COBIT-Based
Corporate Governance & Risk Management

1. General Overview - Best Practice - I.

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/

Disclaimer

The followings represent my personal opinion on / interpretation of the subject.
Some results of my research are also included, of course, in a marked way.

Neither ISACA nor ITGI, NIST, nor the other professional organizations
quoted here are liable for the followings or
would be bound any way by its contents.

Note:
Should the original English formulation be inexact,
I present my own version, too.
The source is clearly identified.

Szenes Katalin

the goal of the study materials

- to contribute to the operational excellence of the firms
- especially to corporate governance, and
- to risk management excellence

- to support IT staff in encountering IS audit / auditors
  - IT is regularly audited both in the government and in the business sector,
  - every member of the IT staff, even the developers of either data processing applications or embedded systems have to prepare to work with auditors, who check if their results support
    - governance,
    - business continuity planning, and
    - other aspects of IT security
  - from the viewpoint of
    - supporting the strategic goals of the institution,
    - complying both to the national laws and EU directives
    - and **?**

introducing myself

- As chief information security officer in Erste Bank Hungary I built up the information security infrastructure and procedures, then served in CIB Bank as senior information security advisor.
- I have been teaching at the Hungarian CISA Review Course and contributing to the ISACA CISA Review Technical Information Manual from 1999, to ISACA COBIT 5 from 2010.
- In 1998 I established teaching IT Audit and in 2002 that of IT Security at Kando Polytechnics of Technology - the predecessor of University Obuda. In 2006, together with other interested colleaugues, we established a 3-terms long Specialization in Information Security.
- I got my diplom in mathematics in 1973, my doctor university degree in mathematics and computer science in 1977 at the University Eotvos Lorand, Faculty Natural sciences, my PhD in Information Science and Technology in 2014 in Obuda University. I presented numerous lectures in international conferences, and I have 25 independent references to my publications.

Society work:

- founder president of Budapest Chapter of (ISC)2
- president of IT Committee of European Organisation for Quality Hungary Branch
- president of Dept. Computer Technics of Scientific Society for Infocom
- member of ISACA (Information Systems Audit and Control Association)

Table of Contents

1. General Overview

O the sources of best practice
& designations for auditors' & security experts

- ISACA, ISC2, designations
- one of the most important sources of these transparents: COBIT
- COSO, one of the predecessors

O an answer to the well-being of the companies: security & strategy

O for solving the problems to be handled - first: classify / their parameters
- choosing the parameters

O the use of this classification
O an important part of the problem solving: problem / risk maintenance

O examples for the problems to be handled
- social, technical attacks
- disorder

Table of Contents

kind of *REMEDIES*

a "to do" list according to the best practice of ISACA and others

governance

- O corporate governance - OECD
- O corporate / IT governance in COBIT
- O relation of risk - value - IT governance in the CISA study materials
- O COBT 4.1 - COSO / Internal Control—Integrated Framework
- O stakeholders role in IT governance
- O advantages of IT governance
- O problems with IT governance
- O documents relating to IT governance

Table of Contents

the COBIT way of best practice advice:
LIST of TERMS
SERVING INFORMATION SECURITY ➔ CORPORATE GOVERNANCE

O **IT processes in COBIT 1998 - 2007, and in COBIT 5**
  O IT processes in the COBIT before COBIT 5

O **the predecessors of my excellence criteria:**
  special goals - "evaluative" goals -
  the predecessors of my excellence criteria:
  - COBIT ➔ COBIT 4.1 (1998 - 2007) information criteria
  - COBIT 5 - ? the metrics, but ...
  - (ISO requirements)

  - . / .

Table of Contents

the COBIT way of best practice advice:
LIST of TERMS
SERVING INFORMATION SECURITY ➔ CORPORATE GOVERNANCE

O **the predecessors of my excellence criteria** cont'd:

- the important characteristics of [corporate operations] in COSO
  the information [quality] criteria in COSO

- COBIT information [quality] criteria
  1998 ➔ 2007: COBIT ➔ COBIT 4.1

- COBIT 5 Information Attributes

a good advice on the best practices – but...

references

the sources of these transparents, designations for auditors' & security experts

www.isaca.org
www.isc2.org
www.coso.org

CISA – Certified Information Systems Auditor,
CISM - Certified Information Security Manager,
CGEIT - Certified in Governance Enterprise IT
designator:
ISACA: Information Systems Audit and Control Association - USA

CISSP - Certified Information Security Professional
designator:
ISC2 International Information Systems Security Certification Consortium - USA

another best practice: the ISO standards

☠ and there are many more

other useful sources

- ISO standards:
  ISO/IEC - International Organization for Standardization /
  International Electrotechnical Commission

- W3C - World Wide Web Consortium
- OASIS - Organization for the Advancement of Structured Information Standards - www.oasis-open.org
  e-business guidelines, non-profit
- OWASP - Open Web Application Security Project
  www.owasp.org
  development of "secure"? - reliable? applications

one of the most important sources of these transparents: COBIT

the methodology of ISACA: COBIT + the Review Manuals

C **C**ontrol
OB **OB**jectives
I for **I**nformation
T and Related **T**echnology

the basic terms (- till 2011 ??):
control objectives + control measures
these are suggested to IT processes in COBIT

(at first such kind of advice brings in my personal experience)

COSO, one of the predecessors - a source of some basics in the ISACA materials

- the Committee of Sponsoring Organisations of the Treadway Commission
  abbreviated as: Treadway Committee (1st chairman: James C. Treadway, Jr.)
- a voluntary organization of the private sector, founded in 1985, in order to support the National Commission on Fraudulent Financial Reporting
- recommendations for SEC (Security Exchange Committee of the NY Stock Exchange), for enterprises, for auditors
- supporting organizations:
  - AICPA (American Institute of Certified Public Accountants),
  - AAA (American Accounting Association),
  - FEI (Financial Executives International),
  - IIA (Institute of Internal Auditors),
  - IMA (Institute of Management Accountants).

(www.coso.org)

an answer to the well-being of the companies: security & strategy
or: strategy & security?

what kind of rules and procedures do we need?
to serve all of the stakeholders
to allocate rights, responsibilities,
to support decision planning?

- a structure that supports the setting of the goals of the company
- advice, how to achieve these goals
- advice, how to avoid / manage risks meanwhile
- advice, how to monitor performance
- etc.

solution: an adequate governance
that is: a strategy-based governance

➔ strategic goals ➔ first: lower-level, more *practical* goals
that can be assigned to the staff - here comes in COBIT

for solving the problems to be handled - first: classify
➔ find parameters

- ways of classifications
- viewpoints of classifications
- subjects of the measures

choosing parameters

- ways of classifications
  let's choose:
  - (set of) lower level goals to higher level goals
  - activities, contributing to goals

- viewpoints of classifications
  - top-down: starting from strategic goals
    - popular criteria
    - company-specific parameters
      (pillars of operations)

  - bottom-up: starting from identified problems
    (actually these also start from strategic goals)

classifying the problems to be handled
- subjects of the measures - an ISACA *asset* classification

- physical assets
- financial assets
- intellectual assets
- information - see the COBIT resources till 4.1
- know-how (I would've put it to info)
- relationships
- reputation and brand value

but this doesn't cover the possibilities
suggestion: pillars of operations

an important part of the problem solving: problem / risk maintenance

how to do this?

1st step: identification:

- (usually directed) investigations, ethical hacking, etc.
- best practice advice

THEN any kind of subject classification can be used
ISACA's asset classification or any other set of subjects
& characteristics of the problem
➔ a possibility to design matrices for the research

for *example:*

- rows: asset classifications
- columns: asset handling excellence criteria
- in the elements of the matrices:
  - advice on the excellent operations

examples for the problems to be handled /
social hacking: starting from a LinkedIn invitation - 2015

"You could see them talking about where they were going and where they were in Afghanistan and Iraq ... some were uploading pictures with geolocation information, and we were able to see them," says Thomas Ryan, the mastermind behind the social network experiment and co-founder and managing partner of cyber operations and threat intelligence for Provide Security, who will present the findings later this month at Black Hat USA in his "Getting In Bed With Robin Sage"

"Robin's Facebook profile was able to view coordinates information on where the troops were located. "If she was a terrorist, you would know where different [troops'] locations were,"

- http://www.darkreading.com/risk/robin-sage-profile-duped-military-intelligence-it-security-pros-/d/d-id/1133926?

7/6/2010 06:21 PM

14 July, 2015

technical, e.g. APT
- what is this?

advanced persistent threats =
a long-term pattern of targeted, sophisticated attacks
(now this will do)

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)

we will come back to this **!**

APT examples

- the earliest published attack on military research establishments:
  "The Cuckoo's Egg"
- Moonlight Maze
- an innocent target:
  NASA: National Aeronautics and Space Administration
- Titan Rain
- Sykipot
- Operation Aurora
- Gozi

nowadays fashionable:
- vulnerability in a mobile operating system

- ! etc. !

REMEDIES - kind of

a "to do" list according to the best practice of ISACA and others

the methodological tools:

o governance, IT governance

o special goals
- practical goals, that are able to contribute to strategic goals

o kind of "excellence criteria":
- ISO requirements /
- COBIT ➔ COBIT 4.1 (1998 - 2007) information criteria
- COBIT 5 - ? no corresponding attribute?

o "more general" goal: the control objective

o activity: operational measure, control measure

o domain of activity:
- COBIT ➔ COBIT 4.1: ? resources
- COBIT 5 enablers (- are they similar?)

best professional practice & suggestions

in governance

corporate governance - OECD

corporate governance - corporate wellness, market success, growth
OECD (Organisation for Economic Cooperation and Development):

➔

- "ethical corporate behaviour by directors or others charged with governance in the creation and presentation of wealth for all stakeholders"
- "the distribution of rights and responsibilities
  - among different participants in the corporation, such as
  - board, managers, shareholders and other stakeholders
- and (it) spells out
  - the rules and procedures for making decisions on corporate affairs"

[quoted from: CRM]

corporate governance - OECD

(OECD on public governance:

"Good, effective public governance helps to strengthen democracy and human rights, promote economic prosperity and social cohesion, reduce poverty, enhance environmental protection and the sustainable use of natural resources, and deepen confidence in government and public administration." **)**

(quoted from CRM: OECD website on Public Governance and Management)

corporate governance - OECD

- The Organisation for Economic Cooperation and Development (OECD) states: "Corporate governance involves
  - a set of **relationships** between a company's management, its board, its shareholders and other stakeholders.
  - Corporate governance also provides the **structure** through which the objectives of the company are set, and
  - the **means** of attaining those objectives and monitoring performance are determined.
- Good corporate governance should provide
  - proper **incentives** for the board and management to pursue objectives that are in the interests of the company and its shareholders and
  - should facilitate **effective monitoring.**." (OECD 2004, OECD Principles of Corporate Governance, p.11) "

corporate & IT governance in COBIT

COBIT 4.1:

enterprise governance involves:
- o the need for assurance about the **value** of IT
- o the management of IT-related **risks**
- o the increased requirements for **control** over information

COBIT 4.1 -
bases of IT governance:

- o value
- o risk
- o control (?)

💣 this is not the control measure but more probably the control system !

relation of risk - value - IT governance in the CISA study materials

Two issues of IT Governance:

/1 IT delivers value to the business
this is driven by:
strategic alignment of IT with the **business**

/2 IT risks are managed
this is driven by:
embedding **accountability** into the enterprise

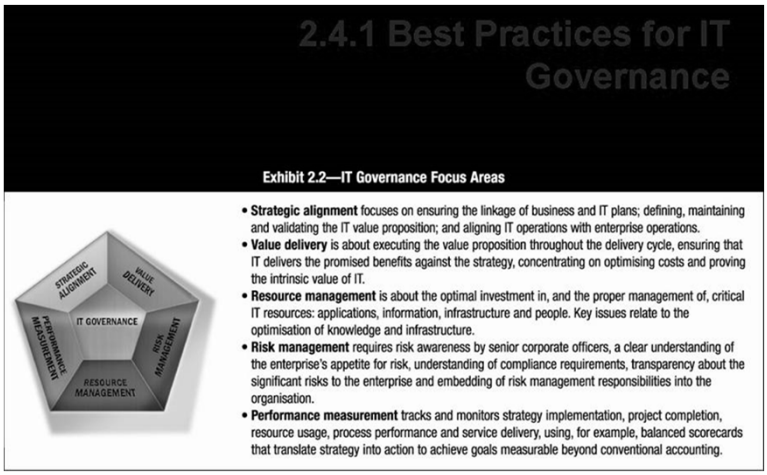
source: CISA® Review Course transparents, ISACA

what is the "ISACA - relation" between

strategy - risk management - value & performance? ● / ●

relation of risk - value - IT governance in the CISA study materials

best practice for IT governance - IT governance focus areas:
source of this exhibit is also: CISA® Review Course transparents, ISACA



COBT 4.1 / COSO / Internal Control—Integrated Framework

Requirements - ***the ancestors of the COBIT "advising frame"***

- Organisations should satisfy the
  - quality,
  - fiduciary and
  - security (?)

requirements for their information, as for all assets.

- Management should also optimise the use of available IT resources, including
  - applications,
  - information,
  - infrastructure and
  - people.
- To discharge these responsibilities, as well as to achieve its objectives, management should
  - understand the status of its enterprise architecture for IT and
  - decide what governance and control [measures] it should provide.

stakeholders role in IT governance

IT governance implies a system where
every stakeholder
gives input to the decision making process:

- Board
- Internal customers
- Finance

source: CISA® Review Course transparents, ISACA

an early ISACA method, that resulted in great benefit: IT Steering Committee

advantages of IT governance

IT governance has become significant due to:

- Demands for better return from IT investments
- Increases in IT expenditures
- Regulatory requirements for IT controls - control √
- Selection of service providers and outsourcing
- Complexity of network security
- Adoptions of control frameworks
- Benchmarking

source: CISA® Review Course transparents, ISACA
think: which control is meant here **?**

problems with IT governance

Indicators of potential problems *include*:

- Unfavorable end-user attitudes
- Excessive costs
- Budget overruns
- Late projects
- High staff turnover
- Inexperienced staff
- Frequent hardware/software errors

source: CISA® Review Course transparents, ISACA

documents relating to IT governance

The following documents should be reviewed
at least:

- IT strategies, plans and budgets
- Security policy documentation
- Organization/functional charts
- Job descriptions
- Steering committee reports
- System development and program change procedures
- Operations procedures
- Human resource manuals
- Quality assurance procedures

source: CISA® Review Course transparents, ISACA

the COBIT way of best practice advice:
LIST of TERMS
SERVING INFORMATION SECURITY ➔ CORPORATE GOVERNANCE

IT processes in the COBIT

1998 - 2007 - COBIT base
2000 - COBIT 2000
2005 - COBIT 4
2007 - COBIT 4.1

the COBIT way of best practice advice:
LIST of TERMS
SERVING INFORMATION SECURITY ➔ CORPORATE GOVERNANCE

IT processes in the COBIT before COBIT 5:

COBIT generic process model = 4 domain of IT activities:

plan and organise - PO
acquire and implement - AI
deliver and support - DS
monitor and evaluate - ME

to the process – resource – criteria triple
➔ control objectives are assigned, and to these:
➔ control measures / procedures that realize these goals

the COBIT way of best practice advice:
LIST of TERMS
SERVING INFORMATION SECURITY ➔ CORPORATE GOVERNANCE

IT processes in the COBIT before COBIT 5:

- Plan and Organise (PO)

Provides direction to solution delivery (AI) and service delivery (DS)

- Acquire and Implement (AI)

Provides the solutions and passes them to be turned into services

- Deliver and Support (DS)

Receives the solutions and makes them usable for end users

- Monitor and Evaluate (ME)

Monitors all processes to ensure that the direction provided is followed

the COBIT way of best practice advice:
LIST of TERMS
SERVING INFORMATION SECURITY ➔ CORPORATE GOVERNANCE

the 5 new COBIT 5 IT processes - processes for governance of enterprise IT

- Evaluate, Direct and Monitor
- Align, Plan, and Organise
- Build, Acquire and Implement
- Deliver, Service and Support
- Monitor, Evaluate and Assess

the COBIT *(and then my new)* ***way of best practice advice:***
LIST of TERMS
SERVING INFORMATION SECURITY ➔ CORPORATE GOVERNANCE

- Best Practice - I. *traditional*
  - information criteria
  - resources
  - control objectives
  - control measures
- Best Practice - II. *new*

  information security ↔ corporate operations mutual support
  - operational excellence criteria
  - pillars of corporate operations
  - operational objective
  - operational measure

the predecessors of my
operational **excellence criteria**

the best professional practices
used to emphasize the *quality of the information:*

COSO
ISO
COBIT

I suggest to tie the criteria
to the *excellence of operations*

the important characteristics of [corporate] operations in COSO

the fiduciary formulation of
the Treadway Commission
- COSO :

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

COSO versus the usual information [quality] criteria: ● / ●

the information [quality] criteria in COSO

COSO requirements:
quality + fiduciary + security

where:
- o quality: quality - cost - delivery

- o fiduciary:
  effectiveness and efficiency of operations
  reliability of financial reporting
  compliance with laws and regulations

- o security:
  availability - confidentiality - integrity

COBIT - Control Objective for Information Technology
information [quality] criteria - információ [minőségi] kritériumok:

- a célnak való megfelelés - célravezető információ - effectiveness
- eredményesség - efficiency
- bizalmasság - confidentiality
- integritás, sértetlenség - integrity
- rendelkezésre állás - availability
- külső követelményeknek való megfelelés - compliance
- megbízhatóság - reliability [of information]

(I *think* these are ***the*** appropriate Hungarian terms)

ISO (first CCITT, then BSI, and then ISO)

- availability
- integrity
- confidentiality

COBIT information [quality] criteria 1998 ➔ 2007: COBIT ➔ COBIT 4.1

effectiveness:

the information is

- relevant and pertinent to the business process
- delivered in a timely, correct, consistent and usable manner

efficiency:

the provision of information through the optimal (most productive and economical) use of resources

confidentiality:

the protection of sensitive information from unauthorised disclosure

↗ **!** this above is not enough

access according to the roles - job descriptions

COBIT information [quality] criteria 1998 ➔ 2007: COBIT ➔ COBIT 4.1

integrity:

- o accuracy and completeness of information
- o its validity in accordance with business values and expectations

it is frequently mixed with: ... *well, with??*

availability - erroneous and deficient:

- o the information is available when required by the business process now and in the future
- o the safeguarding ?! of necessary resources and associated capabilities.

√ predictability

reliability:

- o appropriate information for management to operate the entity
- o to exercise its fiduciary and
- o governance responsibilities

.

COBIT information [quality] criteria 1998 ➔ 2007: COBIT ➔ COBIT 4.1

compliance:

complying with those

- o laws,
- o regulations and
- o contractual arrangements

to which the business process is subject, i.e.,

- o externally imposed business criteria, as well as
- o internal policies - [!] guidelines & procedural rulebooks

COBIT 5 Information Attributes

Information Attributes
from the COBIT 5 "Good Practices":

– Physical (Carrier, Media)
– Empirical (User Interface)
– Syntactic (Language, Format)
– Semantic (Meaning), Type, Currency, Level
– Pragmatic (Use),
includes: Retention, Status, Contingency, Novelty
– Social (Context)

(Enabling Information - COBIT 5 An ISACA Framework - see references)

take care ! best practices are not omnipotent!
- even if this is not absolutely perfect, either

even my excellence criteria are not omnipotent, let's take my
➔ documentation

one of the possible common mistakes adopting COBIT 5:
o **"Making implementation all about policy and process documentation.** Many organizations believe documenting their processes equals GEIT implementation. In reality, documentation is only 10% or less of the overall GEIT journey. The remaining 90% is about managing the organizational changes by **educating people,** helping them to follow new processes and practices, reviewing and refining the processes, and reviewing the effectiveness of the change."
(GEIT - Governance of Enterprise IT)

Sreechith Radhakrishnan, COBIT Certified Assessor, ISO/IEC 20000 LA, ISO/IEC 27001 LA, ISO22301 LA, ITIL Expert, PMP:
5 Common Mistakes in Adopting COBIT 5
COBIT Focus | 11 May, ISACA

(there is no omnipotent best practice, but the critics is not faultless, either)

references

the base - personal involvement from 1999: contributor as a member of the ***Quality Assurance Team***
year nnnn CISA Review Technical Information Manual
editor: Information Systems Audit and Control Association
Rolling Meadows, Illinois, USA, nnnn-1 → updated yearly

the COBIT development process:

- ***COBIT*** Executive Summary
  April 1998 2nd Edition
  Released by the COBIT Steering Committee and the Information Systems Audit and Control Foundation
- ***COBIT***® 3rd Edition, July 2000
  Released by the COBIT Steering Committee and the IT Governance Institute™
  editor: Information Systems Audit and Control Association - ISACA
- ***COBIT***® 4.0
  Control Objectives, Management Guidelines, Maturity Models
  Copyright © IT Governance Institute® , 2005

- ***COBIT***® 4.1
  Framework, Management Guidelines, Maturity Models
  Copyright © IT Governance Institute®, 2007 **. / .**

references

then: the COBIT 5

- COBIT® 5 Design Paper Exposure Draft
  © 2010 ISACA

other COBIT® 5 materials followed
- personal involvement: I was member of the **Subject Matter Expert Group**

- COBIT 5.0 Vol. I – The Framework" and "COBIT 5.0 Vol. IIa – Process Reference Guide © 2011 ISACA, working paper

- Enabling Processes - COBIT 5 An ISACA Framework
  Copyright © 2012 ISACA, ISBN 978-1-60420-239-7

- COBIT Focus articles, e.g. I got this in January, 2014:
  Vishal Salvi, Avinash W. Kadam:
  Information Security Management at HDFC Bank:
  Contribution of Seven Enablers

- Enabling Information - COBIT 5 An ISACA Framework
  Copyright © 2013 ISACA, ISBN 978-1-60420-350-9

references

the predecessors of ISO 27001, ISO 27002 are:
CRAMM, ISO/IEC 17799

o ISO 27001 International Standard ISO/IEC 27001 First edition 2005-10-15
Information technology - Security techniques - Information security management systems - Requirements
Reference number: ISO/IEC 27001:2005 (E)

at 1st: Copyright © ISO/IEC 2005, then new edition: in 2013

o ISO 27002 International Standard ISO/IEC 27002 First edition 2005-06-15
Information technology — Security techniques — Code of practice for information security management
Reference number: ISO/IEC 27002:2005(E)

at 1st: Copyright © ISO/IEC 2005, then new edition: in 2013

references - a short sample from my publications
used in the transparents describing excellence criteria, pillars, etc.

- Building a Corporate Risk Management Methodology and Practice
  EuroCACS 2002 - Conf. for IS Audit, Control and Security Copyright 2002 ISACA, Tutorial
- "IT GRC versus ? Enterprise GRC
  but: IT GRC is a Basis of Strategic Governance"; EuroCACS 2010
- Enterprise Governance Against Hacking. Procds. of the 3rd IEEE International Symposium on Logistics and Industrial Informatics - LINDI 2011 August 25–27, 2011, Budapest, Hungary
- 2011:Serving Strategy by Corporate Governance - Case Study: Outsourcing of Operational Activities; Procds. of 17th International Business Information Management Association - IBIMA November 14-15, 2011, Milan, Italy, ed. Khalid S. Soliman
- K. Szenes: Operational Security - Security Based Corporate Governance
  in: Procds. of IEEE 9th International Conference on Computational Cybernetics (ICCC); July 8-10, 2013 Tihany, Hungary, IEEE Catalog Number: CFP13575-USB (pendrive); CFP13575-PRT (printed) ISBN: 978-1-4799-0061-9 (pendrive); 978-1-4799-0060-2 (printed) Copyright @2013 by IEEE. p. 375-378

references

- ISACA / APT
  Advanced Persistent Threats: How to Manage the Risk to Your Business
  © 2013 ISACA, **ISACA**
  3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008 USA
  www.isaca.org; www.isaca.org/Cyberattack
  www.isaca.org/knowledge-center