Secure Application Development

SecAppDev 2016

Certification of Application Security

Secure Application Development

ICT CONTROL
Your Trusted Advisor

Solvay Brussels School Economics & Management

Cogentas.ca
Application Security Institute

Secure Application Development

Learning objectives

- Introduce a new paradigm to build and verify software security based on new ISO/IEC Standard
- Understand how to create a Security Design pattern which can be tracked through the development process
- Describe methods to certify application security through the review of Application Security Controls (ASC)

Certification of Application Security

Speaker

Georges ATAYA

Career Summary

- Professor and Academic Director (SBS-EM)
- Managing Director ICT Control advisory firm
- Past International Vice President at ISACA
- Past Partner Ernst & Young
- Deputy International CIO ITT World Directories
- Previously Project Manager and Senior IT Auditor

Expertise Summary

- IT Governance (development of Cobit 4 and COBIT 5)
- IT Governance and Value governance (co-author VALIT and supervision CGEIT BOK)
- Information Security Management (Co-author CISM Body of Knowledge)
- IT Audit and Governance
- Information security and risk
- Strategy and Enterprise Architecture and IT Sourcing

Education/ Certification

- Master in Computer Science (faculty of Sciences ULB)
- Postgraduate in Management (Solvay Brussels School ULB)
- CISA, CISM, CRISC, CISSP, CGEIT

Secure Application Development

ICT CONTROL
Your Trusted Advisor

Solvay Brussels School Economics & Management

Cogentas.ca
Application Security Institute

Certification of Application Security

Speaker

Alain CIESLIK

Career Summary

- Enterprise Security Architect (Stib)
- Participate in the development of an autorisation provider (European commission)
- ISO 27034 Lead Implementer Trainer (Nitroxis)
- Security consutlant (ICT Control)

Expertise Summary

- Secure Development lifecycle
- Application security
- Security assessment
- Security Awareness
- Digital Forensics

Education / Certification

- Master in IT Management Solvay
- Master in computer Science
- Graduat en informatique de gestion
- ISO 27034 Lead implementer
- ISO 27001 Lead Implementer
- GWAPT: Web Application Penetreation tester
- CISSP, CSSLP

Secure Application Development

ICT CONTROL
Your Trusted Advisor

Solvay Brussels School Economics & Management

Cogentas.ca
Application Security Institute

Certification of Application Security

ISO 27034 father

Luc POULIN

Career Summary

- President of the Application Security Institute – Cogentas inc
- Senior Advisor on Open Information Systems and Chief Information Security Officer (CISO) at the Computer Research Institute of Montréal (CRIM)
- Senior application security advisor at nurun
- Principal/security architect at schlumberger
- Specialized in security concerns within the information system life cycle for more then 15 years.

Expertise Summary

- Chief Information Security Officer
- Information / Application Security Advisor
- Lead Technological and Functional Architect
- Security Architect
- Functional and Technological Analyst
- Conference speaker and trainer
- Application Security Evaluator / Auditor
- University Lecturer

Education/Certification

- A Ph.D in Software Engineering/ Application Security in Montreal at *School of Advanced Engineering, University of Quebec*
- Master's Degree in Computer Security (thesis) at *Laval University*
- Post-graduate Diploma in Software Engineering at *Laval University*
- Bachelor's Degree in Computer Science at *Laval University*
- Certified ISO/IEC 27034 Application Security Lead Auditor (CASLA), Certified ISO/IEC 27034 Application Security Lead Implementer (CASLI)
- CSSLP, CISA, CISM, CISSP-ISSMP

Secure Application Development

ICT CONTROL
Your Trusted Advisor

Solvay Brussels School Economics & Management

Cogentas.ca
Application Security Institute

Certification of Application Security

Agenda

1. Introduction
    1. Definition
    2. Scenario
    3. ISO 27034 Concepts
2. How can we certify security inside an application ?
    1. Phase 1: Risk Assessment
    2. Phase 2: Application Security Controls
    3. Phase 3: Audit Process
3. ISO 27034 Information Repository
4. Conclusion

Annex I: Workshop – How can we trust frameworks used inside the company ?

Annex II: Training – ISO 27034 Lead Implementer

Certification of Application Security

1.1 Introduction

Information security

Preservation of confidentiality, integrity and availability of information (ISO 27000:2013)

Application security

- Preservation of confidentiality, integrity and availability of information collected, processed, stored or communicated
- Protection of the information involved by an application

Certification of Application Security

1.1 Introduction

Validation

The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders

Verification

The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process

Certification of Application Security

1.1 Introduction

Audit

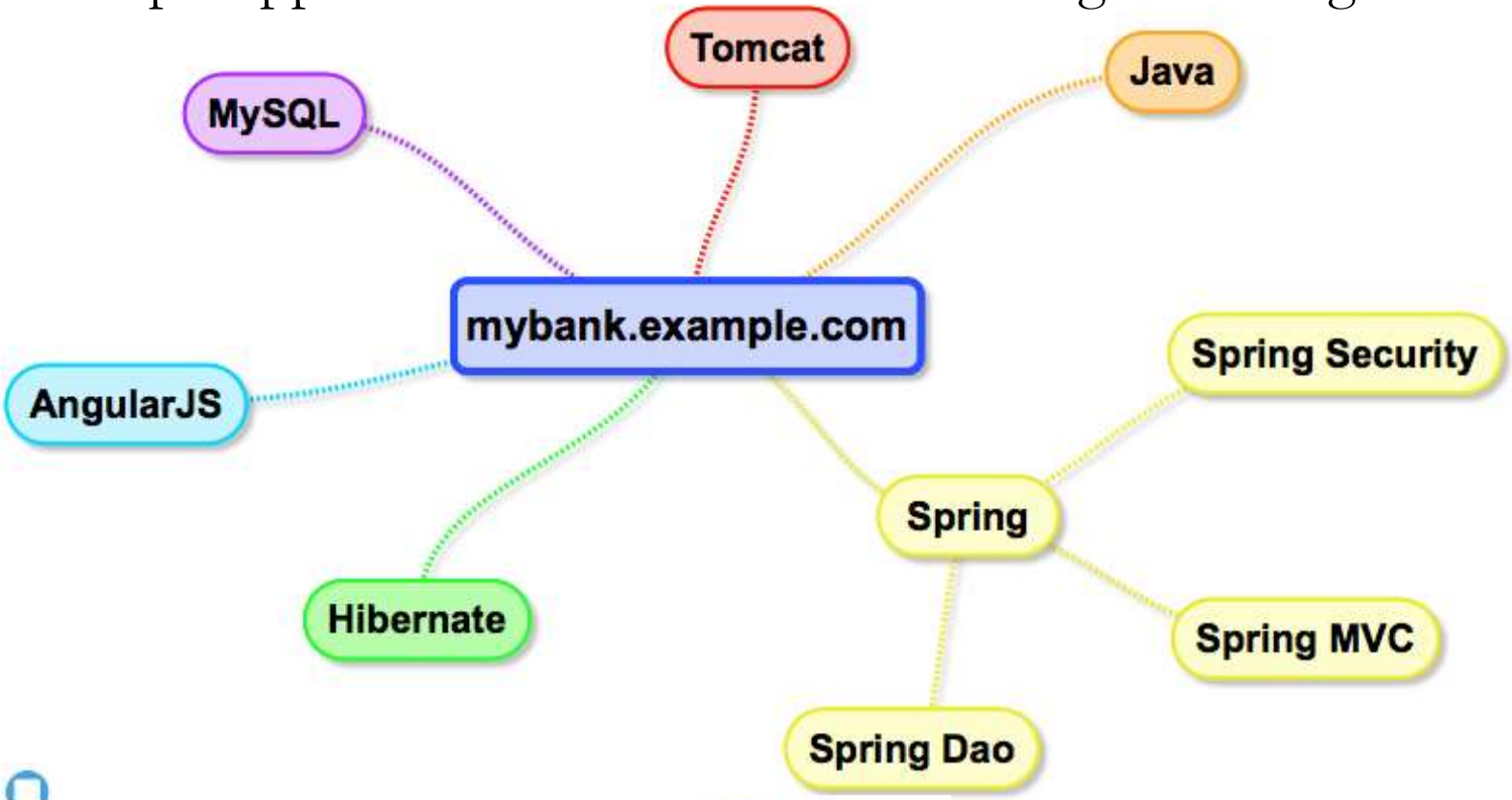
Systematic, independent and documented process for obtaining audit evidence [records, statements of fact or other information which are relevant and verifiable] and evaluating it objectively to determine the extent to which the audit criteria [set of policies, procedures or requirements] are fulfilled (ISO 19011:2011)

Certification of Application Security

1.2 Scenario

My Bank's website, mybank.example.com.

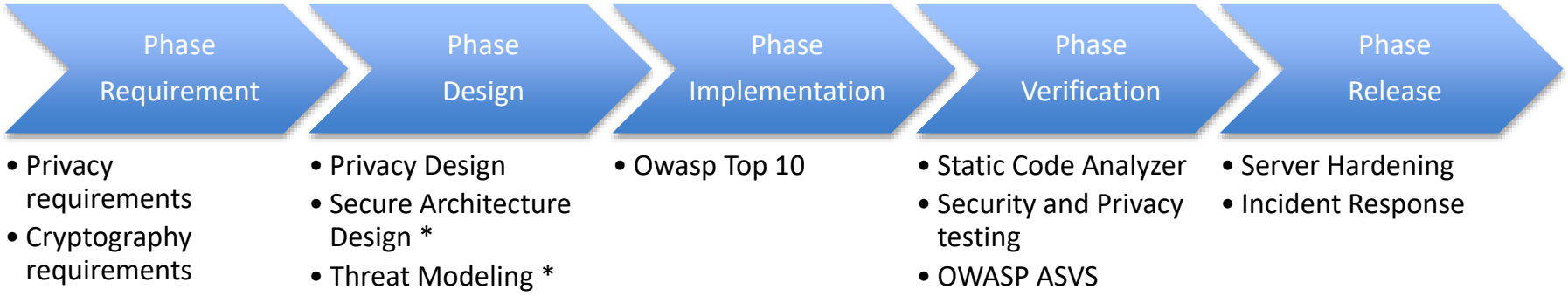
This sample application is based on the following technologies.



Certification of Application Security

1.2 Scenario

Our Secure Development lifecycle based on Microsoft SDL and is composed of several phase.



Within each phase, we can find security processes or tasks that have to be done.

(*): see SecAppDev training sessions

Certification of Application Security

1.2 Scenario

How secure we are?

Certification of Application Security

1.2 Scenario

Security is critical for organizations

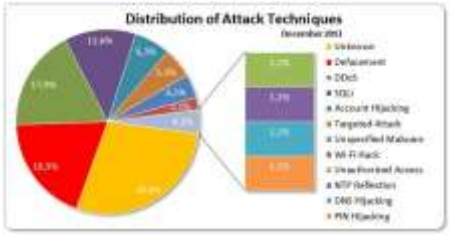
- Can we trust third parties framework used inside our applications ?
- Can we use logs or other evidences in front of court in case of security incident ?
- Can we assure the board that everything is under control ?
- Do we effectively respect Data privacy of our clie
- Could we prove our PCI-DSS compliance ?

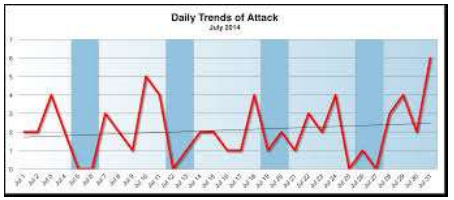
Certification of Application Security

1.2 Scenario

… What cannot be measured …

cannot be managed…





Certification of Application Security

1.2 Scenario

We need to create trust between Business and IT

Security software must be assessed with evidences…

Certification of Application Security

1.3 ISO 27034 Concepts

This presentation is based on key ISO 27034 elements

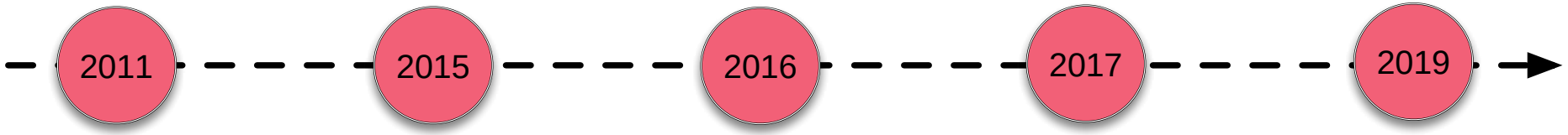
ISO 27034 is composed of the following parts:

- PART I: Overview and concepts
- PART II: Organization Normative Framework
- PART III: Application Security Management Process
- PART IV: Application Security Validation
- PART V: Protocols and application security control data structure
- PART VI: Case studies

Certification of Application Security

1.3 ISO 27034 Concepts

ISO 27034 publication planning



2011 — ISO 27034-1

Concept & overview

2015 — ISO 27034-2

ONF Management

2016 — ISO 27034-6

Security guidance for specific applications

2017 — ISO 27034-3

Application security management process

ISO 27034-5

Protocols and application security control data structure

2019 — ISO 27034-4

Application security validation

Certification of Application Security

1.3 ISO 27034 Concepts

I. Principles

1. Security is a requirement

1. Application security should be managed

1. Application security is context-dependent

1. Appropriate investment for application security

1. Application security must be demonstrated

Certification of Application Security

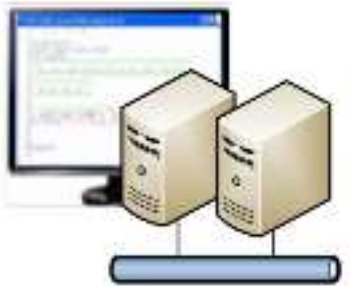
2.1 Phase 1: Risk assessment

Where risks come from ?

Three sources have an impact on Application Security

People

Processes

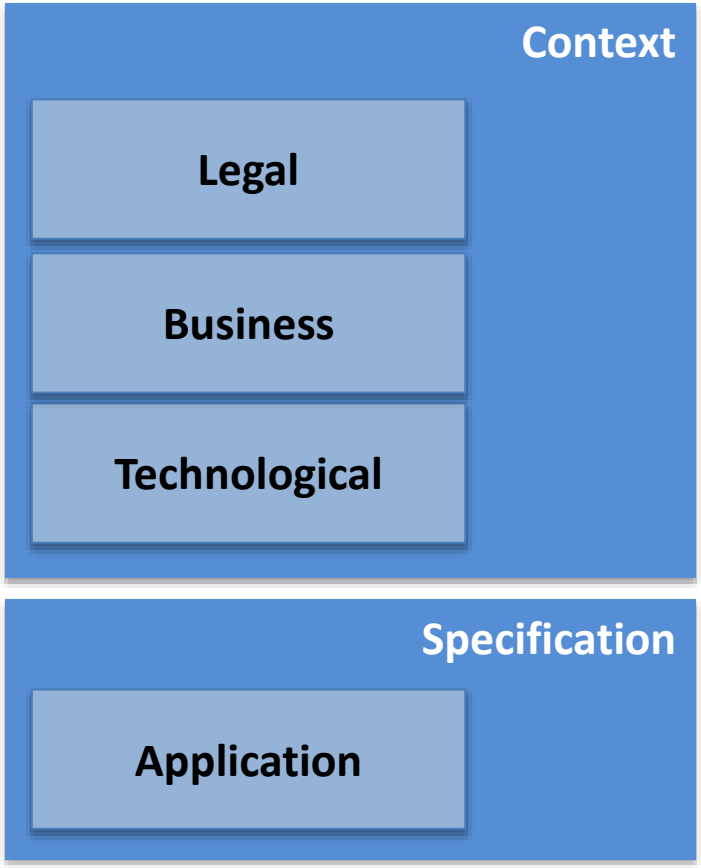


Technology

Certification of Application Security

2.1 Phase 1: Risk assessment

Where risks come from ?



Global Data Protection Act, Patriot Act, …

PCI-DSS, Internal Policies, …

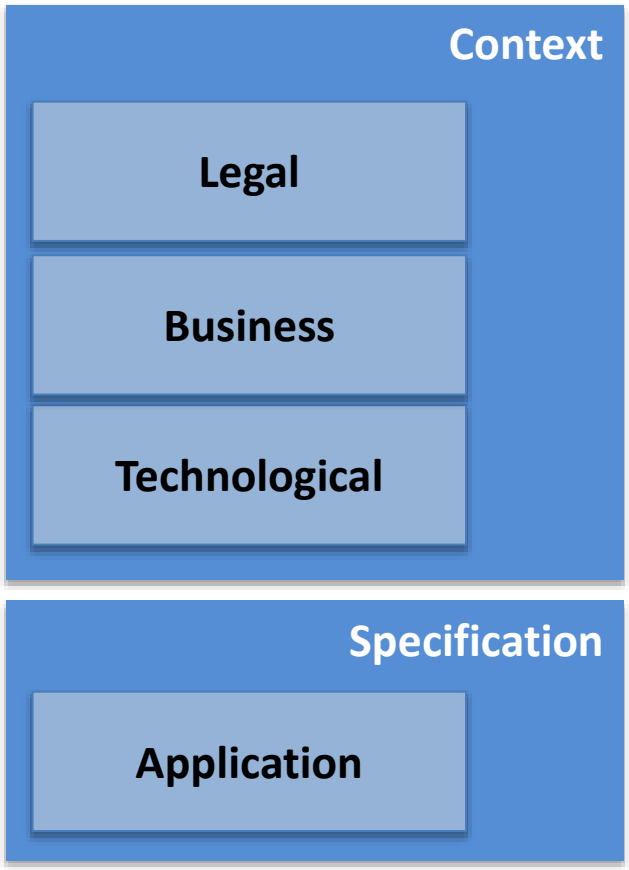
Java, C#, C++,…

File Upload, Dashboards, Sending mails, …

Certification of Application Security

2.1 Phase 1: Risk assessment

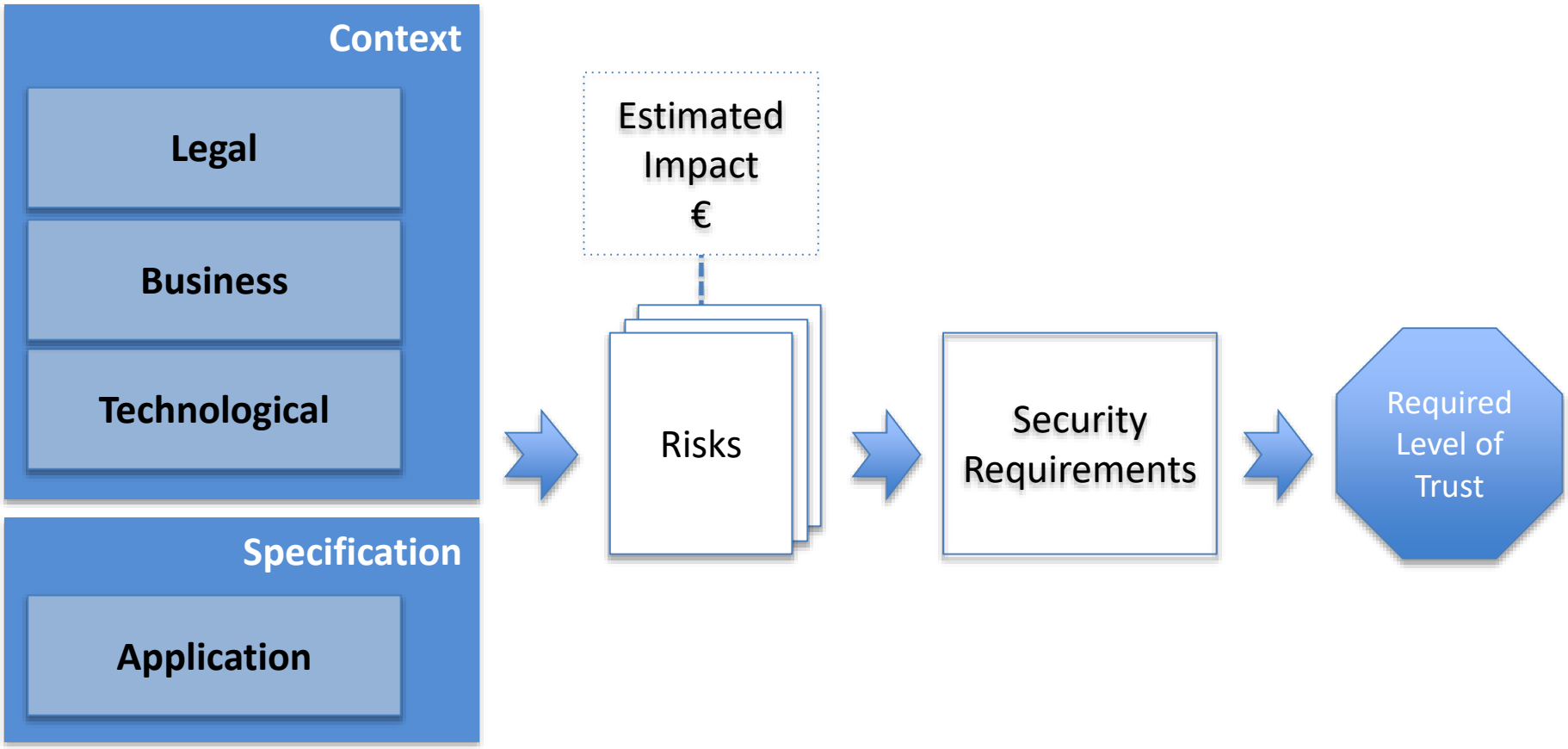
Where do the risks come from ?



Certification of Application Security

2.1 Phase 1: Risk assessment

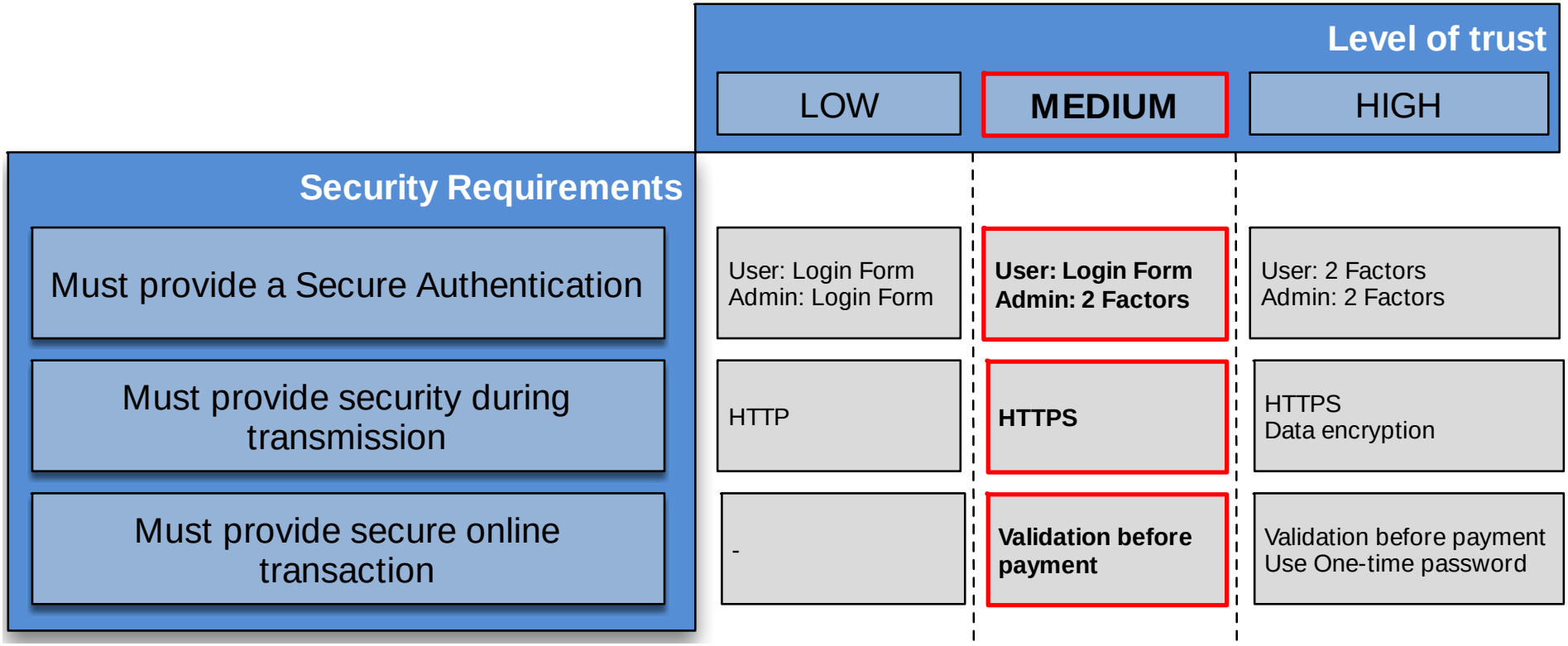
Where do the risks come from ?



Certification of Application Security

2.1 Phase 1: Risk assessment

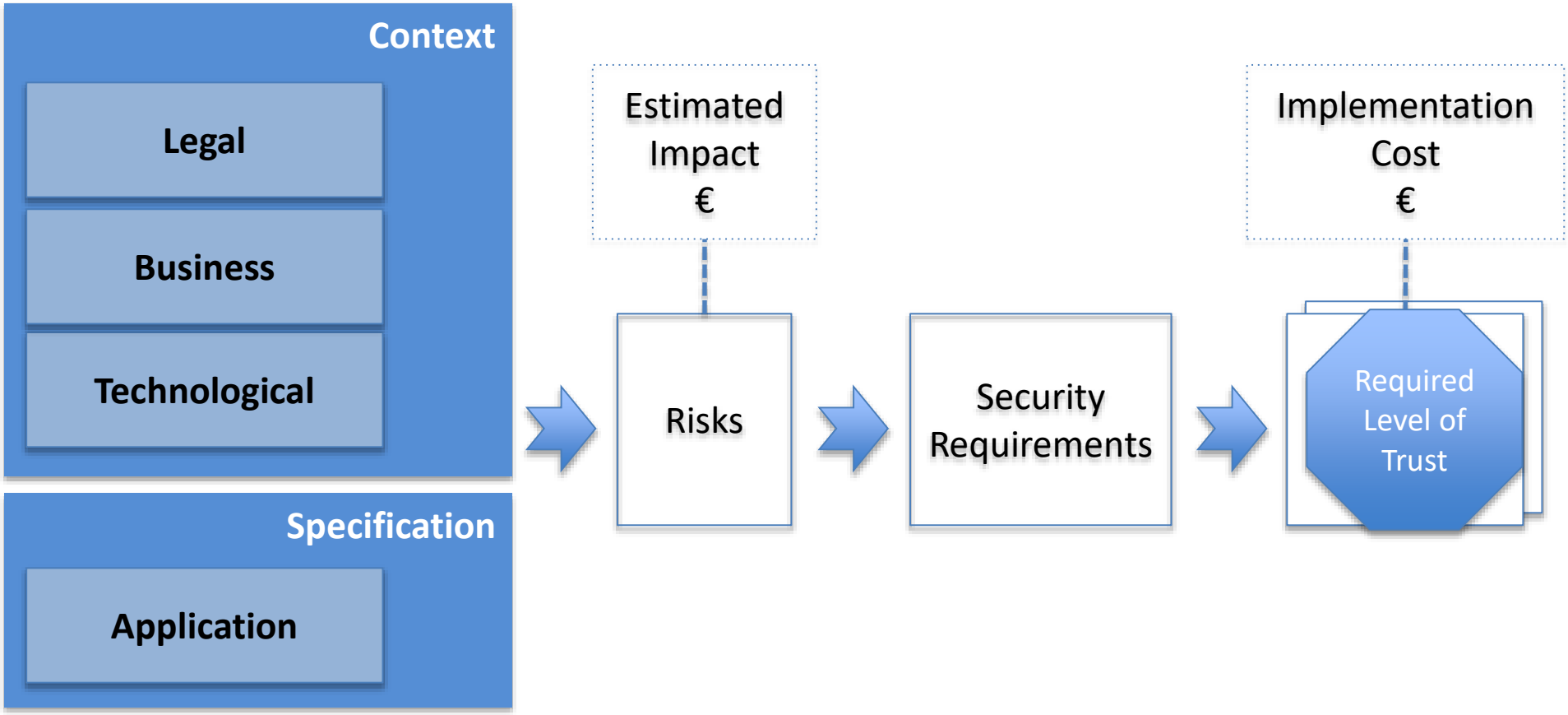
Where do the risks come from ?



Certification of Application Security

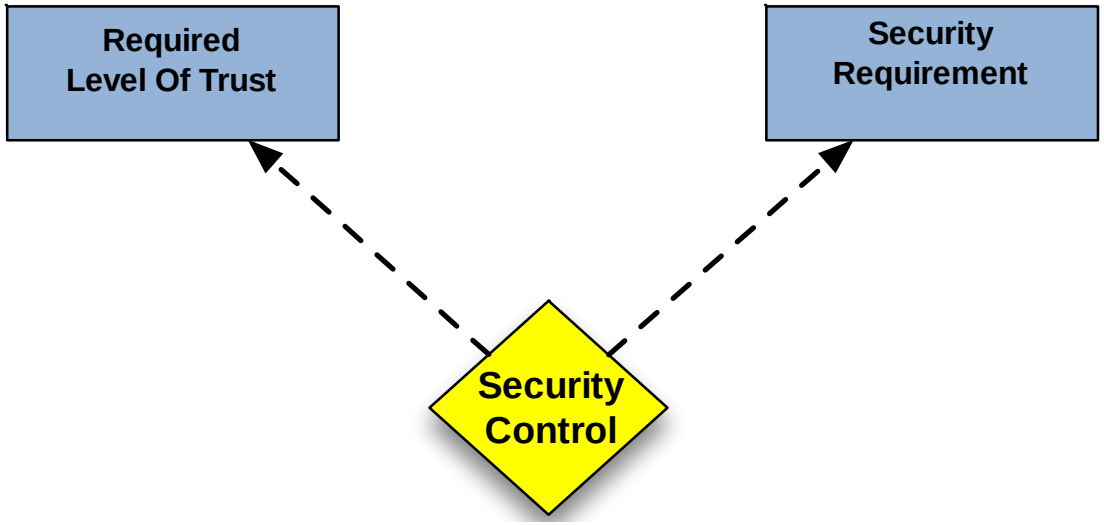
2.1 Phase 1: Risk assessment

How can we mitigate a risk ?



2.1 Phase 1: Risk assessment

Application Security Controls



Certification of Application Security

2.2 Phase 2: Application Security Controls

A. Different types of Security Controls

	Preventive (Before)	Detective (During)	Corrective (After)
Administrative	Security awareness and technical training	Security reviews and audits Required vacations	Penalty
Technical	Access control software Antivirus software	Audit Trails	Restore the system
Physical	Locks and keys	Motion detectors. Smoke and fire detectors.	Fire extinguishers

Certification of Application Security

Phase 2: Application Security Controls

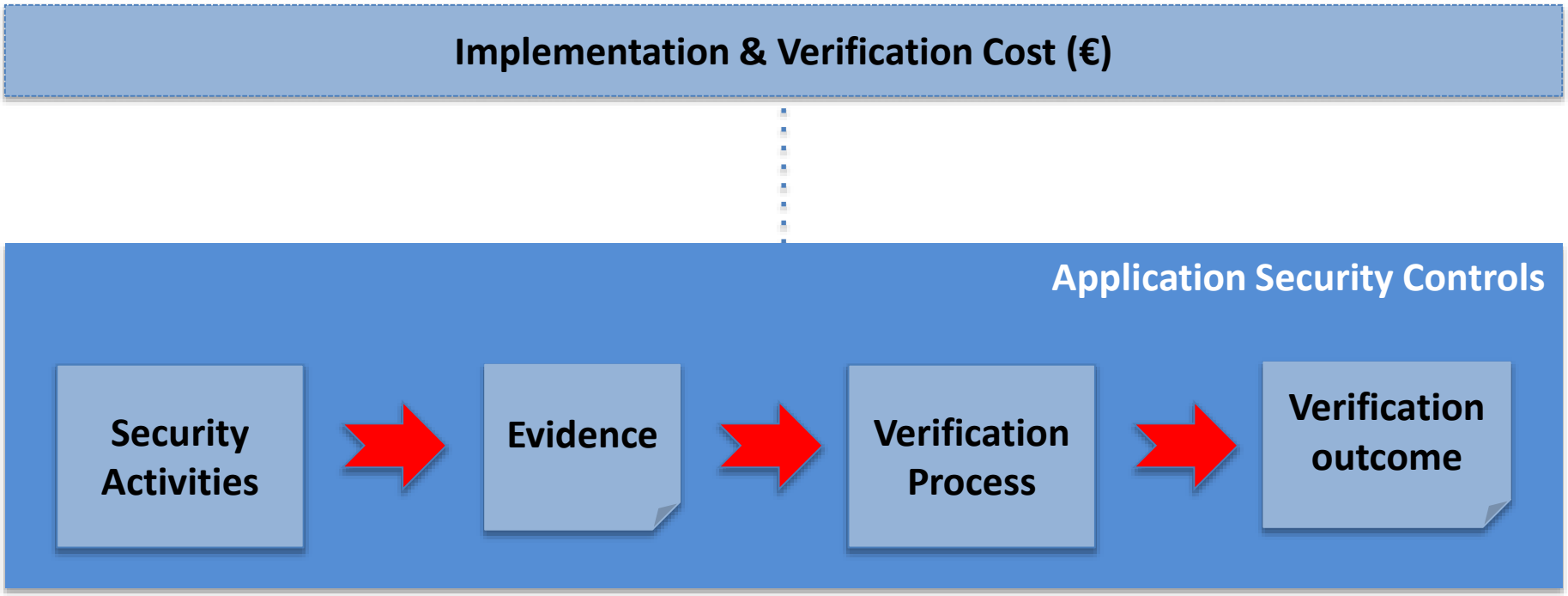
Objectives

- Security Design Pattern (Knowledge documentation)
  - Security activity
  - Security verification
- Translate the Security Requirements into a concrete set of tasks
- Use by the project to implement a Security Control
- Use by the business to estimate the cost
- Use by the project manager to estimate the time
- Use by the quality manager to verify the implementation
- Use by the auditor to certify the application
- Improve the organization's Application Security Maturity

Certification of Application Security

2.2 Phase 2: Application Security Controls

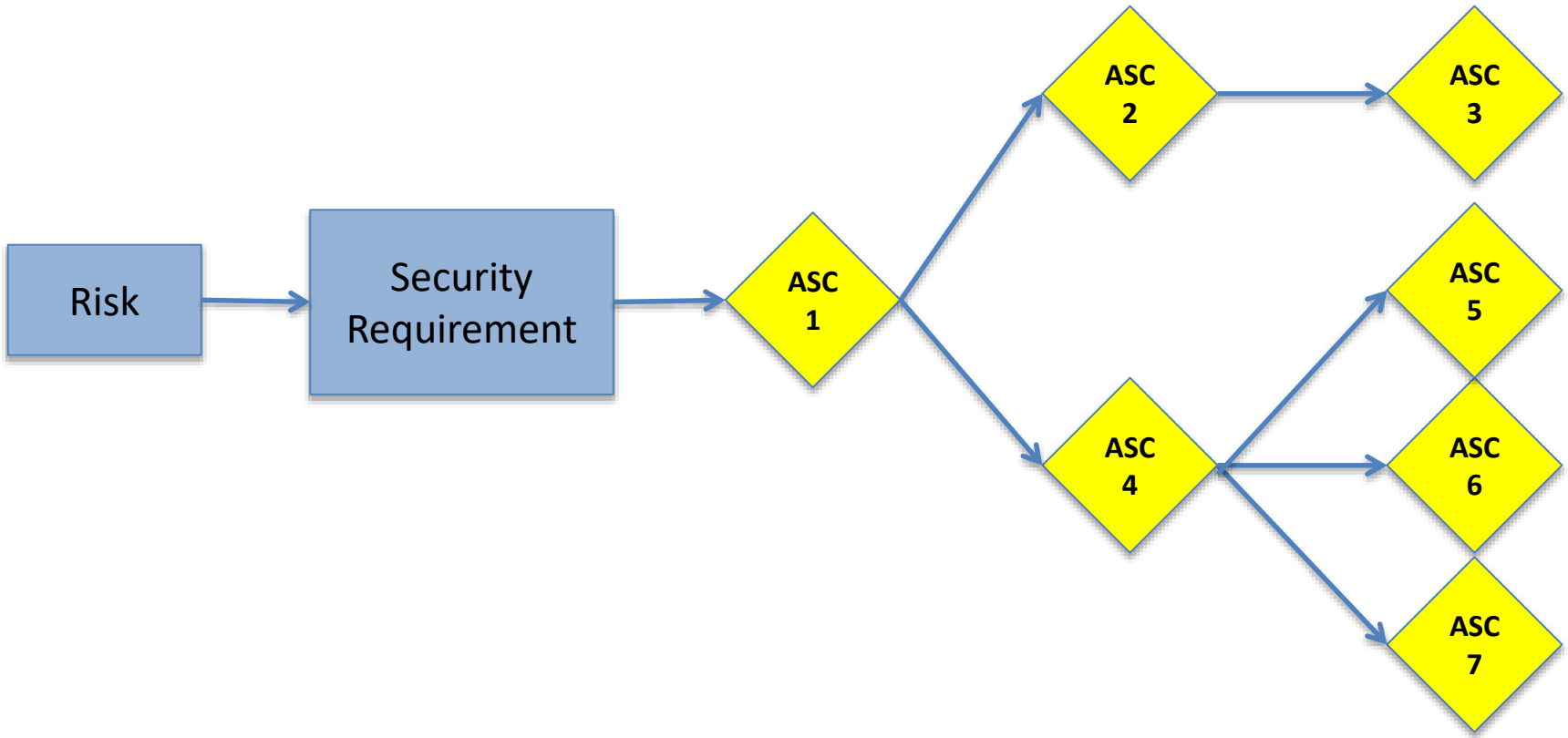
Security Design Pattern (Knowledge documentation)



Certification of Application Security

2.2 Phase 2: Application Security Controls

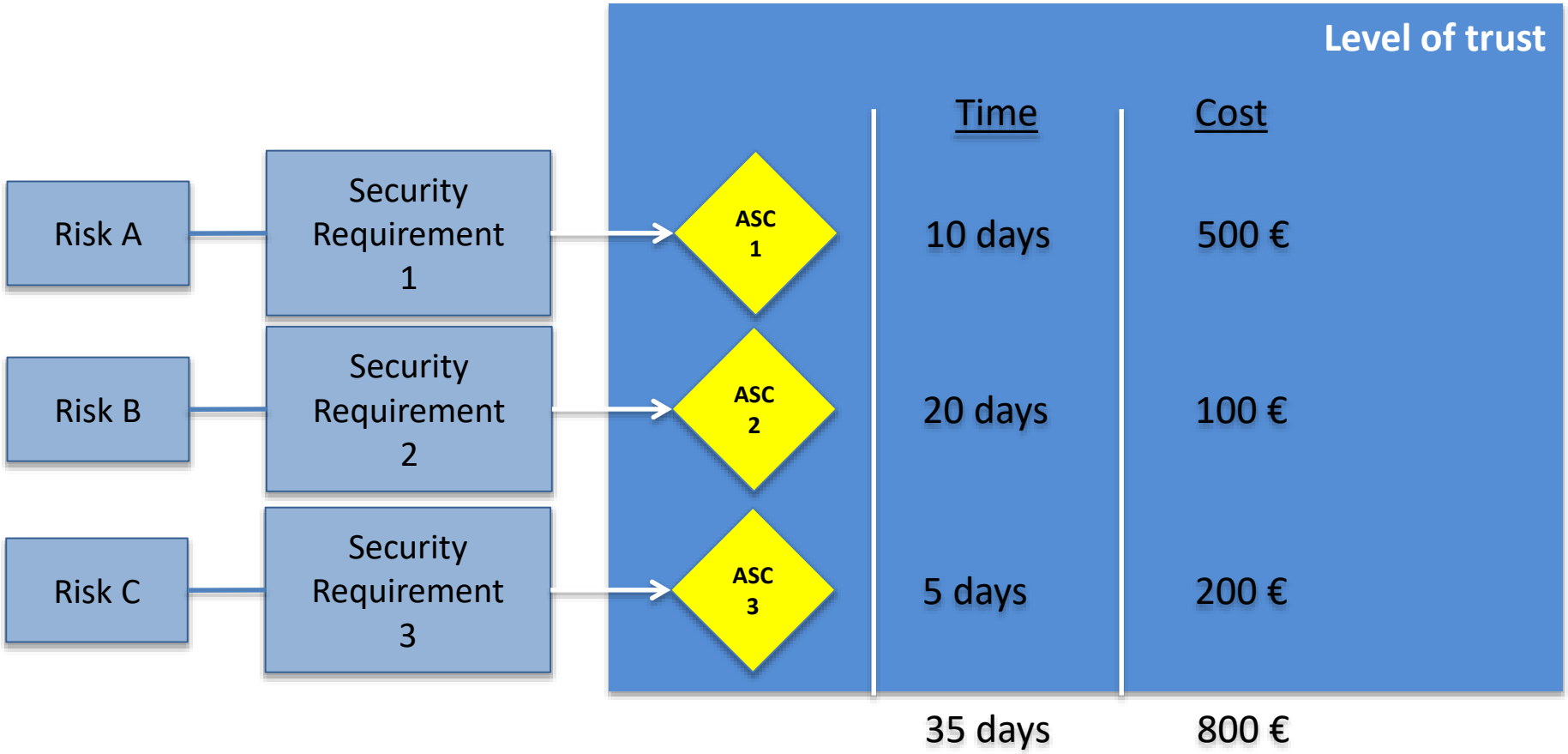
Translate Security Requirements into concrete set of tasks



Certification of Application Security

2.2 Phase 2: Application Security Controls

Mitigation cost of security requirements



Certification of Application Security

2.2 Phase 2: Application Security Controls

C. Application Security Life Cycle Model

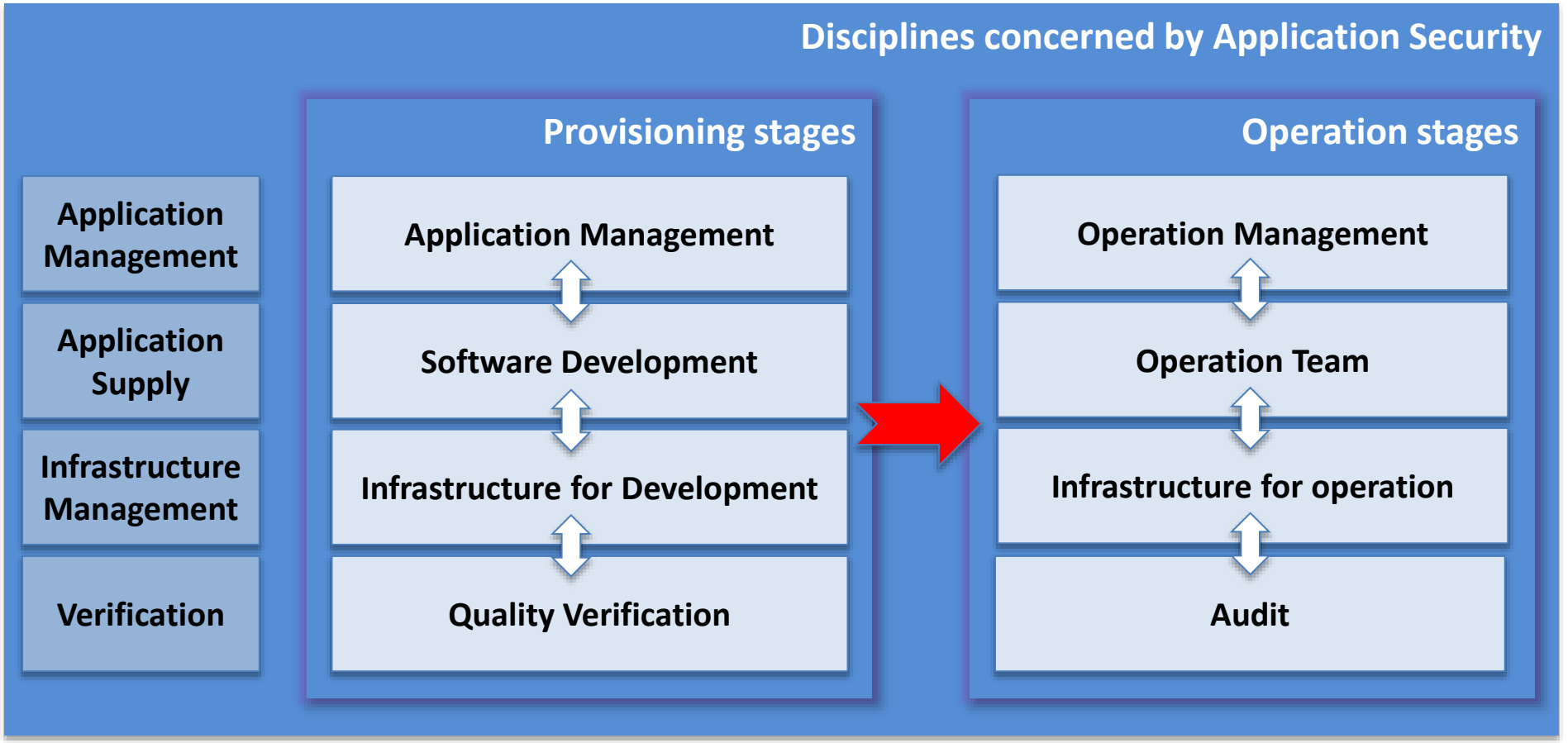
ISO 27034 proposes a global life cycle model

Layers	Disciplines concerned by Application Security		
Application Management	Governance	Enterprise Architecture	Project Management
Application Supply	Software Development	Operation Team	
Infrastructure Management	Network	Server	
Verification	Audit		

Certification of Application Security

2.2 Phase 2: Application Security Controls

C. Application Security Life Cycle Model

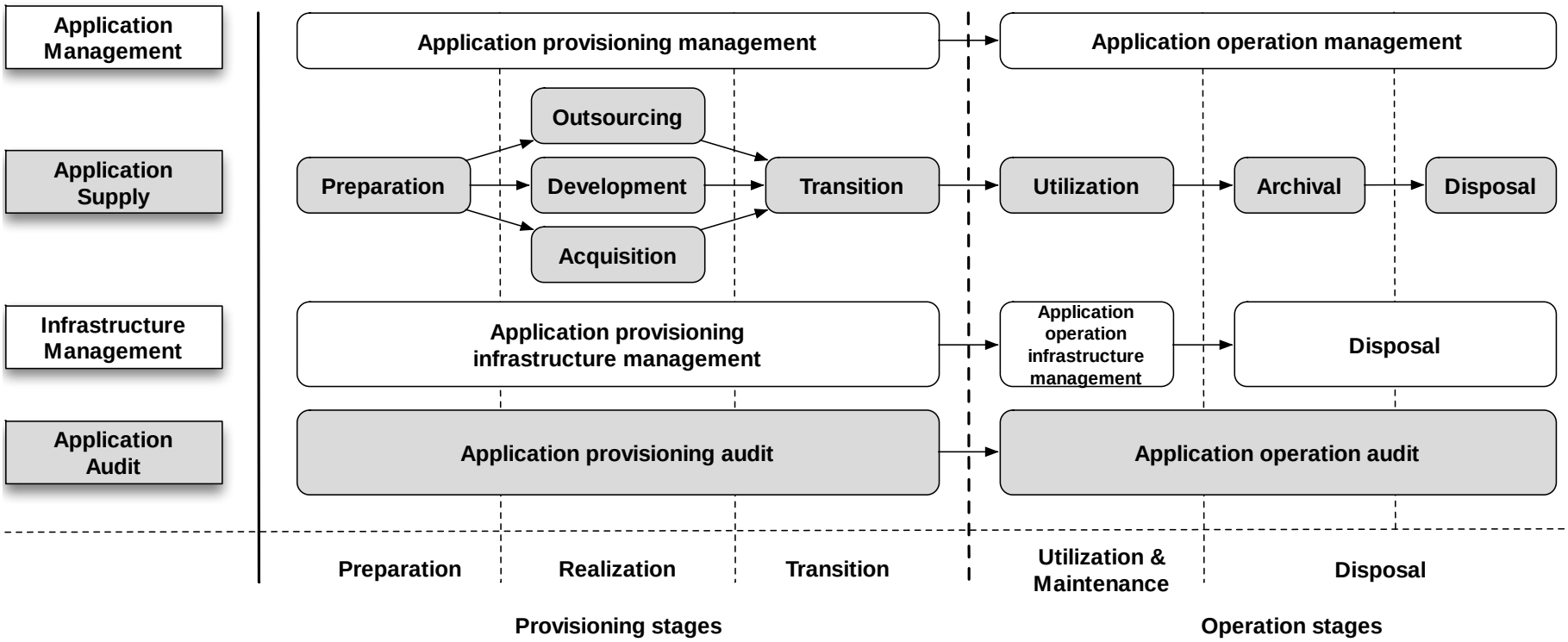


Certification of Application Security

2.2 Phase 2: Application Security Controls

C. Application Security Life Cycle Model

A reference Model aligns different disciplines required to produce Secure Application



Secure Application Development

ICT CONTROL Your Trusted Advisor

Solvay Brussels School Economics & Management

Cogentas.ca Application Security Institute

C. Application Security Life Cycle Model

What are the advantages of such model ?

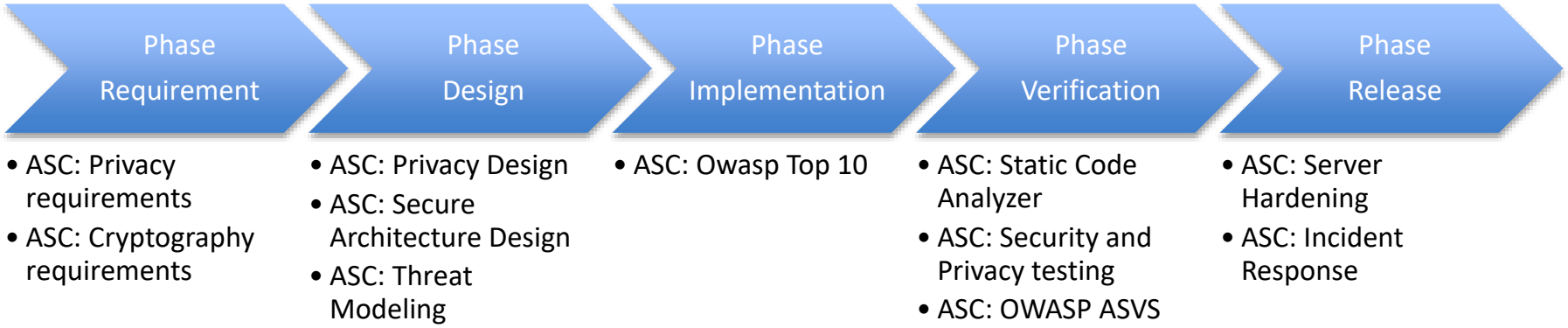
- Create a Helicopter view of different disciplines under the scope of Application Security
- Allow to identify what are missing areas within the organization
- Allow different disciplines to communicate in an effective way
- Allow to choose the right place for an Application Security Controls

Certification of Application Security

2.2 Phase 2: Application Security Controls

C. Application Security Life Cycle Model

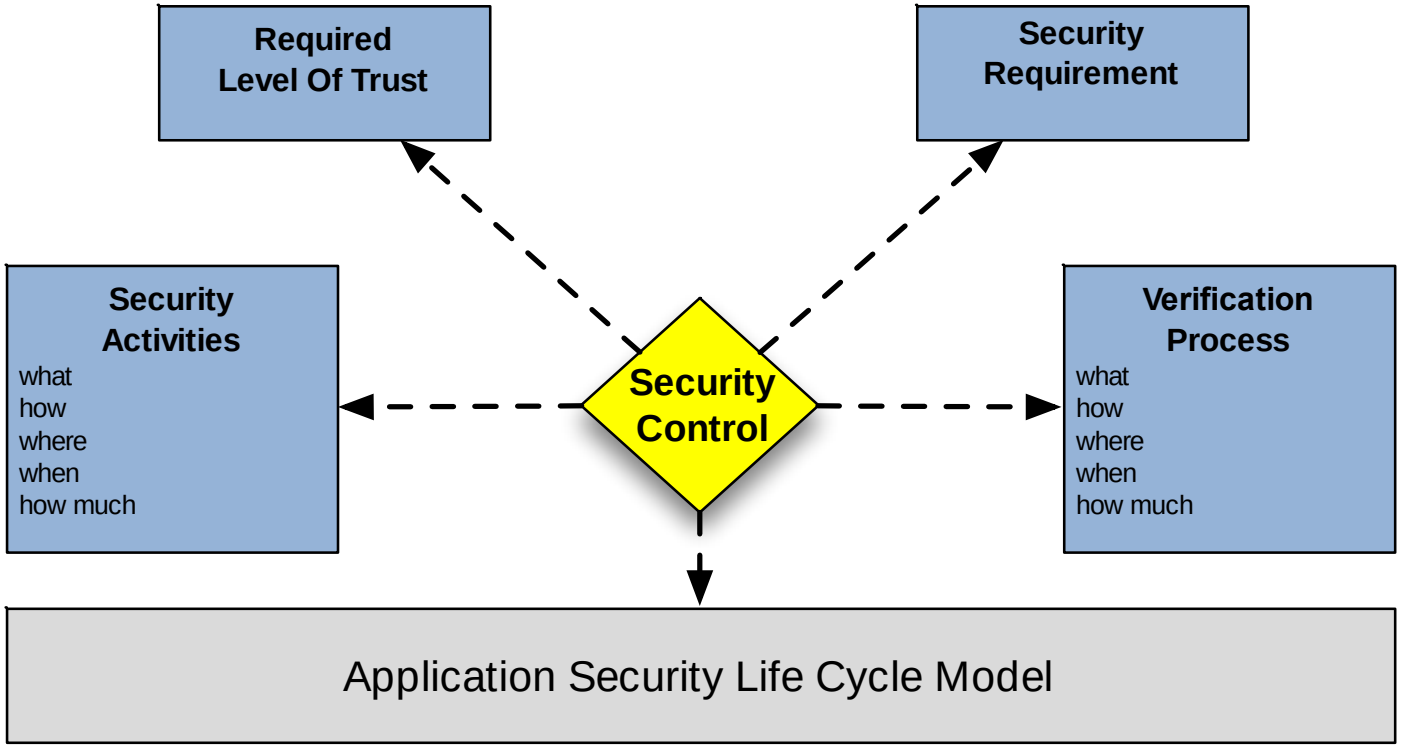
What relation exists between the SDLC of our initial sample and the ISO 27034 reference life cycle model ?



Certification of Application Security

2.2 Phase 2: Application Security Controls

C. Application Security Life Cycle Model



Certification of Application Security

4. Conclusion

In 2016, Application Security cannot be a feeling…

- A security control cannot be taken in account if there is no evidence it fulfills his purpose.
- It provides a way to demonstrate that an application reaches a specific level of trust within the organization.
- It provides a way to evaluate the application security cost.

Certification of Application Security

Annex III: Trainings

CERTIFIED ISO 27034 LEAD IMPLEMENTER

5 Day course

Next course dates:

- May 23-27, 2016
- October 3-7, 2016

Useful links

- http://www.ictcontrol.eu/Services/Training/CERTIFIED-ISO-27034-LEAD-IMPLEMENTER.aspx
- http://www.ictcontrol.eu/Media/pdf/iso-27034-lead-implementer_4p.pdf