BiZdesign

Enterprise Architecture-Based Risk and Security Modelling and Analysis

Henk Jonkers & Dick Quartel

GraMSec 2016
Lisbon, June 27, 2016

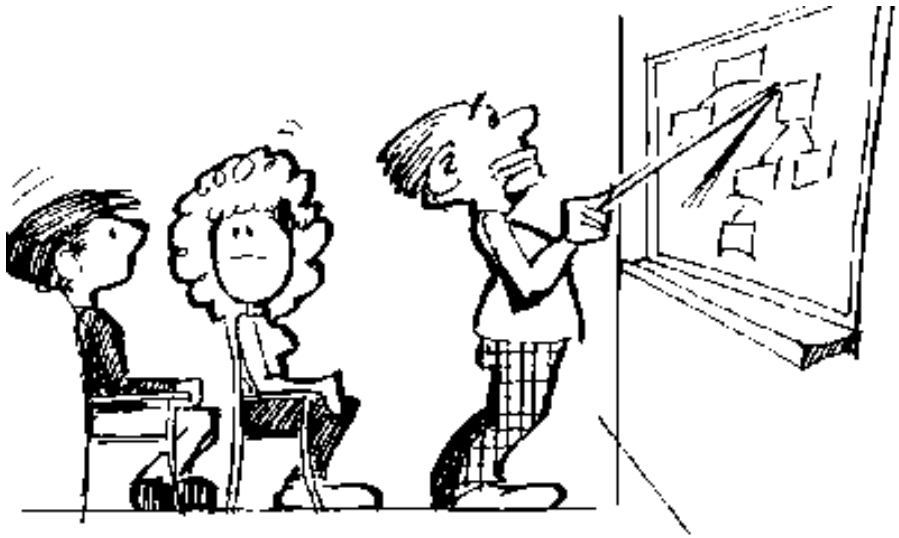
About BiZZdesign

- Global software company, founded in 2000
- Tools, methods & best practices, training, consultancy
- Collaborative business design platform for powerful, integrated modelling across multiple disciplines
- Strong roots in research and innovation
- Industrial partner in TRESPASS

Enterprise Architecture | Business Process Management | Portfolio Management | Business Model & Strategy | Governance, Risk & Compliance | Business Logic | Data Management

Agenda

- Why Enterprise Risk & Security Management (ERSM)?
- Enterprise Architecture & ArchiMate
- Risk & Security Modelling in ArchiMate
- The ERSM Cycle
- Risk Analysis & Visualisation
- Example & Demo
- Summary & Conclusions



Problem Statement

- Organizations are increasingly networked and thus more complex
- Attacks on information systems are getting more sophisticated
  - Attacks use digital and physical access, and social engineering
- Traditional risk management methods cannot handle the resulting complexity

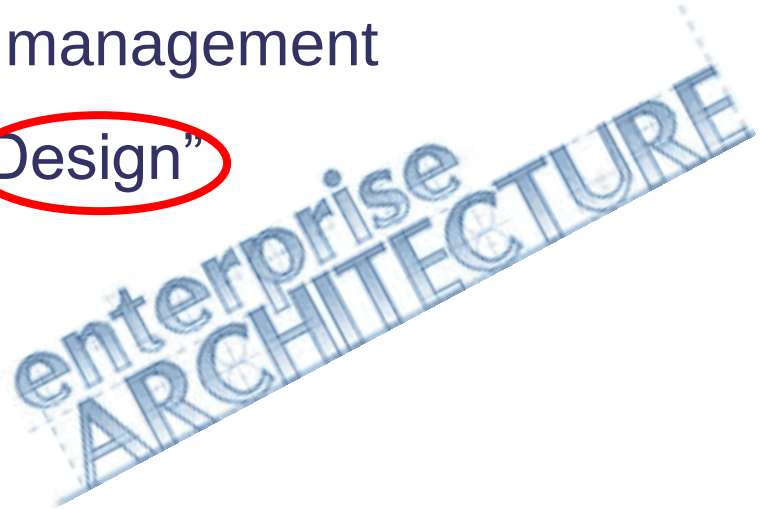
Limitations of Traditional Approaches

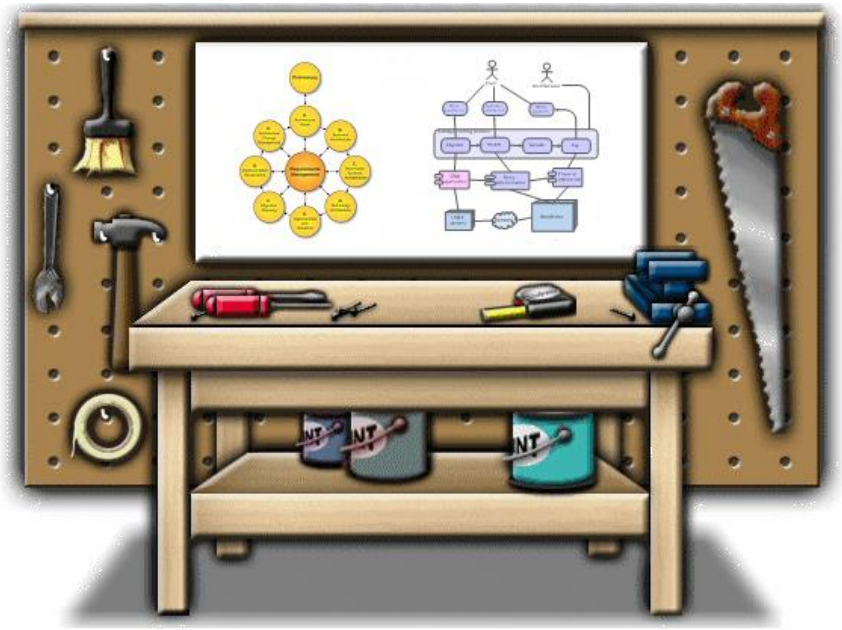
- Existing information security and risk management methods do not systematically identify potential attacks
  - They are based on, e.g., checklists, heuristics and experience
  - Security controls are applied in a bottom-up way
  - They are not based on a thor
  - No explicit definition of securi
- Focus on just IT/informati
  - They have difficulties in deali complex attacks on socio-tec systems, which combine phys digital access, as well as soci
- Focus on preventive secur
  - Corrective and curative contr are not considered

→ *Trade-off between security, costs, and usability (Avoid "security overkill")*

Enterprise Risk & Security Management

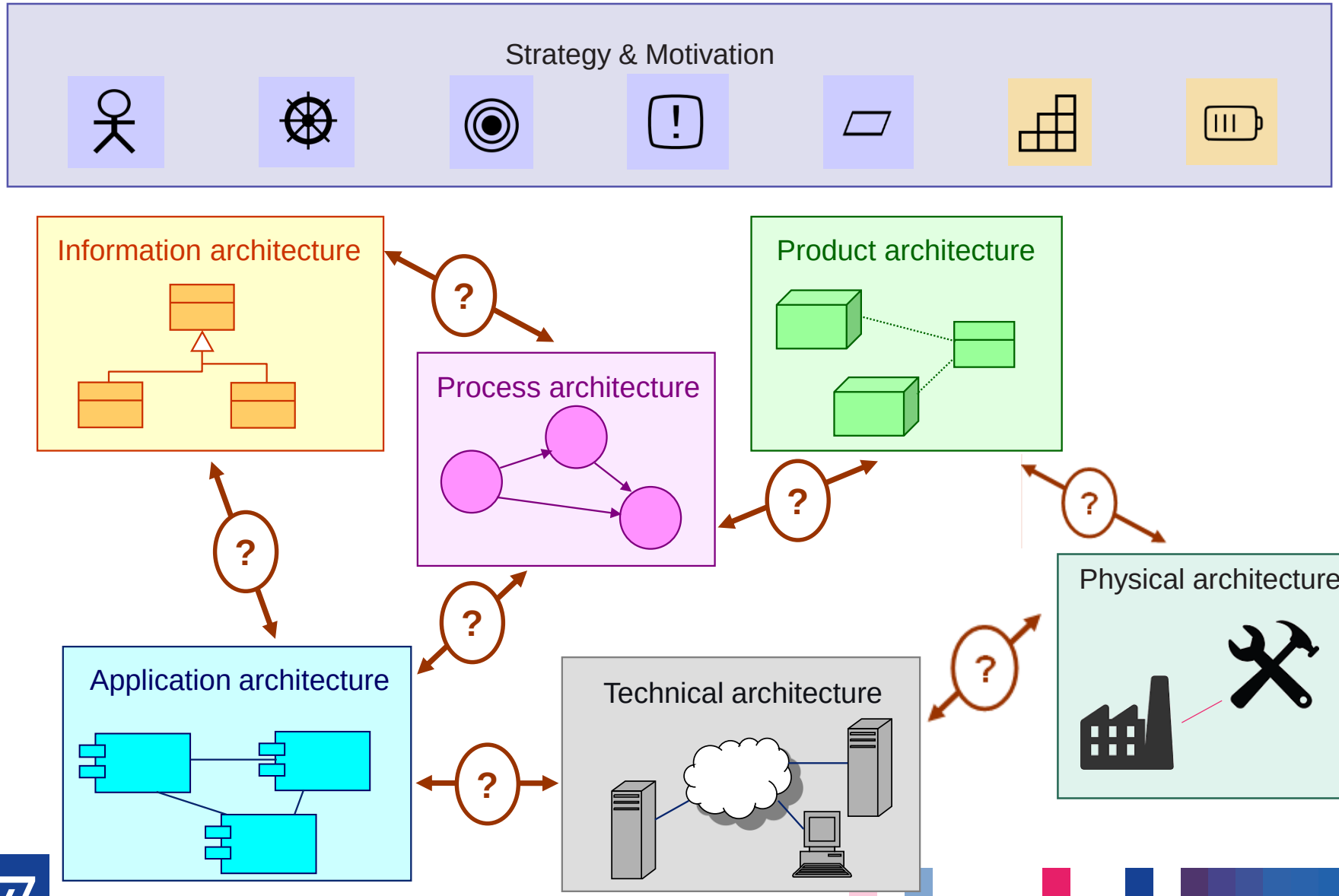
- Integral approach to security: protection of business, information, application and technology assets
- Structured identification and analysis of risks and vulnerabilities
- Supports strategic risk management
- Supports “Security by Design”



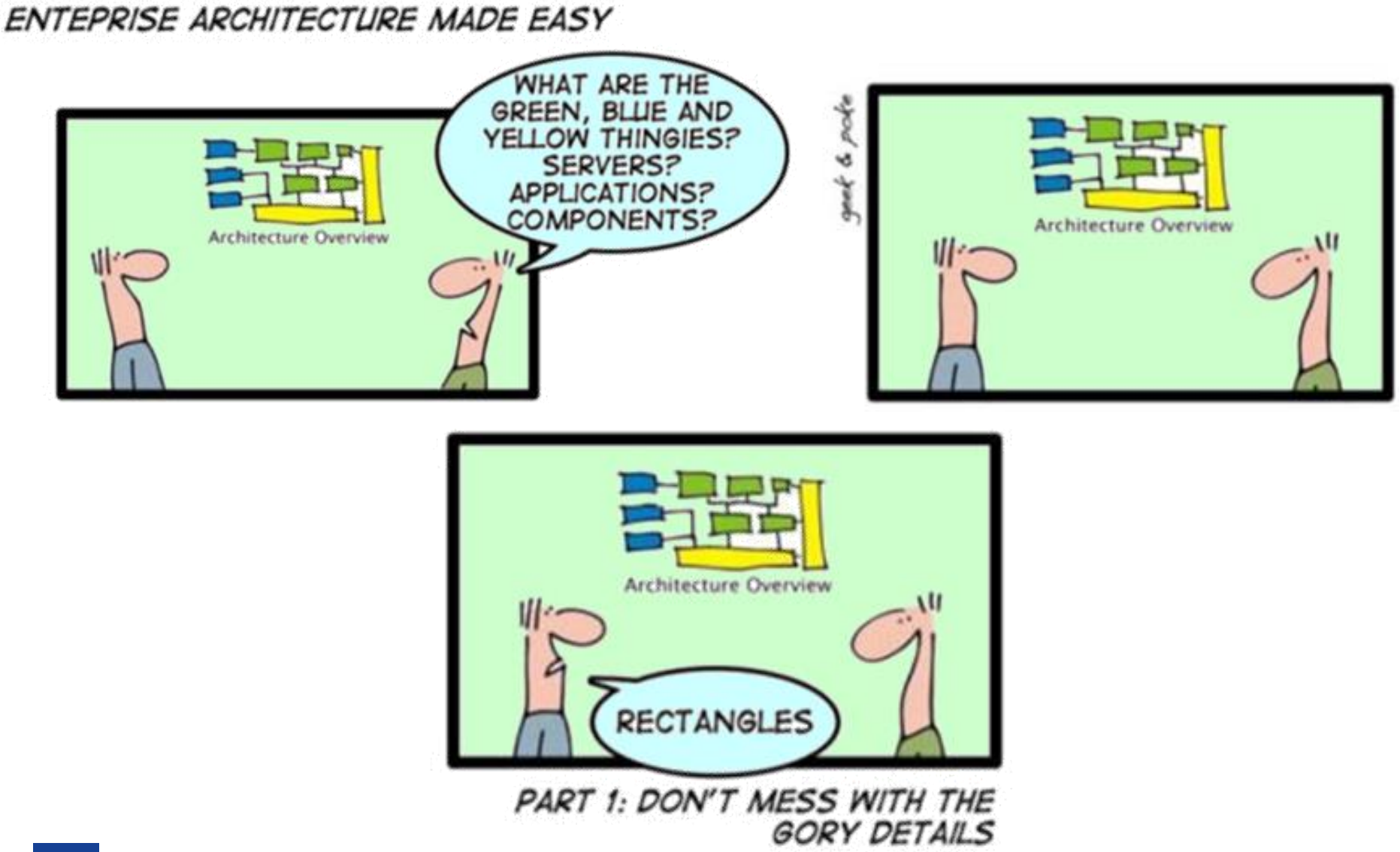


Enterprise Architecture & ArchiMate

EA / ArchiMate: Integrated Models



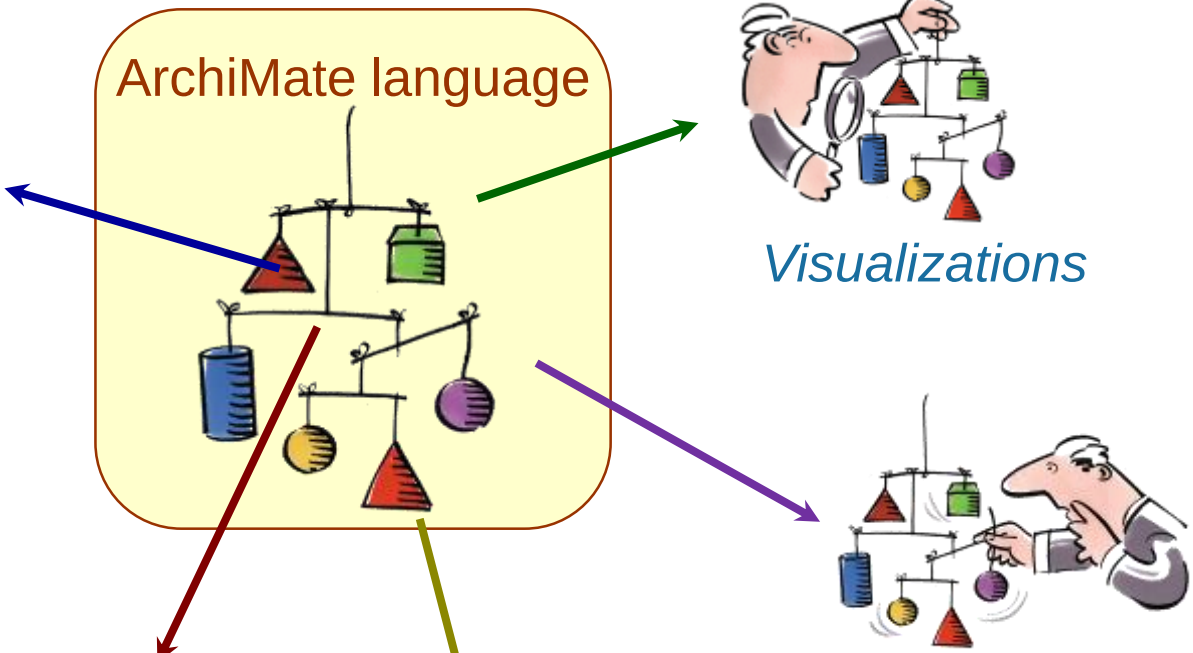
The Case for Enterprise Architecture



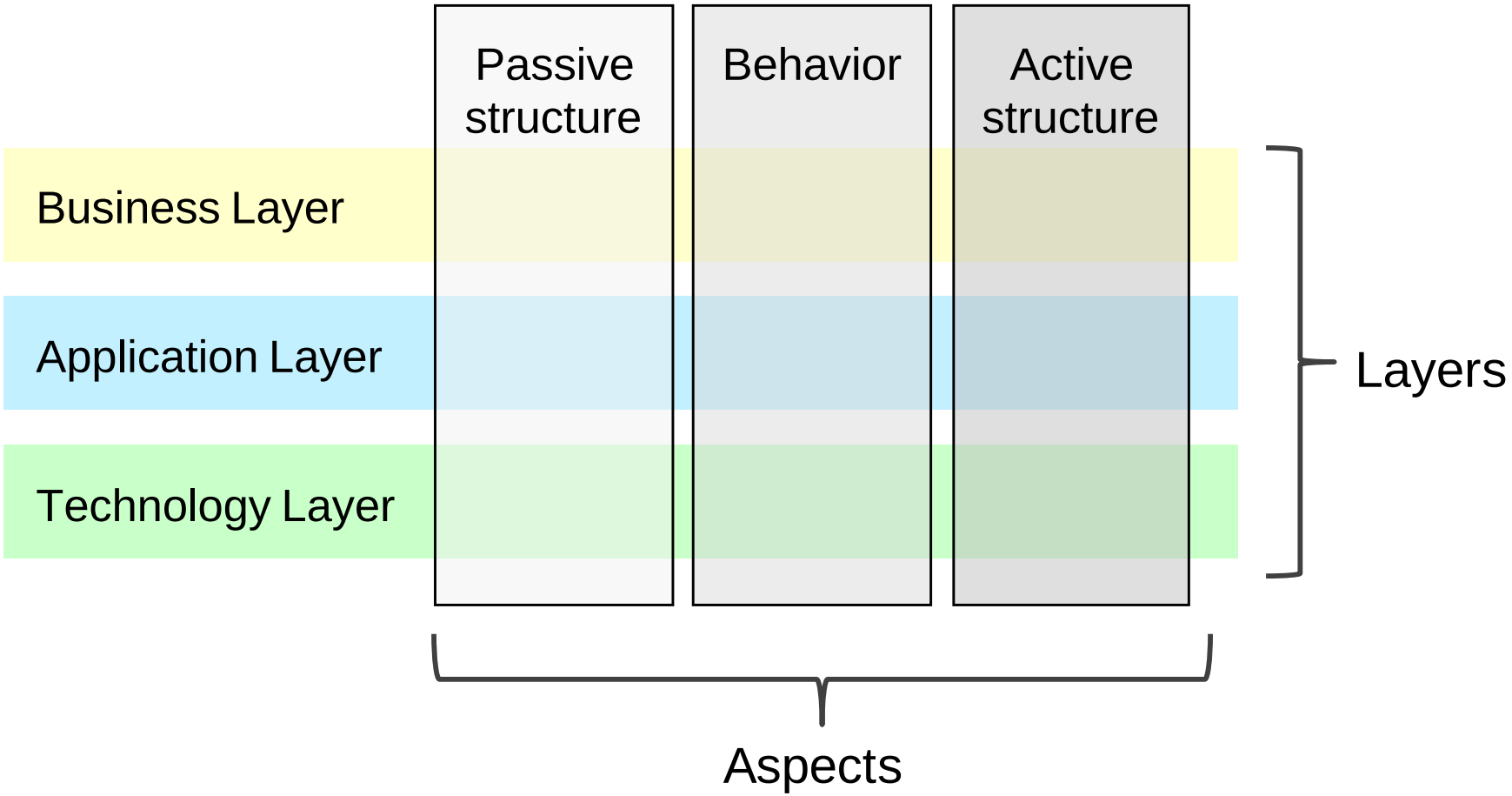
The ArchiMate Language

A basis for

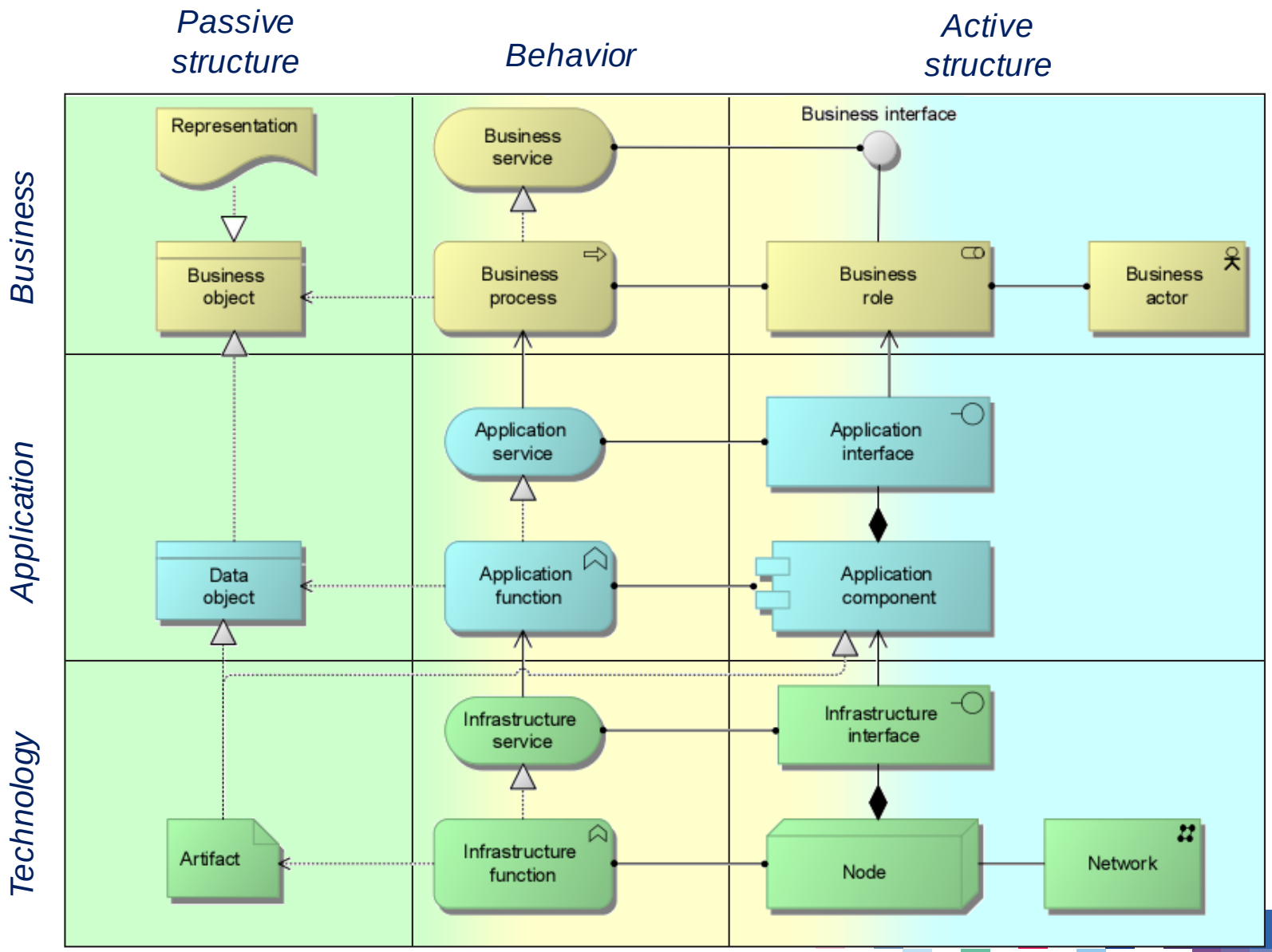
High-level modelling *within* domains



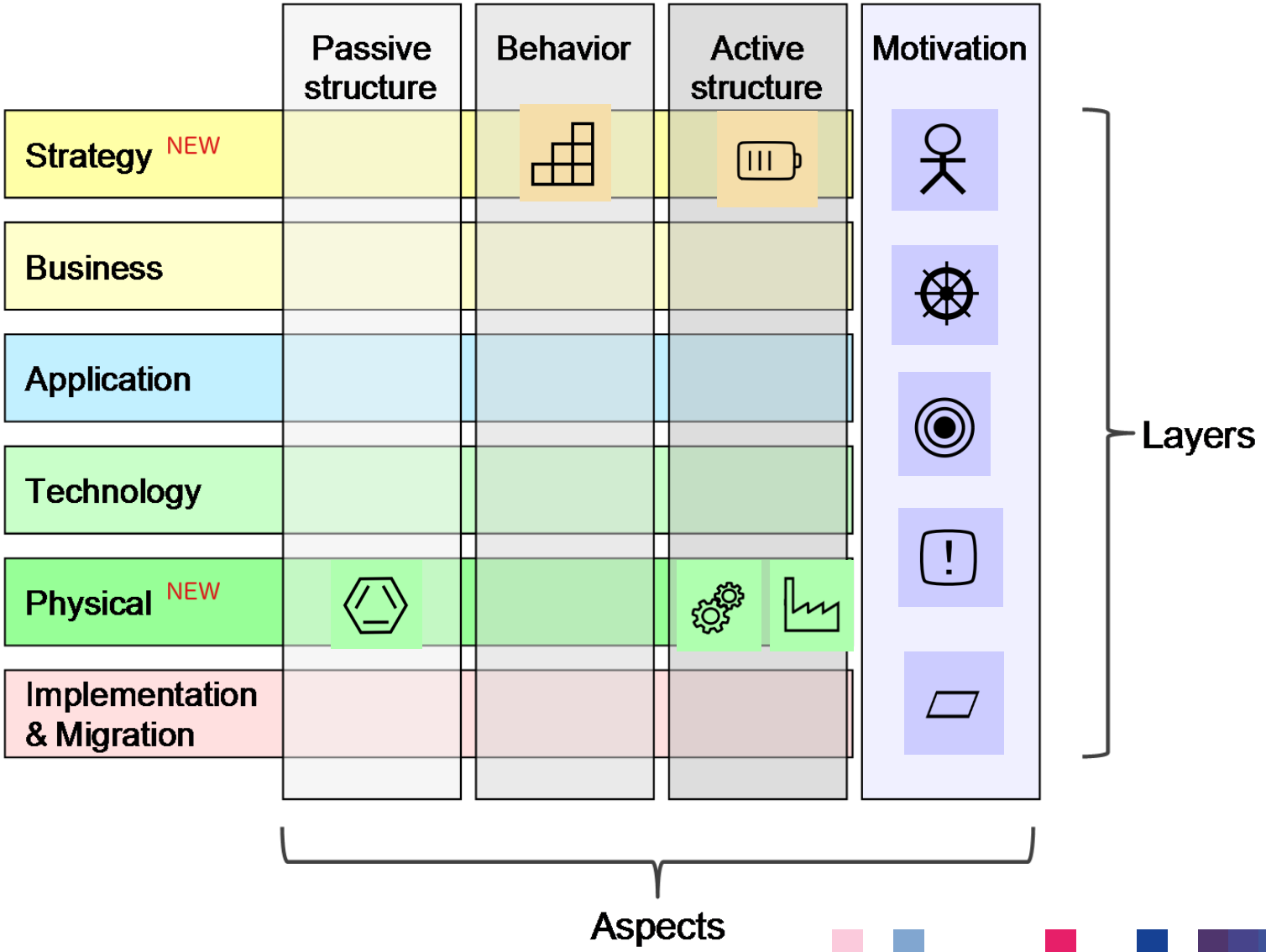
ArchiMate Core Framework

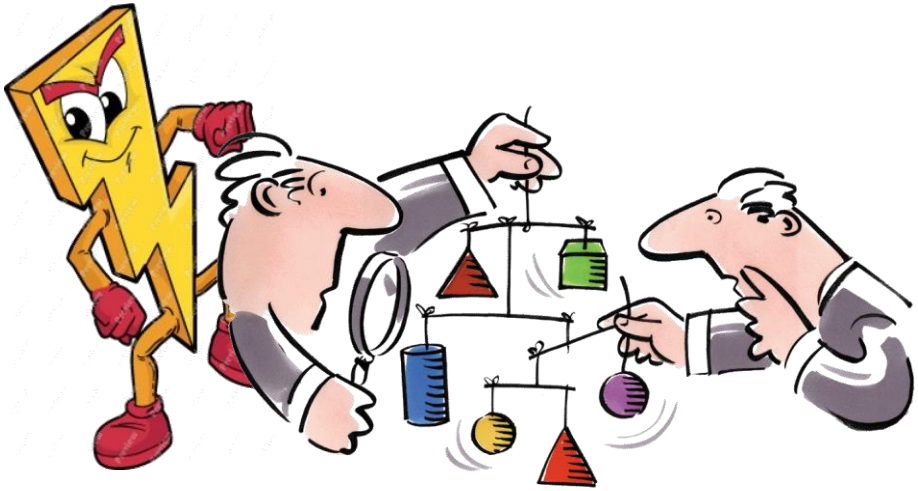


ArchiMate Core Language



ArchiMate 3.0 Framework

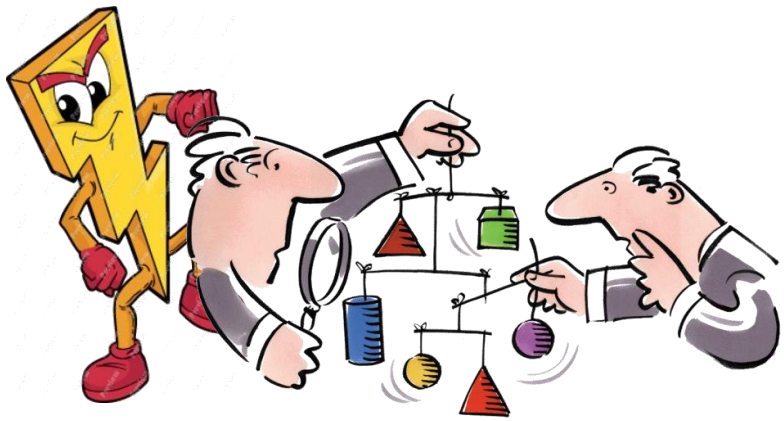




Risk & Security Modeling with ArchiMate

ArchiMate Risk Project

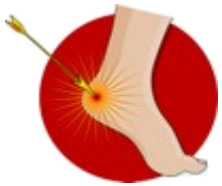
- Collaboration of ArchiMate Forum and Security Forum
- Two areas of concern:
  - Risk analysis
  - Security deployment (risk mitigation)
- Investigate how (specializations of) existing ArchiMate concepts (Core and extensions) can be used
- Inspired on well-established risk and security standards and frameworks, including COSO, ISO 27001, FAIR, SABSA
- White paper published



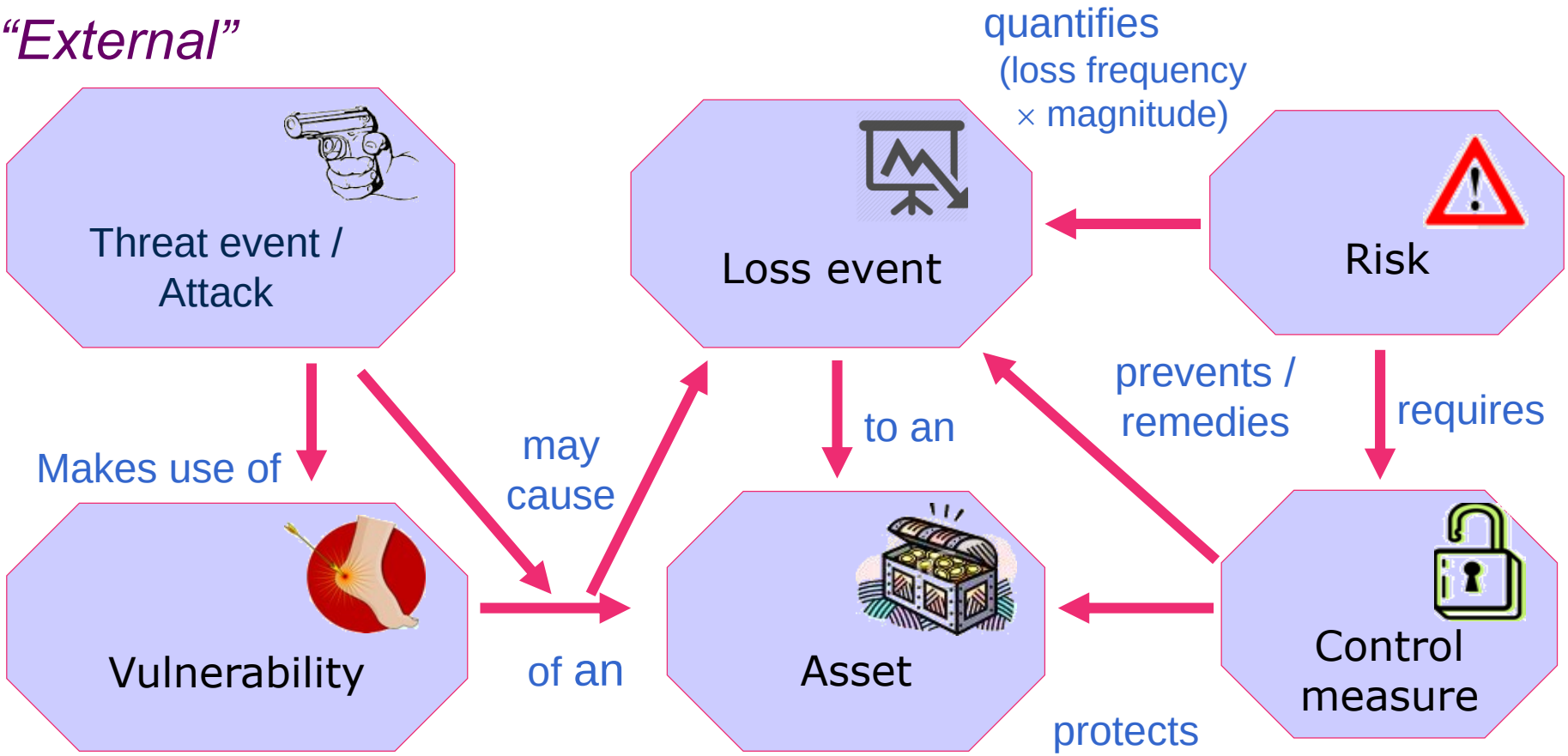
Concepts

- Risk
- Threat (event)
- Threat agent
- Attack
- Loss event
- Vulnerability
- Domain
- Control objective
- (Required) Control measure
- Asset (at risk)
- (Risk / Security) Policy
- (Risk / Security) Principle

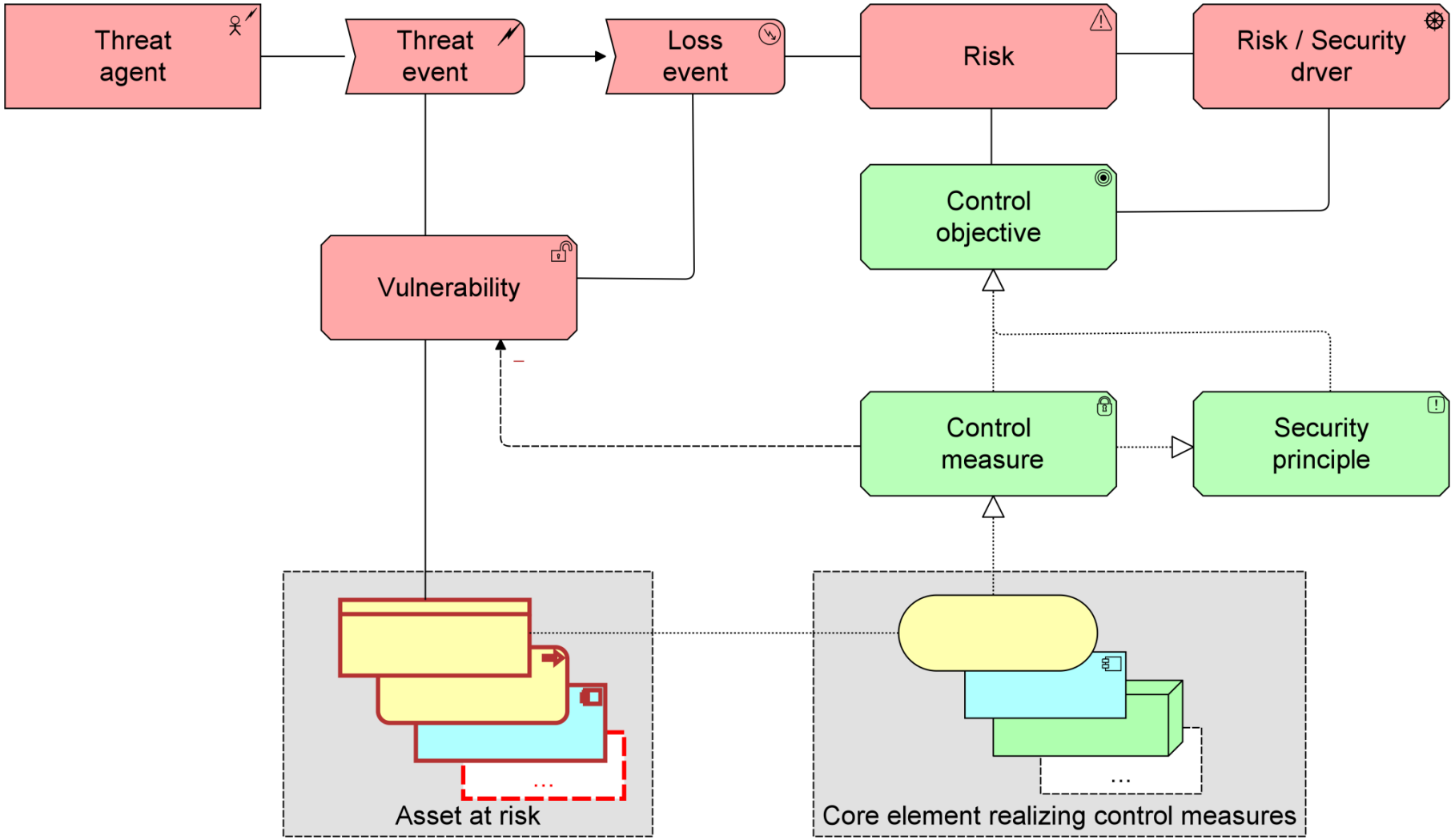



Main Risk & Security Concepts (Informal)



A “Risk Overlay” for ArchiMate



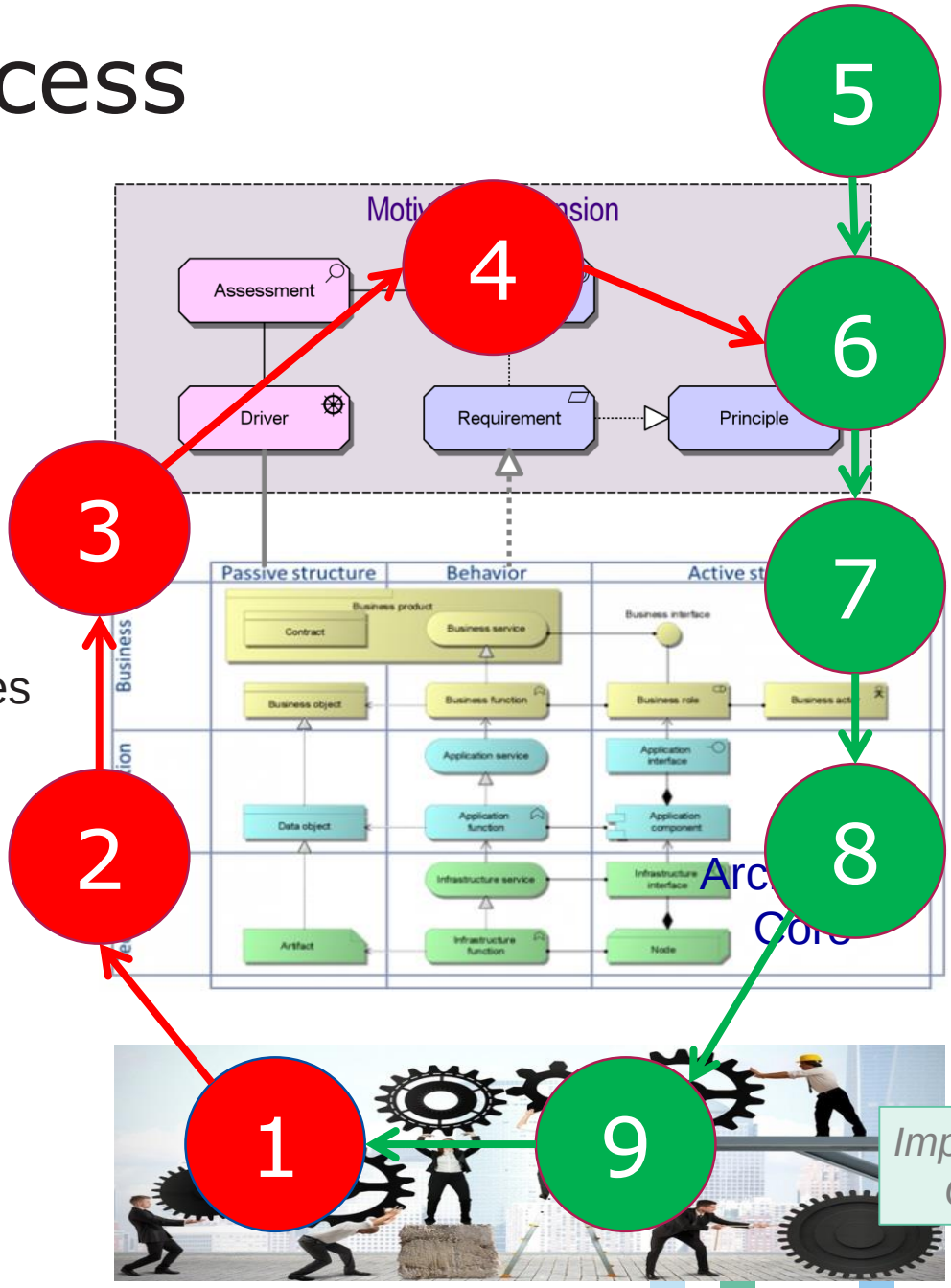
ERSM Process

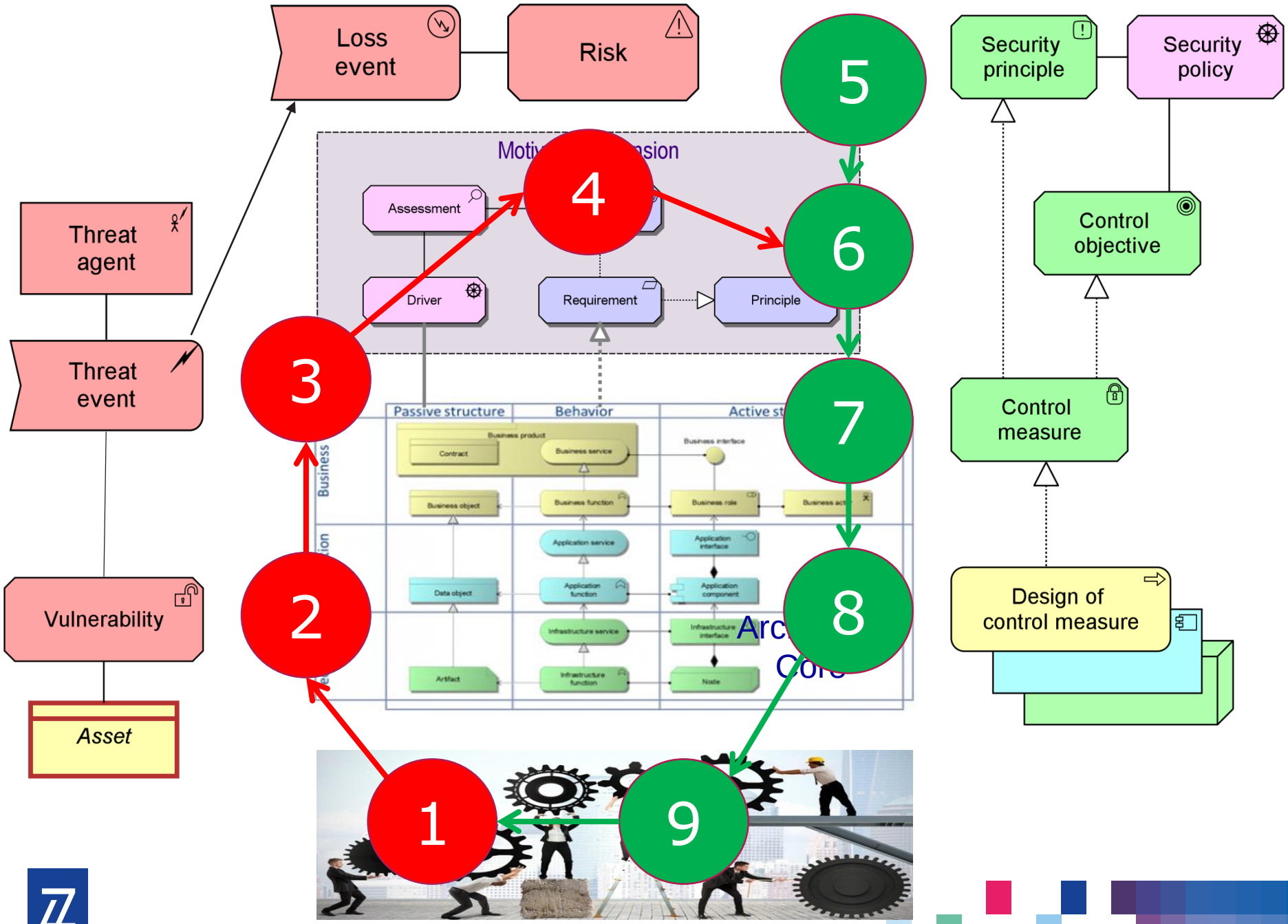
Risk assessment

1. Monitoring
2. Vulnerabilities
3. Threats
4. Risks

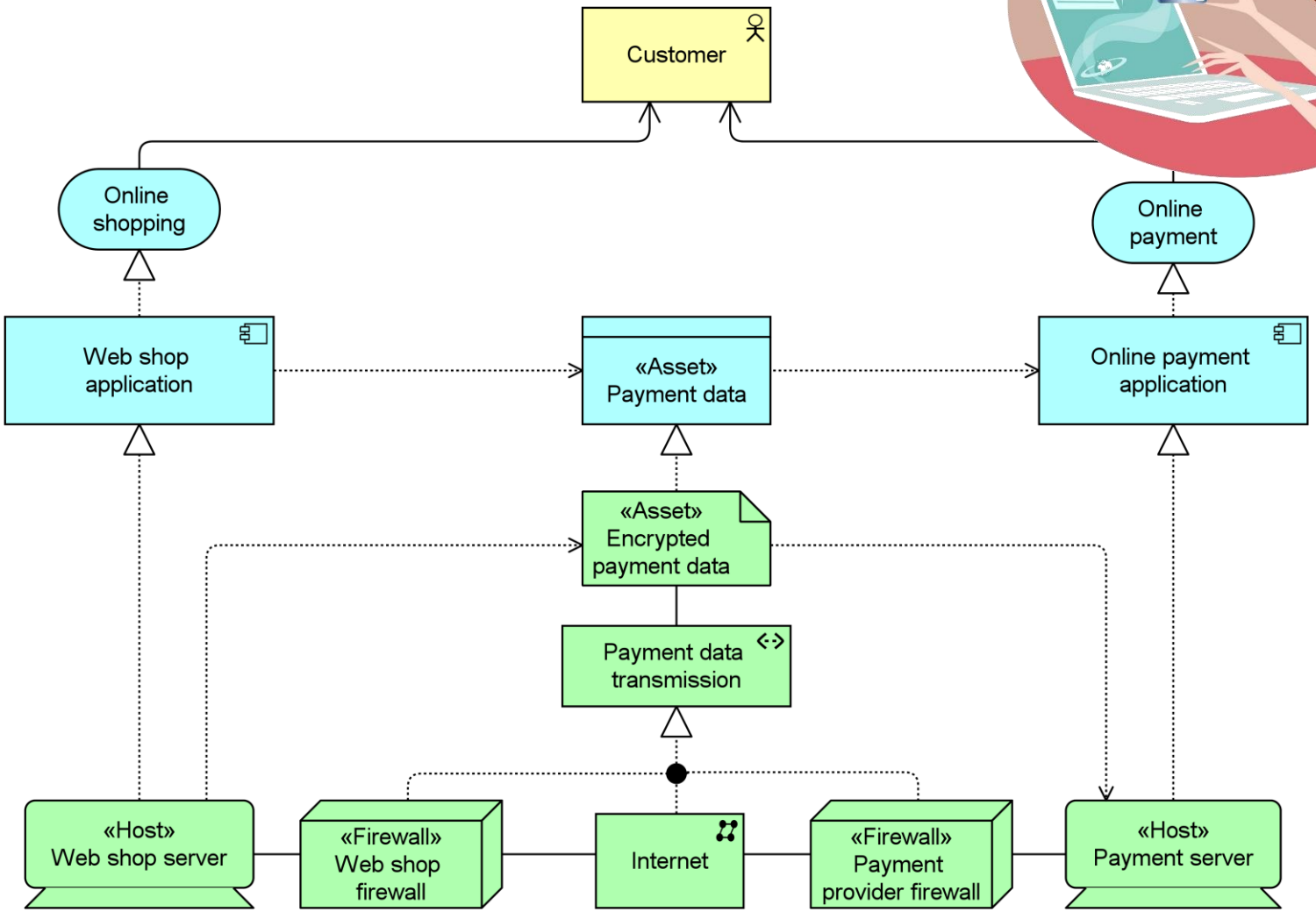
Security deployment

5. Security policy & principles
6. Control objectives (Security requirements)
7. Requirements for control measures
8. Design of control measures
9. Operational control measures



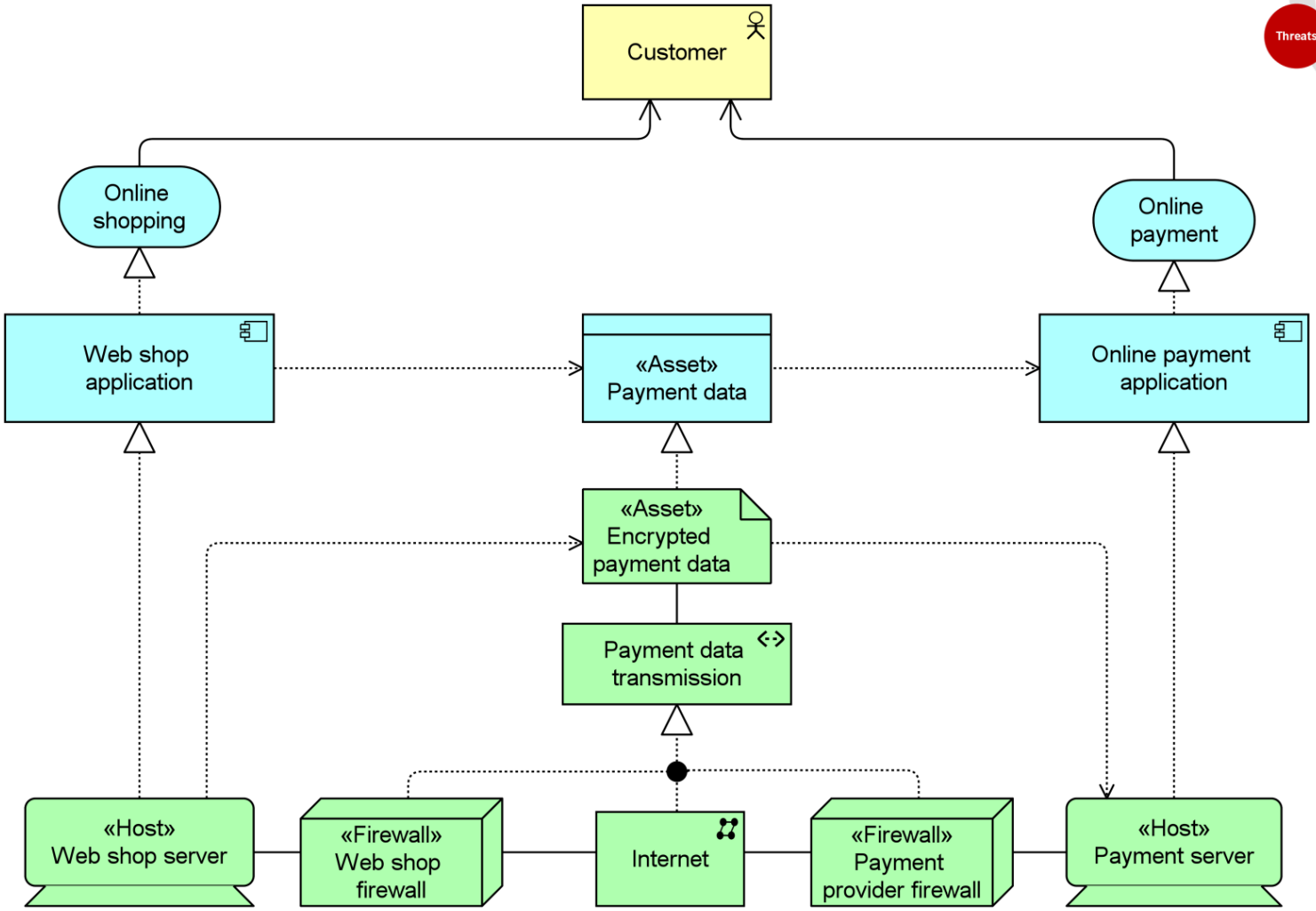

Loss event
Risk
Threat agent
Threat event
Vulnerability
Asset
Assessment
Driver
Requirement
Principle
Passive structure
Behavior
Business product
Contract
Business service
Business object
Business function
Application service
Data object
Application function
Infrastructure service
Artifact
Infrastructure function
Business interface
Business role
Application interface
Application component
Infrastructure interface
Node
1
2
3
4
5
6
7
8
9
Security principle
Security policy
Control objective
Control measure
Design of control measure

Example: Online Payment

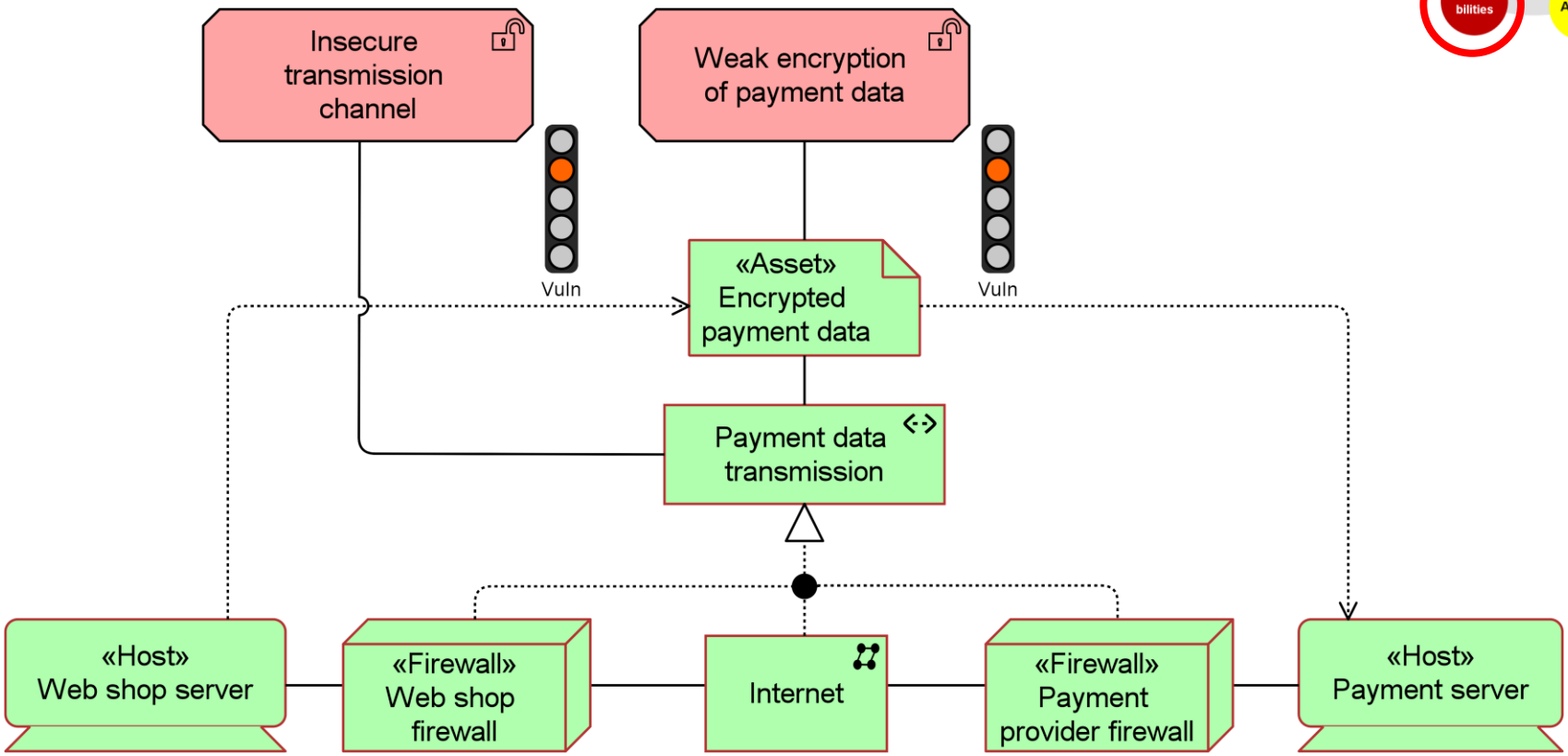


Assets


Security Policies & Principles
Control Objectives
Risks
Required Control Measures
ERSM
Threats
Design of Control Measures
Vulnera bilities
Assets

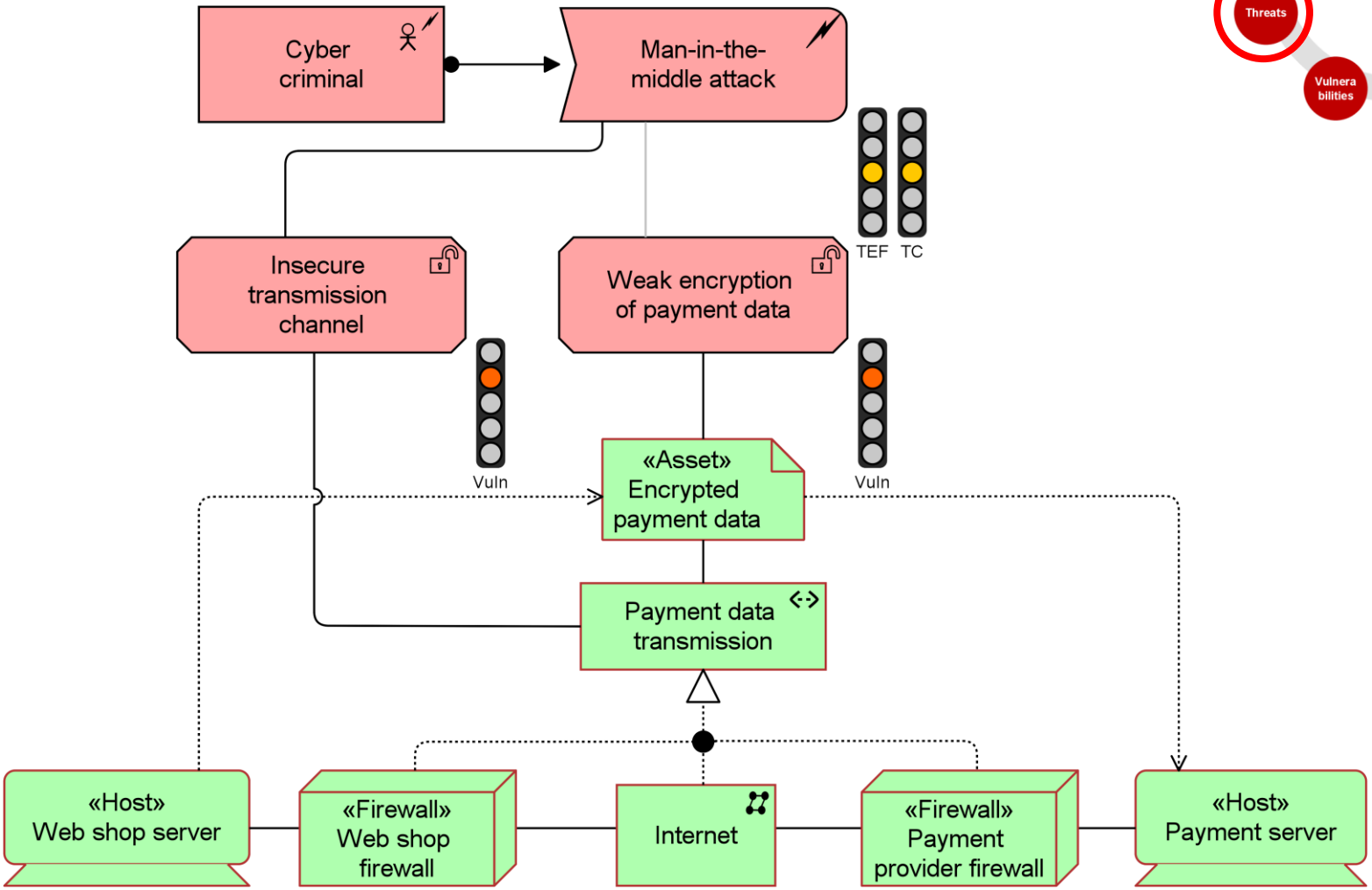

Customer
Online shopping
Online payment
Web shop application
«Asset» Payment data
Online payment application
«Asset» Encrypted payment data
Payment data transmission
«Host» Web shop server
«Firewall» Web shop firewall
Internet
«Firewall» Payment provider firewall
«Host» Payment server

Vulnerabilities

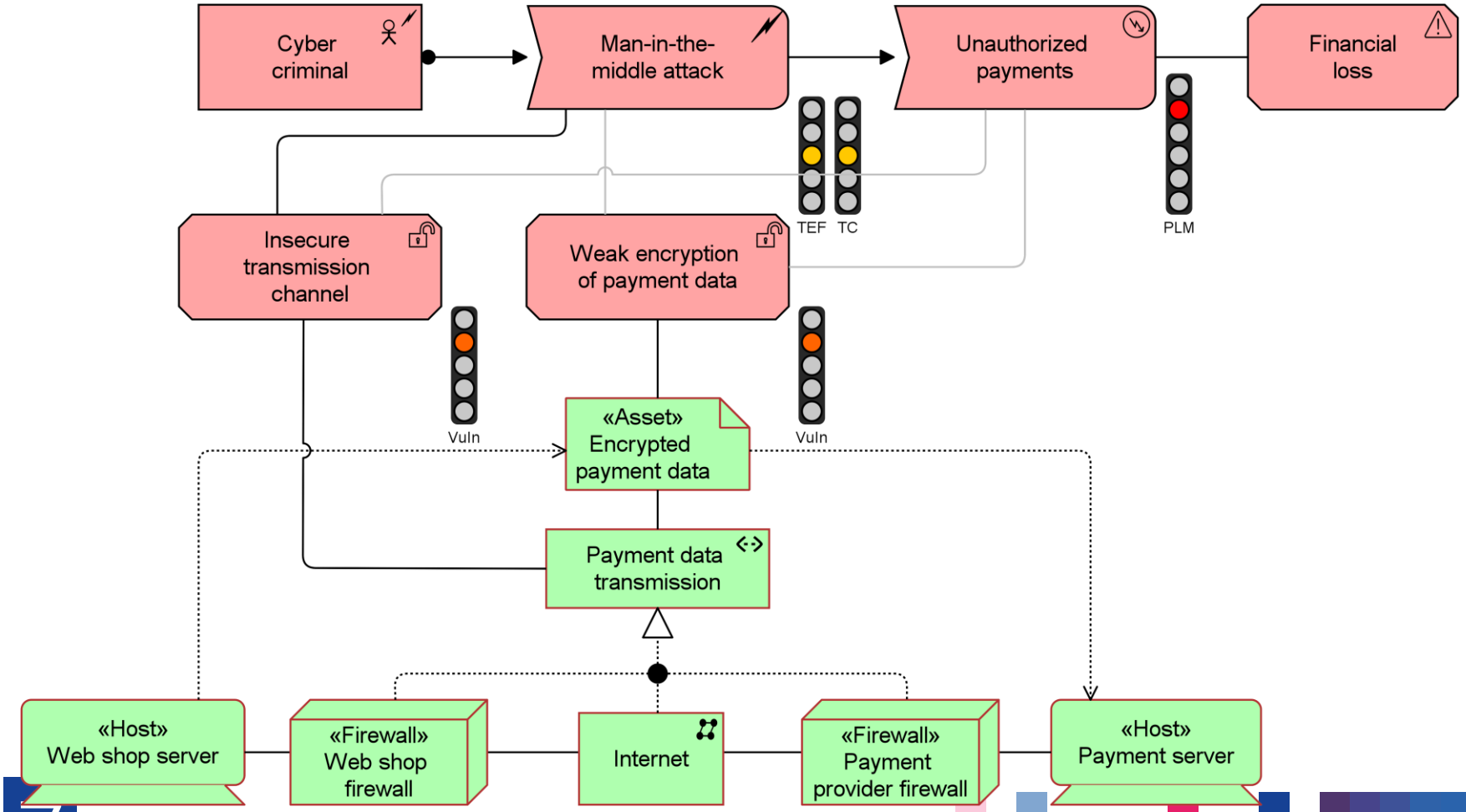


Threats

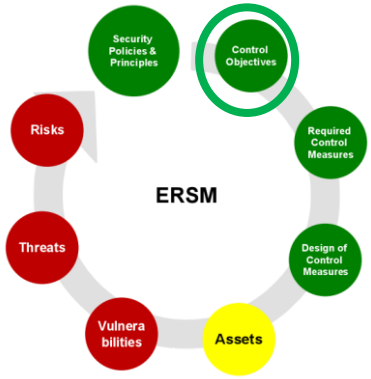

Security Policies & Principles
Control Objectives
Risks
Required Control Measures
ERSM
Threats
Design of Control Measures
Vulnera bilities
Assets

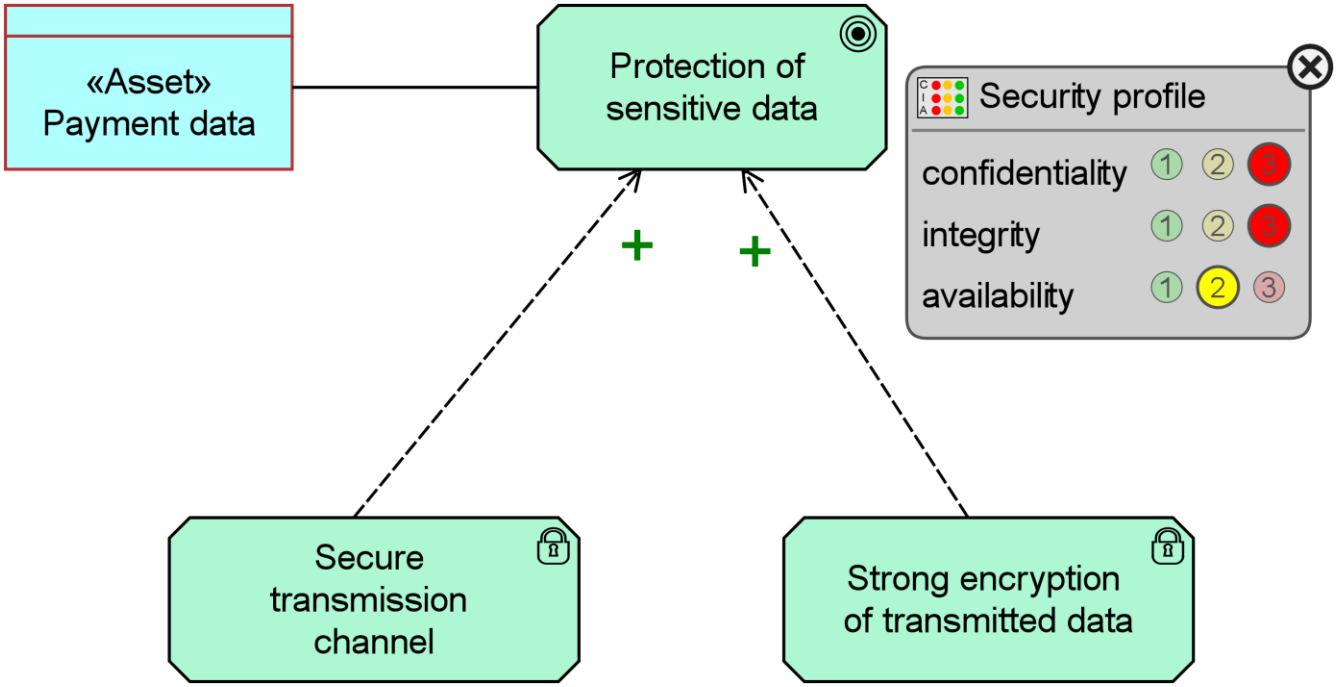

Cyber criminal
Man-in-the-middle attack
TEF
TC
Insecure transmission channel
Weak encryption of payment data
Vuln
Vuln
«Asset» Encrypted payment data
Payment data transmission
«Host» Web shop server
«Firewall» Web shop firewall
Internet
«Firewall» Payment provider firewall
«Host» Payment server

Risk Assessment

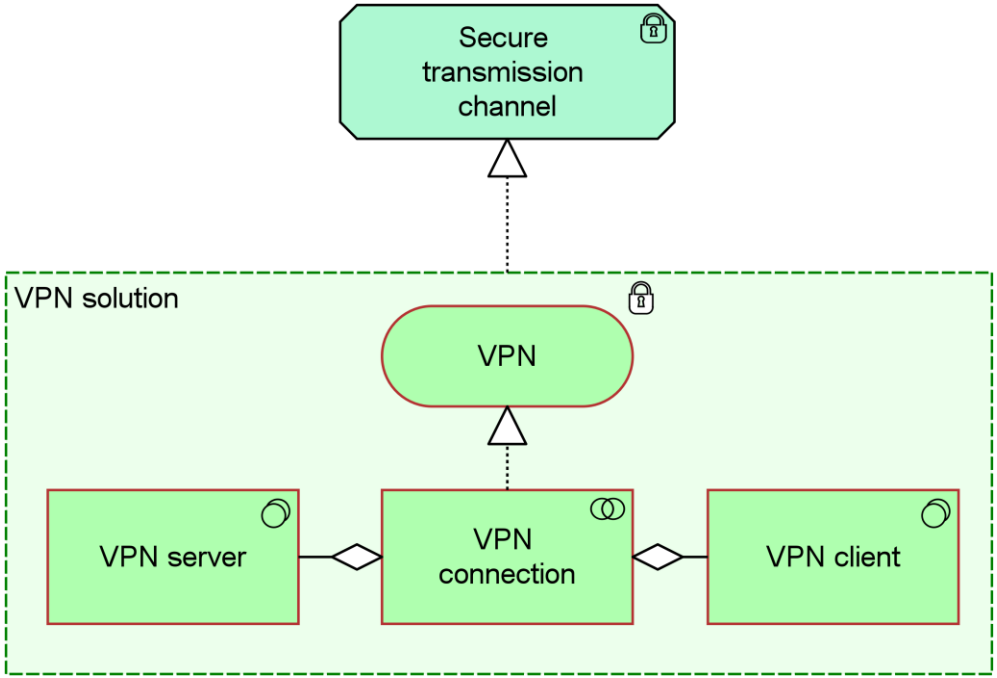


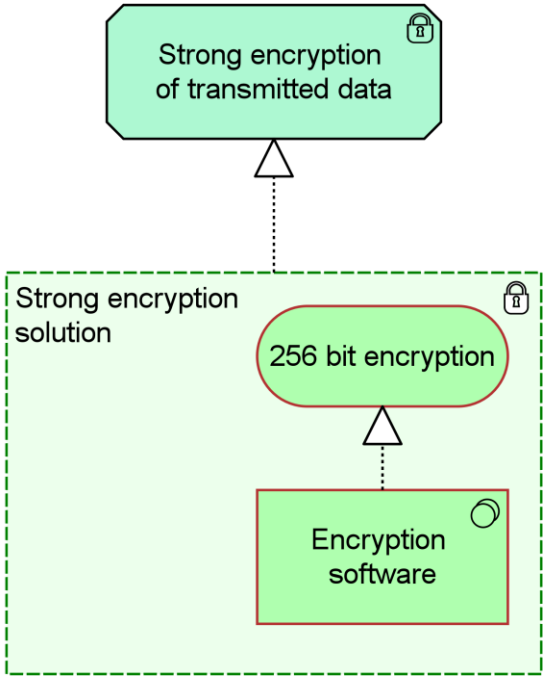
Control Objectives



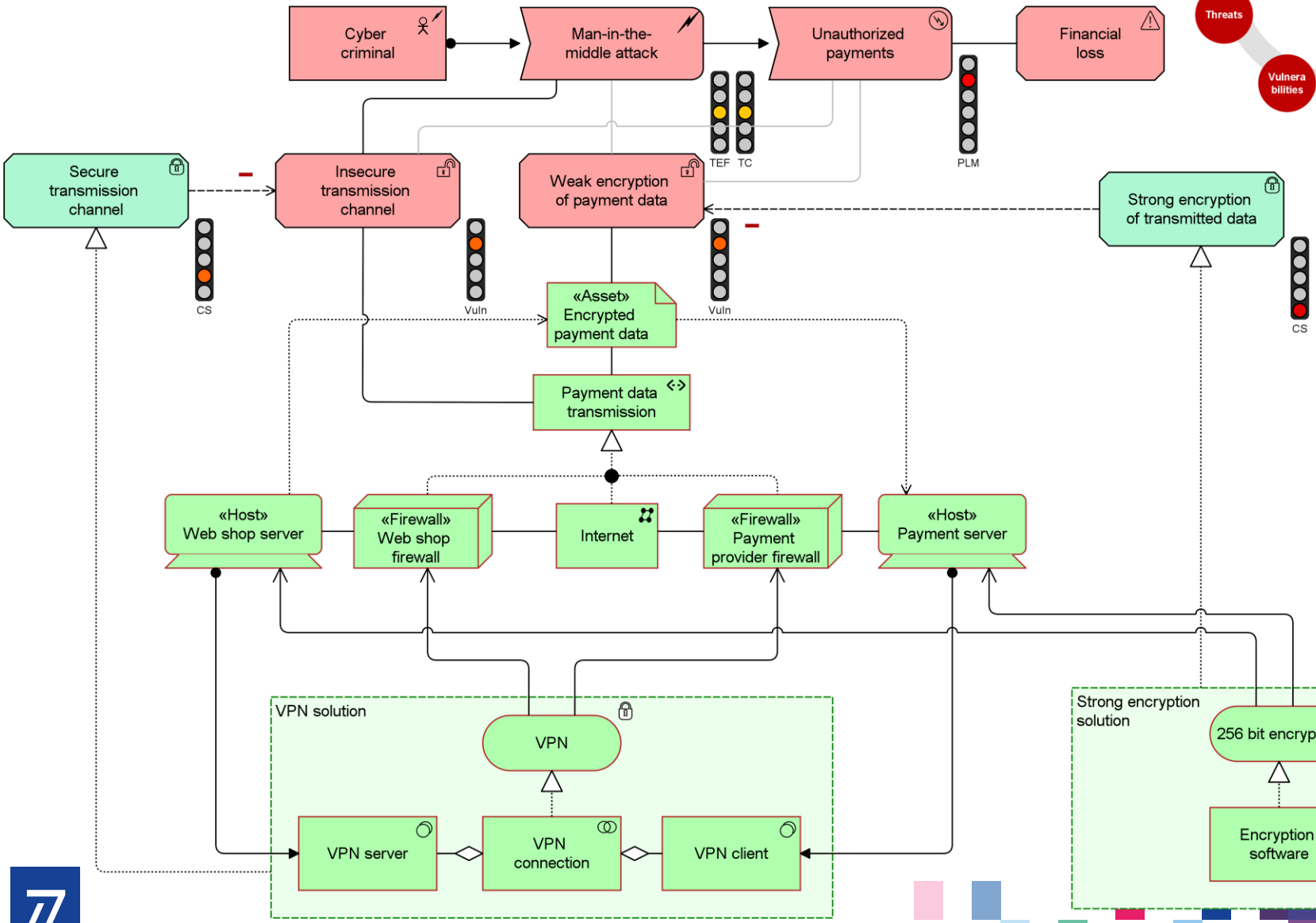


Design of Controls





Deployment of Controls



Conclusions

- Current risk management approaches, working in isolation, fall short in the complexity of current organizations
- The ArchiMate language provides the hooks for integrated risk & security modeling, integrated with EA
- Specializations of existing ArchiMate concepts suffice for risk and security modelling
- ArchiMate 3.0 offers new possibilities for modelling, among others, physical risk and security
- Risk & security-enhanced ArchiMate models support risk analysis and visualization, and “Security by Design”