

# Implementing Criteria in the Production of Security Technology



Prof. Dr. Sachar Paulus  
Senior Vice President  
Product Security Governance  
SAP

# Agenda



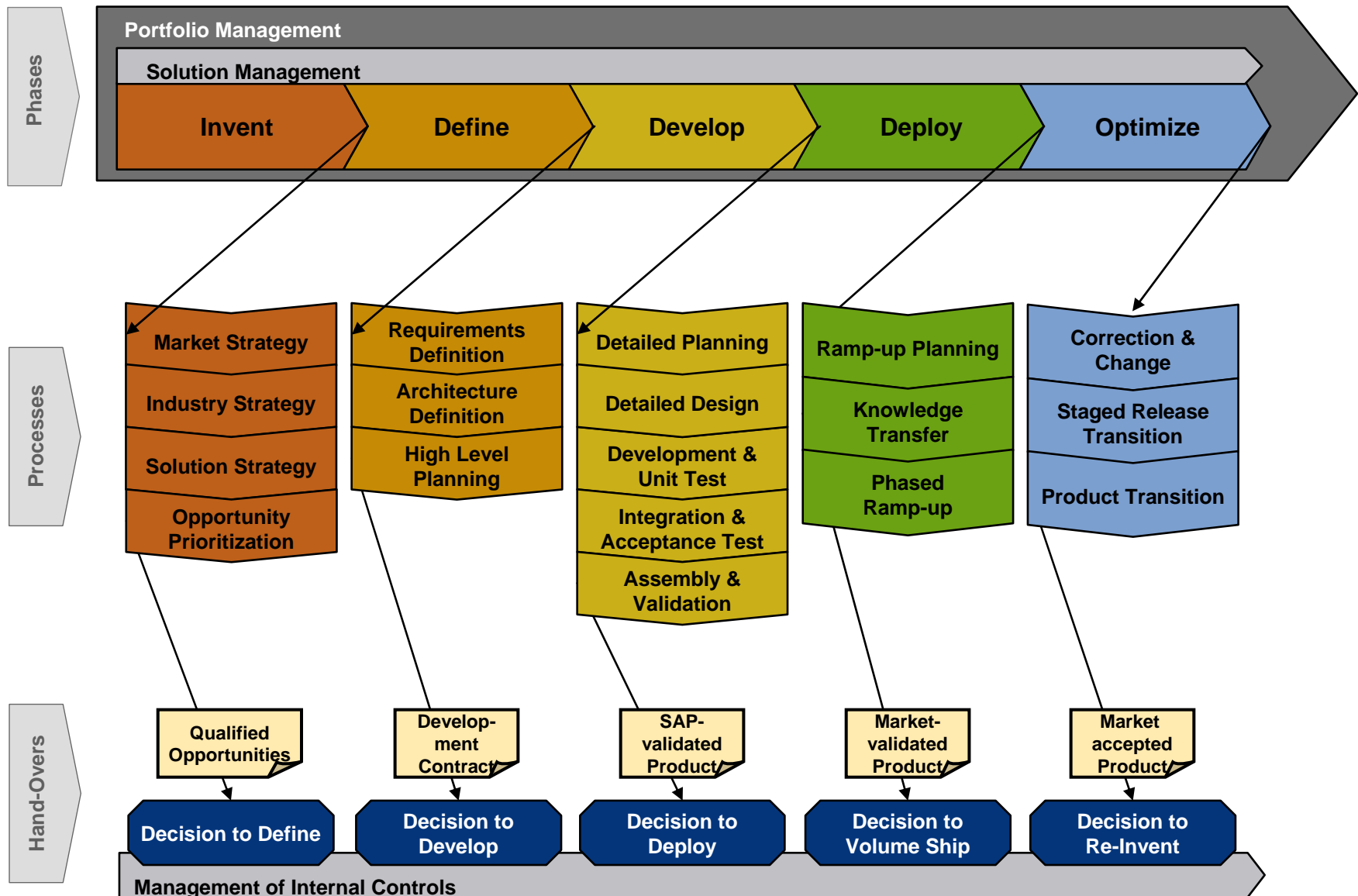
1. Claim: don't limit the criteria to security technology!
2. The Product Innovation Lifecycle at SAP
3. Addressing non-functional requirements
4. Mapping legal privacy requirements to technical controls
5. Who is responsible for what?
6. Separating functional and non-functional privacy related requirements
7. How it works in practice
8. 10 Principles for Secure Software Development

# Don't limit the criteria to security technology!



- Privacy related requirements are ubiquitous
  - It is useless to protect the transmission and storage of public camera recordings, if the search and retrieval afterwards is possible from everywhere to everyone
  
- Privacy related requirements are not bound to specific technology
  - Every data consuming system will need to apply data privacy criteria
    - CRM systems
    - Case management systems
    - Public surveillance
    - Health care systems
  
- Privacy related requirements cannot be uniquely assigned to manufacturers
  - Massive data integration, motivated by
    - Public Security
    - Business demand
  - Will lead to privacy issues „on the other side of the fence“

# The Product Innovation Lifecycle (PIL) at SAP



# Addressing non-functional requirements: the „PIL Product Standards“



## Standard

- Accessibility
- Application Integration and Interfaces
- Business Solution Configuration
- Data Archiving
- Development Environments
- Documentation
- Functional Correctness
- Globalization
- Multiple Clients
- Open Source
- Performance
- Security**
- IT Service & Appl. Mgmt.
- Technical Implementation and Change Mgmt. (TICM)
- Third Party
- Usability

## Product standards

Accessibility

## Development

- Apply standards
- Control usage

## Validation

- Check compliance prior to mass shipment

## Market

- Give feedback
- Communicate new requirements

## Standard Owner Advisory & Review Boards



- Change Management: keep standards up to date
- All stakeholders represented

Feedback Loop

- Legal requirements are not directly usable as technical requirements for software engineering
  - Responsibility has to be sorted out first
  - Concrete technical use case must be deduced
  
- Example: „Data shall be stored according to its purpose“.
  - In software, the purpose must be defined concretely in terms of functions
  - The formulation does not prohibit data aggregation technology to be applied after storage, „on-the-fly“, as e.g. done by Data Warehousing tools
  
- Good examples for technical requirements:
  - „Privacy related data must be marked as such by the requirements engineer“
  - „Privacy related data shall be stored only once“
  - „Aggregation of privacy related data shall be subject to an additional approval process“

- Not all requirements are actually to be addressed to the manufacturer, there is a shared responsibility for the whole system to be „privacy compliant“:
  - The manufacturer(s) shall provide the technology according to the privacy related requirements
  - The system integrators shall configure the system according to privacy related requirements
  - The operator shall run the system according to privacy related requirements
  
- Examples:
  - „Deleting old data“ functions are the manufacturer’s responsibility
  - Configuring the usage of that function is the responsibility of the system integrator
  - Actually deleting the data is the responsibility of the operator
  
- Tip: run an extra mile to map the technical requirements to the responsible stakeholders

- Similar to security, you need both functions and qualities of a system to achieve privacy.
  
- Example: look at the requirement „delete privacy related data“
  - One needs the deletion function (making sure there will be no inconsistencies in other data).
  - One also needs the label „privacy related“, which every developer must actually manage.
  
- The functional requirements are treated differently than non-functional requirements.
  - Functional requirements need a business case to be developed, thus decision makers can get around them.
    - Good: there is a market for specialized software makers, concentrating on „Privacy Enhancing Tools“
  - Non-functional requirements cannot be avoided, they are set by a central standards board.
    - But they also may be escaped if missing market pressure lowers the priority.



## PIL Security Standard:

- 200 non-functional requirements in total
- Section on privacy
  - see right
- Implementation is subject to priorities set by decision makers in development

## Data Privacy Guides:

- To help system integrators and operators
- ...for R/3: 2001 (currently re-worked)
- ...for BW: 2003
- ...for CRM: 2005

## Additional products:

- Few available
- Many internal audit support tools can help, though

SAP Software shall provide the capability to comply to local data protection and privacy regulations.

Administrators shall not have access to person-related data, if not necessary.

The access to logs shall be restricted according data protection regulations.

The access to person-related data shall be logged.

Anonymized data processing shall be enforced if the relation to a person is no needed.

SAP applications shall provide the capability to avoid unnecessary storage of person-related data.

SAP Software pre-configuration shall be compliant to data protection rules.

The documentation shall contain guidelines and recommendations about how to use the application regarding data protection/privacy.

SAP software shall provide a report functionality for all personal data stored for each person.

SAP applications shall provide the capability to notify a person if data related to this person is stored initially.

SAP Software shall support deletion of personal data.

It shall be possible to store the agreements of the affected person for the storage of his/her personal data.

Processing of person-related data shall be limited to the primary storing purpose.

Person-related data that has stored for different reasons shall be stored separately.

The transfer of person-related data to other systems (especially to a 3rd party) must be logged.

# 10 principles for secure software – they also apply to respect privacy!



- *During the requirements gathering process, the supplier shall define the security assurance properties of the product.*
- *The design and the implementation of the product shall be reviewed whether it will not jeopardize the security assurance properties.*
- *Before shipping, the product shall be tested whether the desired security assurance properties are present.*
- *The software shall be able to run in “secure mode” after installation.*
- *Security administration of the product shall be easy to understand and simple to use.*
- *Necessary secure configuration of the software environment of the product shall be documented and actively communicated to customers.*
- *During the product enhancement process, the supplier shall check that new requirements are not jeopardizing the existing security assurance properties of the product.*
- *Software updates shall not jeopardize the security properties of the product.*
- *The supplier shall implement a response process for effectively addressing security issues*
- *Security issues detected in the product shall be communicated responsibly to users*

The supplier shall strive for developing measurement techniques for the principles mentioned above to continually improve the security of its products.

Thank you for your attention!

Prof. Dr. Sachar Paulus  
Senior Vice President  
Product Security Governance  
SAP