KEMA

TU/e

Software Quality Themamiddag

Platform Informatiebeveiliging (PI) 19 april 2006

Dr.ir. Jos J.M. Trienekens

Senior consultant KEMA
Associate Professor TU/e

KEMA

TU/e

Content

Experience you can trust.

KEMA

TU/e

Software quality – Information security?

- Software quality
- Information system quality
- Information security
- Information security management systems
- Information security risk management

KEMA

TU/e

How is software quality defined?

Software quality consists of a set of non-functional characteristics:

- not specifically concerned with the 'WHAT' of a system
- place restrictions on the software product and development process
- specify external constraints that a software application must meet

Views on software quality (ISO9126)

TU/e

levels	*safety view*	*economy view*	*security view*	*environmental view*
A	many people killed	financial disaster (company will not survive)	protection of strategic data and services	unrecoverable environmental damage
B	threat to human lives	large economic loss (company engaged)	protection of critical data and services	local pollution
C	damage to property, few people injured		protection against error risk	no environmental risk
D	small damage to property, no risk to people		no specific risk identified	

KEMA

KEMA

TU/e

How is information security defined?

(Slay and Koronios, 2006)

- Confidentiality: restricted availability

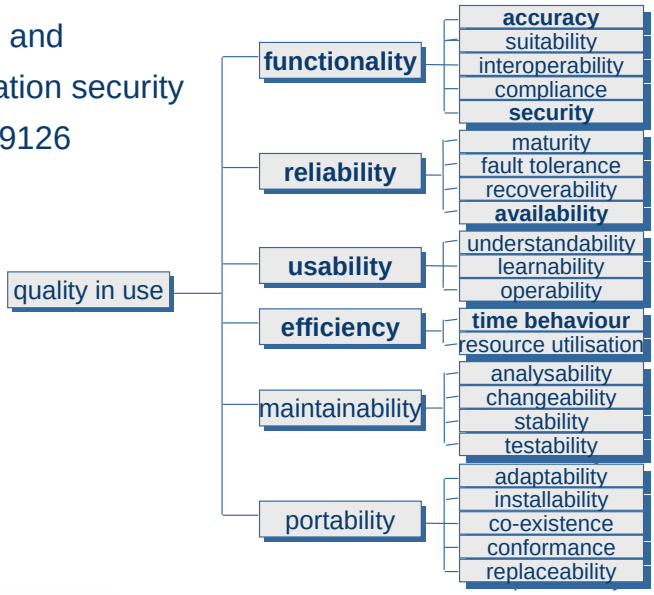
- Integrity: accuracy and completeness

- Availability: accessibility and time-behavior

Experience you can trust.

TU/e

Quality and Information security in ISO 9126



KEMA

KEMA

TU/e

Information security management systems: Guidelines for information security risk management (BS7799-3:2006)

Process approach:

- **Understanding business information security requirements**
- Selecting, implementing and operating controls in the context of managing business risks
- Monitoring and reviewing the performance and effectiveness of the ISMS
- Continual improvement based on objective risk measurement

Experience you can trust.

TU/e

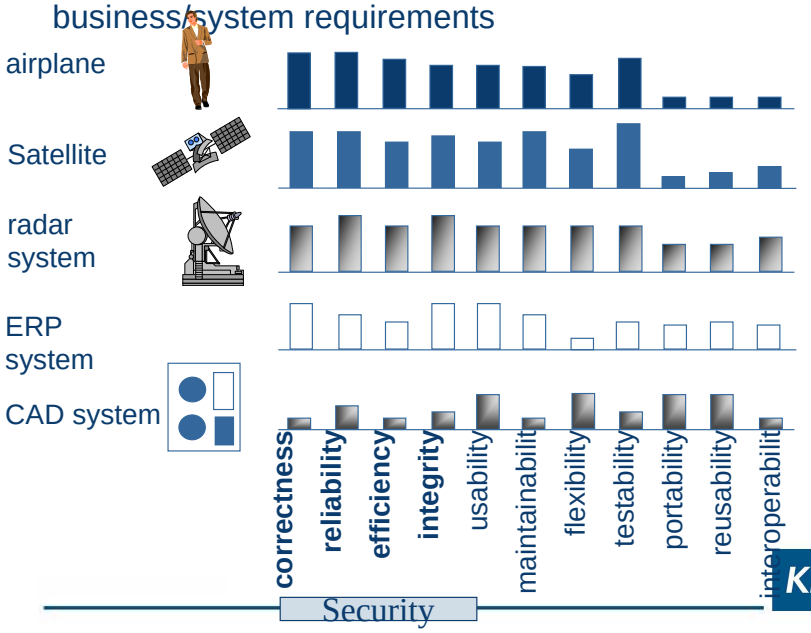
2: Dealing with software quality: business requirements as starting point

- Deriving software quality from business requirements:
  - how to identify wishes and expectations of business systems regarding software quality (and security)?
  - how to specify and quantify software quality (and security)?
  - how to prioritise quality (security) characteristics?
- And:
  - how to implement quality (security) characteristics?
  - how do quality (security) characteristics influence each other?

KEMA

TU/e

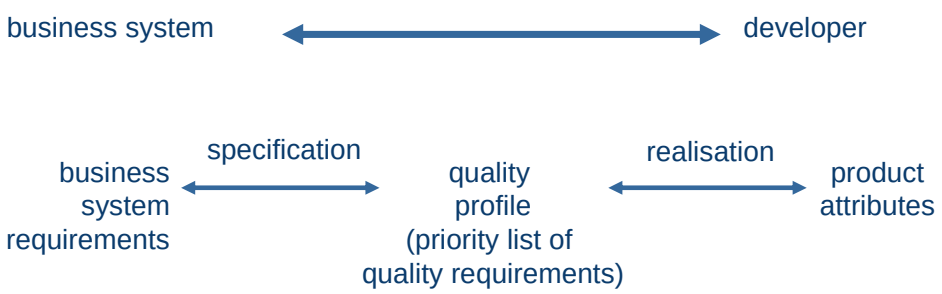
Information security requirements are related to business/system requirements



KEMA

TU/e

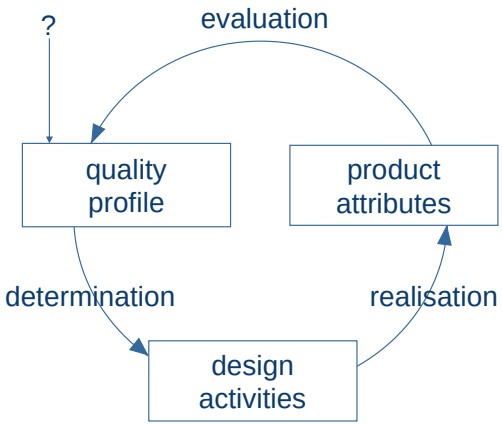
Dealing with quality requirements: specification en realisation



KEMA

TU/e

Realisation of quality requirements: the 'quality cycle' for engineers

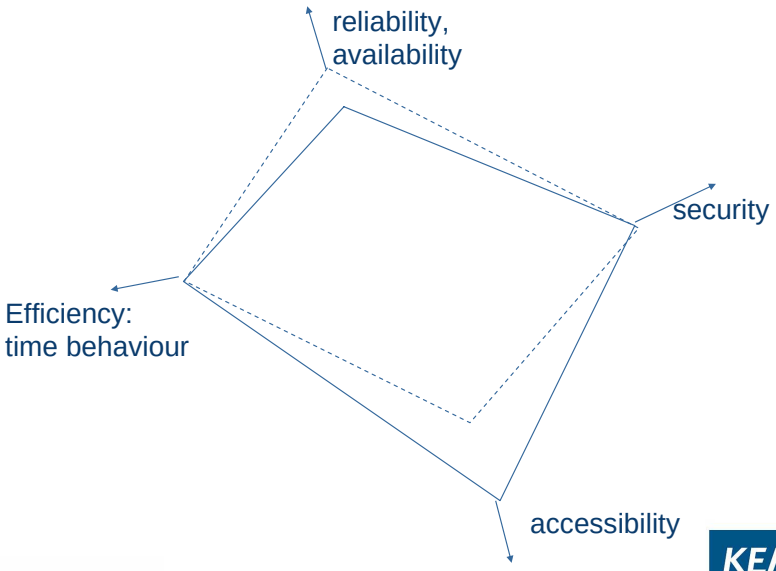


- quality requirements (examples)
  - security
  - efficiency, time-behaviour
  - availability
  - etc.
- design activities (examples)
  - access control mechanisms
  - optimalisation of algoritms
  - deconcentration of subsystems, back-up's
  - etc.

KEMA

Quality requirements: mutual interactions

TU/e



KEMA

Realisation of quality requirements: categories of design activities

TU/e

(according to SERC, 1992)

	functionality	reliability	efficiency	usability	maintainability	portability
modeling	+		-			
controlling		+	-			
optimalisation			+		-	
styling				+		
tracing		+	-		+	+
strengthening					-	
transfering	+					

KEMA

KEMA

TU/e

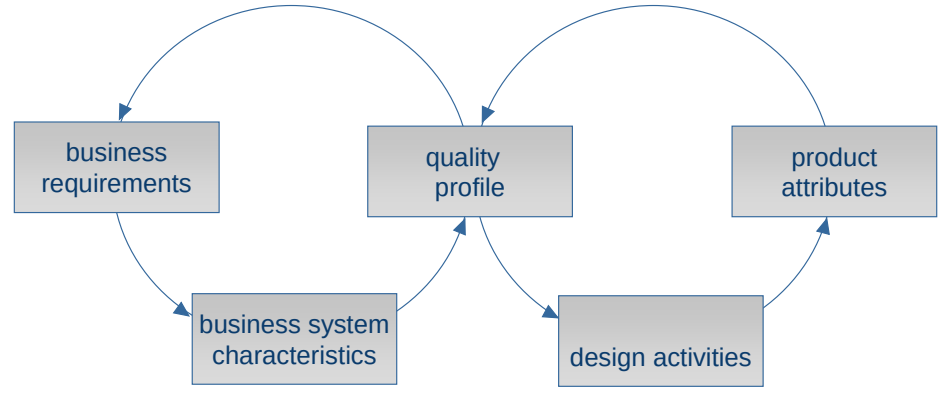
Identifying quality requirements

Not adequately covered by most requirements engineering methods, because they are:

- often related to specific functional requirements
- often highly subjective
- conflicting and contradicting each other
- difficult to measure
- sometimes related to design solutions

A double 'quality cycle' for the specification and realisation of quality requirements

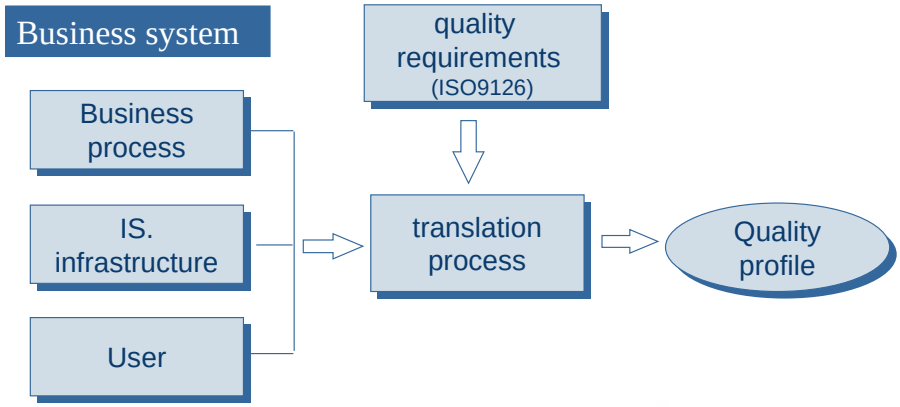
TU/e



KEMA

3: Business system requirements

TU/e



KEMA

Business system requirements as starting point (Trienekens, Kusters, 1994, 2001)

TU/e

- business process characteristics:
  - complexity
  - dynamics
  - scope
- user characteristics:
  - experience (business process, IT)
  - education (business process, IT)
- information system infrastructure characteristics:
  - software language
  - hardware platform

KEMA

TU/e

3.1: Business system as starting point: analysing **business process** characteristics

- complexity (e.g. # control parameters in the process, # subprocesses, # interrelations)
- dynamics (e.g. # changes / time in business process)
- scope (e.g. # departments, # business functions)

→ determine risks with respect to information security

KEMA

Example

TU/e

Business process characteristics:

- processes that are critical for the business as a whole and that need operational continuity

➢ Points to strong requirements for reliable software (in particular availability)

KEMA

Metrification of reliability (availability and recoverability)

TU/e

- **availability:**

  the capability of the software to be in a state to perform a required function at a given point in time, under stated conditions of use

  ex: Relative Availability Percentage =

  The ratio of time the software product is available to the time it is needed

- *recoverability:*

  the capability of the software to re-establish its level of performance and recover the data directly affected in the case of a failure

  ex: Mean Down Time =

  The total down time of a system divided by the number of observed breakdowns

KEMA

3.2: Business system as starting point, investigating **user characteristics**

TU/e

User characteristics, a.o.:

- type of users (# different types, e.g. management, operators, end-users, remote users)
- level of knowledge (educational background, # courses in IT and/or business systems)
- experience (amount of time regarding business systems, information technology)

➢ determine risks regarding information security

KEMA

Example

TU/e

User characteristics:

- time-critical business processes
- highly experienced users, real-time software application

  ➢ points to strong requirements for efficiency (e.g. time behaviour)

KEMA

Metrification of efficiency:

TU/e

the capability of the software to provide the required performance relative to the amount of resources used, under stated conditions

Efficiency sub-characteristic:

•*time behaviour:*

the capability of the software to provide appropriate response and processing time and throughput rates when performing its function, under stated conditions

ex: Response Time =

Average time between (end of a) command and the moment of gaining a result

KEMA

TU/e

3.3: Business system as starting point: investigating information system **infrastructure** characteristics

- Type of software:
  - computer languages
  - standard packages/custom made
  - amount of reuse
- Type of hardware: computers/network
- Type of usage:
  - on-line/batch
  - intensity/frequency
  - time criticallity

➢ determine risks regarding information security

KEMA

TU/e

Example

IS infrastructure characteristics:
- type of software: ERP (HRM, financial applications)
- many batch-jobs (e.g. salary calculations)
- mainframe computer

➢ leads to strong requirements for confidentiality and integrity

KEMA

TU/e

Setting priorities: a 'quality' profile (example)

	Importance levels				
Information security req.	-	D	C	B	A
Accuracy (integrity)			✓		
Availability				✓	
Efficiency, time-behaviour		✓			

A complete 'security' profile contains:

- prioritised and specified security requirements derived from business system characteristics (business process, user, information system infrastructure)
- importance levels for security requirements, with explicit motivation based on business system characteristics metrification of security characteristics

KEMA

TU/e

4: Summary

From business system requirements to an information security profile:

1. risk based investigation of business requirements (business processes, IS infrastructure, user characteristics)
2. linking business system characteristics to information security requirements
3. develop information security profile
4. determine importance levels for information security requirements and add metrics
5. quality profile is the back-bone for the Information Security Management System (ISMS)

KEMA

KEMA

TU/e

Questions?

Thank you for your attention.