Auditing Information Systems - an MSc Course
Part - II

Obuda University
John von Neumann Faculty of Informatics
Institute Applied Informatics

Dr. Univ. 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.

A következők saját személyes véleményemet és értelmezésemet tükrözik.
Néhány kutatási eredményem is szerepel itt, természetesen jelölve.
Sem az ISACA, sem az ITGI, NIST, sem a többi, itt idézett szakmai szervezet nem felelős az itt következőkért, amely számukra semmilyen kötelmet nem jelent.

Szenes Katalin

note 1: the English formulation doesn't always follows the original either
1. megjegyzés: az angol fogalmazás sem mindig egyezik az eredetivel
the comments, where the subjectivity are to be emphasized are denoted by "comment" or [ ]
hangsúlyozottan szubjektív megjegyzéseimet a "comment" vezeti be, vagy [ ] -be teszem

note 2: the bilinguality - where it is present - is to support the related vocabulary of the Hungarian students
2. megjegyzés: az egyes helyeken alkalmazott kétnyelvűség a magyar hallgatók ide tartozó szókincse fejlesztését szolgálja

goal of education I. a counter-hacking strategy

the keys of this strategy:

- an excellent corporate operations
  - identifying the strategic goals for the sustainaibility of the company
  - identifying the business goals contributing to the strategic goals
  - finding the supporting
    - criteria for excellent operations
    - asset handling excellence criteria

    necessary to the business goals
- risk management excellence

goal of education II. for the firms that employ our students

- I hope to contribute to the operational excellence of the firms, where our students work
- the goal is 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 **?**

goal of education III. - to help our students to be able:

- to contribute to the operational excellence of the firms, where / to which they work

- to support the staff in encountering IS (Information Systems) audit / auditors
  - the IT of both the government business sector is regularly audited
  - every member of the staff, especially the IT, even the developers of either data processing applications or those of embedded systems have to prepare to work with auditors, who check if they comply with the requirements of the
    - region (e.g. EU),
    - local authorities, professional unions,
    - mother companies - actually everybody, who is authorized to audit
  - from the viewpoint of different
    - best practice methods
    - national, regional, branch, etc. laws and directives
    - and ?

TOC - tartalom

PART - I

REMEDIES ?

see the PART I transparents

TOC - tartalom

PART - II

- risk - kockázat
  - traditional definition
  - my new definition for risk
  - the factors, that affect risk value
  - managing risk
  - inherent risk - "elidegeníthetetlen" kockázat
- procedures concerning contracts
- auditing contracts - RFP
- IT governance in the ISACA Audit Standards Framework (S10)

TOC - tartalom -
alapfogalmak magyarázata COBIT 4.1 segítségével IS
- explanation of some basic notions using COBIT 4.1

when the auditor is awakened at night ...
ha az auditort éjjel álmából költik ...

- COBIT 4.1 process owner - folyamat tulajdonos
- COBIT roles and responsibilities - szerepkörök és felelősségek
- segregation / separation of duties - a (jó) kötelességelhatárolás
  on the organizational hierarchy
  tasks in the organizational basic pillar
- Note on the Subject Guideline - Policy - Procedural Rulebook
  megjegyzés - az irányelvek, politikák, (eljárási) szabályzatok témához
- authentication - authorization
  hitelesítés - feljogosítás
- COBIT Policy, Plans and Procedures
  - Szabályzatok, irányelvek, tervek, eljárások

TOC - tartalom

from ISACA CISA ® Review Course transparents:

- on the audit
  - audit, information sytems (IS) audit
  - classification of audits
  - [some] general audit procedures
  - [some] procedures for testing & evaluating IS control [systems]; GAS
  - [on the] phases of audit

TOC - tartalom

from ISACA CISA ® Review Course transparents:

- measuring the performance
  - (possible) phases
  - (some) considerations

- special problems
  - on the outsource - forrás: Az Informatikai biztonság kézikönyv

- data privacy
  - laws, examples

Explanations - Magyarázatok
References - Irodalomjegyzék

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

PART - II

risk

it is often said:

= "equal to"

how can we be that sure?!?

unfortunately, only
~ "proportionality"
can be stated

risk - kockázat

- **quantitative risk assessment: probability** ← **mennyiségi**
- **qualitative risk assessment: likelihood** ← **minőségi**

- **the** - less stupid - **traditional definition:**
  risk is proportional to: likelihood * impact
  kockázat ~ a bekövetkezés valószínűségével, és
  a hatással

where:

probability = the likelihood of an outcome
this probability could be "measured" by fractions, or decimals

***but*: likelihood ~ vulnerability of the asset**
a baj bekövetkezése a vagyonelem sérülékenységével arányos
***but*: vulnerability reversely proportional to the effort of the staff**
az erőfeszítéssel a sérülékenység fordítva arányos

risk - kockázat

risk - is connected closely to strategy
or: risk is the risk of failing in its fulfillment
➔ asset value depends mostly on the *strategic* value of the asset
⬇
my definition deals with: *asset* risk

risk ↗ strategic value of the asset * probability of the threatening
and
reversely proportional with:
the vulnerability of the asset

homework:
think about the relations between:
strategic value; probability of attack; vulnerability (maintenance)

the factors, that affect risk value

risk (asset, goal) ~ distance (asset, goal)
probability (asset, goal, attack)
vulnerability (asset, goal, effort)

➔ transparency

managing risk - kockázatkezelés

the short version of my definition for a
strategy-driven goal and risk management excellence

- is based on the responsibility of the top management,
  - concerning corporate strategy, and
  - the definition and update regularly the strategic goals to be reached in order to ensure market success

- involves the elaboration of
  - a system composed of a managing process and a requirement system, where the latter
  - requires given requirements to be satified by top management and staff

managing risk - kockázatkezelés

- these given requirements reflect management commitment
  - to support,
  - or even to initiate, the efforts of the staff,

  having concrete tasks in the asset risk processing,

- these tasks of the staff include at least the followings:
  - devising methods to the *asset* risk processing
  - detecting points of *operations*, where concrete measures - activities are to be executed, in order to detect, prevent undesirable events, or correct their effect, if the decision had been to accept their occurence

- and where predefined part of the steps of the process are to be repeated regularly

- these tasks are obligatory part of an "excellent" risk processing cycle

managing risk - kockázatkezelés

roughly speaking (rough: in mathematical sense)
some of the most important steps of risk management

- choosing methodology
- identifying problems - prestige, physical, financial, etc.
  - assigning responsibilities,
  - marking important assets,
  - ***etc.***
- classifying everything according to every currently useful aspects
  - using either expressing or arbitrary aspects
- risk management
  = solving the problems, that are worth to solve
  = mitigating the risks
  by the means of control objectives / -measures /-procedures **. / .**
- review of the situation, focusing on the issues of previous audits

managing risk - kockázatkezelés

- mitigating the risks
  by the means of
  - control objectives
    excellence criteria, or
    other goals, contributing to strategic / business goals
  - measures / -procedures
    activities on the domain of the 3 pillars
    ranging to the same or other pillar

- regulation
- organization
- technics

risk - kockázat

(

a note only - for use in answering CISA questions
csak egy megjegyzés! CISA kérdésekhez

egy hivatalos def. a könyvből -
an official definition

inherent risk - elidegeníthetetlen, a dolog természetében rejlő kockázat:
derived from the *nature* of the business
az üzlet *természetéből* ered
(no inheritance - nem öröklés!)

)

procedures concerning contracts
source: **CISA® Review Course transparents, ISACA**
Chapter 2: IT Governance

There are various phases to
computer hardware, software and IS service contracts,
including:

- Development of contract requirements and service levels
- Contract bidding process
- Contract selection process
- Contract acceptance
- Contract maintenance
- Contract compliance

auditing contracts - RFP
source: **CISA® Review Course transparents, ISACA**
Chapter 2: IT Governance

RFP - request for proposal
what is this process?

- what needs to be reviewed in an RFP

in general, and from a governance perspective?

- the evaluation criteria and
- methodology of an RFP, and
- the requirements to meet organizational standards

auditing contracts
source: **CISA® Review Course transparents, ISACA**
Chapter 2: IT Governance

the adequacy of the following terms and conditions are at least to be audited:

- Service levels
- Right to audit or third party audit reporting
- Software escrow
- Penalties for noncompliance
- Adherence to security policies and procedures
- Ownership of intellectual property (IP)
- Protection of customer information
- Contract change process
- Contract termination and any associated penalties

+ my experience:

- identification of the contact persons
- the difference between delivery/receipt ▲ completion

IT governance in the ISACA IS Auditing Standards Framework
source: **CISA® Review Course transparents, ISACA**
Chapter 1: The IS Audit Process

S10 IT Governance

- Review and assess the IS function's alignment with the organization's mission, vision, values, objectives and strategies
- Review the IS function's statement about the performance and assess its achievement
- Review and assess the effectiveness of IS resource and performance management processes
- Review and assess compliance with legal, environmental and information quality, and fiduciary and security requirements
- Use a risk-based approach to evaluate the IS function
- Review and assess the organization's control environment
- Review and assess the risks that may adversely affect the IS environment

role of COBIT references here - COBIT hivatkozások szerepe itt

source - forrás:

COBIT control requirements to its generic process model
COBIT ellenőrzési követelmények az átfogó folyamatmodelljéhez

to explain:
owner, role, policy, plans and procedures

tulajdonos, szerepkör, szabályzatok, irányelvek, tervek, eljárások magyarázata

COBIT - process owner
COBIT - folyamat tulajdonos

PC2 Process Ownership

- Assign an owner for each IT process, and
- clearly define the roles and responsibilities of the process owner.

Include, for example,
- responsibility for process design,
- interaction with other processes,
- accountability for the end results,
- measurement of process performance and
- the identification of improvement opportunities.

COBIT - process owner
COBIT - folyamat tulajdonos

PC2 A folyamat tulajdonlása

A folyamat tulajdonos
- kijelölése
- szerepköreinek és
- felelősségének definiálása

Példa felelősség tárgyaira:
- a folyamat megtervezéséért
- más folyamatokkal való kölcsönhatásáért - együttműködéséért [**!**]
- a végeredményekért való elszámoltathatóságért
- [mindezek **!**] mérhetőségéért
- a folyamat teljesítményének mérhetőségéért
- e fejlesztési lehetőségek felismeréséért.

COBIT Roles and Responsibilities
COBIT Szerepkörök és felelősségek

PC4 Roles and Responsibilities

- Define
  - the key activities and
  - end deliverables of the process.
- Assign and
- communicate
  - unambiguous roles and responsibilities

  - for effective and efficient execution of the key activities and
  - their documentation as well as
  - accountability for the process end deliverables.

COBIT Roles and Responsibilities
COBIT Szerepkörök és felelősségek

PC4 Szerepkörök és felelősségek

Meg kell határozni a folyamat

- kulcstevékenységeit és
- végtermékeit.

Egyértelmű szerepköröket kell

- kiosztani és
- kommunikálni, a következők érdekében:
  - a folyamat kulcstevékenységeinek hatékony és célravezető
    - dokumentálása és
    - végrehajtása
  - a folyamat végtermékeiért való elszámoltathatóság.

segregation / separation of duties - a (jó) kötelességelhatárolás

requirements:

- the duties / the forbidden things have to be known
- too extensive scope might be dangerous
- to every duty at least 2 persons should be available
- *the roles of executor and supervisor shouldn't belong the same job description*
- etc.

means:

- order in the organization
- organized organization - tasks of units, and
- their relations are well-determined
- *job descriptions, and*
- *access rights - identity management (IDM)* - **have to be aligned to them**
- etc., see e.g. COBIT roles, responsibilities

segregation / separation of duties - a (jó) kötelességelhatárolás

követelmények:

- tudni kell, mit kell tenni, és mit nem szabad
- veszélyes lehet a túl széles hatókör
- mindent legalább ketten csináljanak
- végrehajtó és ellenőrző szerepkör ne tartozzék ugyanahhoz a munkakörhöz (job description)
- stb.

eszközök:

- rend a szervezetben
- megszervezett szervezet - az egységek feladata, és
- ezek összefüggései pontosan meg vannak határozva
- *munkaköri leírások, és*
- *ezekhez igazított hozzáférési jogosultságok, IDM*
- stb., ld. pl. COBIT szerepkörök, felelősségek

on the organizational hierarchy

topmost ("above the top management):

Supervisory Committee - shareholders' assembly - parent company

top management
↓

CFO , chief of production, chief of operations, etc.
↓ CIO, CSO - should belong here

↓
still happens: CISO is subordinated to IT or CFO

(CFO: financial officer,
CSO: chief security officer, CISO: chief information security officer)

tasks in the organizational pillar

requirements ⇔	**organizational units**
availability	top management
integrity	IT
confidentiality	physical,
➔ access control measures	logical IT security - independent from IT
legal, regulatory compliance	dept. internal audit
applications & etc. functionality	legal dept.
best professional practice	
	external audit

support:
IT steering committee
risk management shadow organization

authentication - authorization
hitelesítés - feljogosítás

authentication / authorization

authentication:
act of verifying
- the identity of a user
- the user's eligibility to access ...
- prior knowledge info

authentic: accurate, ... authoritative, ... certain, dependable, factual, trustworthy, ...

authenticate: ... authorize, ... certify, confirm,... guarantee, validate, verify, ...

authentication - authorization
hitelesítés - feljogosítás

authentication – cont'd

The authentication is a 2 step *process* by which the *system* verifies the *identity* of the user

1st : the computer system verifies the validity of the logon ID
2nd :the computer system forces the user to substantiate his/her validity via a password

logon ID: individual ***identification*** and ***authentication***
password: prevents ***unauthorized*** use

authentication - authorization
hitelesítés - feljogosítás

authorize: accredit, ... entitle

authorization:
ability, blank cheque, ... approval, credentials,
leave.. -... permission

user is authorized → has the authority to access

test question:

The password is best described as a method of user
A identification B AUTHORIZATION
C AUTHENTICATION D confirmation

COBIT Policy, Plans and Procedures
- Szabályzatok, irányelvek, tervek, eljárások

PC5 Policy, Plans and Procedures - Szabályzatok, irányelvek, tervek, eljárások IT folyamatokhoz

Define and communicate how
all policies, plans and procedures that drive an IT process are
- documented,
- reviewed,
- maintained,
- approved,
- stored,
- communicated and
- used for training.

Assign responsibilities for each of these activities and, ***at appropriate* times**,
- review whether they are executed correctly.

Ensure that the policies, plans and procedures are
- accessible,
- correct,
- understood and
- up to date.

COBIT Policy, Plans and Procedures
- Szabályzatok, irányelvek, tervek, eljárások

PC5 Szabályzatok, irányelvek, tervek, eljárások IT folyamatokhoz

Meg kell határozni, és
közzé kell tenni,
az informatikai folyamatokat
meghatározó

szabályzatok,	hogyan vannak	dokumentálva	mindezekért	**ki kell jelölni a felelősöket**, és
irányelvek,		felülvizsgálva		*megfelelő*
elvek,		karbantartva		*időközönként*
eljárások		jóváhagyva		
		tárolva		felülvizsgálat, hogy
		közzétéve		mindezt
		oktatásra felhasználva		megfelelően
				hajtják végre.

Biztosítani kell, hogy
a szabályzatok, irányelvek, tervek, eljárások
hozzáférhetőek, helyesek, megértették, naprakészek.

Note on the Subject Guideline - Policy - Procedural Rulebook
megjegyzés - az irányelvek, politikák, (eljárási) szabályzatok témához

egy *lehetséges* felfogás:

irányelv - általános,

politika - szereplők / kötelességek,

szabályzat - ki mit csinál

audit, information sytems (IS) audit
source: **CISA® Review Course transparents, ISACA**
Chapter 1: The IS Audit Process

Definition of auditing

- Systematic process by which a competent, independent person objectively obtains and evaluates evidence regarding assertions about an economic entity or event for the purpose of forming an opinion about and reporting on the degree to which the assertion conforms to an identified set of standards.

Definition of IS auditing

- Any audit that encompasses review and evaluation (wholly or partly) of automated information processing systems, related non-automated processes and the interfaces between them.

classification of audits
source: **CISA® Review Course transparents, ISACA**
Chapter 1: The IS Audit Process

- Financial audits
- Operational audits
- Integrated audits
- Administrative audits
- IS audits
- Specialized audits
- Forensic audits

general audit procedures
source: **CISA® Review Course transparents, ISACA**
Chapter 1: The IS Audit Process

General audit procedures
comment: **involve**

- Understanding of the audit area/subject

comment 1:

- overview of the target - business (goal, strategy, processes)
- checking prior audit reports
- positioning the subject

comment 2: defining + reconciling audit scope

- Risk assessment and
- general audit plan
- Detailed audit planning

general audit procedures
source: **CISA® Review Course transparents, ISACA**
Chapter 1: The IS Audit Process

General audit procedures - cont'd

- Preliminary review of audit area/subject
- Evaluating audit area/subject

- Verifying and evaluating controls **[both** control objectives / measures !]
  (e.g. according to the information + COSO criteria)
  [my comment: actually the whole control system! should be taken into account]

- Compliance testing

comment: compliance to inner / external requirements

- Substantive testing
- Reporting (communicating results)
- Follow-up

Procedures for Testing and Evaluating IS Control *[Measure]*s - Control Systems; GAS
source: **CISA® Review Course transparents, ISACA**
Chapter 1: The IS Audit Process

- Use of generalized audit software - GAS - to survey the contents of data files

Features of generalized audit software:

- Mathematical computations
- Stratification
- Statistical analysis
- Sequence checking

Functions supported by GAS:

- File access
- File reorganization
- Data selection
- Statistical functions
- Arithmetical functions

./.

Procedures for Testing and Evaluating IS Controls - Control System
source: **CISA® Review Course transparents, ISACA**
Chapter 1: The IS Audit Process

procedures [involve] - cont'd

- Use of specialized software to assess the contents of operating system parameter files
- Flow-charting techniques for documenting automated applications and business process
- Use of audit reports available in operation systems
- Documentation review
- Observation

on the phases of audit
source: **CISA® Review Course transparents, ISACA**
Chapter 1: The IS Audit Process

Audit phases [involve]

- Audit subject
- Audit objective
- Audit scope

comment: audit charter:

- Stating management's responsibility and objectives for, and delegation of authority to, the IS audit function
- Outlining the overall authority, scope and responsibilities of the audit function

reconciling audit charter: after changes customer's approval

on the phases of audit
source: **CISA® Review Course transparents, ISACA**
Chapter 1: The IS Audit Process

Audit phases [involve] - cont'd

- Pre-audit planning

[resources: auditors / auditee, time tables, etc.]

- Audit procedures and steps for data gathering

[see continuous audit, CAAT - Computer Assisted Audit Tool]

- Procedures for evaluating the test or review results

[substantive audit, evidences, audit materiality]

- Procedures for communication with management
- Audit report preparation
- [follow up]

measuring the performance - possible phases
source: **CISA® Review Course transparents, ISACA**
Chapter 2: IT Governance

The broad phases of performance measurement are:

- Establishing and updating performance measures
- Establishing accountability for performance measures
- Gathering and analyzing performance data
- Reporting and using performance information

measuring the performance - some considerations
basis: **CISA® Review Course transparents, ISACA**
Chapter 2: IT Governance

- Processes should be driven by performance indicators
- Optimization refers to the process of improving the productivity of information systems to the highest level possible without unnecessary, additional investment in the IT infrastructure
- Model—A model is built or established first to evaluate the performance and alignment with the business objectives.
- Measurement error—Conventional measures do not properly account for the true inputs and outputs.
- Lags—Time lags between expense and benefit are not properly accounted for in current measures.
- Redistribution—IT is used to redistribute the source of costs in firms; there is no difference in total output, only in the means of getting it.
- Mismanagement—The lack of explicit measures of the value of information makes resources vulnerable to misallocation and overconsumption by managers. As a result, proper performance measurement techniques will play an increasing role for program managers and investment review boards.

special problems - **on the outsource**
forrás: Az Informatikai biztonság kézikönyve
Dr. Szenes Katalin: Az informatikai erőforrás-kihelyezés auditálási szempontjai

egy oszlop a fejezet 1. ábrájából:

(Példa ***informatikai biztonsági szempontok*** felügyelhetőségére
aszerint, hogy

- a Vevőnek a Szállító, vagy saját munkatársai dolgoznak-e,
- honnan (Vevőtől / Szállítótól)
- hová - kinek a telephelyére)

szempontok:

- változáskezelés az infrastr. elemekre
- dokumentáció az infrastr. elemekre
- lehetőleg sz.géppel felügyelt jogosultságkezelés
- infrastr.elemek beszerzési, karbantartási, és üzemeltetési rendje
- inf. üzletmenet folytsági terv és rendszeres tesztje
- kapacitásmenedzsment
- távoli bejelentkezés biztonsága
- adatcsere biztonsága

data privacy

European Union:
the good old:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
  Official Journal L 281 , 23/11/1995 P. 0031 - 0050

Hungary - stronger requirements:

- year 1992, No. LXIII.
  On the privacy of personal data, and on the publicity of data of public interest
- modification (e.g.?) for financial institutions: year 2003, No. XLVIII.
  effective from 1st January, 2004
- numerous modifications, e.g. on the cost of data delivery, 2015

now: GDPR - see Part I

data privacy - an interesting approach in court

- no matter, how
- no matter what

http://www.ugyvedvilag.hu/rovatok/szakma/e-mail-mint-magantitok

A más magántitkát tartalmazó elektronikus levelezés anyaga mint bizonyíték a bírósági eljárásban felhasználható, ha az a per tárgyával releváns módon összefügg, és az igazság érvényesülését biztosítja.

Explanations - Magyarázatok

Evidence

S14 Audit Evidence

source: IT governance in the ISACA IS Auditing Standards Framework
(CISA® Review Course transparents, ISACA
Chapter 1: The IS Audit Process)

- Includes procedures performed by the auditor and results of those procedures
- Includes source documents, records and corroborating information
- Includes findings and results of the audit work
- Demonstrates that the work was performed and complies with applicable laws, regulations and policies

Explanations - Magyarázatok

Materiality

1 anyagiasság; material: fontos, jelentős, lényeges, a kérdéshez tartozó

2 S12 Audit Materiality

source: IT governance in the ISACA IS Auditing Standards Framework
(CISA® Review Course transparents, ISACA
Chapter 1: The IS Audit Process)

- The IS auditor should consider audit materiality and its relationship to audit risk
- The IS auditor should consider potential weakness or absence of controls [both objectives / measures, of course] when planning for an audit
- The IS auditor should consider the cumulative effect of minor control deficiencies or weaknesses
- The IS audit report should disclose ineffective controls or absence of controls

[here: both kind of]

Explanations - Magyarázatok

- allegation - (tény)állítás
- corroboration - megerősítés, alátámasztás, hitelesítés, igazolás
- empowerment - feljogosít, képessé tesz
- inherent risk - elidegeníthetetlen, a dolog természetéből eredő kockázat
- incumbent - háruló, tartozó, to be incumbent on: v.kire hárul; itt: tisztviselő
- intrinsic - belső, lényeges, valódi
- " argument - tételből levont érv
- leverage - ... befolyás;... emelőerő; ... eszköz cél elérésére
- purview - látókör, hatókör, működési terület, ...
- repercussion - káros következmény, -utóhatás
- pertain - hozzátartozik, vele jár, v.minek a jellemző tulajdonsága (to)
- pervasive - széles körben szétterjedt, mindent átjáró/ áthatő/ átitató
- stipulation - feltétel, megszorítás, szerződési kikötés
- stratification - osztályozás

References - Irodalomjegyzék

the base - personal involvement from 1999: contributor as a member of the ***Quality Assurance Team***

No "n" CISA Review Technical Information Manual
editor: Information Systems Audit and Control Association
Rolling Meadows, Illinois, USA, "n" -1 → updated yearly - formerly, now we do not know

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 - Irodalomjegyzék

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 Vol. 1, January, 2014:
  Vishal Salvi, Avinash W. Kadam:
  Information Security Management at HDFC Bank:
  Contribution of Seven Enablers
  ©2014 ISACA

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

References - Irodalomjegyzék

then: the COBIT 2019

COBIT®

as Expert Reviewer, I am a member of COBIT Working Group 2017-2018

I participated in:

- [COBIT 2019, 2018, Gov] COBIT 2019 Framework: Governance and Management Objectives
  ISBN 978-1-60420-728-6
  Copyright © 2018 ISACA

- [COBIT 2019, 2018, Intro] COBIT® 2019 Framework:
  Introduction and Methodology
  ISBN 978-1-60420-644-9
  Copyright © 2018 ISACA

References - Irodalomjegyzék

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

- 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

- 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

see important others in part I !

References - Irodalomjegyzék

- ISO/IEC 15408
  Information technology — Security techniques
  — Evaluation criteria for IT security
  (Common Criteria)
  (ITCSEC, majd ITSEC, majd CC)

- Magyar Szabvány MSZ ISO/IEC 12207:2000
  Magyar Szabványügyi Testület
  Informatika. Szoftveréletciklus-folyamatok
  Information technology. Software life cycle processes
  megfelel: az ISO/IEC 12207:1995 verziónak

- **ETC. !! - *see others in part I !***

References - a short sample from my publications used in the transparents excellence criteria, pillars

- 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 - a short sample from my publications used in the transparents book chapters in "Az informatikai biztonság kézikönyve"

Az Informatikai biztonság kézikönyve
Verlag Dashöfer, Budapest, Hungary, ISBN: 963 9313 122

- Az ISACA auditálási alapelvei, és a COBIT® módszertan bemutatása
  Az Informatikai biztonság kézikönyve, 21. aktualizálás
  Verlag Dashöfer, 2006. augusztus, 7.2.1. old. - 7.2.83. old. - 83 oldal

- A számítógéphálózatok biztonságának felülvizsgálata
  Az Informatikai biztonság kézikönyve, 28. aktualizálás
  Verlag Dashöfer, 2008. február, 5.3.1 1. old. - 5.3.1.18. old. - 18 oldal

- Kockázatkezelés szempontrendszerrel irányított értékelési módszerrel
  Az Informatikai biztonság kézikönyve, 32. aktualizálás
  Verlag Dashöfer, 2009. február, 8.6.1. old. - 8.6.5.2.2.6 old. - 62 olda

References - a short sample from my publications used in the transparents book chapters in "Az informatikai biztonság kézikönyve"

- Szenes, K.: Az informatikai erőforrás-kihelyezés auditálási szempontjai
  Az Informatikai biztonság kézikönyve,
  I. rész: 36. aktualizálás, 8.10. 1. old. – 26. old. (26 oldal)
  Verlag Dashöfer, Budapest, 2010. február
  II. rész: 39. aktualizálás, 2010. december
  8.10. 27. old. – 158. old.

- K. Szenes: Governance - Risk - Security
  keynote lecture at: SecureCEE Conference, April 21, 2015
  organized by:
  International Information Systems Security Certification Consortium (ISC)2
  available at: (ISC)²'s InterSec:
  https://isc2intersec.leveragesoftware.com/default.aspx

other 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

- https://www.gartner.com/newsroom/id/3812063 - Gartner newsroom at January 2018