COBIT-Based
Corporate Governance & Risk Management
2. Problems & Practical Solutions,
Best Practices Differences

Obuda University
John von Neumann Faculty of Informatics
Institute Applied Informatics

Dr. Katalin Szenes
CISA, CISM, CGEIT, CISSP, PhD
honorary associate professor
szenes.katalin@nik.uni-obuda.hu
http://users.nik.uni-obuda.hu/szenes/

Table of Contents

Table of Contents

SUGGESTED REMEDIES

o a revisited transparent on problem solving

o the requirements to be extended

o other new - extended requirements: the new problem classification tools
suggested NEW SUBGOALS

O a *usable* governance definition - from my practice

O corporate governance / IT governance

O a *usable* operational security definition - from my practice

O governance goals ↔ information security - IT audit methods
→ consequences of this approach

O governance ↔ operational security

Table of Contents

O contributing to the solution - overview only

- ❑ supporting the fulfillment of the strategic goals:
  what / how and their dimensions
  - ● suggested "subgoals":
    - excellence criteria
    - operational objective

operational excellence criteria:

- effectivity, efficiency, compliance, reliability,
- risk management excellence,
- functionality,
- order

asset handling excellence criteria:

- availability, integrity, confidentiality

disclaimer: the names are taken from COSO and ISACA COBIT, but
the interpretation is derived from my practice

Table of Contents

O contributing to the solution - overview only cont.'d

- 3 pillars of operation

  {pillars} = domain & range of those activities & objectives
  that contribute to the strategic goals (e.g. to the excellence criteria)
  : ➔ organizational, technical, regulational
  (szervezet,szabályozás - technika
  ➘ detective - preventive - corrective

- IT architectural infrastructure elements
- operational activity - and its useful attributes

Table of Contents

OFFICIAL REMEDIES

the COBIT predecessors of my user-given subgoals / tools to the strategic goals:
the predecessors of my operational objectives /activities

🕮 control objective 🕮 control measure 🕮 resource 🕮 enabler

O basic audit notions - COBIT / personal opinion / COSO

- ❑ control objective
- ❑ control measure / procedure
- ❑ what kind of *assurance* is *reasonable*?
- ❑ predecessors of my pillars ?
  - resources (COBIT ➔ COBIT 4.1) and
  - enablers (COBIT 5)

Table of Contents

one of the hot IT topics: applications

- example for **COBIT** advice on control objectives and control measures
  - AI2 Acquire and Maintain Application Software
    - advice taken from the COBIT reference manual (see references)

- example for a more or less similar problem from **ISO 27001**
  a standard for: "Information technology - Security techniques - Information security management systems - Requirements"

  brave new world?
  a comparison between its versions from this applications point of view

TECHNICAL PROBLEMS

examples for technical problems
a typical problem in 2015: the Android mobile

a *GOVCERT* alarm notice (6th August, 2015)

- the operating system Android has a vulnerability, that facilitates the remote execution of a code

➔ the attacker can take over the control of the device

- the way of attack: a specially crafted MMS message

ű

- for Hungarians: http://tech.cert-hungary.hu/vulnerabilities/CH-12489 (Stagefright)
- for foreigners: http://www.androidcentral.com/stagefright

GovCERT-Hungary (Kormányzati Eseménykezelő Központ**)**
Tel: +36-1-336-4833
Fax: +36-1-336-4886
alarm report: cert@cert-hungary.hu

everybody has a mobile

a GovCERT alarm notice on 6th August, 2015:

- the operating system Android has a vulnerability, that facilitates the remote execution of a code

➔ the attacker can take over the control of the device

- the way of attack: a specially crafted MMS message

http://tech.cert-hungary.hu/vulnerabilities/CH-12489 (Stagefright)

CERT: originates from the USA Department of Defense
Hungarian:
GovCERT-Hungary
Tel: +36-1-336-4833
Fax: +36-1-336-4886
alarm report: cert@cert-hungary.hu

a great fright: the APT - what is this?

old definition, taken from ISACA materials:

"an APT is as an adversary that

- *possesses sophisticated levels of **expertise***
- *and significant **resources** which allow it to create opportunities to achieve its objectives*
- *using **multiple attack vectors** (e.g., cyber, physical and deception).*

- *These objectives typically include*
  - ❑ *establishing and extending footholds **within the IT infrastructure** of the targeted organizations for purposes of*
    - *exfiltrating information,*
    - *undermining or impeding critical aspects of a mission, program, or organization; or*
    - *positioning itself to carry out these objectives in the future*

. / .

great fright: APT - what is this? cont.'d

" The advanced persistent threat:

- *(i) pursues its objectives repeatedly over an extended period of time;*
- *(ii) adapts to defenders' efforts to resist it; and*
- *(iii) is determined to maintain the level of interaction needed to execute its objectives."*

National Institute of Standards and Technology (NIST), *Computer Security Incident Handling Guide*, Special Publication 800-61, USA, 2008, *csrc.nist.gov/publications/PubsSPs.html*

instead of this, what I found: ***. / .***

APT - what is this?

what I could find:

advanced persistent threats = a long-term pattern of targeted, sophisticated attacks

NIST Special Publication 800-39
Managing Information Security Risk
Organization, Mission, and Information System View

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930
March 2011

(1st September, 2015)

examples / the earliest published attack on military research establishments:
The Cuckoo's Egg

around 1980:
origin: West German hacker, Markus Hess, university student
penetrated networked computers in California to steal secrets of the "Star Wars" program

investigating
a minor accounting discrepancy problem in the computer usage accounts
Stoll from Lawrence Berkeley National Laboratory noticed
an intrusion from a West German university, coming across a satellite link

Stoll made a trap with interesting details of a fictional Star Wars contract

the West German authorities located the hacker, it turned out, that
he had been selling the stolen information to the Soviet KGB
he was tried and found guilty of espionage in 1990 and sent to prison

Clifford Stoll book:
The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage
Doubleday, USA, 1989

examples / Moonlight Maze

around 2000:

series of attacks, undetected for nearly two years
presumed origin: Russia

targets:
ogovernment sites,
osystems at the Pentagon, NASA , US Department of Energy,
ouniversities, research labs, doing military research

stealing tens of thousands of files:
omaps of military installations
otroop configurations
omilitary hardware designs

loss: many millions of dollars - the Russian government denied any involvement
the information was probably offered for sale to the highest bidder

a target: NASA - https://www.nasa.gov

NASA: National Aeronautics and Space Administration

o NASA's Vision: To reach for new heights and reveal the unknown so that what we do and learn wil

Topics:
ointernational space station
ojourney to Mars
oEarth
otechnology
oetc.

Note: sometimes hackers mix NSA, NASA, NIST

examples / Titan Rain

2003:
presumed origin: China - Chinese government denied any involvement
targets:
oUS defense contractors: Lockheed Martin, Sandia National Laboratories
Redstone Arsenal
oNASA

novelty of this cyberespionage attack:
othe level of deception
othe use of multiple attack vectors (channels of attack)

a combined, well-researched social engineering attack on *targeted* individuals
ostealthy Trojan horse attacks
ousing malware techniques bypassing contemporary security countermeasures.
➔ government secrecy ➔ **?** choosing targets from industry:
oaerospace, defense, energy, financial services, manufacturing, pharmaceutical

examples / Sykipot

2006:
ospear-phishing emails with malicious attachment or
olink to an infected web site,
ozero-day exploits

➔ found later, and then:

targets: in USA, in UK
odefense, computer sector, telecommunications, energy, chemicals, government

collecting and stealing secrets and intellectual property,
odesign, financial, manufacturing and strategic planning information

servers mostly in China, belonging perhaps to an intelligence agency

examples / Operation Aurora

2009:
oused a zero-day exploit to install a malicious Trojan horse, Hydraq
➔ :

targets:
according to McAfee:
oto gain access to and modify source code repositories

companies:
o! January 2010 Google disclosed the attacks, the others did not dare !

oAdobe, Juniper, ...
obanks, defense
ocontractors, security vendors, oil and gas companie

o+ Chinese human rights activists **!**

examples / Gozi

2007:
- o by the means of attached to pdf documents
- o intercepts & modifies browser traffic

➔ :
captures and transmist personal banking information,

targets:
- o banks
- o computers in USA, UK, Germany, Poland, France, Finland, Italy
- o NASA systems

creator: Nikita Kuzmin - with others
a renting / selling service to crimnal customers

new variant of Gozi, in 2013:
- o infects the hard disk master boot record—an attack that cannot be easily
- o reformatting, reinstalling does not help

REMEDIES - again:
SUGGESTED REMEDIES

a revisited transparent on problem solving

- ways of classifications
- viewpoints of classifications
  - new viewpoints of classifications:
    extension of the ISO / COBIT information criteria
- subjects of the measures

the requirements to be extended

they were the so-called ISO / COBIT information criteria:

ISO (first CCITT, then BSI, and then ISO) & COBIT criteria
o availability
o integrity
o confidentiality

COBIT - till COBIT 4.1:
o effectiveness
o efficiency
o confidentiality
o integrity
o compliance
o reliability [of information]

the new - extended requirements: the new problem classification tools
suggested NEW SUBGOALS

- *criteria* characterizing *excellent* operations:
  - effectivity,
  - efficiency,
  - compliance,
  - reliability,
  - strategy-driven goal & operational risk management excellence,
  - functionality,
  - order

- *asset handling excellence criteria*:
  - availability,
  - confidentiality,
  - integrity

a *usable* corporate governance definition - from my practice

enterprise governance

o it is the responsibility of the *whole staff,* top management included

o top management has to

- direct the company the best possible way towards market success,
- taking the conditions defined by the economical environment into consideration depending on the interests of the enterprise, and
- based on the strategy of the institution

defining and maintaining this strategy belongs to the responsibilities of the top management, while the staff is responsible for supporting the top management in fulfilling the strategic goals

? what about the *environmental* aspects?

notes to my corporate governance definition

o no hidden details are "involved".

o the double responsibility of the top management is very important, the strategy is actually the *document, on*

- *how* do they to perform their work,
- in the given inside and
- outside circumstances

o these have to be kept constantly under surveillance, and

o the results have to be taken into consideration

corporate governance / IT governance

IT governance
(my definition)

- one of the *necessary conditions* of successful enterprise governance,
  - by directing IT in such a way, that
    - it serves enterprise governance according to the intentions of the top management.

- every member of the IT staff is responsible for it
  - the weight of their responsibility is directly proportional to their weight in the company hierarchy
  - the top management of the company is responsible for the supervision of the IT governance

a *usable* operational security definition - from my practice

I define *operational security,* as
such an organizational, regulational, and technical *system*,
- to be established in a company,
- by the means of
  - identifying
    - strategy-related operational objectives and
    - operational activities,
  - and by contributing to the fulfillment of these objectives,

that
- *satisfies* the governance & operational excellence criteria
- prioritized by the top management,
  or by their delegates in the business areas
- in a predictable, measurable, and scalable way

➔

governance goals ↔ information security - IT audit methods
→ consequences of this approach

relying on the *direct* connection
between governance goals and information security - IT audit methods,
this mutual direct support yields:

o an effective and efficient support of enterprise strategy by derivating
  - concrete everyday improving goals and
  - actions from strategic goals

o a possibility of tailoring and
o tuning the strategy
based on a *direct,* and *operations-related* feedback
o provided by collecting those basic problems of institutional operations,
  that are to be solved using information security method

governance goals ↔ information security - IT audit methods
→ consequences of this approach

trivial example:
customers' satisfaction, data confidentiality

o without customers there is no success in the market,
o success = important goal of corporate strategy

➔ customers' satisfaction = a strategic base for confidentiality
starting from security we got to corporate strategic level

other way around:
market success = a good reason why confidentiality has to be satisfied

💣information security methods contribute to the achievement of strategic goals
💣from strategic goals, information security tasks could be derived

governance ↔ operational security

- direction from security towards corporate governance:
  = improving the quality of corporate management
  by the means of information security / IT audit methods

- other way around:
  = serving security by governance
  = devising governance issues from security requirements

top management might accept security requirements as their own, if these requirements are derived from unquestionable governance requirements

contributing to the solution: supporting the fulfillment of the strategic goals
what / how and their dimensions

- the subgoals, contributing to the strategic goals
- the activities, contributing to the subgoals & strategic goals
- the scope of the activities, and
- the range of the activities
- their "components", a list of "*more* atomic" activities

  - their material &
  - human resources
    - executors,
    - those, who give the necessary permissions
    - those, who acknowledge
    - supervisors, etc.

! the details of these will follow

suggested "subgoals": criteria of excellent governance

operational excellence criteria:

- *effectivity,*
- *efficiency,*
- *compliance,*
- *reliability,*
- *risk management excellence,*
- *functionality,*
- *order*

asset handling excellence criteria:

- *availability,*
- *integrity,*
- *confidentiality*

suggested "subgoals": criteria of excellent governance
operational excellence criteria

An operational activity is ***effective*****,**

- if its result(s) complies with the pre-planned requirements, that had been accepted by every relevant party.

An operational activity is ***efficient,***

- if it is performed in a *pre-planned*, documented, and cost/ effective way, concerning the optimal use of human and material resources, and the way of problem solving.

A company *operates* in a compliant way, or, *shortly*,
the operations of a company complies with the ***compliance*** criterium,

- if it complies, in a *documented* way, to any requirement of those authorities that *have authority* to regulate any aspect of the activities of the company.

suggested "subgoals": criteria of excellent governance
operational excellence criteria

The *operations* of a company is ***reliable***,

- o if it is organized in such a way, that
  it provides for the *preliminary agreed* service(s)
  and, at the same time,
  it supports the work of the staff according to the *best professional practice*.

The ***functionality of the information system*** of a company is *adequate*,

- o if it serves the staff in such a way, that they can fulfill their job requirements in the best possible way.

(the scope of this criterium is restricted to IT, but its fulfillment requires the overview of the whole operations and its requirements)

suggested "subgoals": criteria of excellent governance
operational excellence criteria

Risk management excellence

- o a strategy-driven managing of risks,
- o to achieve the excellence criteria,
- o ordered according to the evaluation of the top management / their business delegates
- o for every goal, asset and effort triple worth to be taken into consideration

e.g. confidentiality versus availabilty, or reliablity versus cost-effectivity

the essence of the risk assessment is just to conduct this evaluation process by the means of matrices , questionnaires, and other ***systems analysts'*** tools

suggested "subgoals": criteria of excellent governance
operational excellence criteria

The ***order*** is by definition ***adequate***, if

- top management takes up the responsibility for the well-being of the institution:
  - for the determination of the strategy, aligning it to the market success,
  - for its continuous maintenance,
- for ensuring, that the company fulfills these strategic goals.

↓

- regulational pillar of operations
  - documentation, business continuity management planning, dynamic inventory, -change / - release management, procedural guidelines, ...
- organizational pillar of operations
  - education, separation of duties ← job / role descriptions, ...
- technical pillar of operations
  - support the enforcing of all these,
    e.g. access provision management for units / roles / tasks ...

example: organizational + regulational:

- organized operational processes → e.g. organized application development,
- document throughout lifecycle of every product, planned test process

operational excellence criteria order

to operational excellence criterium: *order*
belong the following subgoals - among others

- documentation
- separation (segregation) of duties
- access provision management for units / roles / tasks
- dynamic inventory management
- dynamic documentation & change management
- business continuity planning /
- IT business continuity planning /

(these are usually required by the Supervisory Authority
in financial institutions, too)

suggested "subgoals":
criteria of excellent governance - *asset handling excellence criteria*

Confidential asset handling,

- handling confidentially every information about it - those, and only those have *access* to it, who have job to do with it.

The ***integrity of an asset*** is said to be preserved,

- if its handling or processing *does not change it inadvertently*.

Availability of an asset means, that

- if it has a role in a *given matter*,

then

- it is available to every *competent* employee, who is competent in this matter,
- in a *planned*, *predictable,* and *documented* way, according to the preliminary agreements on its accessibility, that have to refer to every *qualitative and quantitative prescription*, that are *relevant* in the matter.

a "general" suggested "subgoal": the operational objective

this is my generalization for the control objective, *towards strategy !*
my operational objectives *contribute*
to the fulfillment of the strategic goals by improving operations

excellence criteria: *special case* of the operational objective

I define the *operational* objective,

- as an objective of one or more operational area(s) or role(s) to be achieved, in order to *contribute* to the fulfillment of strategic goal(s) of the company.

the "*distance of an operational objective from the strategy"*,

- is its degree of importance related to enterprise strategy,
- in other words, as its importance in achieving it.

note - the real life: instead of evaluations of individual objects always comparisons

important systems analysts tool: ***distance***
- the strategic *"importance"* of an operational objective

pillars of operation

3 pillars of operation:
- organizational - technical - regulational
  a működés pillérei: szervezet - szabályozás - technika

- detective - preventive - corrective
  vizsgálati - megelőző - javító

{pillars}
= domain &
= range of the activities & objectives that *contribute to* strategic goals

suggested examples for strategic goals: the excellence criteria
➔ the {pillars}
= domain &
= range of the fulfillment of the excellence criteria

distance: the strategic *"importance"* of an operational pillar element

definition of the *pillars* of operation*: through* enumerating their elements

organizational pillar elements are:
- the whole organizational structure, and
- its parts, that is
  - the individual organizational units, together with
  - the "building parts" of these units, that is
    - the roles, that are assigned, as duties,
      to the employees, working in the unit
- the members of the staff themselves
  (actually their job description - except in personal security matters)

note:
- the description of the assignments themselves,
  that are part of the job descriptions of the employee
  belong to the *regulationa*l pillar

definition of the *pillars* of operation*: through* enumerating their elements

regulational pillar elements are:

- o the procedural rulebooks themselves,
  that regulate the activities of the staff,
- o both the intended, and
  the undesigned relations of these rulebooks to each other

- o this ***involves***:
  - ❑ the facilities to search for given terms or rules,
  - ❑ the hierarchy of the rulebooks themselves, if any,
    with the contradictions embedded,
- o the structure of the whole regulational system
  with the facilities of its handling

- o a code of ethics defining the principles of staff behaviour

definition of the *pillars* of operation*: through* enumerating their elements

Technics covers

- o all physical, /
- o infrastructural property assets,
  that are necessary to perform operational activities,
- o together with the technical conditions, that determine their use.

Example for technical elements are:

- o the elements of the physical infrastructure,
- o together with the buildings and other facilities,
- o machines,
- o actually the elements of the inventory belong here,
- o together with their ***descriptive*** technical features,
- o and the actual and ***best practice*** technical way of using them.

A special *subset* of the technical elements is the IT architecture of the institution.

IT architectural infrastructure elements

IT architectural infrastructure elements,
or, shortly, IT infrastructural elements are:

- the computers themselves,
- their software (operating systems, utilities),
- the application systems ***serving the business processes***,
- the database management systems,
- the network communication devices,
- the defense elements providing for the quality of the IT services

- actually every component of the IT infrastructure belongs here:
  even those, that have some computer system embedded into them, like the ATM-s of the financial institutions, or other kind of customer serving tools.

The service quality, together with the non-IT type of operations, can be characterized by so-called excellence criteria.

pillars of operation

"predecessors**"**:

- COBIT ➔ COBIT 4.1 (1998 - 2007)
  more or less the same so-called resources
  - see them later, at the traditional notions

- there is something in COBIT 5, which is similar to my pillars: the "enablers":
  - kind of basic factors?
  - see them later, at the traditional notions

operational activity

I define the *operational* activity as such an action, that

- *contributes* to the achievement of operational objective(s)
- operates on operational pillar element(s) as subjects.

Note:

- the subjects here are meant to be elements of any of the three pillars
- the range of an operational activity is also the union of the pillars, even if
- the goal of an operational activity is actually an operational objective
  - special case: excellence criterium / criteria

- thus the possible contradiction of some of the excellence criteria has to be taken into consideration, too

useful attributes, characterizing an operational activity

- the operational objective, or set of operational objectives, that is / are to be served by this activity
- the scope of the activity, the set of its so-called subjects, and
- the range of the activity (both scope and range in terms of pillars of operations),
- the pillar(s), where the expected result(s) belong
- a list of "atomic" activities, comprising the operational activity
- the resources, either branches or roles, of course, different ones for each task, that is to provide for:
- identification of the goals, then
- the activities *possibly* contributing to its fulfillment,
- those of the executors,
- the acknowledgements of both the goal and activity,
- giving the necessary permissions,
- the executors, and their
- supervisors, etc.

REMEDIES - and again:
OFFICIAL REMEDIES

basic audit notions - control objective
warning: missing from COBIT 5

official
control objectives:
generic best practice management objectives for all IT activities

IT control objective: statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

COBIT's control objectives are the [rather :a kind of !]
minimal requirements for - or: the effective control of - each IT process.
(this is the verb "control" here)

COBIT's control objectives are the minimum, that should be prescribed,
in order to be able to effectively implement, operate & supervise the IT processes.

basic audit notions - control objective

private interpretation - my personal opinion

control objective:

an objective, derived from corporate strategy generic taking best practice into consideration - such an objective that the top management wants to achieve

IT control objective:

an objective for IT that is derived from a generic control objective in the form of a statement expressing a desired result. It can be achieved by implementing control measures / procedures concerning IT activities.

basic audit notions - control measure / procedure

private

control measure / procedure: series of measures: procedure

- the organisational structures with their operational procedures and practices
- the guidelines and procedural rulebooks ≠ policy!
- the technical developments and measures

designed to provide *reasonable* assurance

- that the business objectives will be achieved, and
- that undesired events will be

prevented / detected / corrected

preventive - detective - corrective ∃ mitigation, too

basic audit notions - control measure / procedure

reasonable assurance
what is reasonable?

reasonable is, what is efficient:
we spend
- effort,
- money,
- HR,
- etc.,

while it is worth to spend it

basic audit notions - control objective & internal control [measure] - in COSO

COSO control objectives:
(fiduciary)
- effectiveness and
- efficiency

of operations
- reliability of financial reporting
- compliance to the applicable laws and regulations

COSO internal control [measure]:
a process
effected by an entity's board of directors
management
and other personnel

designed to provide reasonable assurance
regarding the achievement of the (COSO) control objectives

predecessors of my pillars? / so called IT resources (COBIT ➔ COBIT 4.1)

- COBIT, in 1998:
  - data: data objects
  - application systems: manual and programmed procedures
  - technology: HW, operating systems, DBMS, networking, multimedia, etc.
  - facilities: that "house" the systems [and staff]
  - people: the staff with its skills, awareness and productivity...

- COBIT 4.1, in 2007:
  - organisation: network of interacting people
  - process:structured activities created to achieve a given outcome
  - technology: practical application of knowledge
  - people: human resources - including the outsource partners

! these are not the exact definitions !

predecessors of my pillars? / COBIT 5 "enablers"

COBIT 5 "enablers"
are factors that, individually and collectively, influence whether something will work—in this case, governance and management of enterprise IT
source: a 2012 ISACA book on Enabling Processes - see References here

Achieving IT-related goals requires the successful application and use of a number of enablers. Enablers include:

- Principles, policies and frameworks are the vehicles to translate a desired behaviour into practical guidance for day-to-day management.

- Processes describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.

. / .

COBIT 5 "enablers" - cont'd

COBIT 5 "enablers" - cont'd

- Organisational structures are the key decision-making entities in an enterprise.
- Culture, ethics and behaviour of individuals and the enterprise are often underestimated as a success factor in governance and management activities.
- Information is pervasive throughout any organisation and includes all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is often the key product of the enterprise.

. / .

COBIT 5 "enablers" - cont'd

COBIT 5 "enablers" - cont'd

- Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with IT processing and services.
- People, skills and competencies are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

For each enabler a set of specific, relevant goals can be defined in support of the IT-related goals.

example for COBIT advice on control objectives and control measures

let's choose from the IT processes of COBIT 4.1 one of the hot topics:
applications

AI2 Acquire and Maintain Application Software

this process has 10 suggested control objectives
in the COBIT reference manual

let's choose:
AI2.6 Major Upgrades to Existing Systems

the suggested control procedure:
In the event of major changes to existing systems that result in significant change in current designs and/or functionality, follow a similar development process as that used for the development of new systems.

AI2 Acquire and Maintain Application Software
- advice taken from the COBIT reference manual (see references)

the business requirement that AI2 should support:
o align available applications with business requirements
- in a timely manner
- at a reasonable cost

o suggested requirements:
- translating business requirements into design specifications
- adhere to development standards for all modifications
- separate development, testing and operational activities

o measure possibilities, e.g.:
- number of production problems per application causing visible downtime
- percent of users satisfied with the functionality delivered

brave new world?

example for a more or less similar problem from ISO 27001

a standard for: "Information technology - Security techniques - Information security management systems - Requirements"

a comparison between its versions

from this applications point of view

more or less the same from ISO 27001, but !

version 2013:

- A.14 System acquisition, development and maintenance
- A.14.1 Security requirements of information systems
  - 3 subgoals
- A.14.2 Security in development and support processes
  - 9 subgoals

    one of my favourites:
  - A.14.2.2 System change control procedures
- A.14.3 Test data
  - 1 subgoal: Protection of test data

more or less the same from ISO 27001, but !

while in the earlier version, date 2005:

- A.12 Information systems acquisition, development and maintenance
- A. 12.1 Security requirements of information systems
  - 1 subgoal
- A. 12.2 Correct processing in applications
  - 4 subgoals, e.g.
  - A.12.2.1 Input data validation
    - •••
  - A 12.2.4 Output data validation

no such goal in the version 2013 **!**

more or less the same from ISO 27001, but !

- A.12.2.3 Cryptographic controls
  - 2 subgoals
- A.12.4 Security of system files
  - 3 subgoals
- A.12.5 Security in development and support processes
  - 5 subgoals
    - •••
  - A.12.5.5 Outsourced software development