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

# 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

## 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 ?

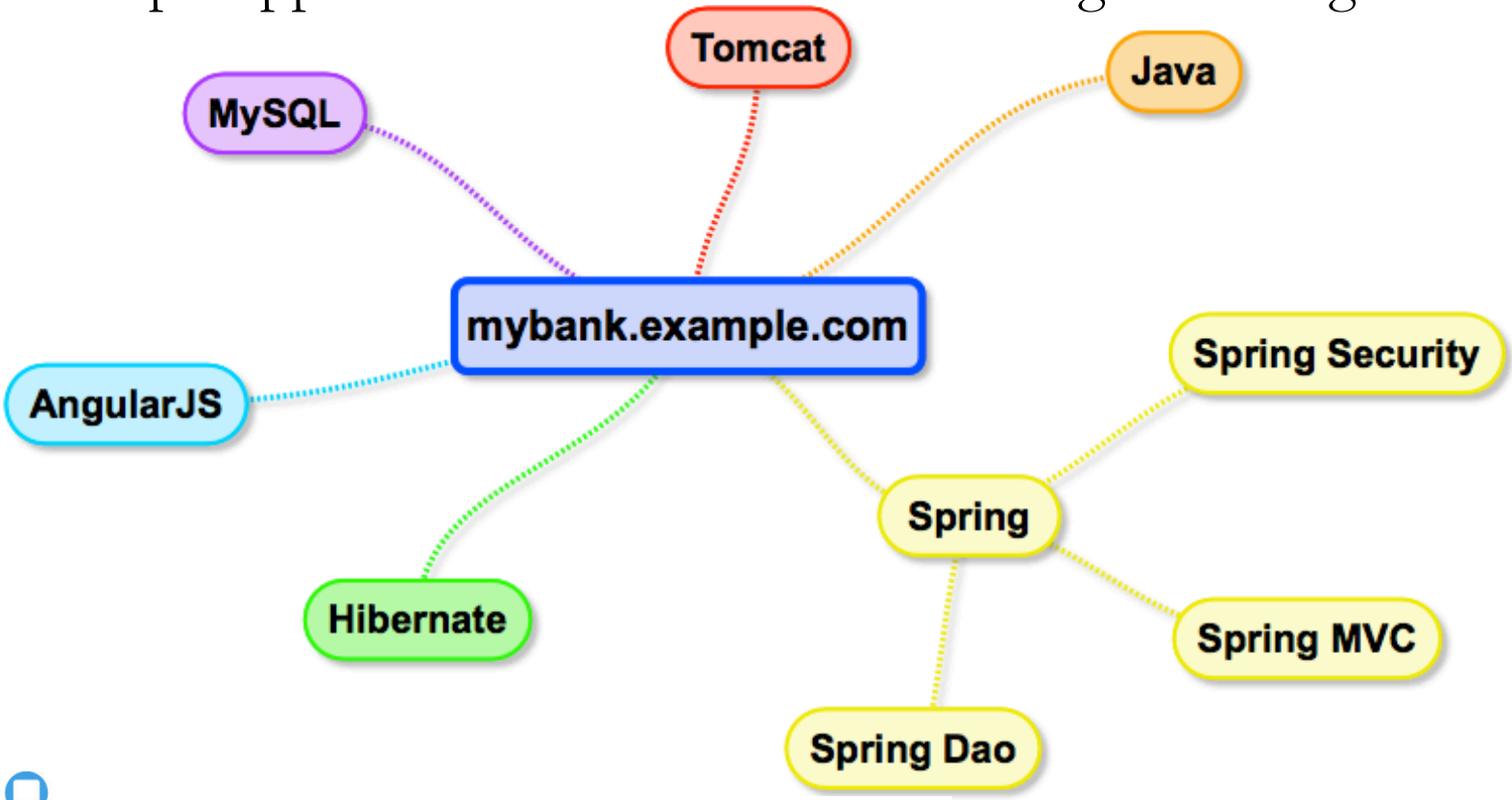
Annex II: Training – ISO 27034 Lead Implementer

# Certification of Application Security

## 1.2 Scenario

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

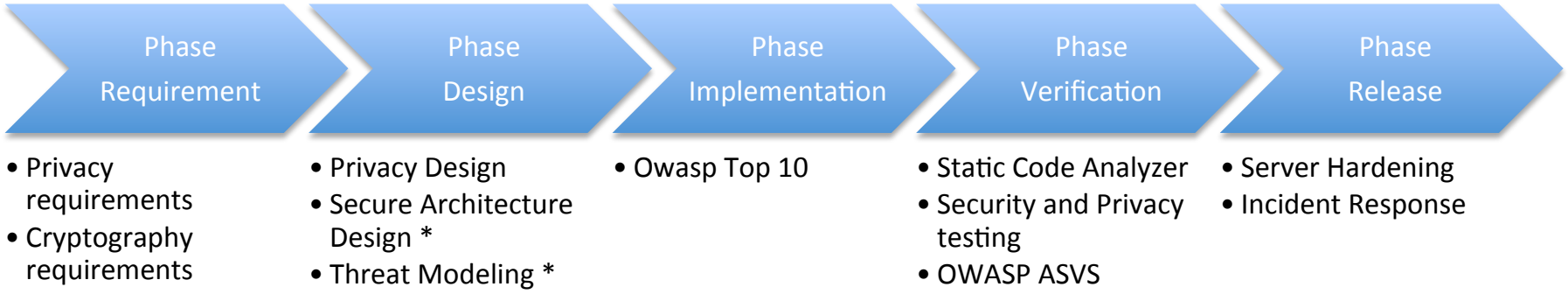
This sample application is based on the following technologies.



# 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

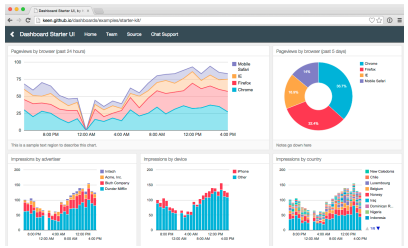
## 1.2 Scenario

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 ?

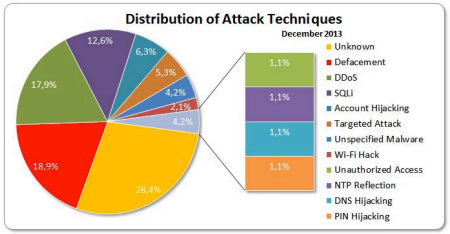
# Certification of Application Security

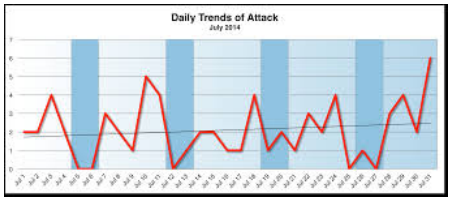
## 1.2 Scenario



… What cannot be measured …

cannot be managed…




Secure Application Development

ICT CONTROL
Your Trusted Advisor

Solvay Brussels School
Economics & Management

Cogentas.ca
Application Security Institute

# 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

## 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

## 1.3 ISO 27034 Concepts

This presentation is based on key ISO 27034 elements

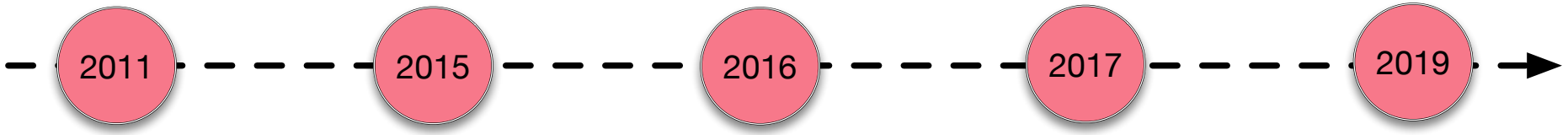

ISO 27034 is composed of the following parts:

- 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

2. Application security should be managed

3. Application security is context-dependent

4. Appropriate investment for application security

5. Application security must be demonstrated

# Certification of Application Security

## 1.3 ISO 27034 Concepts

## II. Type of information that should be protected

**Information Security Scope**

| | |
|---|---|
| Organization & User Data | Business data / Logs / Private key / Configuration /… |
| Roles & Permissions | Authentication data / Authorization data / … |
| Application Data | Application configuration / binary code / source code / … |
| Application specification | Client application specification / server application specification |
| Technological Context | Operating systems / External systems / … |
| Processes involved with the application | Application Update / Process maintenance / repair / … |
| Application life cycle processes | Training of stakeholders / Implementation process / … |

# Certification of Application Security

## Agenda

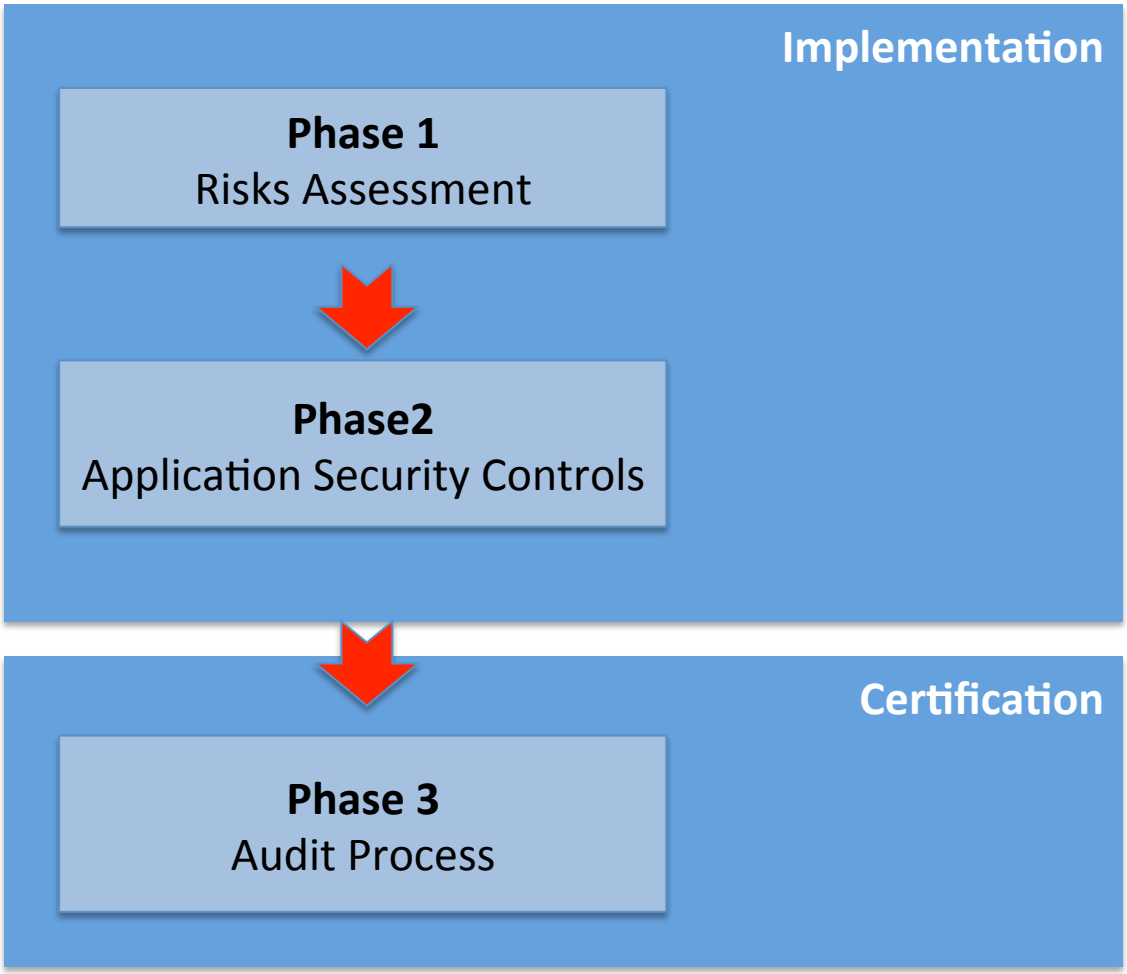
1. Introduction
    1. Definition
    2. Scenario
    3. ISO 27034 Concepts
2. **How can we certify security inside an application ?**
    1. Phase 1: Risk Assessment
    2. Phase 2: Application Security Controls
    3. Phase 3: Audit Process
3. ISO 27034 Information Repository
4. Conclusion

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

Annex II: Training – ISO 27034 Lead Implementer

# Certification of Application Security

## 2. How can we certify security inside an application ?



# 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

## 2.1 Phase 1: Risk assessment

Where risks come from ?

**Three sources have an impact on Application Security**

People

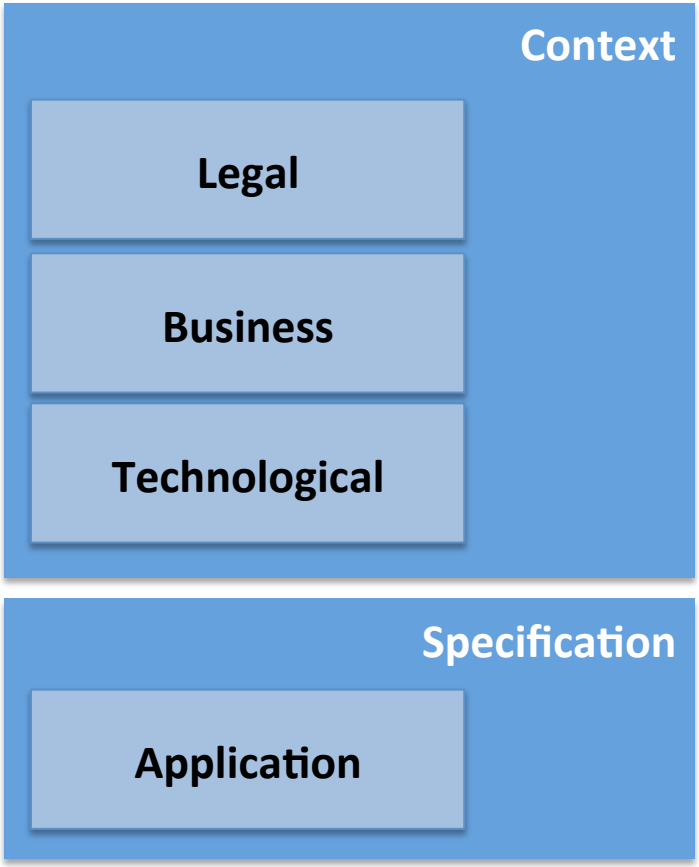
Processes

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, …

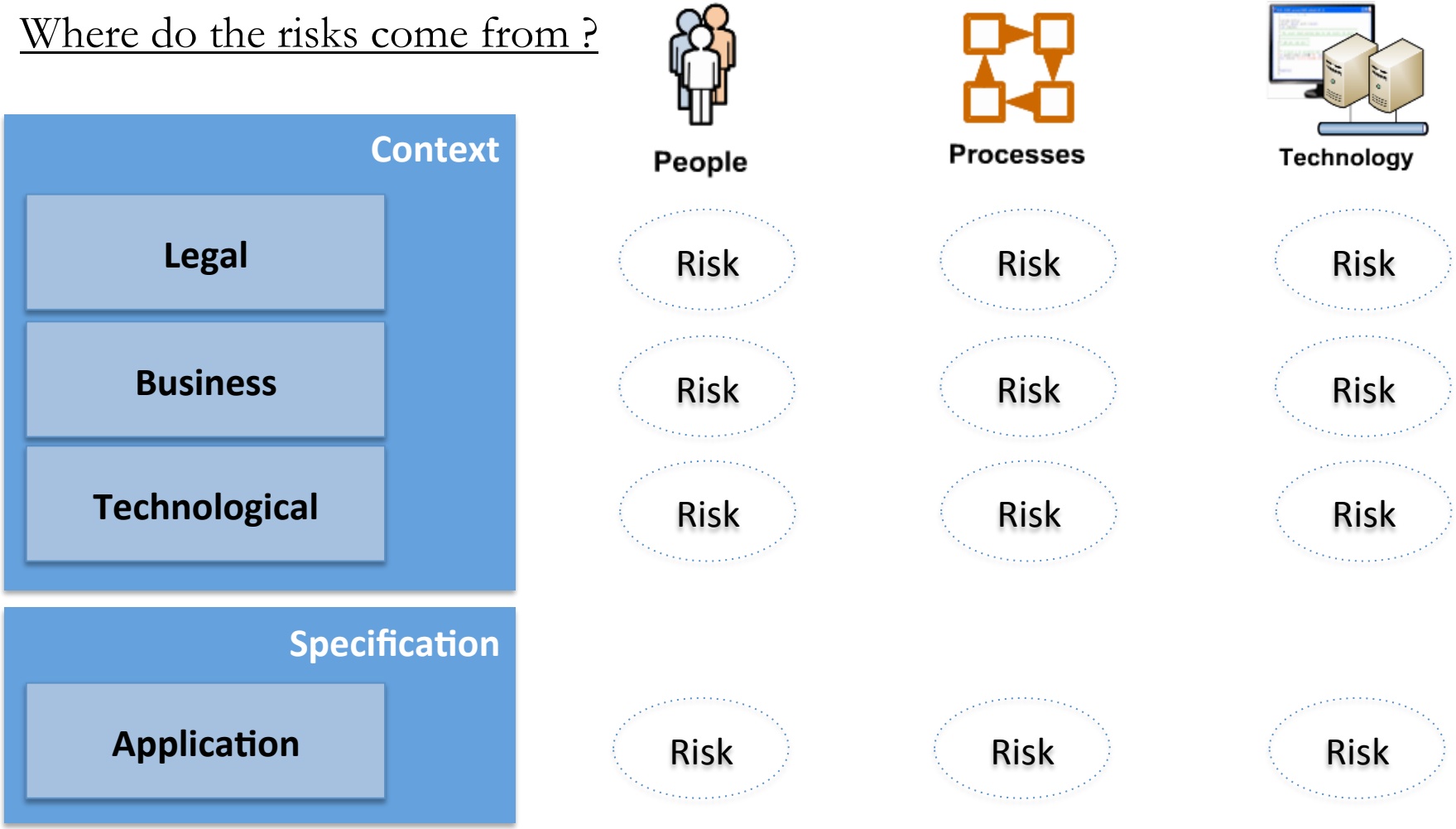
Java, C#, C++,…

File Upload, Dashboards, Sending mails, …

# Certification of Application Security

## 2.1 Phase 1: Risk assessment

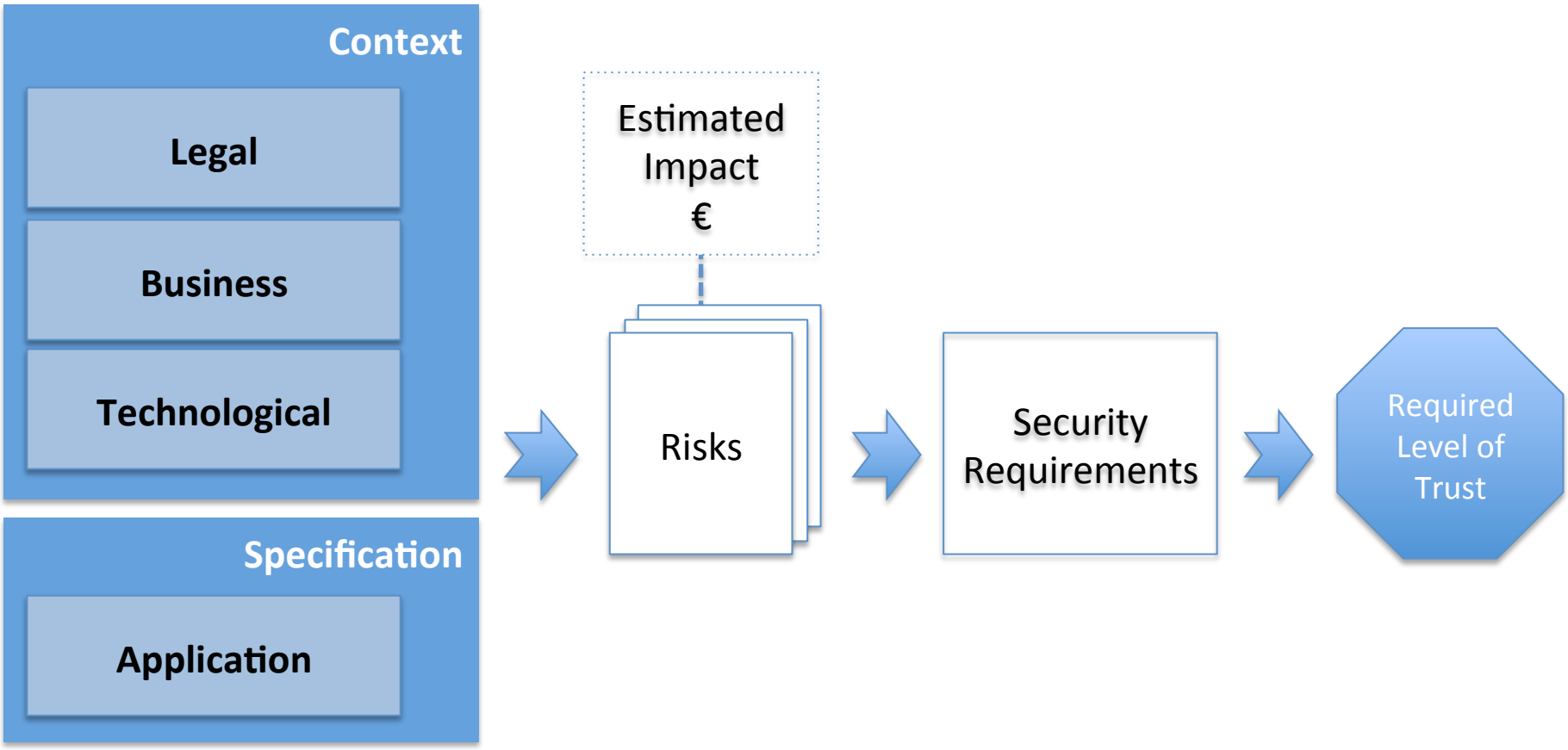
Where do the risks come from ?



# 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

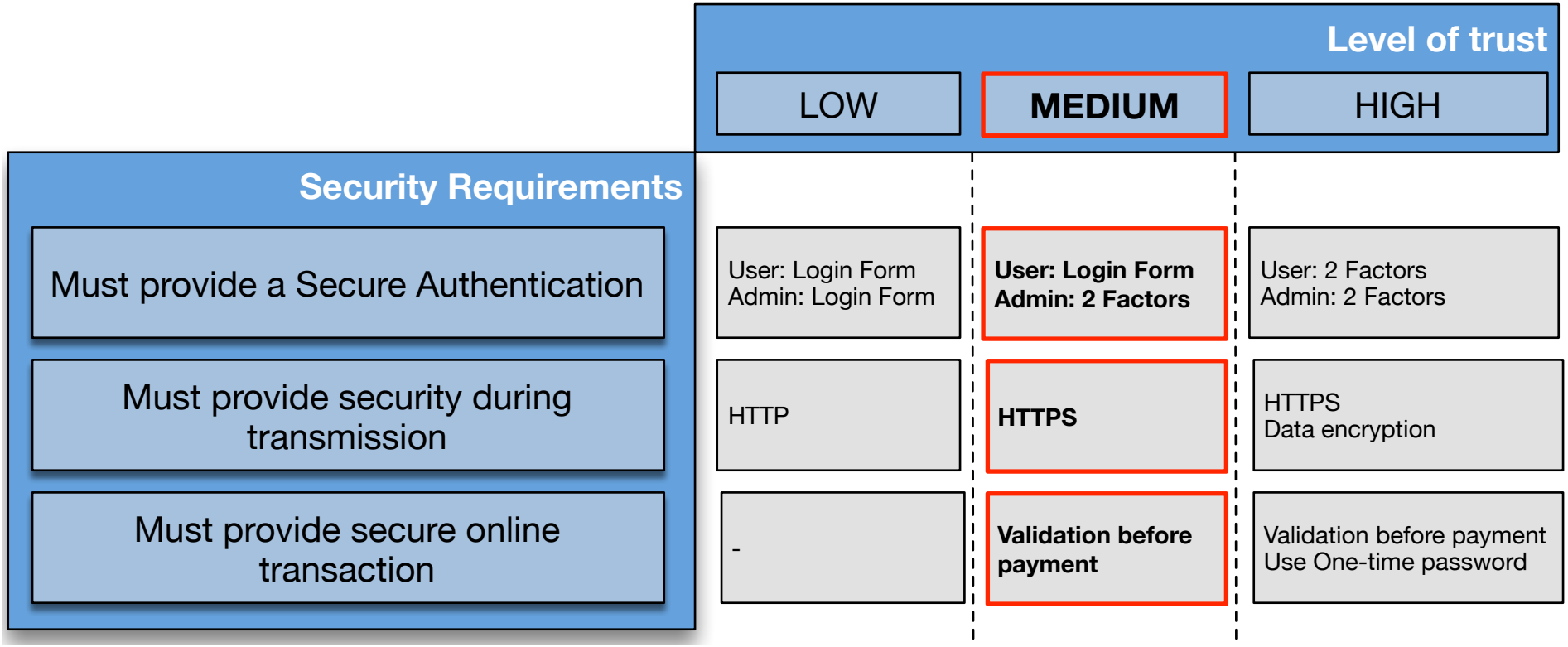
What are the level of trusts ?

- **Security Labels** are used to classify applications inside an organization
- **Describe mandatory security controls** required to provide a minimum security assurance into a level of trust
- **Traceability mechanism** between risks, security requirements and security controls

# Certification of Application Security

## 2.1 Phase 1: Risk assessment

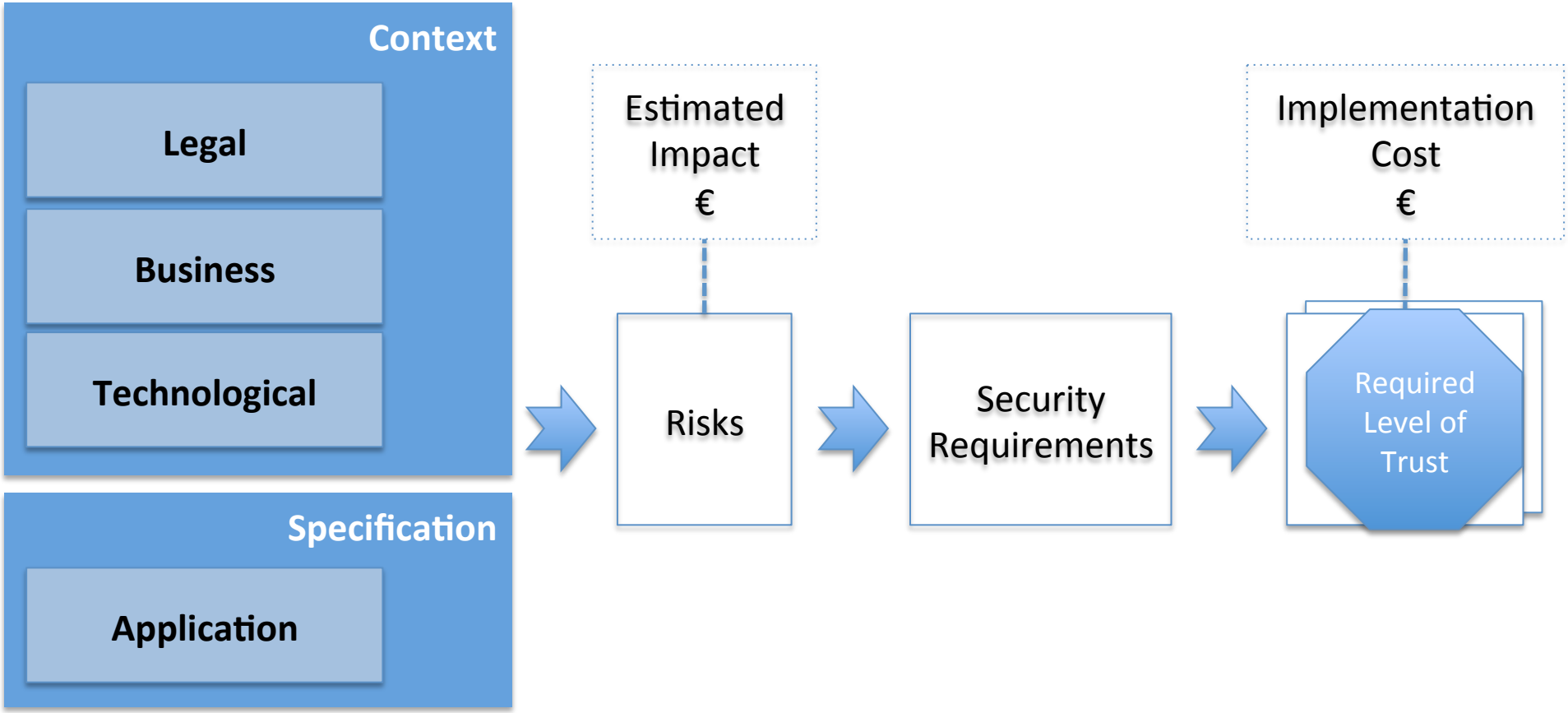
Where do the risks come from ?



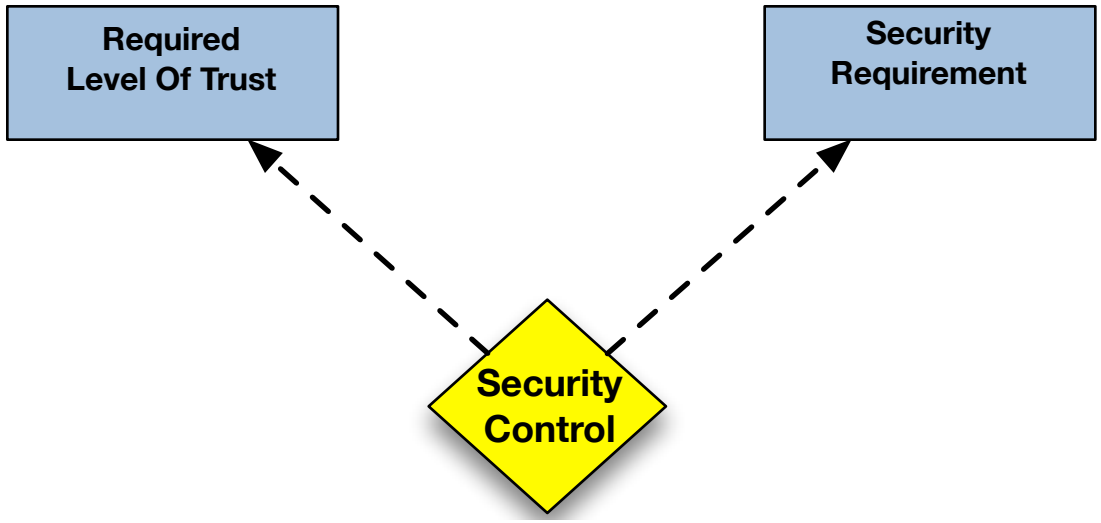
# Certification of Application Security

## 2.1 Phase 1: Risk assessment

How can we mitigate a risk ?



## Application Security Controls



# 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

## A. Different types of Security Controls

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

# Certification of Application Security

## Phase 2: Application Security Controls

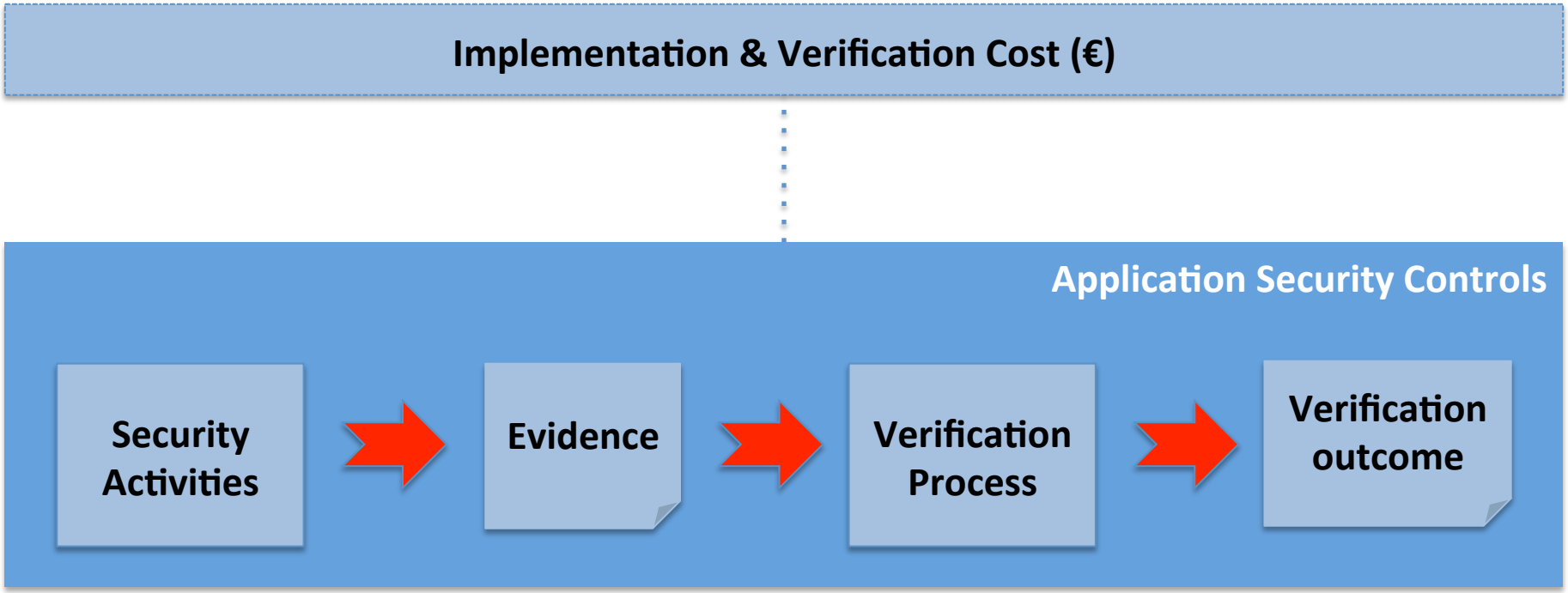
**Objectives**

- 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

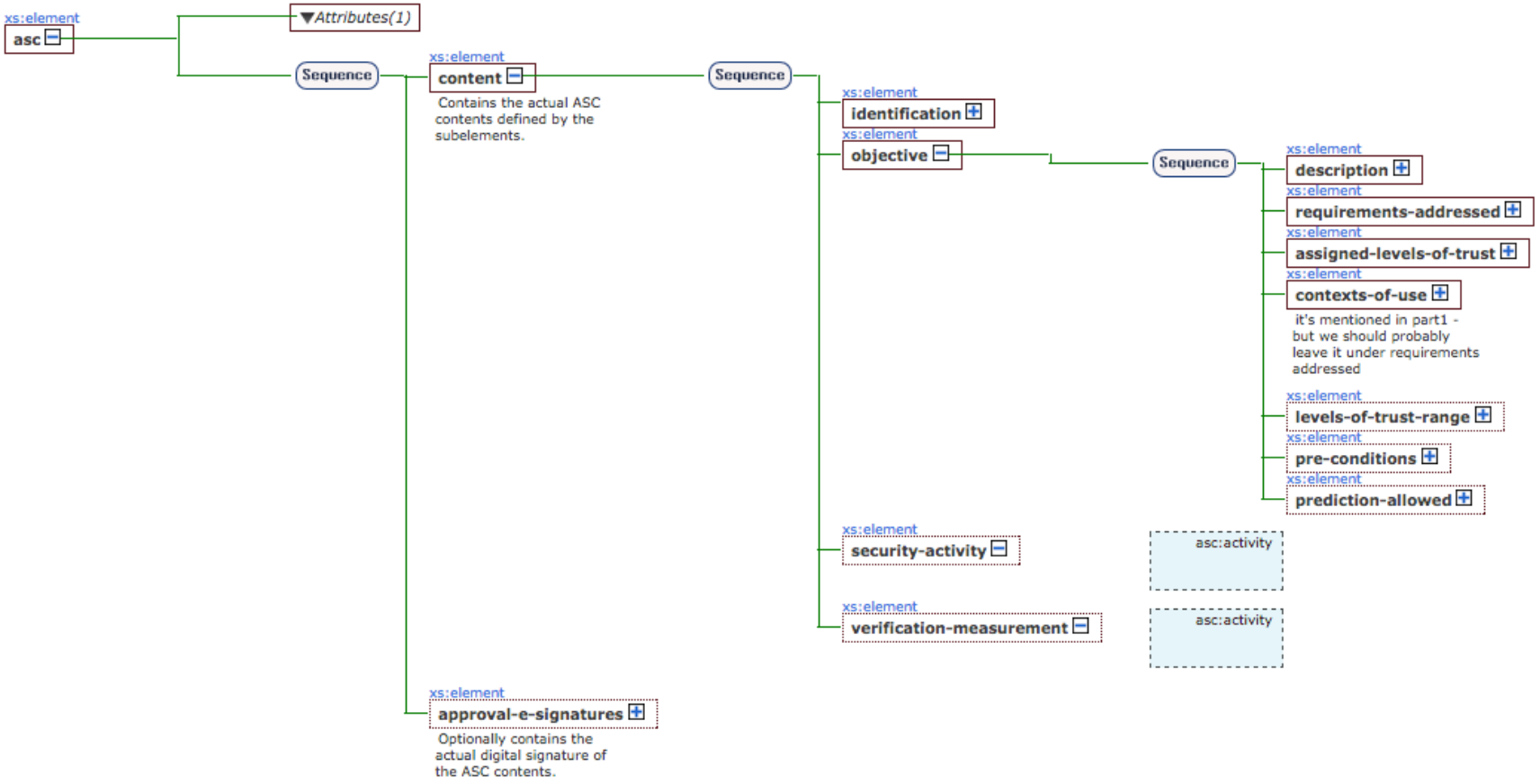
### Security Design Pattern ( Knowledge documentation)



# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

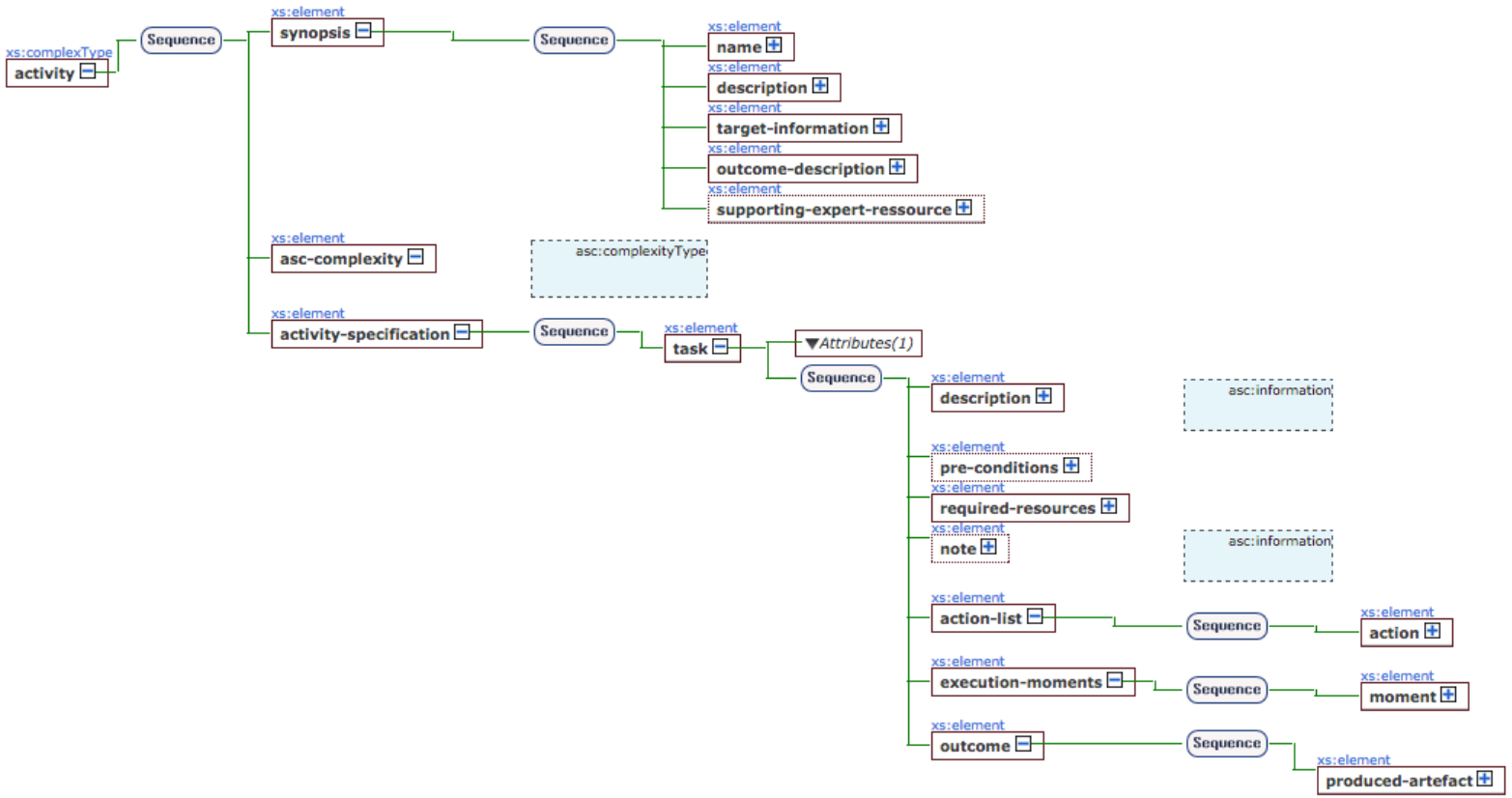
## XML Structure



# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

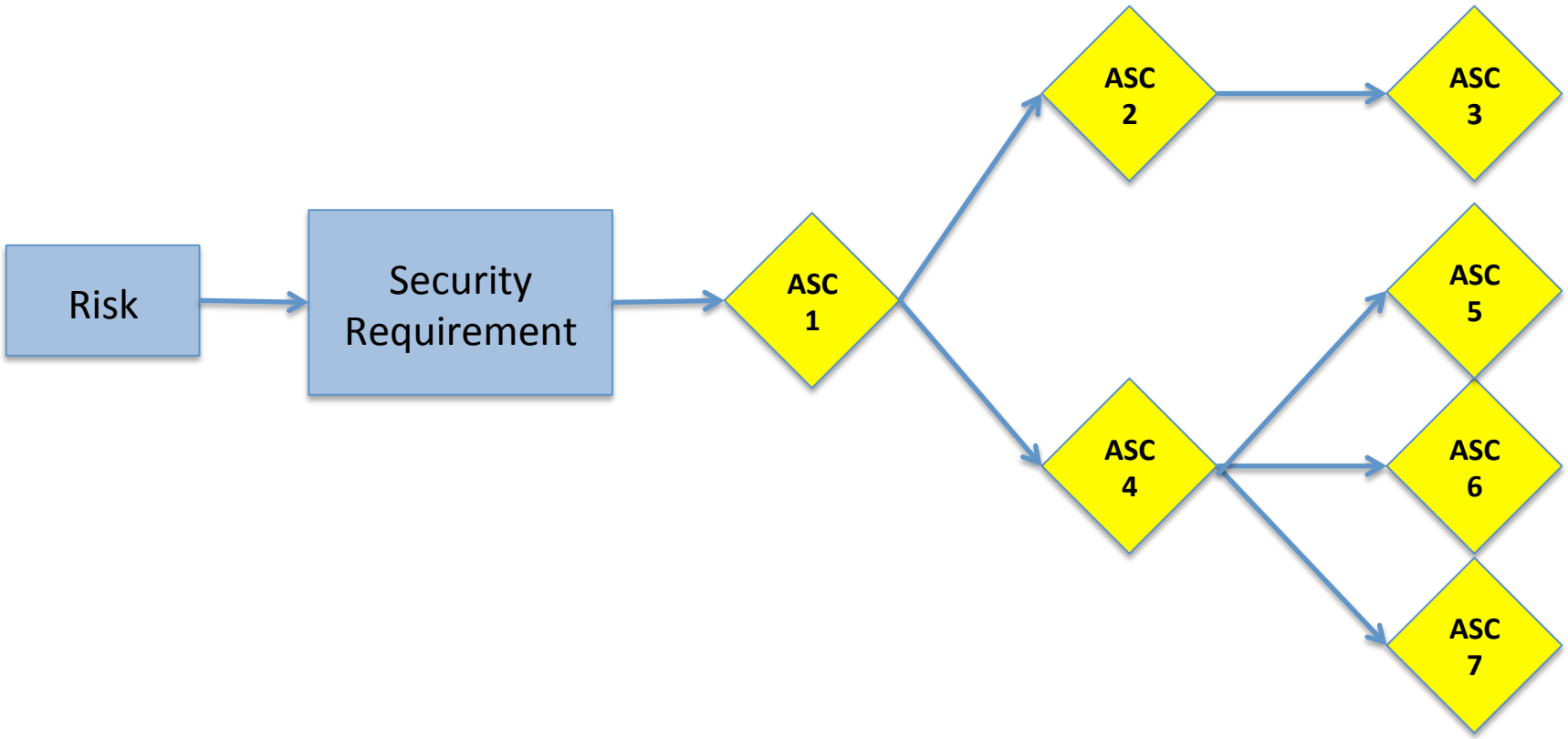
## XML Structure



# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

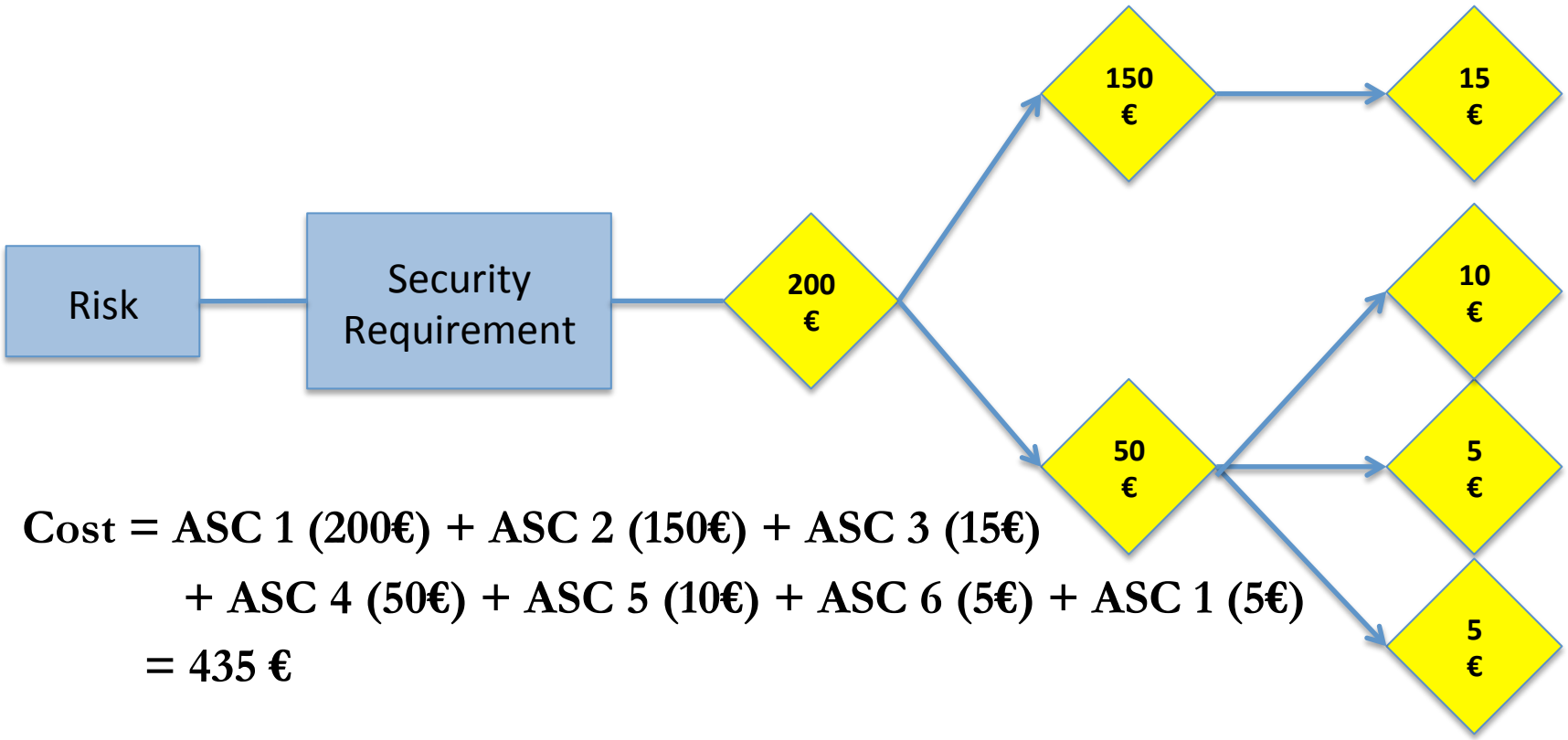
Translate Security Requirements into concrete set of tasks



# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

Use by the business to estimate the cost

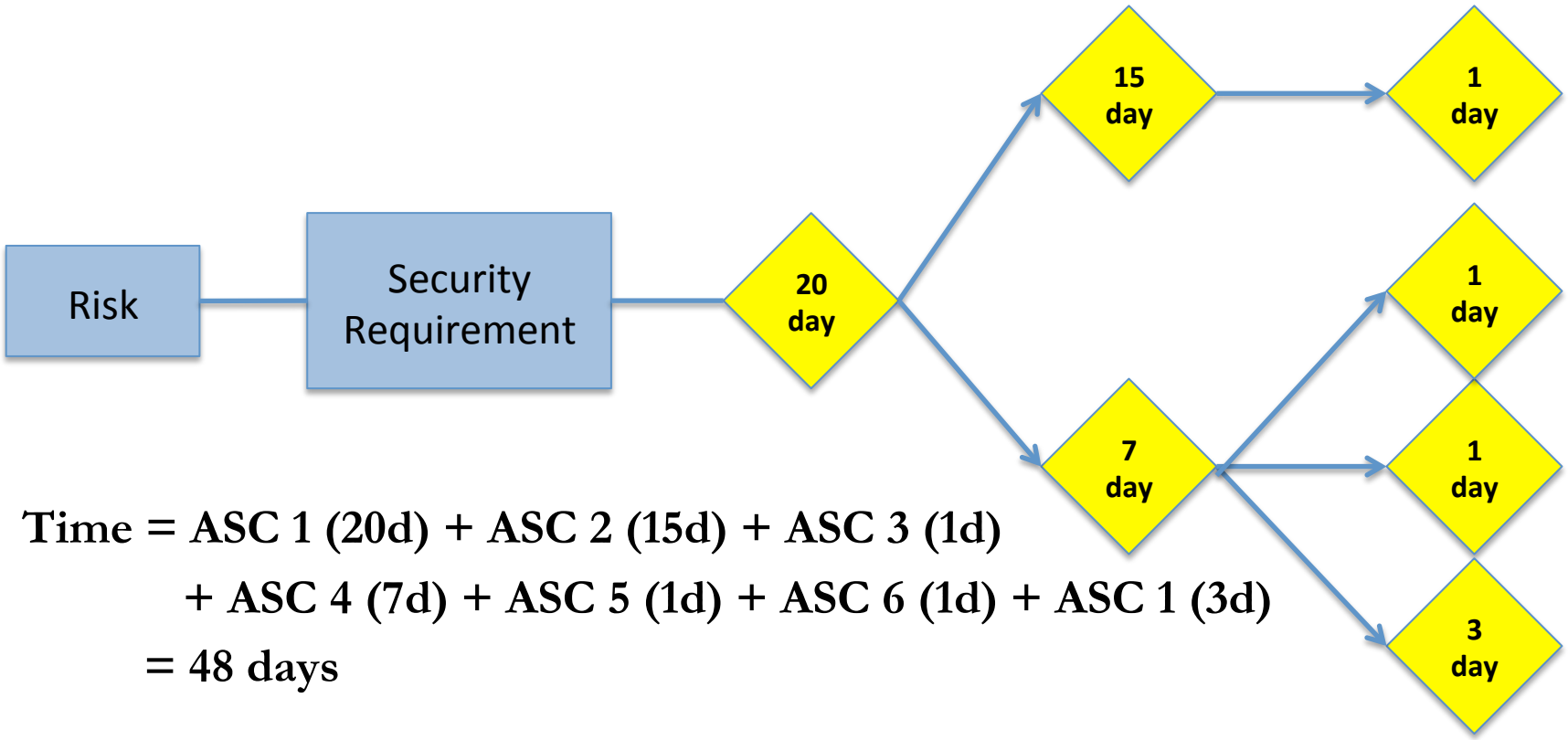



**Cost = ASC 1 (200€) + ASC 2 (150€) + ASC 3 (15€)**
**+ ASC 4 (50€) + ASC 5 (10€) + ASC 6 (5€) + ASC 1 (5€)**
**= 435 €**

# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

Use by the project manager to estimate the time

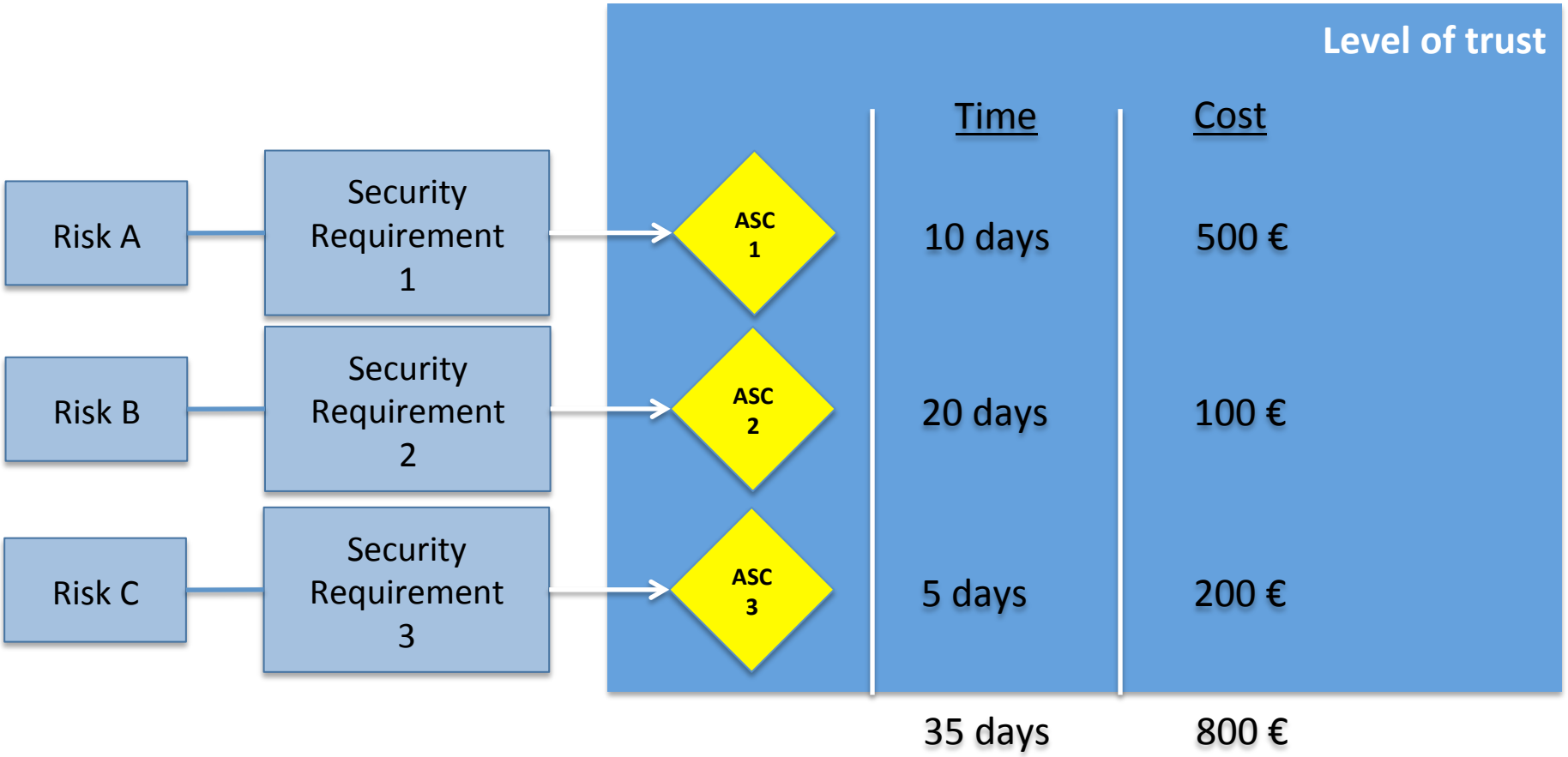



**Time = ASC 1 (20d) + ASC 2 (15d) + ASC 3 (1d)**
**+ ASC 4 (7d) + ASC 5 (1d) + ASC 6 (1d) + ASC 1 (3d)**
**= 48 days**

# 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

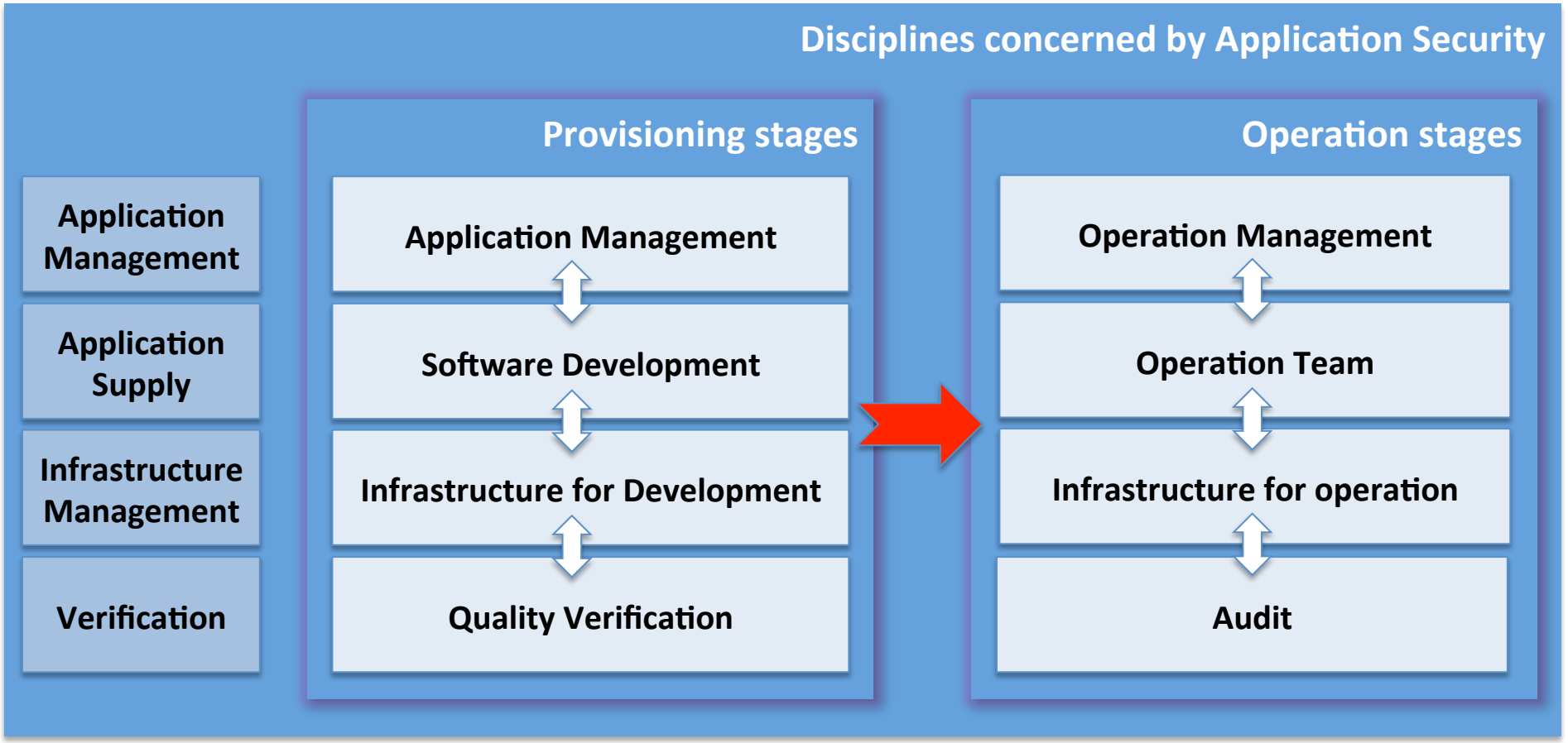
ISO 27034 proposes a global life cycle model

| 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

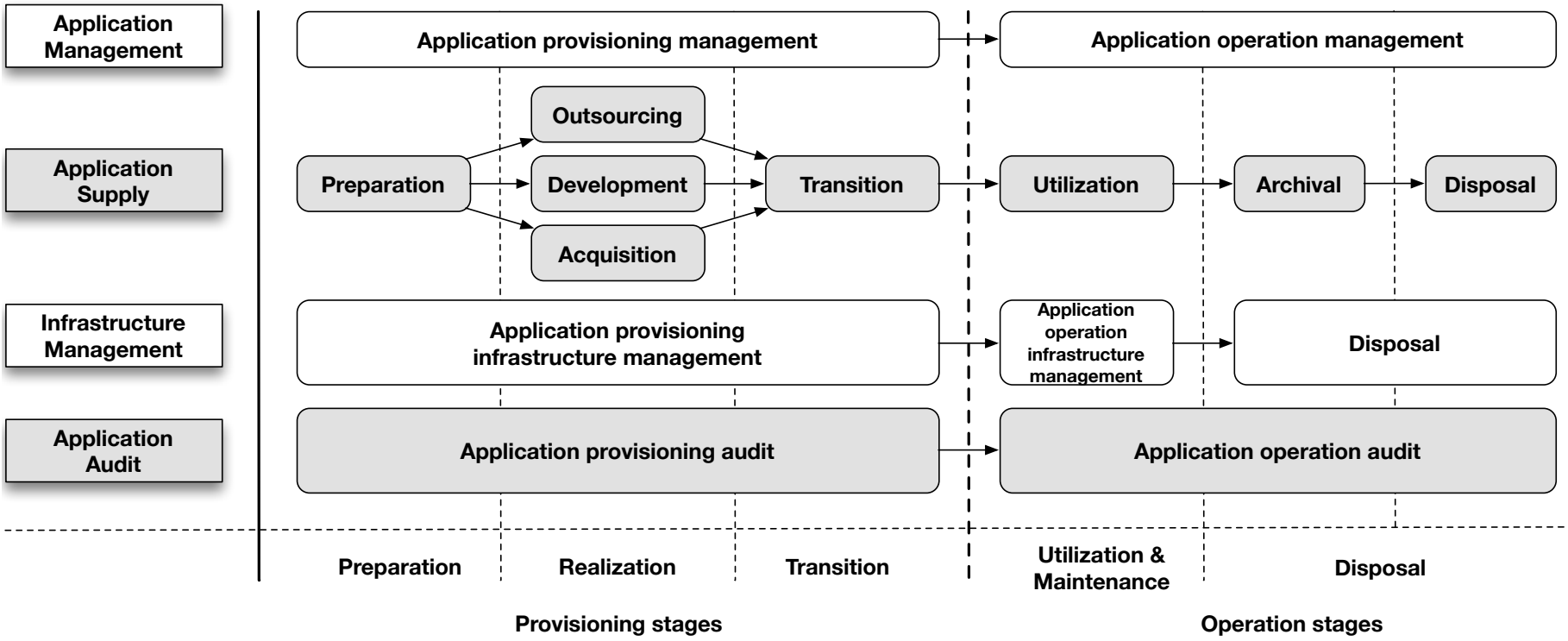


# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

## C. Application Security Life Cycle Model

**A reference Model aligns different disciplines required to produce Secure Application**



## C. Application Security Life Cycle Model

What are the advantages of such model ?

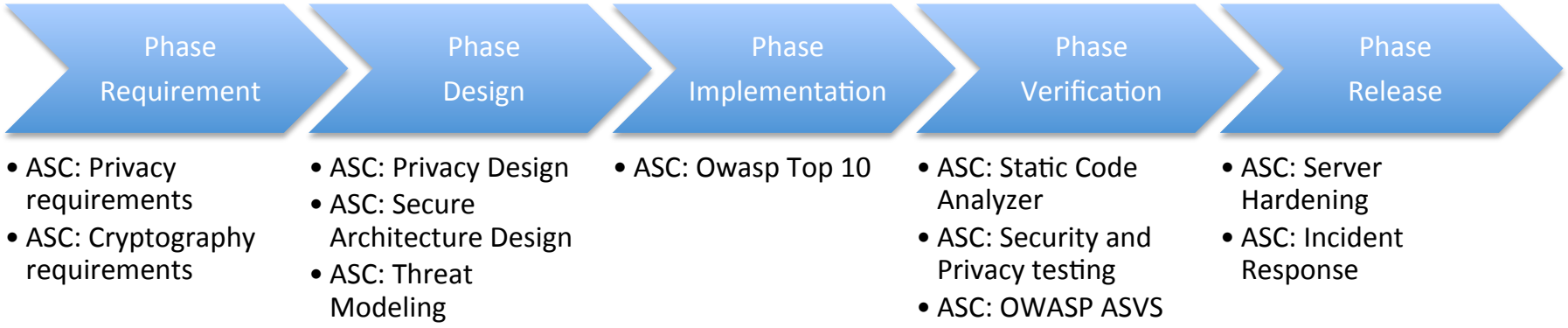
- Create a Helicopter view of different disciplines under the scope of Application Security
- Allow to identify what are missing areas within the organization
- Allow different disciplines to communicate in an effective way
- Allow to choose the right place for an Application Security Controls

# 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 ?

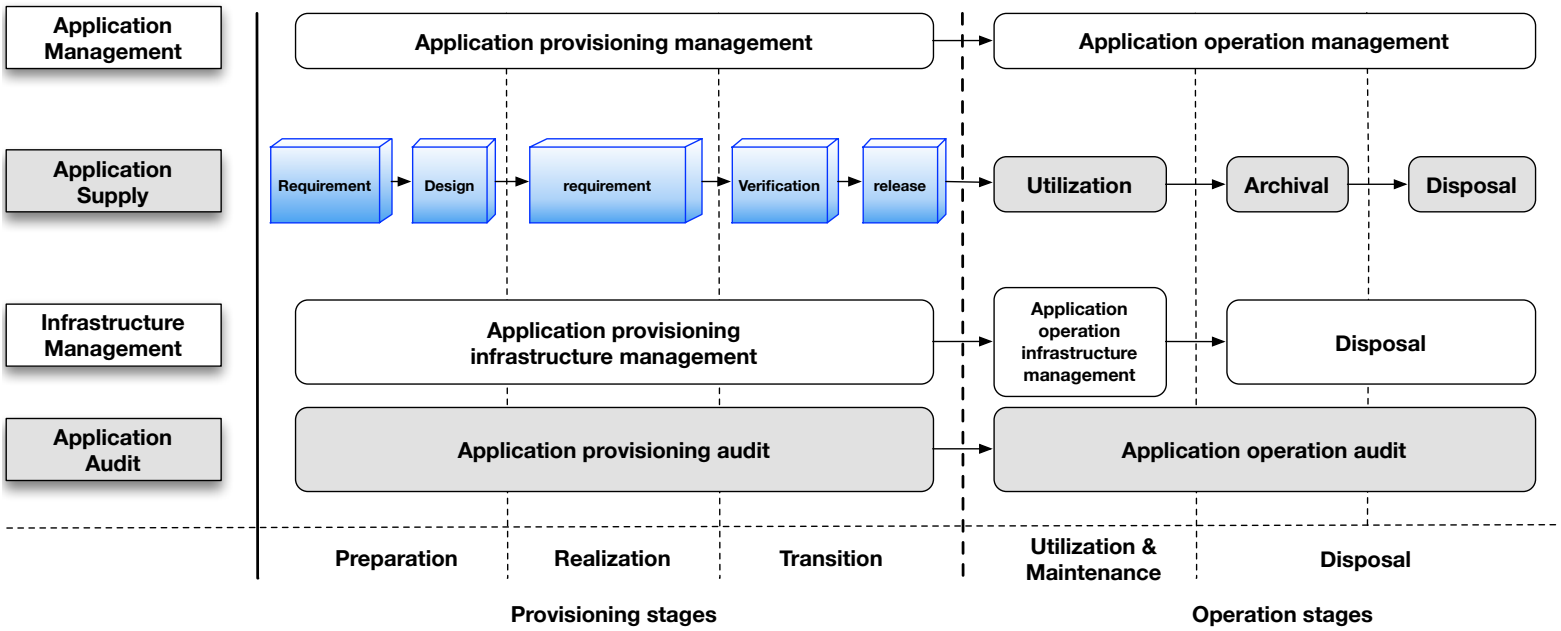


# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

## C. Application Security Life Cycle Model

**Map your current Development life cycle with the reference model**




## Advantages

- Improve the communication between provisioning and operation teams.
- Allow to identify areas not covered by our initial SDLC

Secure Application Development

ICT CONTROL
Your Trusted Advisor

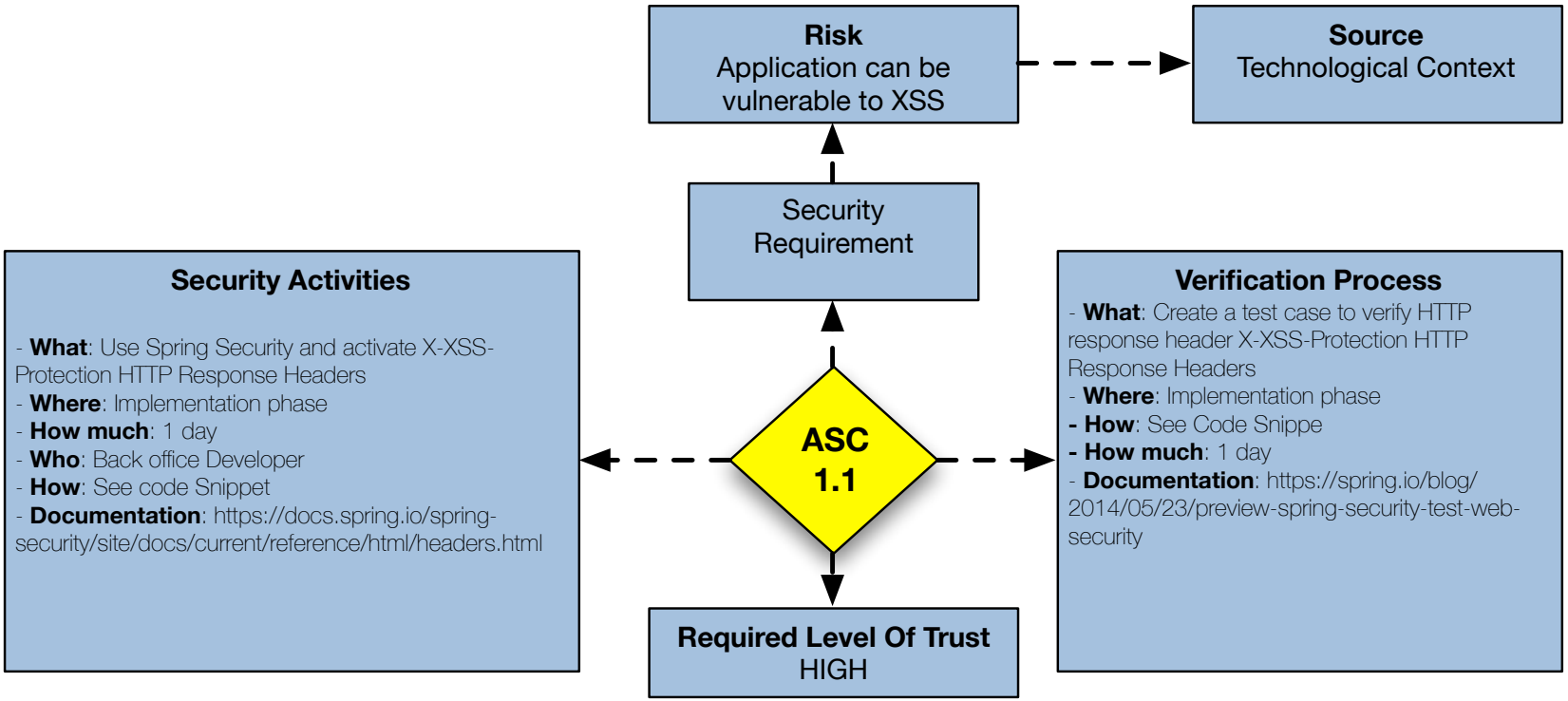
Solvay Brussels School Economics & Management

Cogentas.ca
Application Security Institute

# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

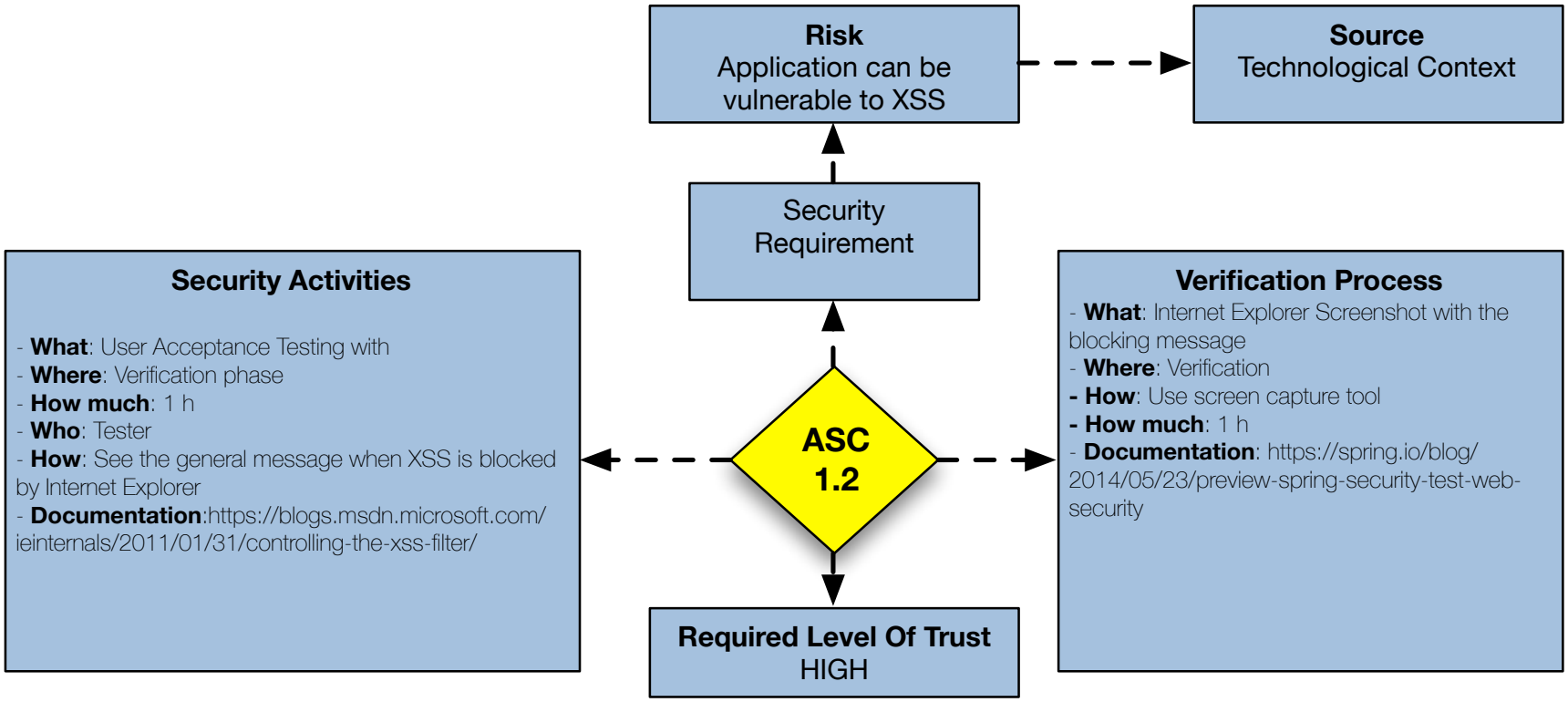
## C. Application Security Life Cycle Model



# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

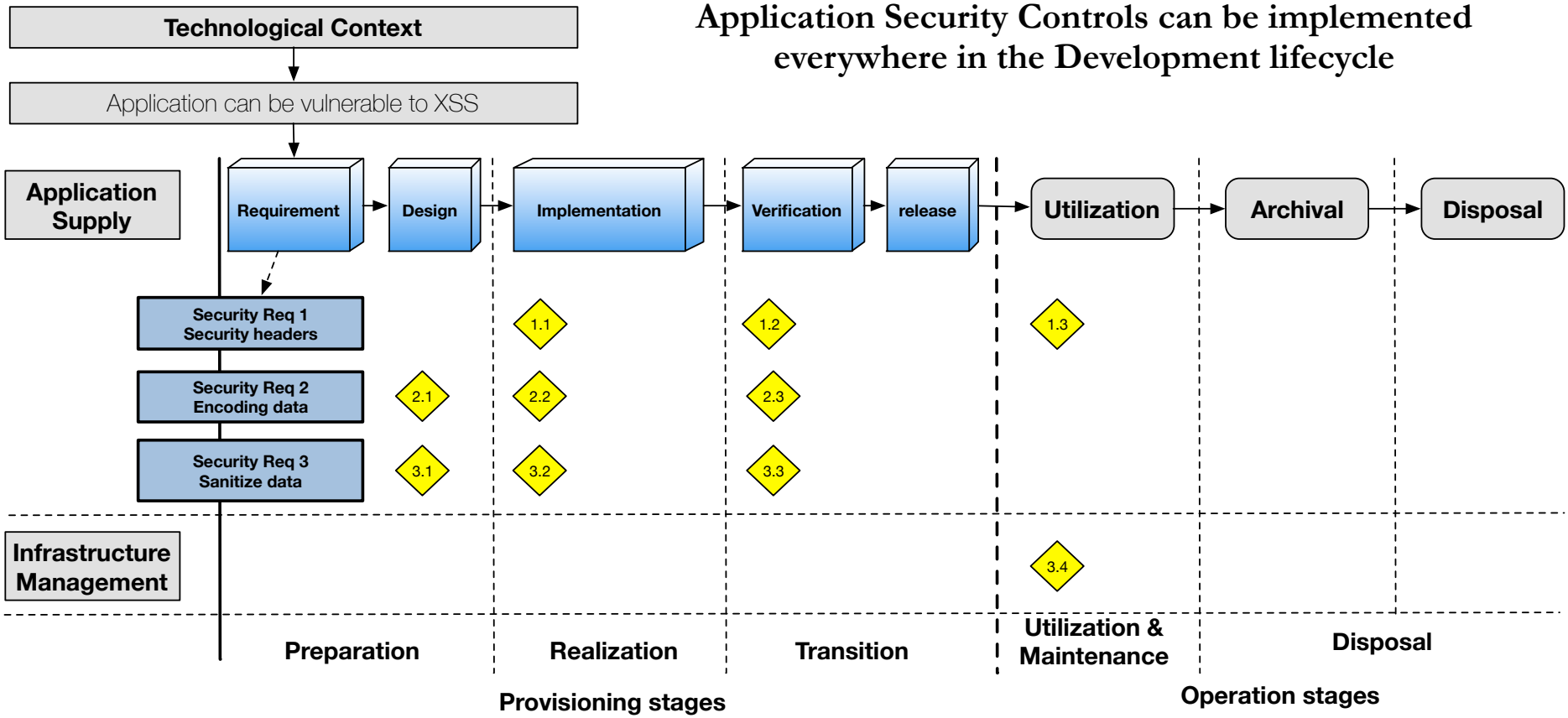
## C. Application Security Life Cycle Model



# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

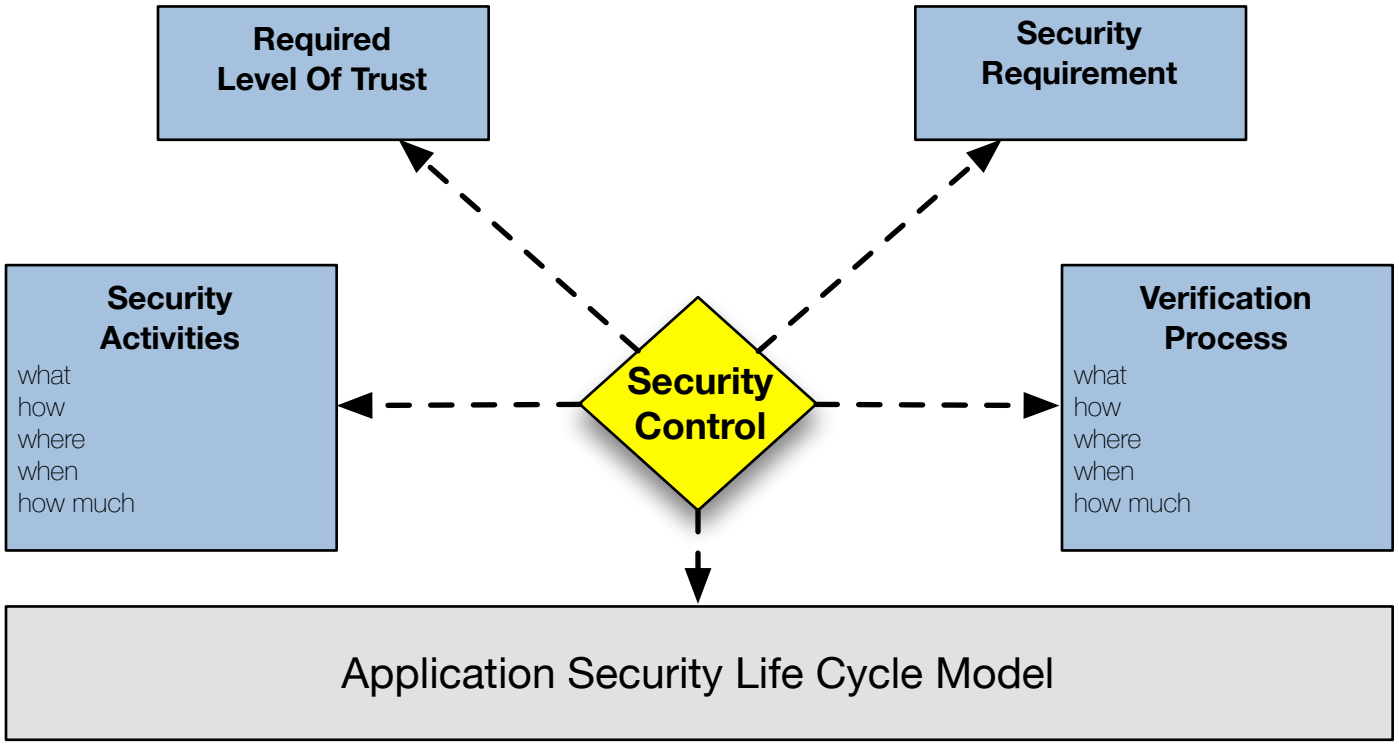
## C. Application Security Life Cycle Model



# Certification of Application Security

## 2.2 Phase 2: Application Security Controls

### C. Application Security Life Cycle Model



# 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

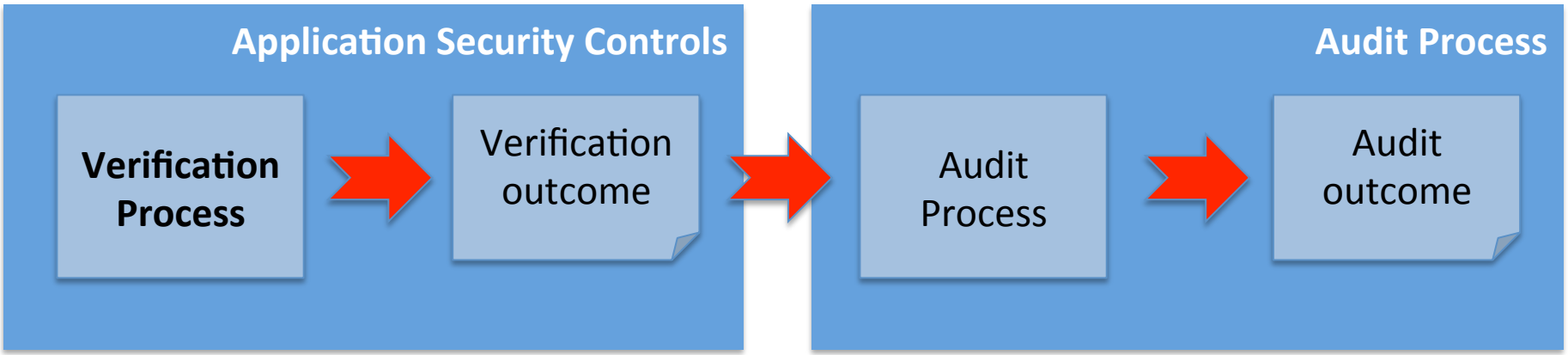
Annex I: Workshop – How can we trust frameworks used inside the company ?

Annex II: Training – ISO 27034 Lead Implementer

# Certification of Application Security

## 2.3 Phase 3: Audit Process

The auditing process starts with the verification outcome



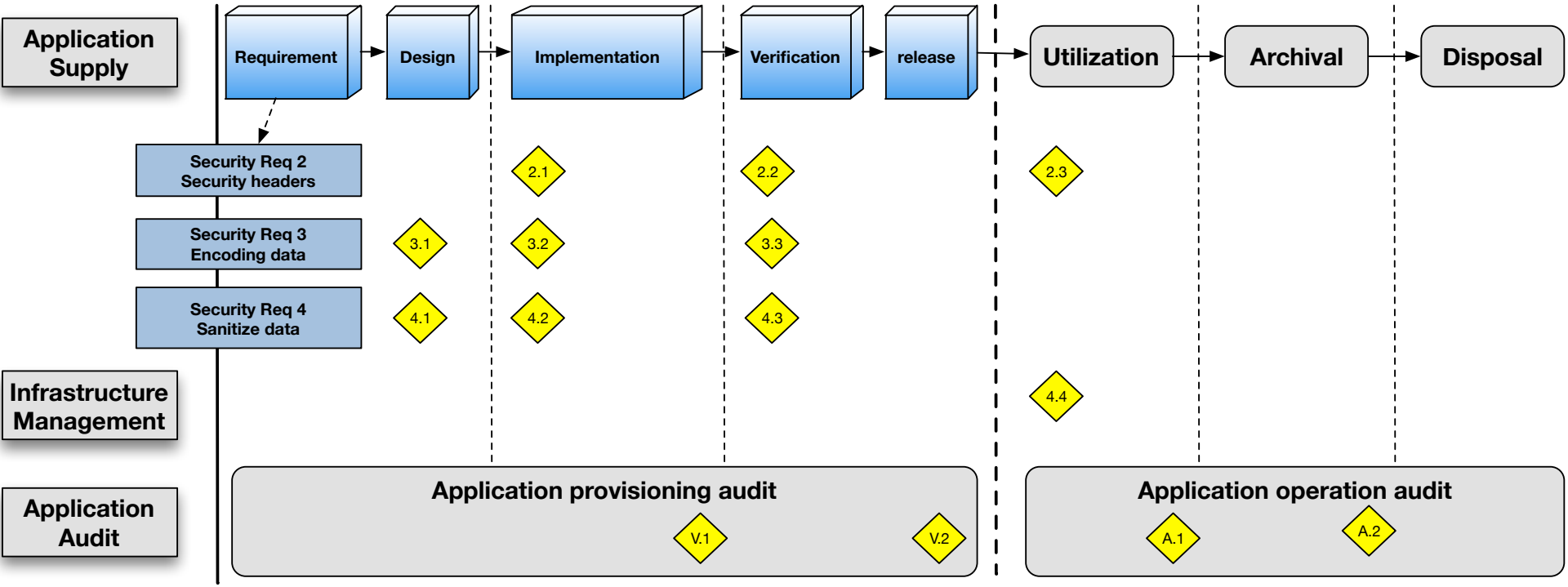

The auditor can check that the verification process was correctly performed.

The auditor can also easily verify the coherence of all the security controls thanks to the helicopter view provided by ISO 27034

# Certification of Application Security

## 2.3 Phase 3: Audit Process

**Audit can be applied anytime during the development lifecycle**




Secure Application Development

ICT CONTROL
Your Trusted Advisor

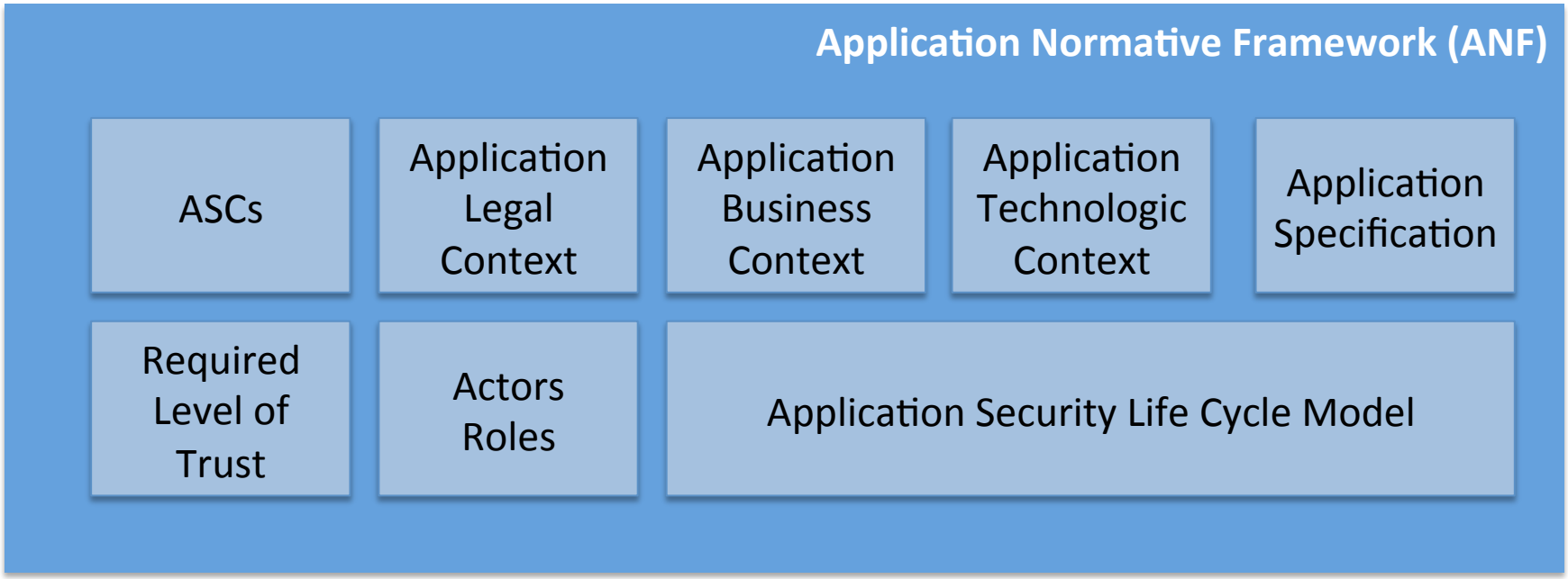
Solvay Brussels School Economics & Management

Cogentas.ca
Application Security Institute

# Certification of Application Security

## 3. ISO 27034 Information Repository

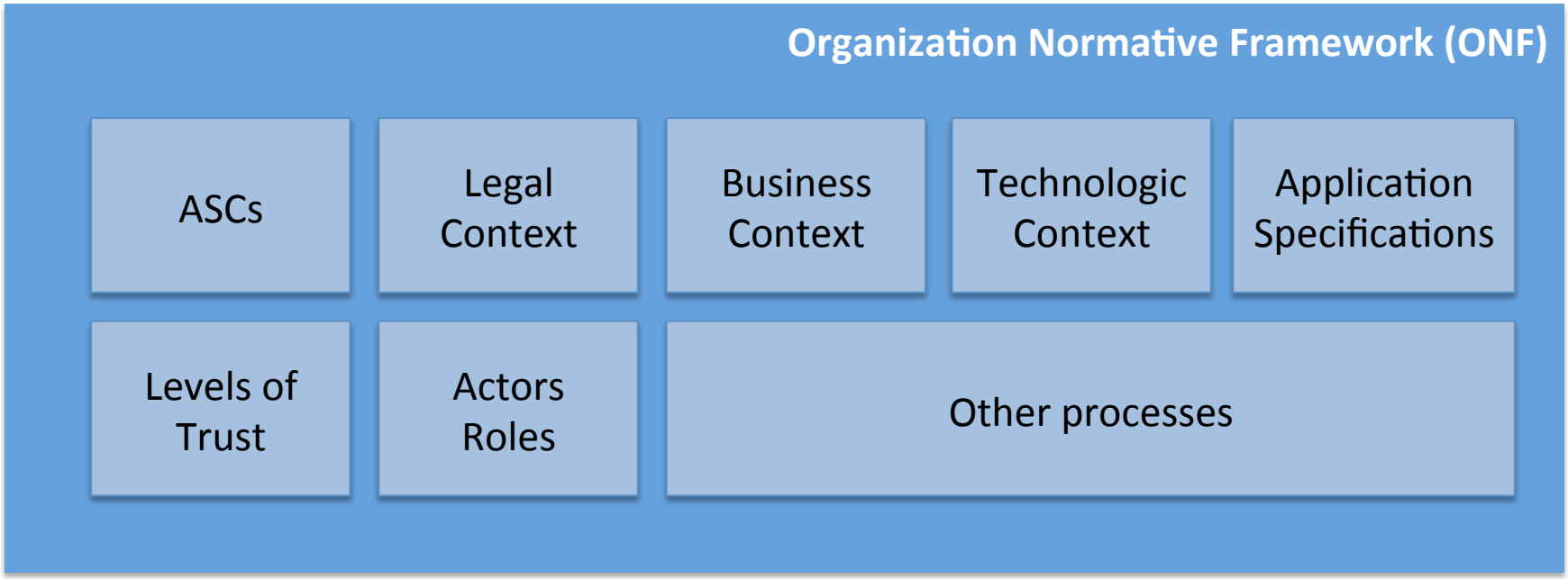
Application Normative Framework is the repository where all files are kept
There is one ANF per application



# Certification of Application Security

## 3. ISO 27034 Information Repository

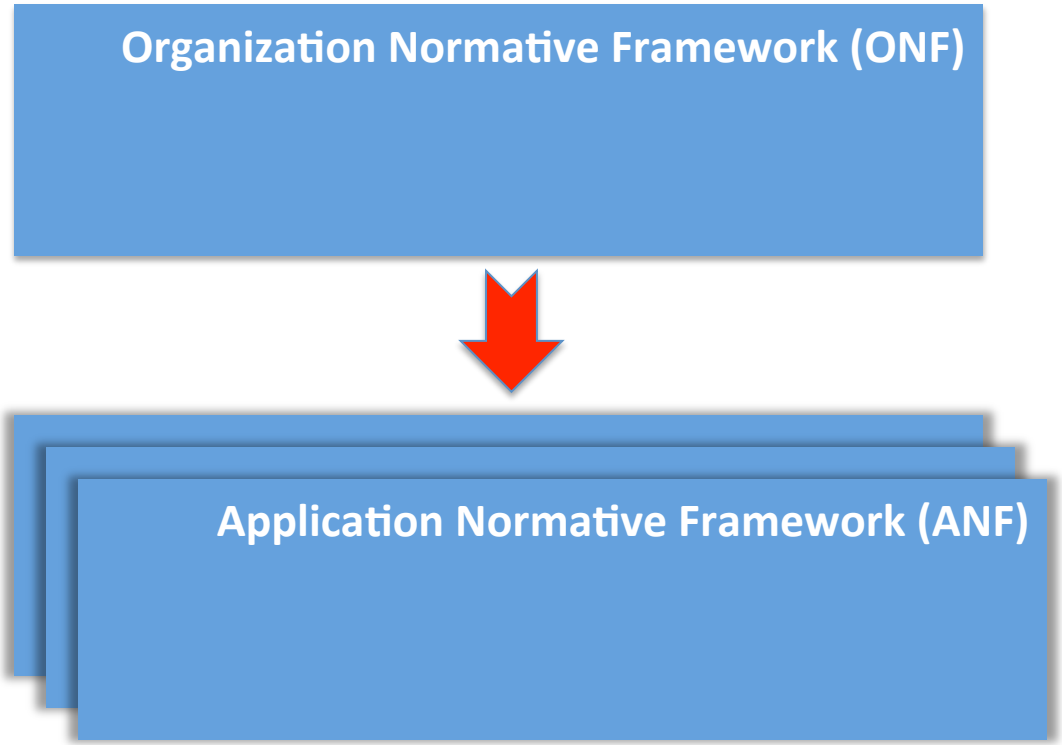
Organization Normative Framework contains all information and it consolidates Application Security across the organization.



# Certification of Application Security

## 3. ISO 27034 Information Repository

Relation between ONF and ANF



# 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: Application Security Controls - XML structure

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

# Certification of Application Security

## 4. Conclusion

ISO 27034 website

http://www.iso27001security.com/html/27034.html

OWASP TOP 10 – ISO 27034: Application Security controls project

https://www.owasp.org/index.php/OWASP_ISO_IEC_27034_Application_Security_Controls_Project

Microsoft SDL conforms to ISO/IEC 27034-1:2011

http://blogs.microsoft.com/cybertrust/2013/05/14/microsoft-sdl-conforms-to-isoiec-27034-12011/

ASIQ: La norme ISO/CEI 27034 – Sécurité des applications

https://asiq.org/evenement/la-norme-iso-cei-27034/

# Certification of Application Security

## 4. Conclusion


In 2016, Application Security cannot be just 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

## 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

## Annex II: Workshop - How can we trust third party frameworks ?

Spring Security is a great framework with a lot of security features. One of them is a mechanism that handle Http Response Headers.

Default Spring Security Headers

- Cache Control
- Content Type Options
- HTTP Strict Transport Security
- X-Frame Options
- X-XSS Protection

# Certification of Application Security

## Annex II: Workshop - How can we trust third party frameworks ?

Documentation: List of usefull HTTP Headers

https://www.owasp.org/index.php/List_of_useful_HTTP_headers

| Header | Spring support |
|---|---|
| Public Key Pinning Extension for HTTP | Custom |
| Strict-Transport-Security | Default |
| X-Frame-Options,Frame-Options | Default |
| X-XSS-Protection | Default |
| X-Content-Type-Options | Custom |
| Content-Security-Policy, X-Content-Security-Policy, X-WebKit-CSP | Custom |
| Content-Security-Policy-Report-Only | Custom |

# Certification of Application Security

## Annex II: Workshop - How can we trust third party frameworks ?

Let's start with a Default HTTP Response:

**HTTP Strict Transport Security Header**

According to the Spring Security documentation

If you omit the https protocol, you are potentially vulnerable to Man in the Middle attacks. Even if the website performs a redirect a malicious user could intercept the initial HTTP request and manipulate the response.

Many users omit the https protocol and this is why HTTP Strict Transport Security (HSTS) was created. A browser can know ahead of time that any request to http://mybank.example.com should be interpreted as https://mybank.example.com. This greatly reduces the possibility of a Man in the Middle attack occurring.

## Annex II: Workshop - How can we trust third party frameworks ?

According to the Spring Security documentation

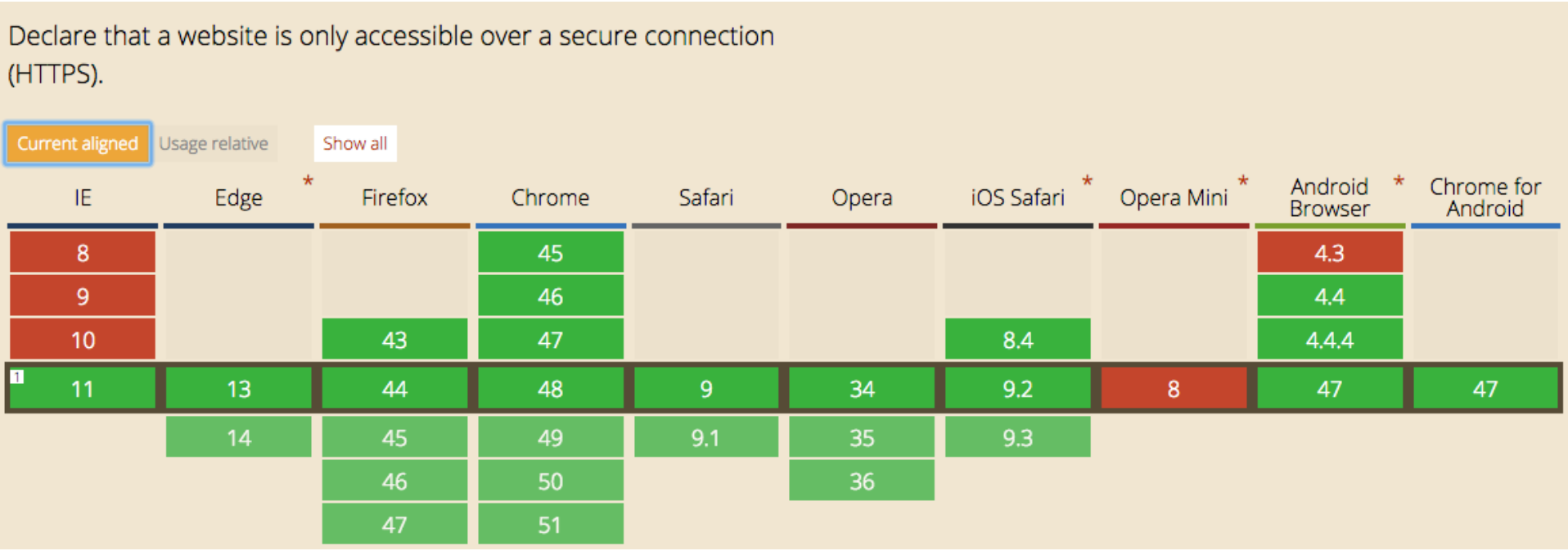
While each of these headers are considered best practice, it should be noted that not all clients utilize the headers, so additional testing is encouraged.

# Certification of Application Security

## Annex II: Workshop - How can we trust third party frameworks ?

Check browser support table for HTTP Strict Transport Security

Source: http://caniuse.com/#feat=stricttransportsecurity




Secure Application Development

ICT CONTROL
Your Trusted Advisor

Solvay Brussels School Economics & Management

Cogentas.ca
Application Security Institute

# Certification of Application Security

## Annex II: Workshop - How can we trust third party frameworks ?

### Security Activity

How to implement HTTP Strict Transport Security with Spring Security ?

```
@EnableWebSecurity
public class WebSecurityConfig extends
WebSecurityConfigurerAdapter {

@Override
protected void configure(HttpSecurity http) throws Exception {
        http
        // ...
        .headers()
                .httpStrictTransportSecurity()
                        .includeSubdomains(true)
                        .maxAgeSeconds(31536000);
}
}
```

Cost: 0,5 day

Who: Developer

Where: Implementation phase

# Annex II: Workshop - How can we trust third party frameworks ?

## Verification Activity

### How to test HTTP Headers

```
public class HstsHeaderWriterTests {
   …

   @Before
   public void setup() {
      request = new MockHttpServletRequest();
      response = new MockHttpServletResponse();
      writer = new HstsHeaderWriter();
   }

   @Test
   public void allArgsCustomConstructorWriteHeaders() {
      writer = new HstsHeaderWriter(AnyRequestMatcher.INSTANCE, 15768000, false);
      writer.writeHeaders(request, response);
      assertThat(response.getHeaderNames().size()).isEqualTo(1);
      assertThat(response.getHeader("Strict-Transport-Security")).isEqualTo("max-age=15768000");
   }
}
```

Cost: 0,5

Where: Implementation Phase

# Certification of Application Security

## Annex II: Workshop - How can we trust third party frameworks ?

Is our testing strategy good enough ?

NO

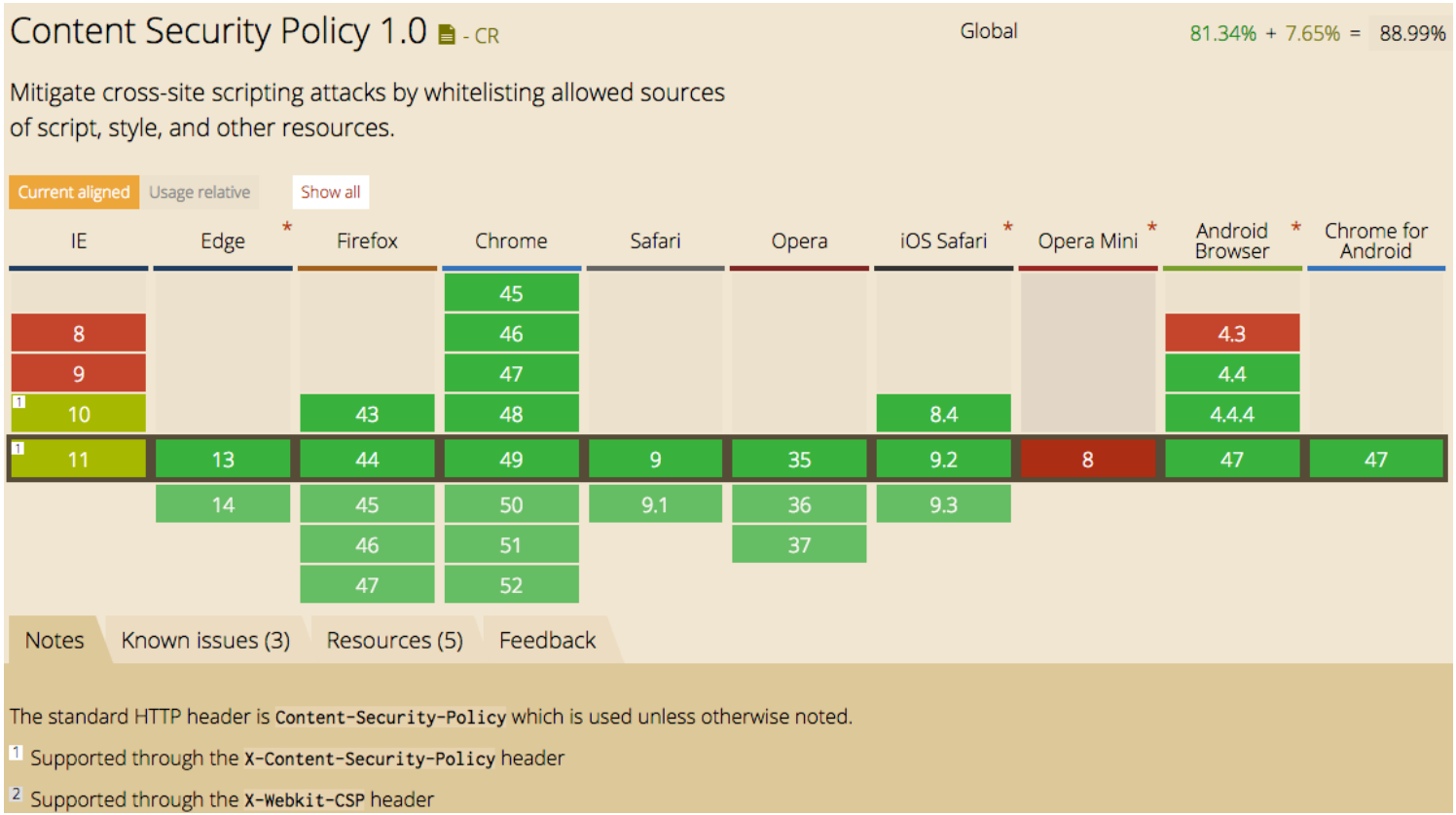
**Unsecure scenario**

- No HTTPS configuration on the production server.
  - ASC: We need another ASC to test Https
- Some browsers do not support the HTTP response header.
  - ASC: How can we discover when a browser is not supporting this header ?

# Certification of Application Security

## Annex II: Workshop - How can we trust third party frameworks ?

Let's continue with a Custom Header: Content Security Policy 1.0




Secure Application Development

ICT CONTROL
Your Trusted Advisor

Solvay Brussels School Economics & Management

Cogentas.ca
Application Security Institute

# Certification of Application Security

## Annex II: Workshop - How can we trust third party frameworks ?

Security Activity

How to implement Content Security Policy 1.0 with Spring Security ?

```
@EnableWebSecurity
public class WebSecurityConfig extends
WebSecurityConfigurerAdapter {

@Override
protected void configure(HttpSecurity http) throws Exception {
        http
        // ...
        .headers()
                .addHeaderWriter(new StaticHeadersWriter("X-Content-Security-Policy","default-src 'self'"))
                .addHeaderWriter(new StaticHeadersWriter("X-WebKit-CSP","default-src 'self'"));
}
}
```

Cost: 0,5 day

Who: Developer

Where: Implementation phase

# Certification of Application Security

## Annex II: Workshop - How can we trust third party frameworks ?

### Verification Activity

How to test HTTP Headers

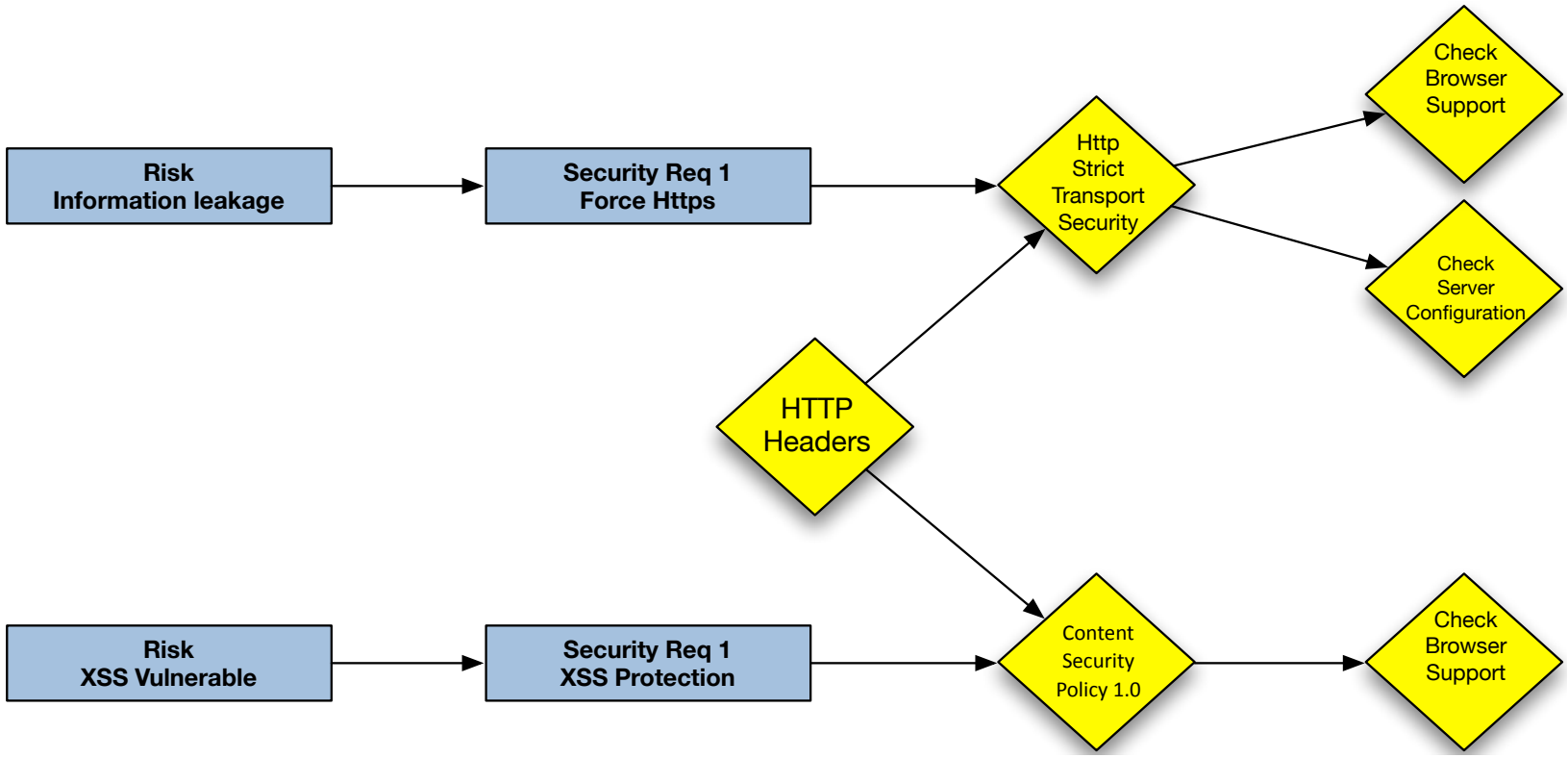
```
public class HstsHeaderWriterTests {
   …

   @Before
   public void setup() {
      request = new MockHttpServletRequest();
      response = new MockHttpServletResponse();
      writer = new HstsHeaderWriter();
   }

   @Test
   public void allArgsCustomConstructorWriteHeaders() {
      writer = new HstsHeaderWriter(AnyRequestMatcher.INSTANCE, 15768000, false);
      writer.writeHeaders(request, response);
      assertThat(response.getHeaderNames().size()).isEqualTo(1);
      assertThat(response.getHeader("Content-Security-Policy")).isEqualTo("default-src 'self'; .");
      assertThat(response.getHeader(" X-WebKit-CSP)).isEqualTo("default-src 'self'; .");
   }
}
```

Cost: 0,5

Where: Implementation Phase

# Certification of Application Security

## Annex II: Workshop - How can we trust third party frameworks ?



# 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

## 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