Agile Information Security Management in Software R&D

Rational and WebSphere User Group Finland Seminar 29.01.2008

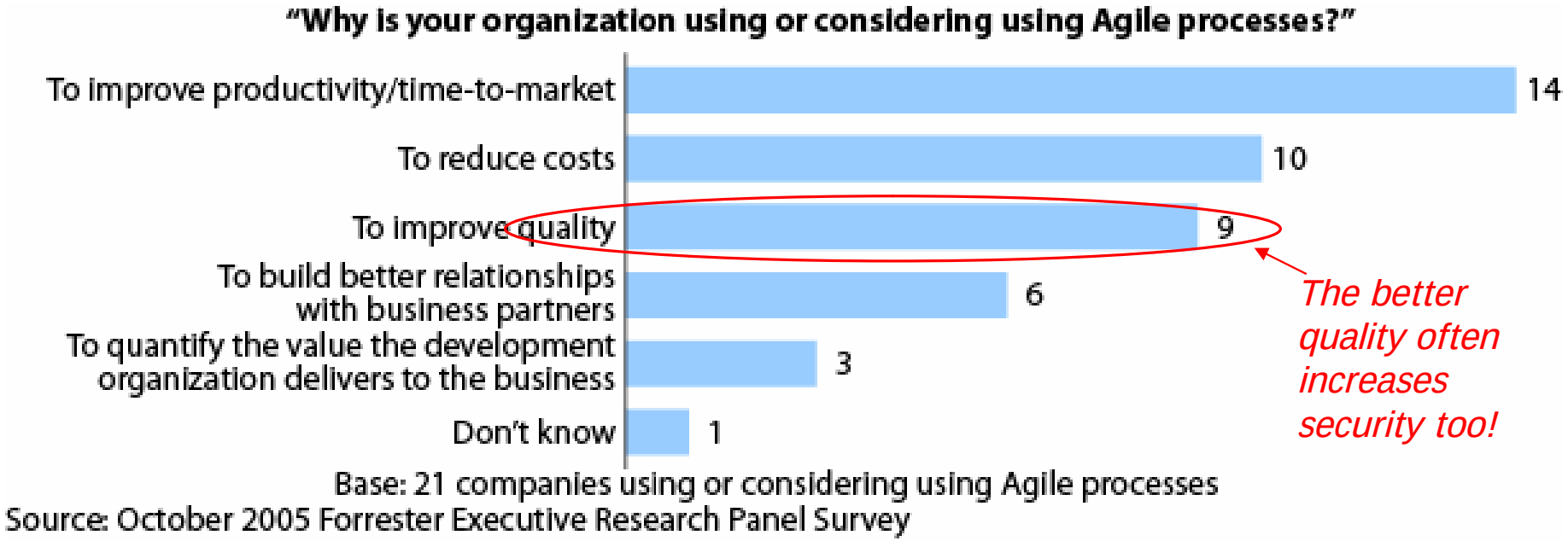
Reijo Savola
Network and Information Security Research Coordinator
VTT Technical Research Centre of Finland

Contents

- Information Security from the Perspective of Agility
- Some Information Security Challenges and Trends
- Security Assurance and Agile Security Development
- Conclusions

I
Information Security from the Perspective of Agility

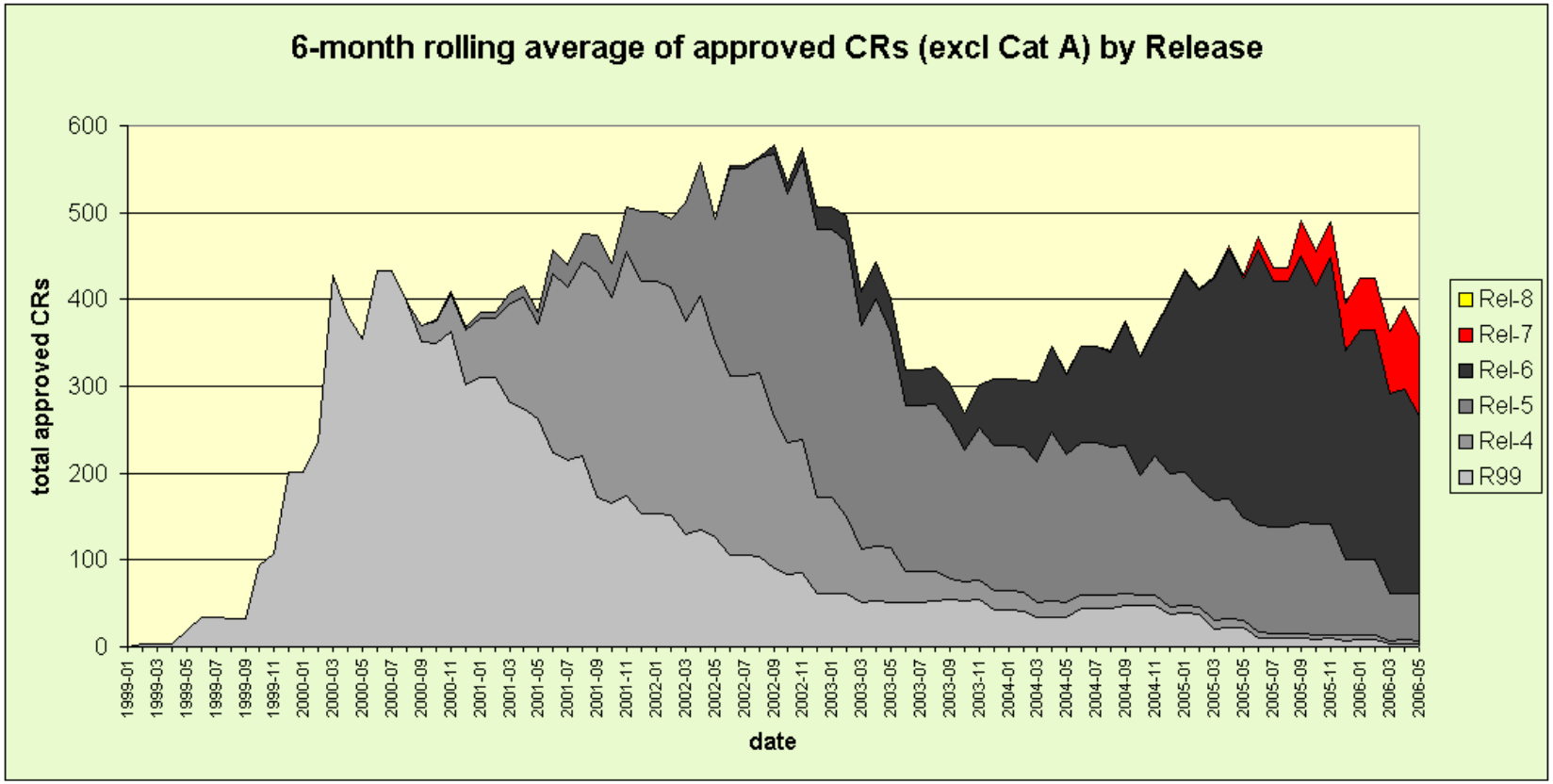
Business Rationale for Agile Adoption



Source: prof. Pekka Abrahamsson / VTT

Change is the Only Certainty in Software Research & Development

The production of Technical Specifications for a 3rd Generation Mobile System based on the evolved GSM core networks.



Change management is very important from security point-of-view

Source: prof. Pekka Abrahamsson / VTT

How Agile Can You Be?

Personnel
(% Level 1B) (% Level 2&3)

40 15
30 20
20 25
10 30
0 35

Criticality
(Loss due to impact of defects)

Many Lives
Single Life
Essential Funds
Discretionary Funds
Comfort

Dynamism
(% Requirements-change/month)

50 30 10 5 1

Size
(# of personnel)

3 10 30 100 300

90 70 50 30 10

Agile
Disciplined

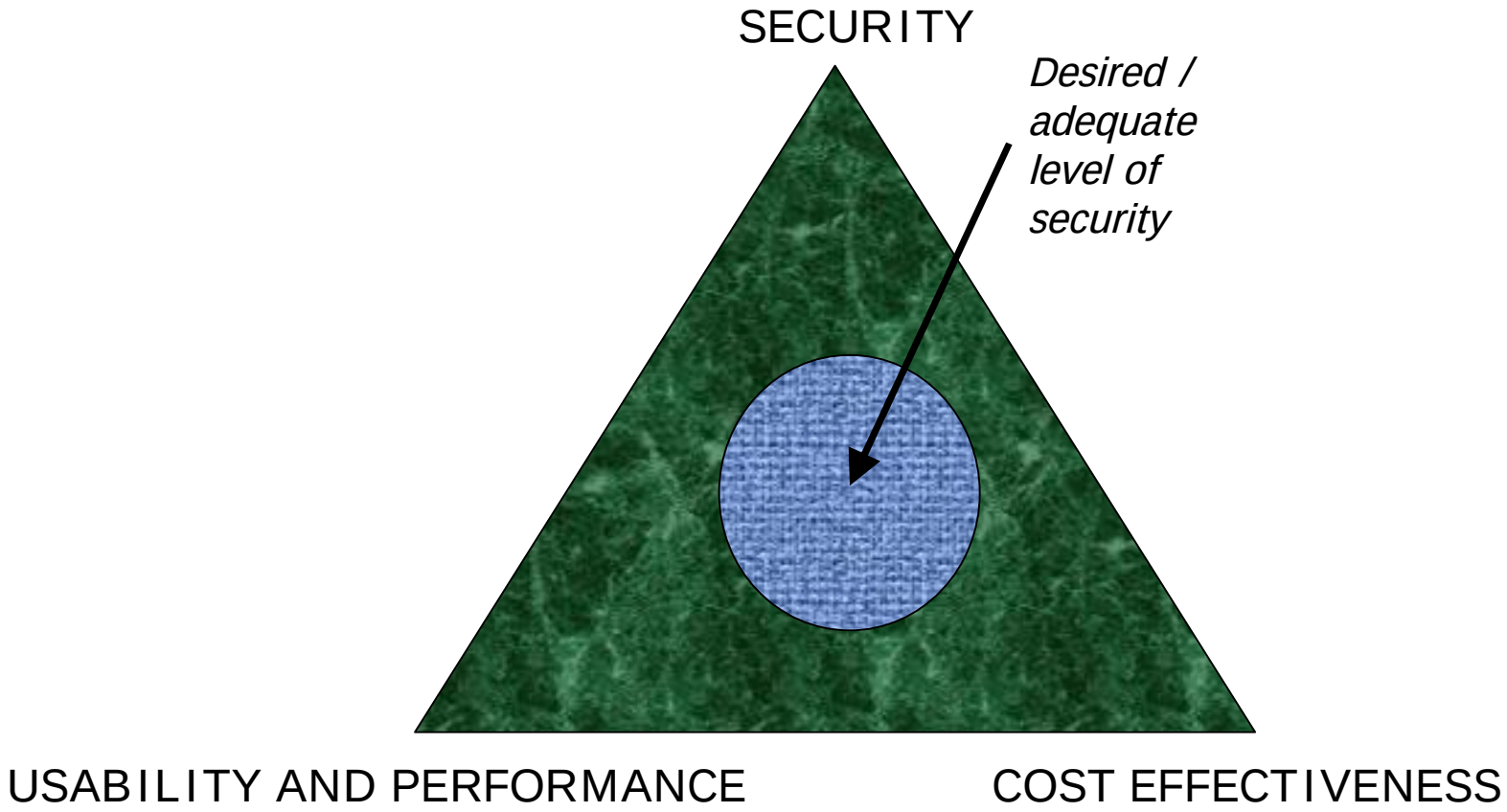
Culture
(% thriving on chaos vs. order)

Source: prof. Pekka Abrahamsson / VTT

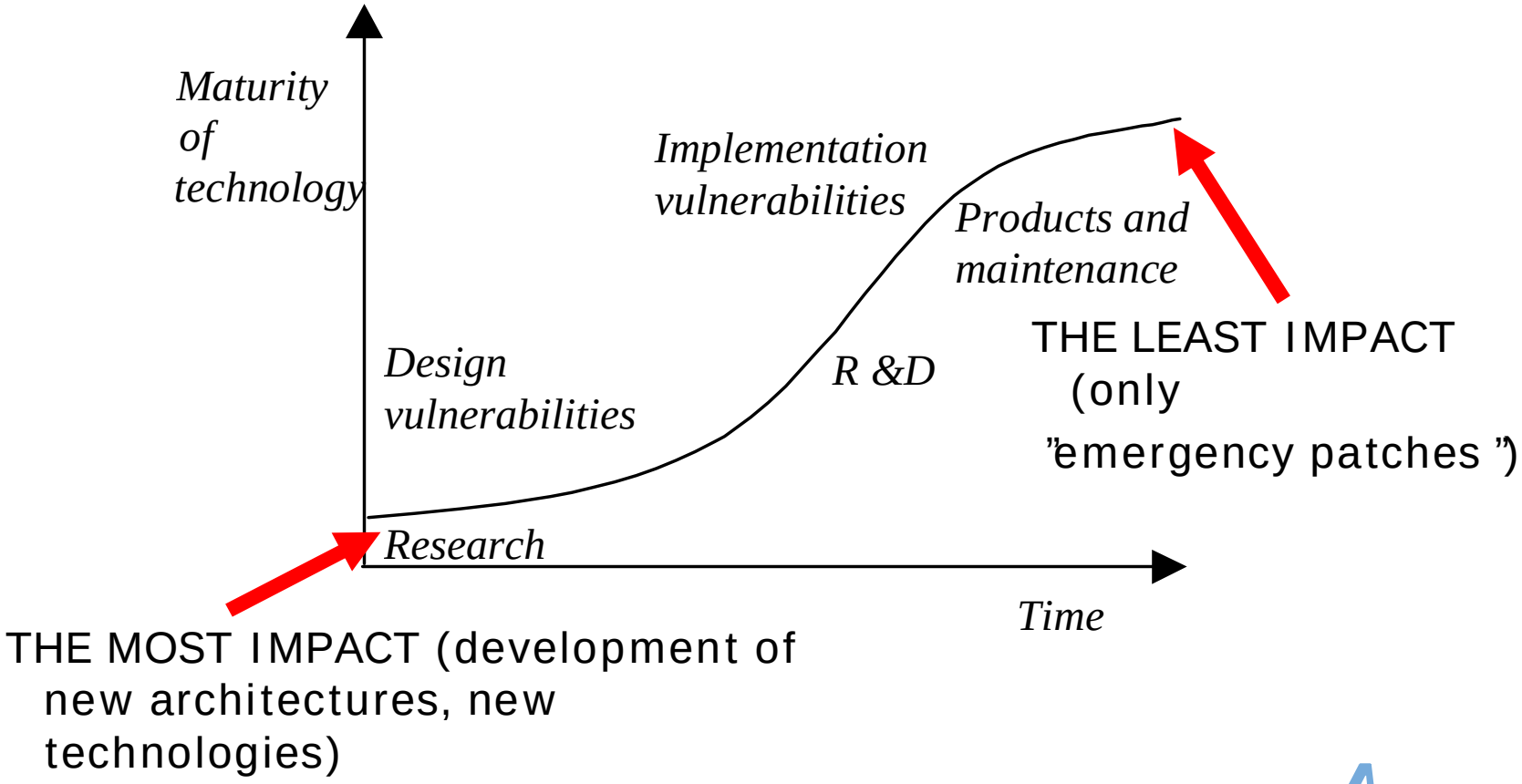
Source: Boehm & Turner (2003)

Fact corner:
Agile is not an absolute Concept.

Goal: Balanced Information Security



Proactive Security Solutions Have Most Impact!



Introduction

The Horizontal Nature of Information Security

- *Telecom engineers:* security is protocols, cryptography, key exchange techniques
- *Software engineers:* security means secure SW architectures
- *Content providers:* security is DRM
- *IT department:* security means proxies, firewalls and audits

and if really needed, security policies

- *Lawyers:* security means how you conform to privacy legislation
- *Process addicts:* security is a business process
- *Managers:* security is OK, but it cannot cost anything
- *Quality people:* security is realized as one or more quality attributes, the meaning of which can be described in an ontology
- *Written definition "everywhere":* security is confidentiality, integrity, availability, non-repudiation, authentication

Security vs. Agility?

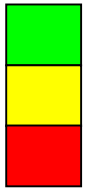
- Agility: developers are more responsive to business concerns
- Security: developers are more responsive to business risk concerns

ØTradeoffs to be managed

Two steps that should be taken care of:

- Increase security awareness among developers and managers
- Build security in the processes, practices and tools

The 12 Agile Principles – Good for Security too!



"Security rating"

1. Satisfy customer through early and frequent delivery	2. Welcome changing requirements even late in the project	3. Deliver working software frequently
4. Business people and developers work together daily throughout the project	5. Build projects around motivated individuals	6. Place emphasis on face-to-face communication
7. Working software is the primary measure of progress	8. Promote sustainable development pace	9. Continuous attention to technical excellence and good design
10. Simplicity is essential	11. The best results emerge from self-organizing teams	12. Team reflects regularly where and how to improve

Source: prof. Pekka Abrahamsson / VTT

II
Some Information Security Challenges and Trends

Security Threats are Increasing

COMPLEXITY AND CONVERGENCE…

Products, value nets, services and telecommunication networks are getting more and more complex

- Holistic understanding of security needed
- Challenge for agility too!

TIGHT TIME SCHEDULES…

Market sets tight time schedules to product development and thequality and security of products is in danger.

- Security awareness should increased

REACTIVE RACE IS BECOMING TOUGHER…

Security threat picture changes all the time. Security work has been lately a race between the attackers and the protection developers.

- Emphasis from reactive to proactive solutions
- Break the passive ”build-break-fix ”cycle!
- Agility helps!

Security Threats are Increasing

DIFFUSION OF ICT SOLUTIONS

ICT solutions are being used in other fields

- § Security awareness and careful planning needed
- § Agility cannot be applied much

DEPENDENCE OF CRITICAL INFRASTRUCTURES ON ICT

In critical infrastructures, such as electricy distribution, ICT solutions are used more and more

- § Understanding of interdependencies needed
- § Agility cannot be applied much

III
Security Assurance and Agile Security Development

Security Assurance: Emerging Novel Techniques and Tools

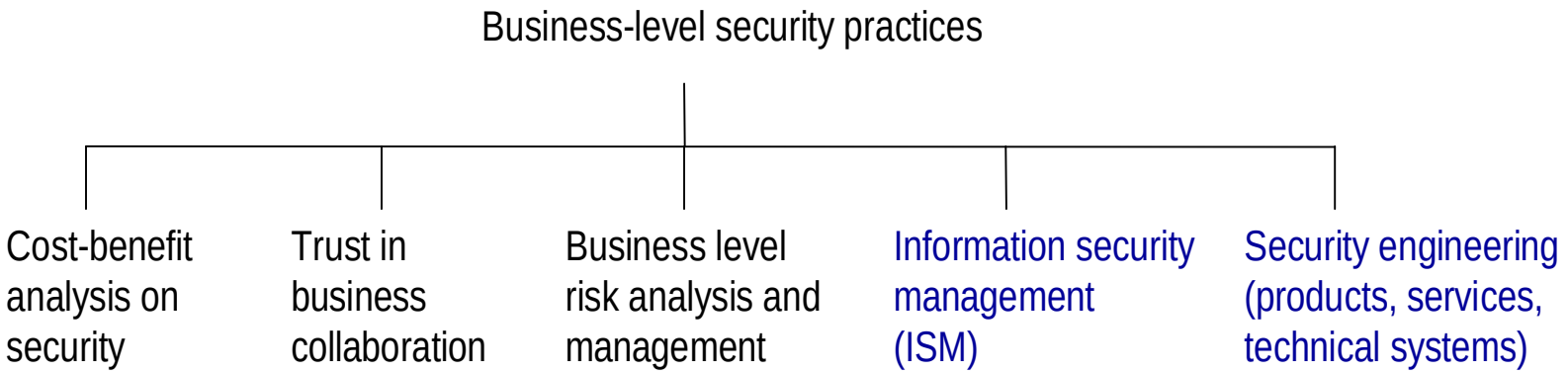
Security assurance activities are needed in agile SW R&D too, and should be integrated into the agile processes!

Examples of security assurance techniques:

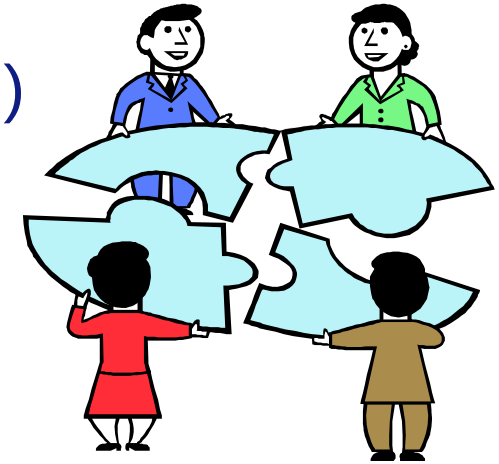
- Security Analysis: threat and vulnerability analysis important, its connection to requirement engineering should be improved, forms the basis for assurance!
  THERE ARE CHALLENGES IN CARRYING OUT SECURITY ANALYSIS IN THE AGILE PROCESSES! (and even in traditional R&D processes!)
- Security Testing: tools available for network level and some for application level testing
- Security Auditing: perspectives: information security management; security engineering
- Security Monitoring: beyond IDS/IPS systems, holistic monitoring, mobile versions (mainly maintenance phase!)

Information Security Management vs. Security Engineering

- 'Information security management (ISM) "is targeted at the security processes and practices in the organisation.
- 'Security engineering "is targeted at the R&D of security solutions in products / services / technical systems.
- Both of them should be addressed in Agile Software Development.

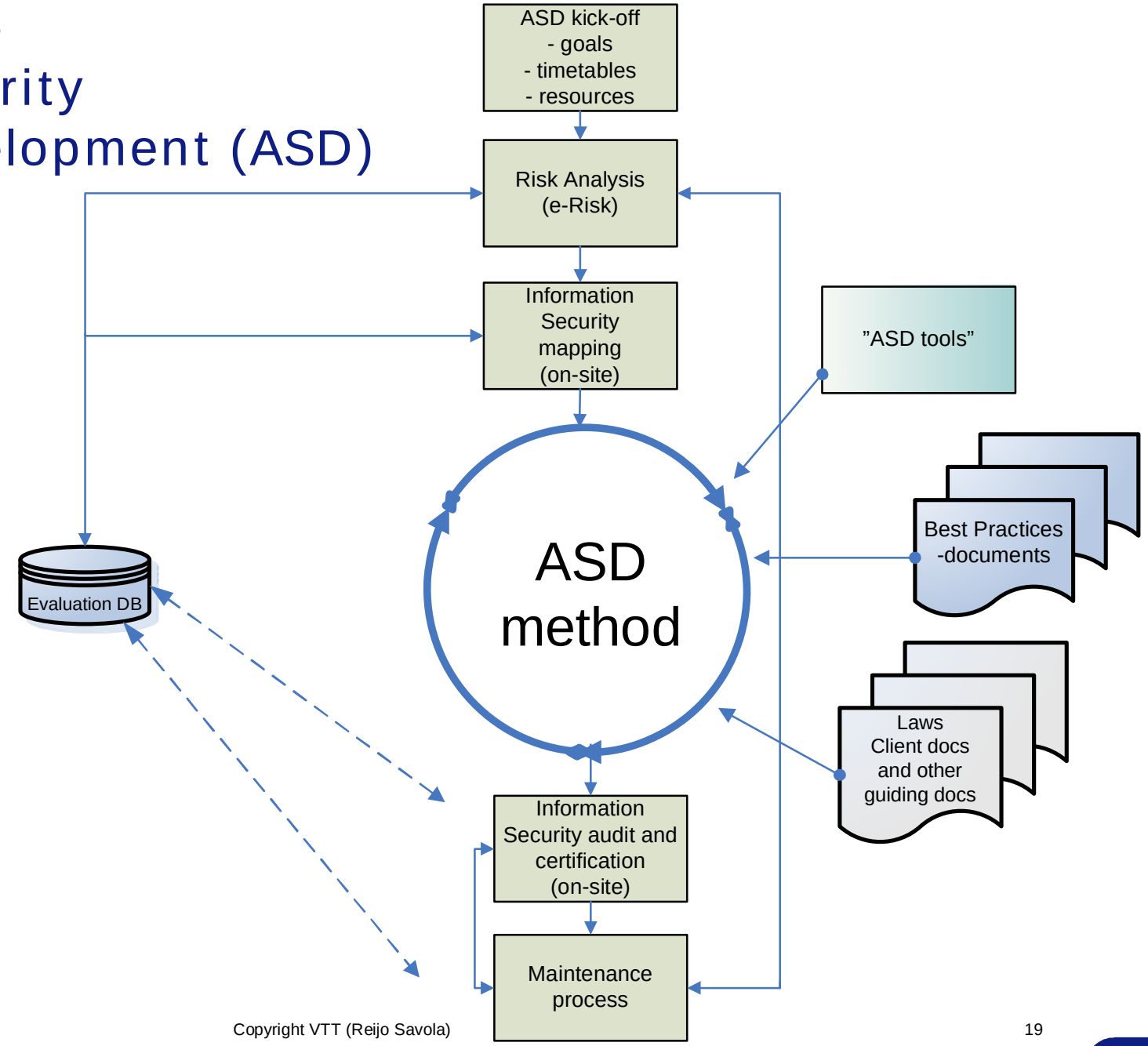


VTT ś Agile Security Development (ASD) Framework

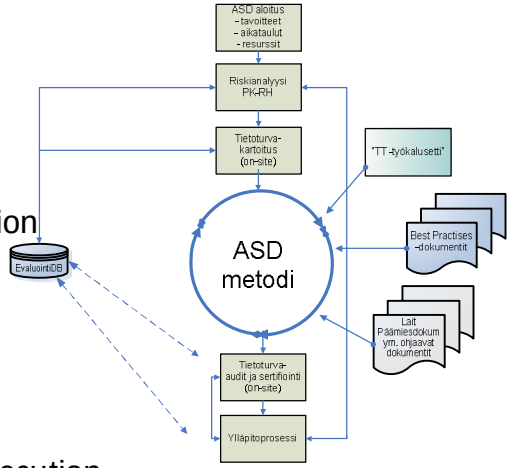


- FOR WHOM: the client – organization, which wants to develop/verify the level of information security of the subcontractors; an SME, which wants to develop information security from it ś own baseline
- WHAT: an agile process model for developing an information security management system, fast and effective improvement of the current information security state and level, ISO 17799 compatibility
- WHY: a clear and feasible model, efficient working model, a) improving and b) maintaining the subcontractor ś or SME ś information security level
- HOW: the guidance and consultation of experts, high utilization of the company ś own resources, targeted to the right need, integrated with the organization ś guidance system
- ASD = Agile Security Development

Agile Security Development (ASD)



Agile Security Development (ASD)



Management meeting
- Requirements in terms of overall organizational function
- Management's statement of commitment

Measurement
- Definition of the measures,
- Testing and execution

Information security policy
- Definition and execution
- Compatibility with interest groups
- Communications

Education
- Definition, materials
- Execution

Strategic security
- Information security organization, clarification of liabilities
- Asset classification and controls
- Personnel safety
- Physical safety

Instructions
- Definition and execution
- Communications
- Scope

Operational safety
- Access control
- Systems usage, development, maintenance, acquisition
- Actions in case of information security incidents

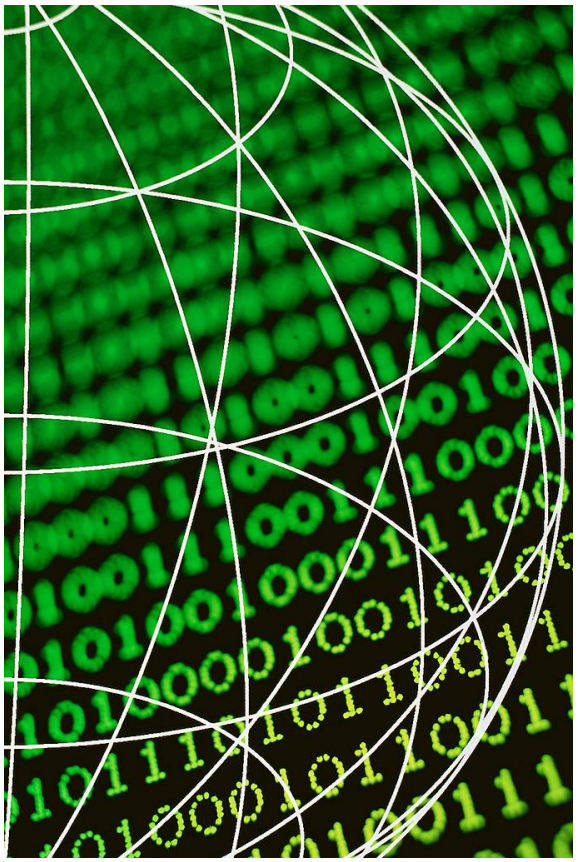
Continuity planning
- Definition and execution
- Creation of the scenarios

Background material of ASD

- ISO 17799, 2700x
- Common Criteria
- Cobit
- ITIL
- ISF
- SSE-CMM
- BSI
- PK-RH
- OCTAVE
- CISSP
- etc. Best Practices documents applied

Conclusions

- Agility and security have tradeoffs, the biggest difference is the emphasis of risks in security.
- Security should be built in to the agile process, practices and tools (e.g. security solution patterns, standard solutions, taking security into account proactively).
- Both information security management (ISM) and security engineering practices are needed in the Agile Software R&D.
- Security assurance should be an integral part of SW R&D.



REIJO SAVOLA

Network and Information Security
Research Coordinator

Tel. +358 20 722 2138

GSM +358 40 569 6380

Fax +358 20 722 2320

Email Reijo.Savola@vtt.fi

VTT TECHNICAL RESEARCH CENTRE OF FINLAND
Network and Information Security Research
Kaitoväylä 1, Oulu, FINLAND
PL 1100, 90571 Oulu, FINLAND

www.vtt.fi

VTT CREATES BUSINESS FROM TECHNOLOGY