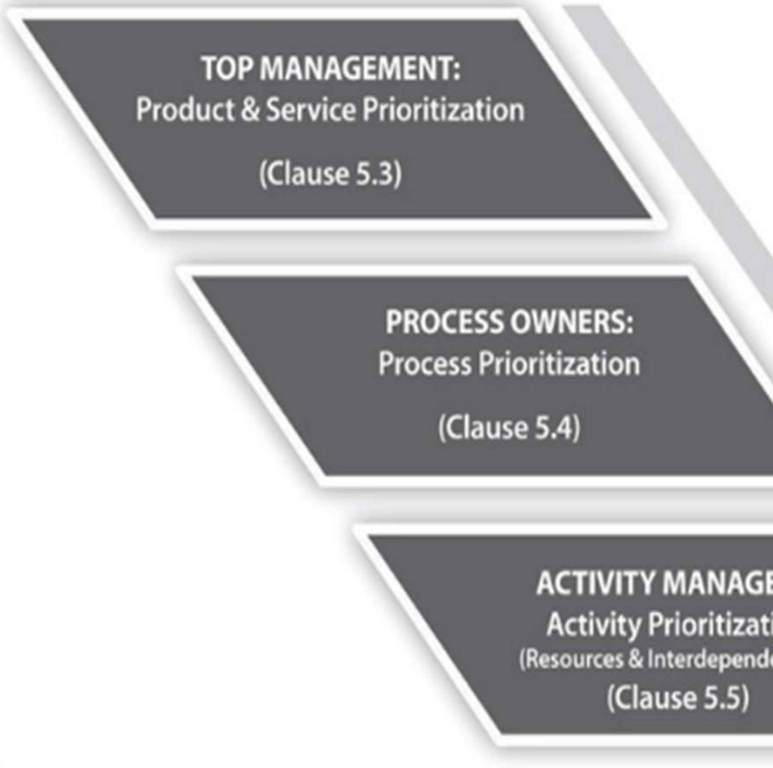
Analysis and Consolidation
(Clause 5.6)

Business impact analysis relationships, source: ISO22317:2015, page 5

SABSA to guide the process



	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Modes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management Support	Security of Sites, networks and Platforms	Security Operations Schedule



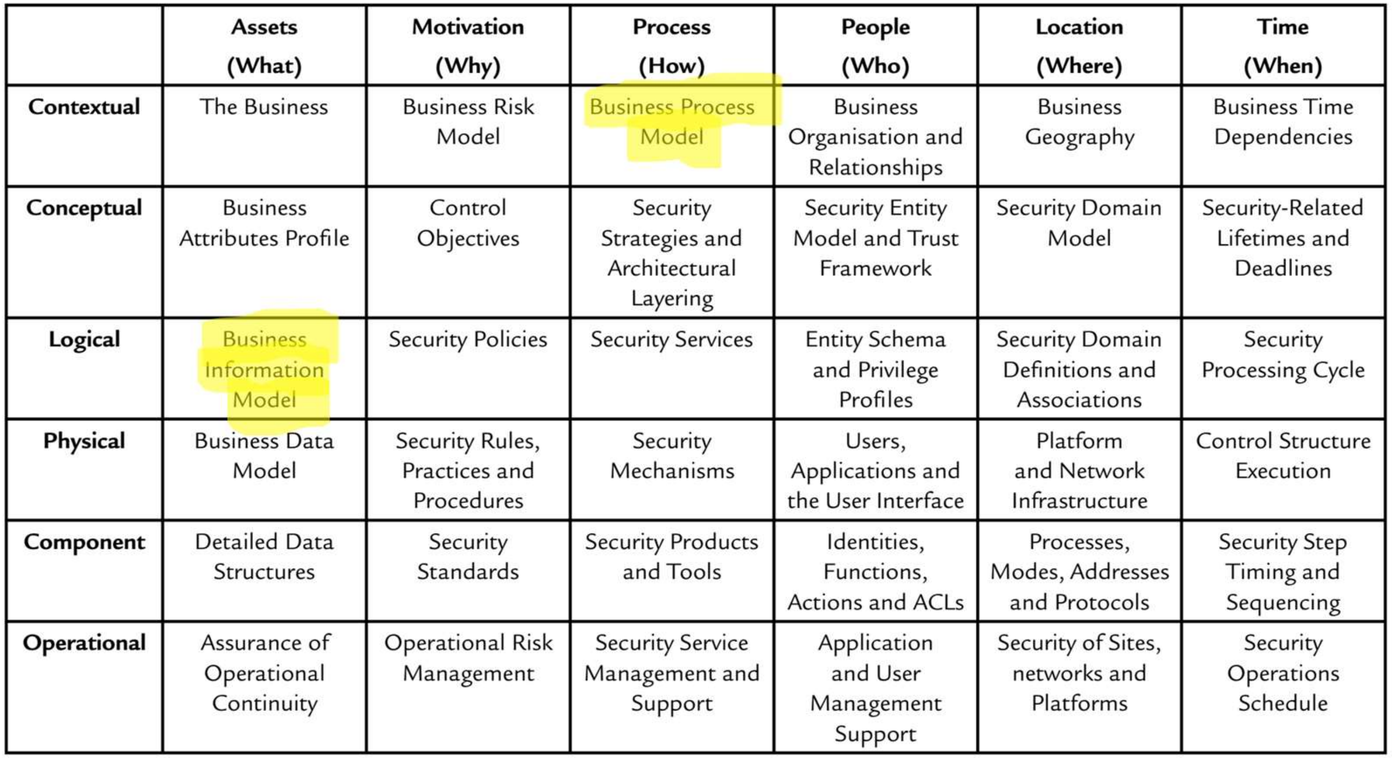
TOP MANAGEMENT:
Product & Service Prioritization
(Clause 5.3)

PROCESS OWNERS:
Process Prioritization
(Clause 5.4)

ACTIVITY MANAGE
Activity Prioritizati
(Resources & Interdepend
(Clause 5.5)

Based on: 36-Cell SABSA Matrix, source: Enterprise Security Architecture, page 42

Gap: business analysis



	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Modes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management Support	Security of Sites, networks and Platforms	Security Operations Schedule

Based on: 36-Cell SABSA Matrix, source: Enterprise Security Architecture, page 42

SABSA does not give any recommendation on formatting or structuring

BPMN – business process modeling language, also does not give any guidance

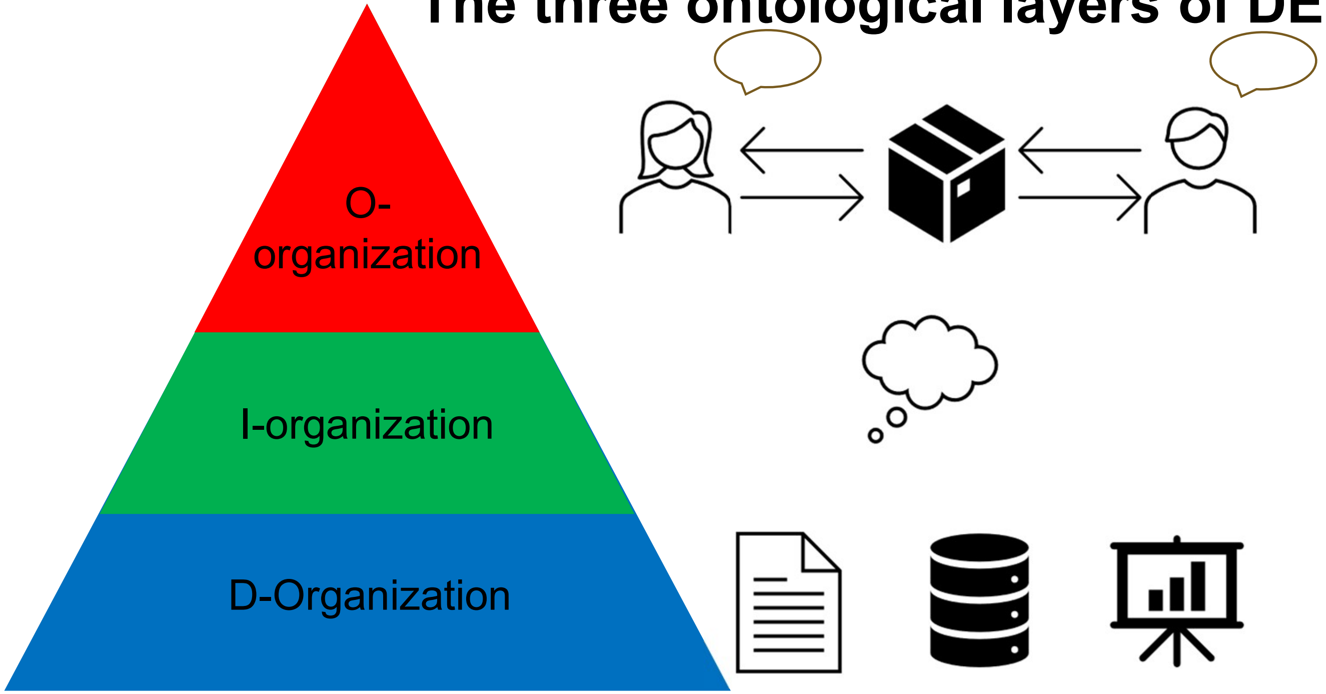
Archimate – Enterprise architecture Modeling language, not proscriptive

So how to give guidance?

What is DEMO?

Design and Engineering Methodology for Organizations

The three ontological layers of DEMO



Actors and Transactions

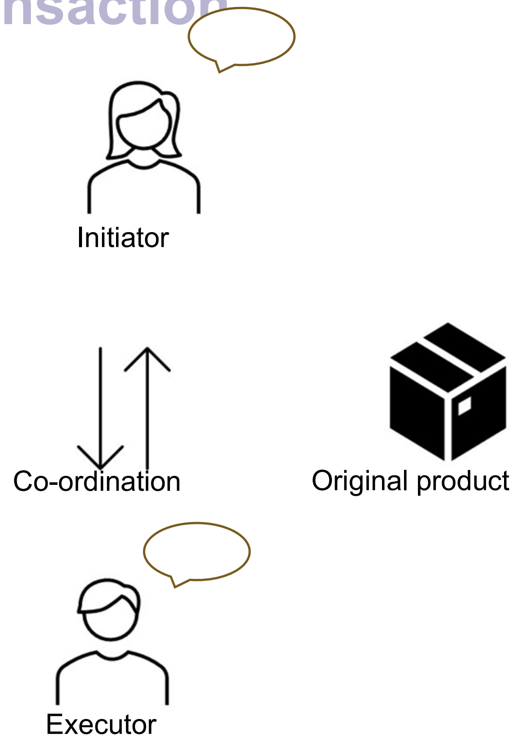
Business Entities, fact model

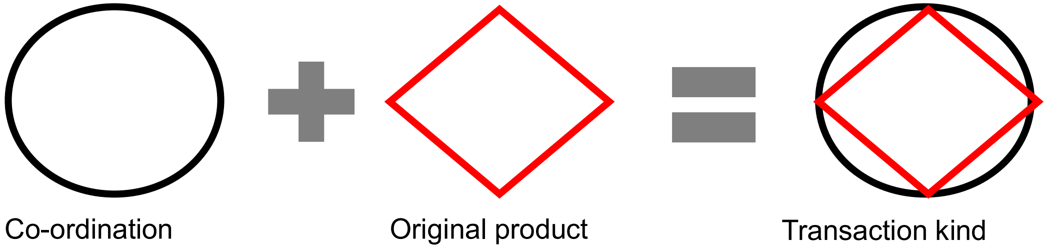
Recording the facts

Inspired on Dietz 2020, P. 230

O-organization

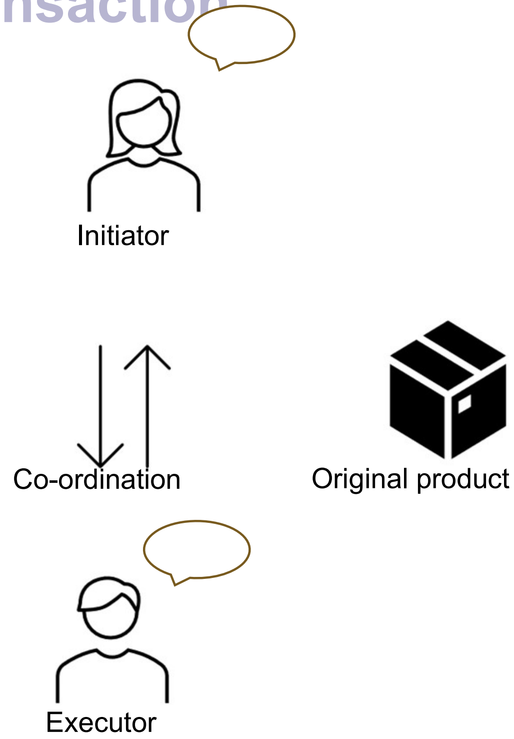
The transaction

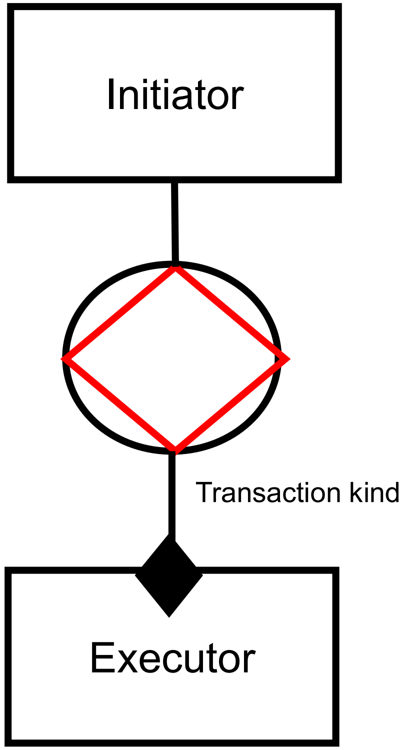




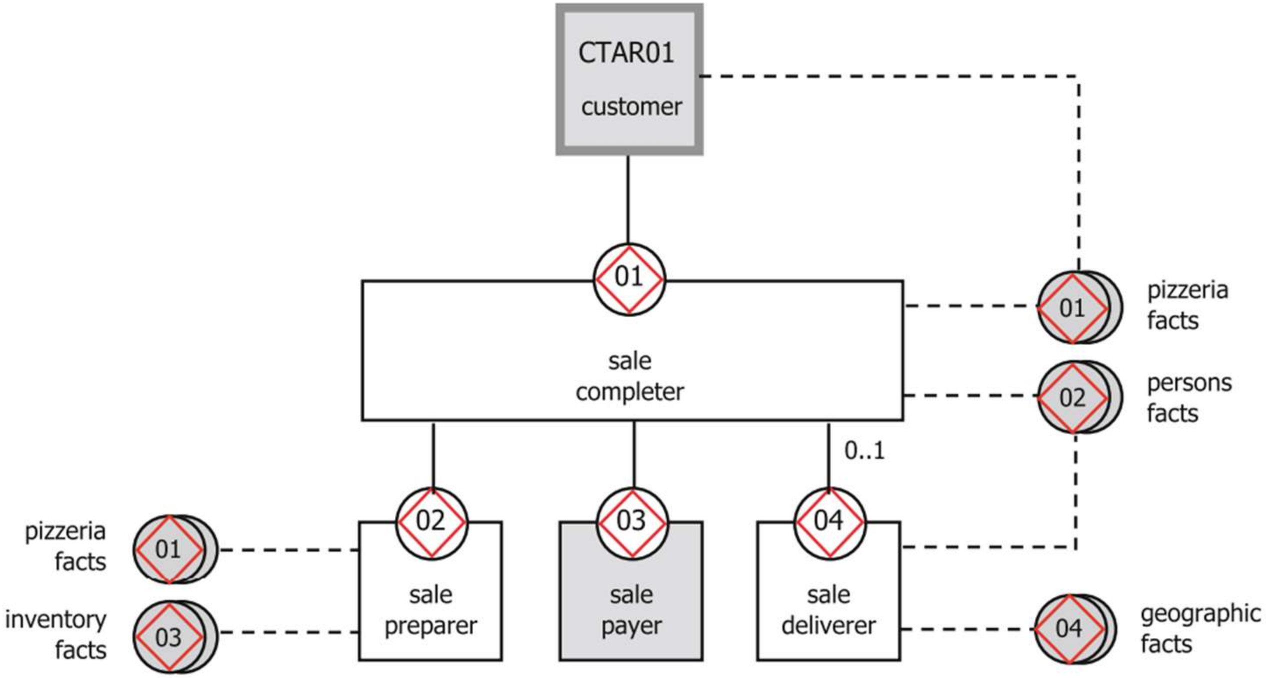
O-organization

The transaction





1) Coordination Structure Diagram

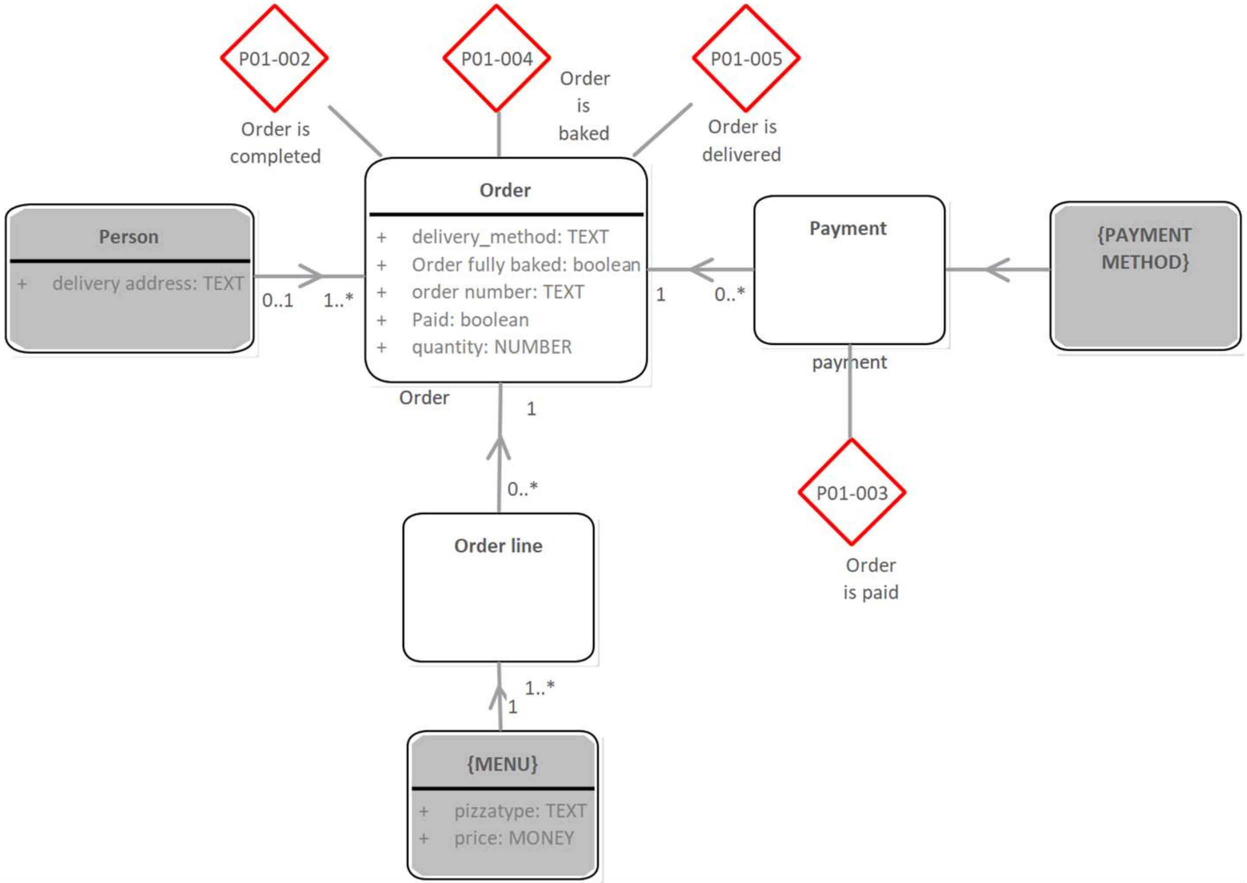


Source: Dietz e.a., 2021, p. 319

Legend Coordination Structure Diagram

- ▨ External actor
- □ Internal actor
- ◇ Transaction kind
- ◈ Fact bank

2) Organization Fact Diagram



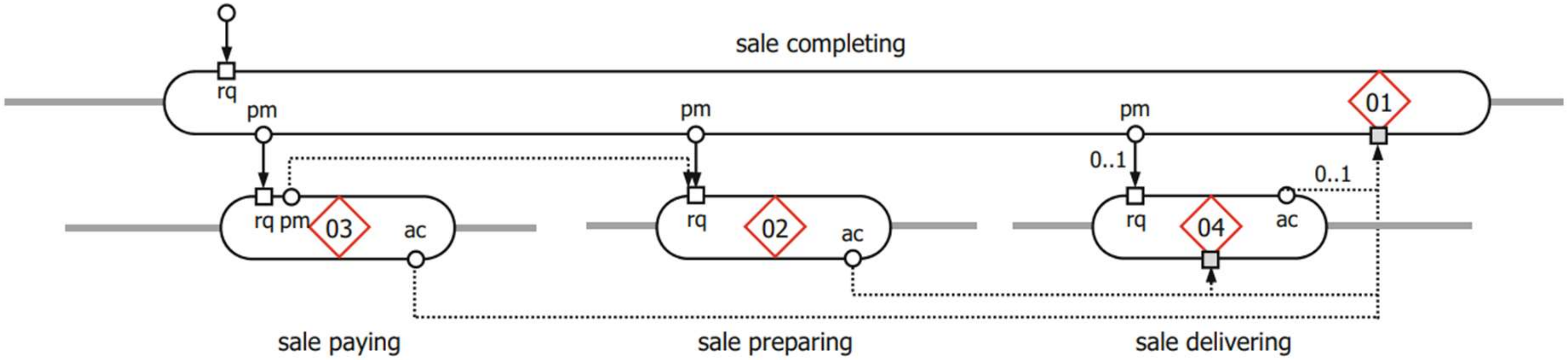
▨ Composite entity

□ Entity

◇ Original product

Diagram created by Author based on excercise in Dietz et al, p. 319

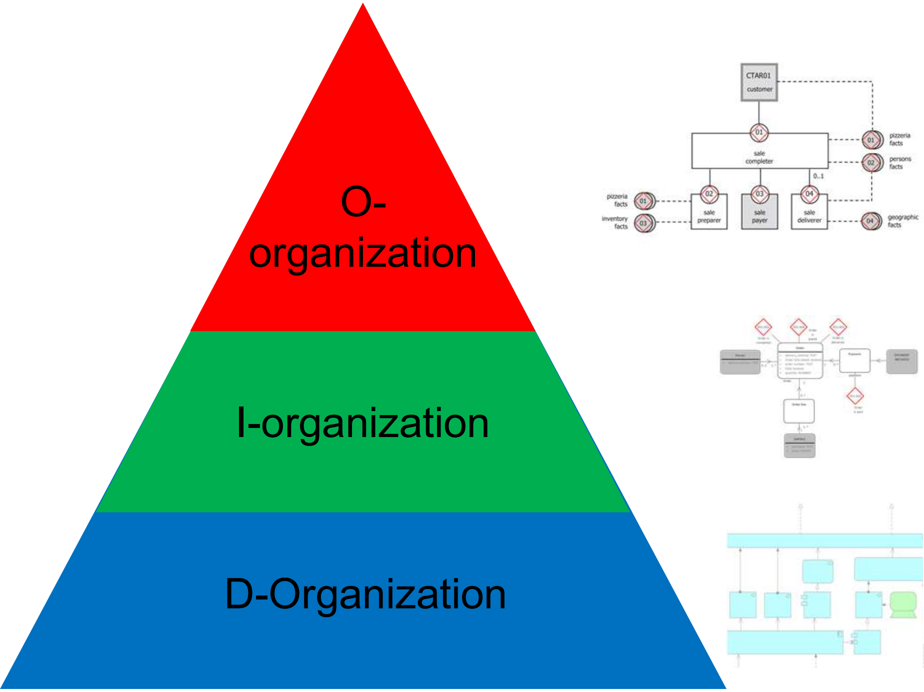
3) Process structure Diagram



PSD diagram for the Pizzeria case: Source: Dietz e.a., 2021, p. 320

Linking DEMO to SABSA

DEMO as input for Contextual and Logical layers



Source: Dietz 2020, P. 230

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Modes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management Support	Security of Sites, networks and Platforms	Security Operations Schedule

Legend

🟥 Performa layer

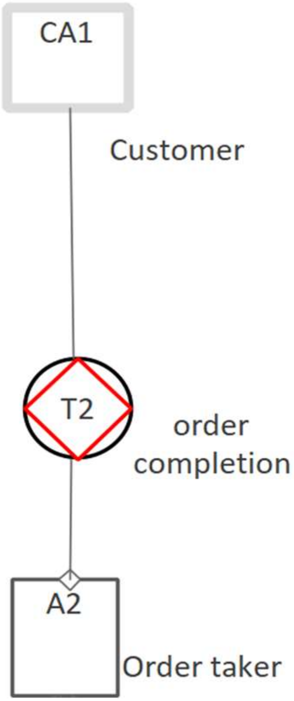
🟩 Informa layer

🟦 forma layer

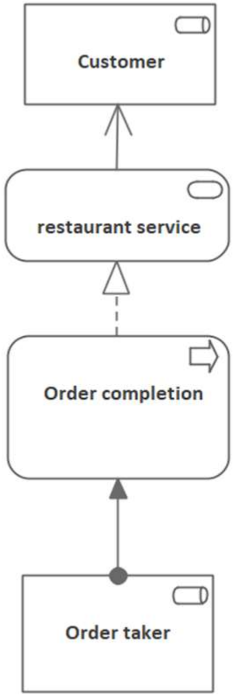
Inspired on: Enterprise security architecture, p. 42

Mapping DEMO to Archimate

CSD of a transaction

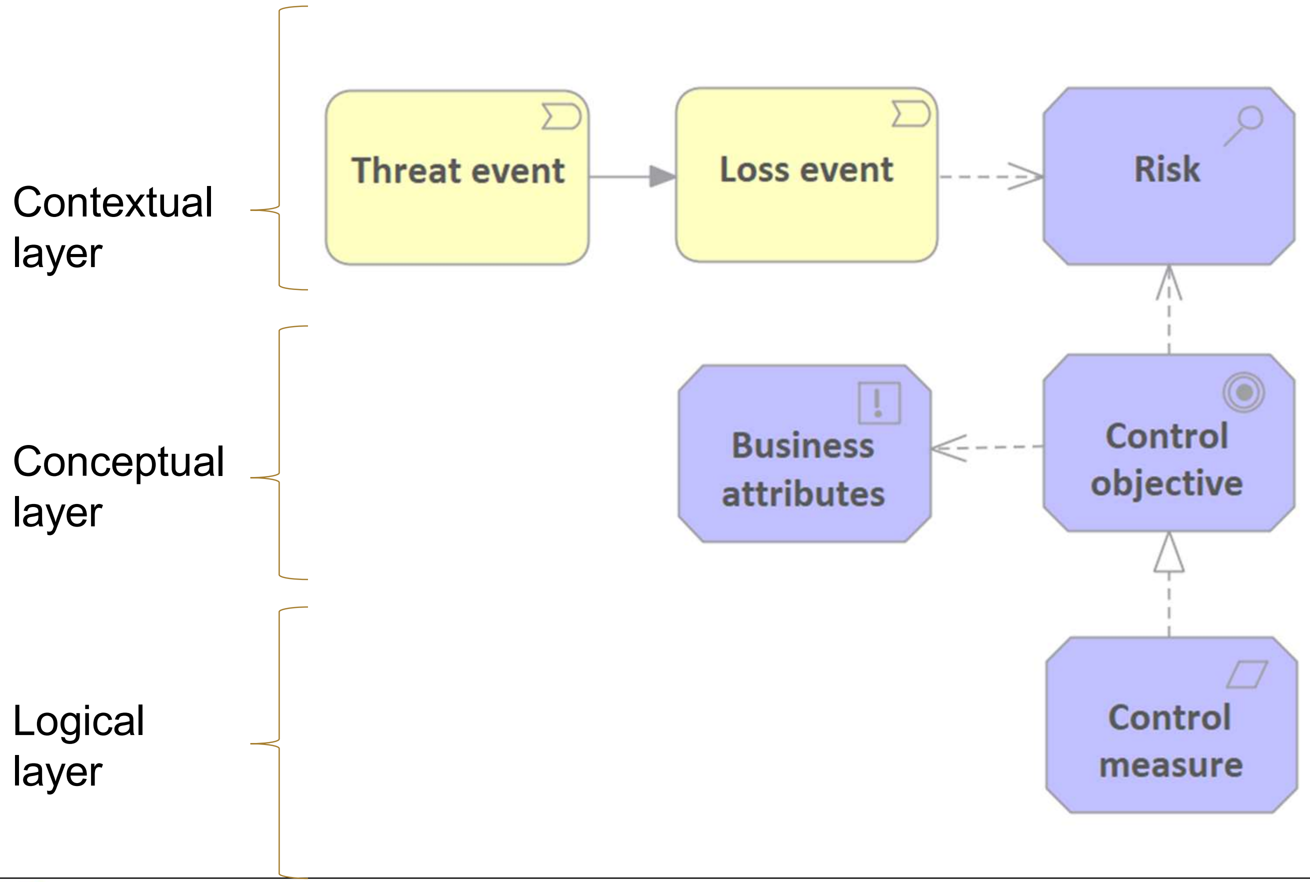


Archimate representation



DEMO	Archimate
Actor Role	Business Role
Transaction Kind	Business process
Organization boundary	Business Service
Entity	Business Object

Modeling risk and controls

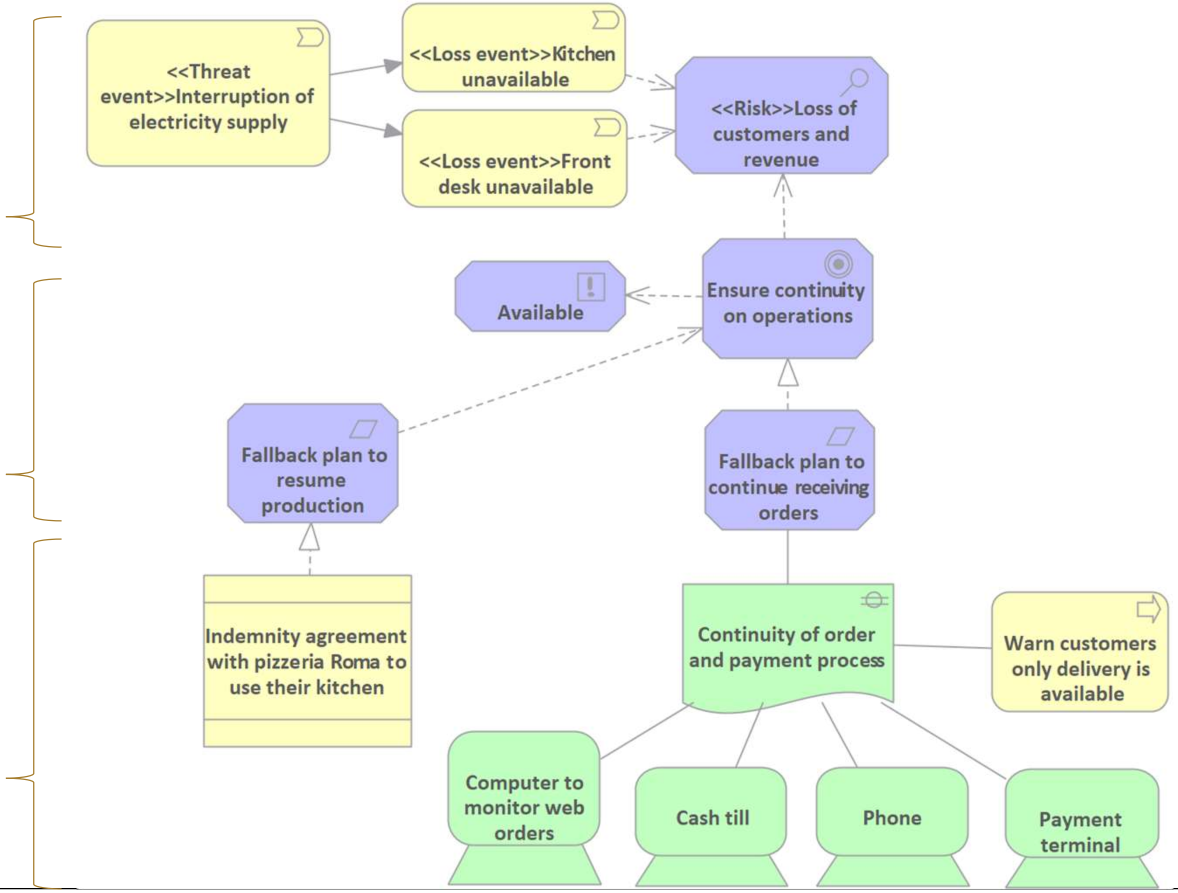


Modeling risk and controls - example

Contextual layer

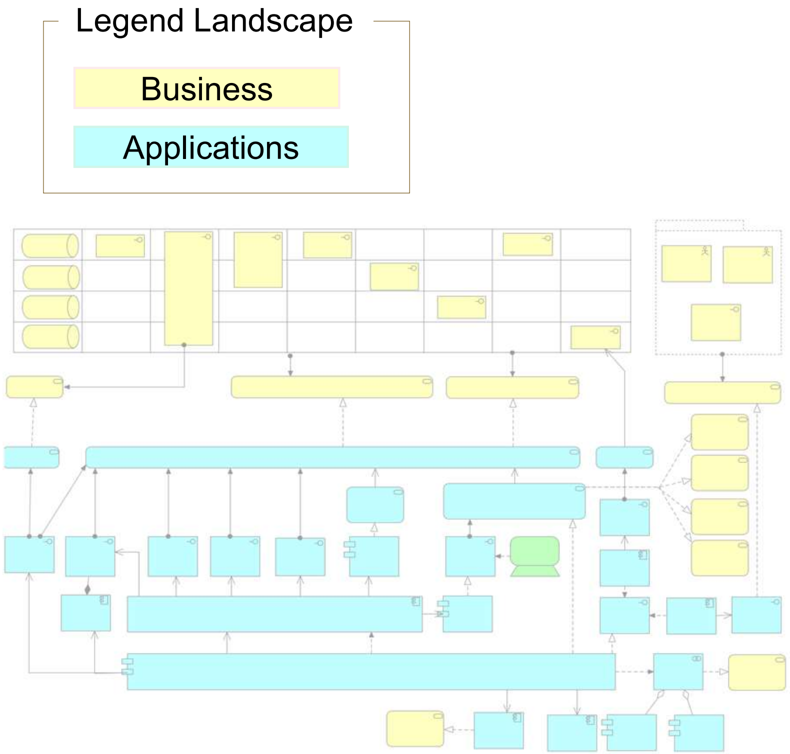
Conceptual layer

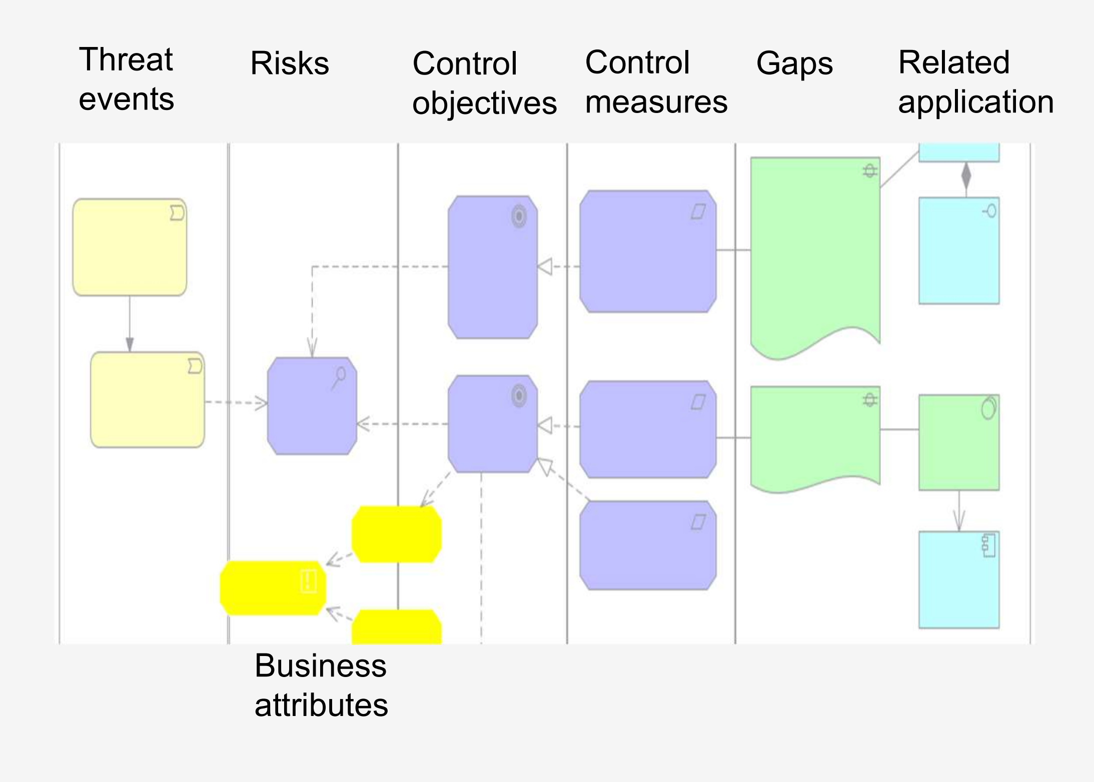
Logical and physical layers



<<Threat event>>Interruption of electricity supply
<<Loss event>>Kitchen unavailable
<<Loss event>>Front desk unavailable
<<Risk>>Loss of customers and revenue
Available
Ensure continuity on operations
Fallback plan to resume production
Fallback plan to continue receiving orders
Indemnity agreement with pizzeria Roma to use their kitchen
Continuity of order and payment process
Warn customers only delivery is available
Computer to monitor web orders
Cash till
Phone
Payment terminal

Modeling SABSA and DEMO in Archimate





Feedback from the use cases

Three use cases, with very positive feedback

- **Fast**
- **Clear view, relevant**
- **Reasons clarified**

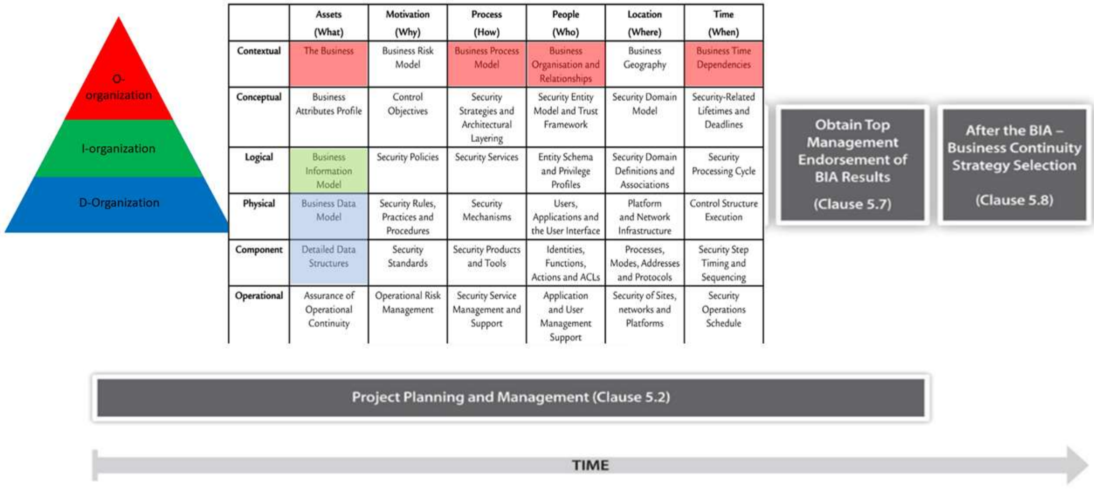
“This report states **why** we should switch asap to the new infrastructure (…) so we can make our most important processes high-available.”

“Clear desire to only collect information which was **relevant** for the interviewee.”

“I think it gives a clear overview where the pain points are, **without irrelevant details**. It describes **utility and necessity**“

“**Clear representation** of the process, which was easy to interpret by the interviewee.**”**

Conclusions


O-organization
I-organization
D-Organization
Obtain Top Management Endorsement of BIA Results (Clause 5.7)
After the BIA – Business Continuity Strategy Selection (Clause 5.8)
Project Planning and Management (Clause 5.2)
TIME

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Modes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management Support	Security of Sites, networks and Platforms	Security Operations Schedule

Outcome

- Obtain **processes**, at **right level of detail**
- collect **Risks,** Control objectives
- control measures, **implementation** and gaps
- Tested on **three organizations of multiple sizes**

Requirements

- Knowledge of SABSA
- Knowledge of DEMO
- Knowledge of Archimate
- Knowledge of BIA
- Tooling: It is possible to create native DEMO diagrams in a selection of enterprise architecture tools

Thank you

If you want a handout explaining the steps in the artifact and additional referential material, please scan this or go to the link below

https://forms.office.com/r/4bDqQtX1mt

Geert Boelens

geert@boelens-ict.be

+32 496 465 732

DEMO resources

- Trainings: https://ee-institute.org/education/educators/
- Books: https://ee-institute.org/endemo/publications/#books