Auditing Information Systems - an MSc Course Part I

Obuda University
John von Neumann Faculty of Informatics
Institute Applied Informatics

Dr. Katalin Szenes
CISA, CISM, CGEIT, CISSP, PhD

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.
idézetnél a szögletes zárójel [ ] az én kommentemet jelöli
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 my subjectivity is 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
insertion to quotations enclosed in braces [ ] denotes my comments

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

- a detour towards fashion - problems / practice
- some of the technology trends

  + explanations
  + explanations to the explanations
  mine / theirs

- challenges:
  - PSD2, GDPR, obligatory recommendations
  - USA and the European privacy trends - ISACA, ISC2
  - ISACA State of Privacy Survey
  - European Payments Council:
    2020 Payments Threats and Fraud Trends Survey
  - from the history of the data privacy approach in the USA - GLB 1999
  - USA: Security and Privacy Controls for
    Federal Information Systems and Organization
    - a sample from Special Publication 800-53 Revision 4
      - the families of the security control [objectives]

- "old" requirements
  - SEC - regulation of securities trade
  - SOX - further -"-

TOC - tartalom PART I

- the "official" best practice sources; designations for auditors & security experts
  - ISACA, ISC2, designations
  - ISACA and
  - NIST materials
  - COSO, one of the predecessors
  - Europe: ISO standards
- some important aspects of defense
- example for *practical* problem solving:
  (proposed) dimensions for classifying the problems to be handled:
    - assets by ISACA classification
    - another classification:
      according to the characteristics of the problem
      and / or according to the excellence criteria
    - ➔ how to use this in practical problem solving

)

TOC - tartalom PART I

- examples for problems to be handled
    - ? ∃ state against state? or:state against enterprises ?
    - typical problem: mobile, e.g. Android mobile
    - social hacking: social media, e.g. a LinkedIn invitation
    - a great fright: APT
      - what is this?
- some of the old classics - examples
  - the earliest published attack on military research establishments:
    "The Cuckoo's Egg"
  - Moonlight Maze
  - NASA: National Aeronautics and Space Administration
  - Titan Rain
  - Sykipot
  - Operation Aurora
  - Gozi
  - ! etc. !

TOC - tartalom PART I

REMEDIES? - kind of

- protection targets / levels - a possible view MIX
  - endpoints
  - network
  - border
  - corporate

  + users' activity-related measures

- turning to corporate level: what is the fashion?
  buzzwords:
  - digitalization
  - big data
  - cloud

TOC - tartalom PART I

REMEDIES? - kind of - cont'd

- turning to corporate level: an other view on the needs
  - solution: governance
- a *usable* corporate governance definition - from my practice
- corporate governance / IT governance
- a *usable* operational security definition
- governance goals ↔ information security - IT audit methods
  → consequences of this approach
- governance ↔ operational security

TOC - tartalom PART I

- contributing to the solution - overview only
  - supporting the fulfillment of the strategic goals: what / how and their dimensions
    - suggested *practical* "subgoals":
      - criteria of excellent governance

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

      asset handling excellence criteria:,
      - *availability, integrity, confidentiality*
      - a "general" suggested "subgoal": the operational objective

TOC - tartalom PART I

- contributing to the solution - overview only cont.'d
  - 3 pillars of operation - a működés pillérei

    {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
  - IT architectural infrastructure elements
  - operational activity - and its useful attributes approach: detective - preventive - corrective

TOC - tartalom PART I

on the "to do" details according to the **best practice** of ISACA and ISO

governance in the best professional practice

- corporate governance - OECD
- relation of risk - value - IT governance in the CISA study materials
- stakeholders role in IT governance
- advantages of IT governance
- problems with IT governance
- documents relating to IT governance

- **the predecessors of my excellence criteria**
  the "quality" of information
  - COBIT till 4.1 and ISO
  - special goals - "evaluative" goals in COBIT 5
  - the information [quality] criteria in COSO

TOC - tartalom PART I

- basic audit notions - ellenőrzési alapfogalmak
  - control objective - ellenőrzési cél - COBIT / magán / COSO
  - control measure / procedure - ellenőrzési intézkedés / eljárás
    - COBIT / magán / COSO
  - what kind of assurance is reasonable? - mi az ésszerű mérték?
  - example for control objectives and measures
    - példa ellenőrzési célokra és intézkedésekre, és
    - a 3-féle "ellenőrzési" intézkedésre
- COBIT history: the relationship of the 4 "old" COBIT domains
  COBIT történelem: a 4 "régi" tartomány összefüggései
- the 5 new COBIT 5 processes - processes for governance of enterprise IT
- take care ! best practices are not omnipotent

(the references are detailed in Part II)

TOC - tartalom PART II

PART II - overview of some important notions - separate series of transparents

- 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 - PART II
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 PART II

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 PART II

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

subjects for the exam

- excellence criteria
  - operations
  - asset handling
- pillars of operations
- preventive - detective - corrective operational activities / control measures
- segregation / separation of duties (Part II.)
- risk versus strategy (Part II.)
- authentication versus authorization (Part II.)

a detour towards fashion - practice
vulnerability assessment

ISACA P8 Security Assessment—Penetration Testing and Vulnerability Analysis
Effective 1 September 2004

some of the guiding requirements:
P8/ 1.1.2
Standard S6 Performance of Audit Work states, "During the course of the audit,

- the IS auditor should obtain
  - sufficient,
  - reliable
  - and relevant evidence to achieve the audit objectives.
- The audit findings and conclusions are to be supported by
  - appropriate analysis and
  - interpretation of this evidence."

COBIT Framework:

- "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this
- responsibility as well as to achieve its expectations, management should establish an adequate system of internal control."

a detour towards fashion - practice
vulnerability assessment

according to P8 (2004) the [main] purpose is:
"to test controls that should be employed to protect against unauthorised access"
"Records should be in sufficient detail to support the findings and conclusions reached as a result of the testing to:

- Defend against accusations of unethical or unauthorised practices against the IS auditor performing the test
- Provide the organisation with a detailed description of the weaknesses and how they were identified and exploited
- Provide an audit log for future testing to provide reasonable assurance that vulnerabilities identified have been addressed
- Demonstrate the possibility and risk of unauthorised access from any determined/willing attacker possessing the skills"

Types:

- external
- internal
- physical access
- social engineering testing
- wireless
- web application (includes:
  - "manual and automated testing of the portal site as an outsider with no login information"
  - "insider through a standard login account")

a detour towards fashion - practice
vulnerability assessment

FIRST: Forum of Incident Response and Security Teams

some of the SIGs of FIRST:

- Academic security
- Big data
- CVSS - common vulnerability scoring system
- Ethics
- Industrial control systems
- Malware analysis
- etc.

a detour towards fashion - practice
vulnerability assessment

CVSS decribes, among others:

- the vulnerability itself, with its main characteristics
- the scoring according to such metrics, as, e.g.
  - complexity
  - required privileges
  - impacts related to:
  - confidentiality
  - integrity
  - availability
- required privileges, etc.

see: https://www.first.org/cvss/

tool e.g.: Tenable Network Security Nessus

note: CVSS-like descriptions are used at GUIs of firewalls, etc.

overview of the basic requirements
🛠 for roles related to audit / security
🧍 for my students

- the duty of every member of the staff:
  - to serve the strategic goals of the company / institution

➔ the duty of the management:

  - to identify & publish the strategy
  - to translate &
  - to decompose, then
  - to delegate the tasks **together** with responsibilities,

but the responsibility can not be given away

  - to check & acknowledge
  - ...

- instead of foggy, not too concrete ideals
  - quality goals are to be set
  - assigned to well-defined units in the hierarchy

- ➔

overview of the basic requirements
🛠 for roles related to audit / security
for my students

- for supporting the excellence of the operations
  operational excellence criteria

- for the support of
  - task identification
  - check

  the pillars of operations

- audit: help in preparing strategy

- business, support and security area:
  help in finding methods

by heart is to be known - the meaning, and not a given definition:
risk, segregation (separation) of duties, etc.

on the tools for supporting the basic requirements

- what is the use of the standards, guidelines, and methods - methodologies?

- they give
- advice?
- prescription?
- or?

for

- the operations of the institution?
- for improving the quality of its products?

  how to:
  - evaluate
  - produce

- what is to be standardized, and what is NOT to be standardized?
- dangers & advantages

anyway - concrete advice is more useful then the dreaming

(Some of the) Technology Trends

- Artificial intelligence, neural networks, machine learning, robotics

- Intelligent things
- Virtual and augmented reality
- Digital twins
- Cloud to the edge
- Blockchains and distributed ledgers
- Conversational systems
- Mesh app and service architecture
- Adaptive security architecture
- Quantum computing
- Big data

etc.

(most of the ecxplanations come from Gartner Top 10 Strategic Trends)

explanations to the trends

- a possible AI definition, this and similar ones: from lots of sources

  Creating systems that learn, adapt and potentially act autonomously will be a major battleground for technology vendors through at least 2020. The ability to use AI to enhance decision making, reinvent business models and ecosystems, and remake the customer experience will drive the payoff for digital initiatives through 2025.

  https://smartconcil.com/news/top-10-tech-trends-for-2018/
  http://www.digitalwhizz.in/blog-1.php

  https://d.facebook.com/story.php?story_fbid=945934932249442&id=581592688683670&__tn__=%2AW-R

I think: a system that behaves as if it were human

explanations to the trends

- A neural network
  is a series of algorithms that endeavors to recognize underlying relationships in a set of data through a process that mimics the way the human brain operates. -
  https://www.investopedia.com/terms/n/neuralnetwork.asp

  Neural networks help us cluster and classify -
  https://pathmind.com/wiki/neural-network

- Conversational Platforms
  interaction between humans and the digital world,

  "The platform takes a question or command from the user and then responds by executing some function, presenting some content or asking for additional input."

explanations to the trends

- Machine Learning

  is an application or the subfield of artificial intelligence (AI). Machine Learning enables the system to automatically learn and progress from experience without being explicitly programmed. Machine Learning is a continuously developing practice. The goal of Machine learning is to understand the structure of data and fit that data into models, these models can be understood and used by people. In Machine Learning generally, the tasks are classified into broad categories. These categories explain how learning is received, two of the most widely used machine learning methods are supervised learning and unsupervised learning.

  https://digitalcloudops.com/2019/08/28/machine-learning-vs-neural-network/

explanations to the trends

- Cloud to the Edge

"Edge computing describes a computing topology in which information *processing*, and content *collection* and *delivery*, are placed closer to the *sources* of this information. Connectivity and latency challenges, bandwidth constraints and greater functionality embedded at the edge favors distributed models. Enterprises should begin using edge design patterns in their infrastructure architectures — particularly for those with significant IoT elements."

"When used as complementary concepts, cloud can be the style of computing used to create a service-oriented model and a centralized control and coordination structure with edge being used as a delivery style allowing for disconnected or distributed process execution of aspects of the cloud service," said Mr. Cearley.

explanations to the trends

- intelligent thing [here]
  "physical things that go beyond the execution of rigid programming models to exploit AI to deliver advanced behaviors and interact more naturally with their surroundings and with people"

- digital twin:
  "digital models of industrial equipment and manufacturing processes"
  https://www.ge.com/digital/sites/default/files/The-Digital-Twin_Compressing-Time-to-Value-for-Digital-Industrial-Companies.pdf

  [the digital representation of a real-world something, it helps testing such complex things as e.g. features of self-driving cars, agricultural developments, etc.]

explanations to the trends

- "A blockchain — originally block chain — is a distributed database that maintains a continuously-growing list of ordered records called *blocks*. Each block contains a timestamp and a link to a previous block. By design blockchains are inherently resistant to modification of the data — once recorded, the data in a block cannot be altered retroactively. Blockchains are "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically."

  https://en.wikipedia.org/wiki/Blockchain_(database)

  bitcoin !

the blocks of the blockchain contain the hash of the previous block

→ **tampering** involves the change of the contents of every previous block

→ very difficult

explanations to the trends

- mesh app and service architecture

  the Google search shows, that already in 2016 this had been a predicted trend issue

  "The device mesh refers to an expanding set of endpoints people use to access applications and information or interact with people, social communities, governments and businesses. The device mesh includes mobile devices, wearable, consumer and home electronic devices, automotive devices and environmental devices — such as sensors in the Internet of Things (IoT)."

  source:

  http://2016.secr.ru/lang/en/program/program-overview/mesh-app-and-service-architecture

  Central and Eastern European Software Engineering Conference

  Moscow, October, 2016

explanations to the trends

- adaptive security architecture
  the Google search shows, that already in 2016 this was already a predicted trend issue

  "It is an information security approach that employs modern tactics and tools to thwart the attack on the network by cybercriminals. It can be considered as a way of "*beating the cybercrime masters in their own game*". Thus, organizations should not solely rely on preventative mechanisms as cybercriminals are continuously "upping" their game and not giving up in launching attacks on vulnerable networks. In simpler terms, ***Adaptive Security Architecture*** means having flexible security measures in place to be able to protect an organization's information. This goes beyond the traditional perimeter defence from potential threats."

https://adaptivesecurityarchitecture247.wordpress.com/2016/04/16/what-is-adaptive-security-architecture-2/

- ! see also the interesting definition of architecture ./.

explanations to the trends

- architecture definition:

John Zachman:
"described architecture as a set of descriptions of representation e.g.

- What? (Inventory sets);
- How? (Process);
- Where? (Distribution);
- Who? (Responsibility);
- When? (Timing cycles);
- Why? (Motivation/Intention)."

https://adaptivesecurityarchitecture247.wordpress.com/2016/04/16/what-is-adaptive-security-architecture-2/

explanations to the trends

- immersive experience

  "Mixed reality, a type of immersion that merges and extends the technical functionality of both AR [- augmented reality] and VR [- virtual reality], is emerging as the immersive experience of choice providing a compelling technology that optimizes its interface to better match how people view and interact with their world."

- event driven

  "Digital business drives the need for IT leaders, planners and architects to embrace event thinking." ... "Business events could be anything that is noted digitally, reflecting the discovery of notable states or state changes, for example, completion of a purchase order, or an aircraft landing. With the use of event brokers, IoT, cloud computing, blockchain, in-memory data management and AI, business events can be detected faster and analyzed in greater detail."

explanations to the trends

- event broker
  - "The *EventBroker* takes the role of a mediator between publishers - instances firing events - and subscribers - instances listening to events. This decouples publisher and subscribers because they only need to know the *event broker* and the event topic they are interested in."

  http://www.appccelerate.com/eventbroker.html

- Continuous Adaptive Risk and Trust

  "To securely enable digital business initiatives in a world of advanced, targeted attacks, security and risk management leaders must adopt a continuous adaptive risk and trust assessment (CARTA) approach to allow real-time, risk and trust-based decision making with adaptive responses. Security infrastructure must be adaptive everywhere, to embrace the opportunity — and manage the risks — that comes delivering security that moves at the speed of digital business."

explanations to the trends

- Smart Space is a physical or digital environment in which humans and technology-enabled systems interact in increasingly open, connected, coordinated and intelligent ecosystems" - explanation: Gartner

- Digital Ethics and Privacy is a growing concern for individuals, organizations and governments. People are increasingly concerned about how their personal information is being used by organizations in both the public and private sector, and the backlash will only increase for organizations that are not proactively addressing these concerns. - explanation: Gartner

- Quantum Computing: operates on the quantum state of subatomic particles (for example, electrons and ions) that represent information as elements denoted as quantum bits (qubits). - explanation: Gartner

explanations to the trends

- *"Big Data (Data Intensive) Technologies*

are targeting to process high-volume, high-velocity, high-variety data (sets/assets) to extract intended data value and ensure high-veracity of original data and obtained information that demand cost-effective, innovative forms of data and information processing (analytics) for enhanced insight, decision making, and processes control; all of those demand (should be supported by) new data models (supporting all data states and stages during the whole data lifecycle) and new infrastructure services and tools that allow obtaining (and processing) data from a variety of sources (including sensor networks) and delivering data in a variety of forms to different data and information consumers and devices."

source:

Demchenko, Yuri, Peter Membrey, Cees de Laat, Defining Architecture Components of the Big Data Ecosystem. Second International Symposium on Big Data and Data Analytics in Collaboration (BDDAC 2014). Part of The 2014 International Conference on Collaboration Technologies and Systems (CTS 2014), May 19-23, 2014, Minneapolis, USA.

Big data - cont'd

the 6V Big Data Properties [versus the usual first 3 here]

- Volume
- Variety
- Velocity
- Value
- Veracity
- Variability

source:

Yuri Demchenko, Emanuel Gruengard, Sander Klous:
Instructional Model for Building effective Big Data Curricula for Online and Campus Education
2014 IEEE 6th International Conference on Cloud Computing Technology and Science
978-1-4799-4093-6/14 © 2014 IEEE
DOI 10.1109/CloudCom.2014.162

explanations to the explanations

- CARTA (Gartner):
  "As part of a CARTA approach, organizations must overcome the barriers between security teams and application teams, much as DevOps tools and processes overcome the divide between development and operations. Information security architects must integrate security testing at multiple points into DevOps workflows in a collaborative way that is largely transparent to developers, and preserves the teamwork, agility and speed of DevOps and agile development environments, delivering "DevSecOps." CARTA can also be applied at runtime with approaches such as deception technologies. Advances in technologies such as virtualization and software-defined networking has made it easier to deploy, manage and monitor "adaptive honeypots" — the basic component of network-based deception."

- DevOps - ISACA Knowledge Center:
  [it requires a big cultural change] DevOps represents a major paradigm shift in how enterprises author software. By integrating the operations side of software deployment into development itself, enterprises can create applications more efficiently, adapt more quickly to changes in user requirements and achieve greater resilience in operations so that applications perform more smoothly over time.

challenges - PSD2 (https://www.eba.europa.eu/)

PSD2 - Directive (EU) 2015/2366 on Payment Services in the internal market
discussed in:
European Banking Authority (EBA)

PSD2 entered into force in the European Union on 12 January 2016
(publication of a draft: consultation paper: August 2016)
in force from: 13 January 2018

techical standards on:

- strong customer authentication
- common and secure communication

"These technical standards will ensure appropriate levels of security, while at the same time maintaining fair competition between all payment service providers and allowing for the development of user-friendly, accessible and innovative means of payment."

the history: the ***problems*** that SOFORT, and the others arise for the banks
the present situation in Hungary:

challenges - GDPR: General Data Protection Regulation

once upon a time:
EU directive 1995, as far, as data privacy was concerned

- http://ec.europa.eu/justice/data-protection/reform/index_en.htm:
  "On 15 December 2015, the European Parliament, the Council and the Commission reached agreement on the new data protection rules, establishing a modern and harmonised data protection framework across the EU"

- "the GDPR will become law in 2018 across all 28 EU member states and will replace the inconsistent laws the EU member states implemented to comply with the 1995 directive"

- data transfer outside the EU
- entities collecting data
- data protection bodies
- legislation, etc.

and see: http://www.naih.hu/

the present situation in Hungary: a kind of legislation effort

USA and the European privacy trends - ISACA

- ISACA, January 2017 - a year before the coming into effect:

THE SEVEN CATEGORIES OF PRIVACY
THAT EVERY ENTERPRISE MUST ADDRESS

privacy of
- person
- behaviour and action
- communication
- data and image - information
- thoughts and feelings
- location and space (territorial)
- association

source: ISACA knowledge center

USA trends - ISACA

- ISACA: State of Privacy Survey, 2020 3rd quarter

question on:
- enterprise privacy hiring practice
- workforce trends
- privacy by design regulations of privacy programs

key findings:

- technical privacy teams appear to be more understaffed than legal/compliance teams
- technical privacy positions often take longer to fill than legal/compliance positions.

. / .

USA trends - ISACA

- ISACA: State of Privacy Survey, 2020 3rd quarter - cont 'd

privacy by design means:

data protection by the means of technology design

➜ important in adhering to GDPR

advisable to follow already in the development phase

- "26 percent of respondents always practice privacy by design when building new applications,
- 29 percent practice it frequently,
- 23 percent sometimes,
- 9 percent rarely and
- 3 percent never
- (11 percent do not know). "

the above is a quotation from the Survey

European Payments Council: 2020 Payments Threats and Fraud Trends Survey

this transparent is based on:

EPC244-20/Version 1.0 / Date issued: 4 November 2020

- card payment fraud:

  from APT (advanced persistent threat) the criminals revert to "old school types of fraud such as lost and stolen, sometimes in combination with social engineering. As e-commerce is still on the rise, CNP (card not present -szk) fraud remains a significant factor for fraud losses"

- other frauds - nothing new?
  - APT
  - denial of service
  - malware
  - social engineering
  - botnets,
  - etc.

USA and the European privacy trends - ISC2

"SIGN OF AN ALREADY CHANGING PRIVACY CULTURE IN THE U.S.
(a year before the coming into effect:)

It appears that GDPR, approved in April 2016, may have already started influencing the culture of privacy in the U.S. On Oct. 27, 2016, FCC leadership voted 3-2 to require, among other items, an opt-in for customers of broadband providers to allow them to use and share sensitive information, including precise geolocation data, financial information, health information, children's information, Social Security Numbers, web browsing history, app usage history and the content of communications. Broadband providers will have a year to comply after the rules are published"

source: Harvey Nusz: GDPR. How do I know I will (or need to be) compliant? *InfoSecurity Professional* January/February 2017

from the history of the data privacy approach in the USA - GLB 1999

FTC: Federal Trade Commission - protecting America's consumers
https://www.ftc.gov/

"expressed views" already around 2000 but even in 2015

BUREAU OF CONSUMER PROTECTIONDIVISION OF FINANCIAL PRACTICES

The Gramm-Leach-Bliley Act Privacy of Consumer Financial Information

- *"financial institutions have restrictions on when they may disclose a consumer's personal financial information to nonaffiliated third parties"*
- **"Financial Institution** *Definition*: Any institution the business of which is engaging in *financial activities* as described in ... an institution must be *significantly engaged* in financial activities to be considered a "financial institution."
- ...

see: the SOX chapter in the Information Security Handbook - Verlag Dashöfer

new challenges - Security and Privacy Controls for Federal Information Systems and Organizations

Special Publication 800-53 Revision 4
developed by NIST
under the Federal Information Security Management Act (FISMA)

Executive Order 13717 signed by *President Obama* on 2-2-2016

helps in:

- selecting security controls [! control objectives]
- documenting the selection
- their structure and ordering into families

see: https://www.nist.gov/node/557866

correspondence to ISO 15408 and others ➔ consequences in Hungary

a sample from Special Publication 800-53 Revision 4

"TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES"

o	"AC	Access Control	MP	Media Protection
o	AT	Awareness and Training	PE	Physical and Environmental Protection
o	AU	Audit and Accountability	PL	Planning
o	CA	Security Assessment and Authorization	PS	Personnel Security
o	CM	Configuration Management	RA	Risk Assessment
o	CP	Contingency Planning	SA	System and Services Acquisition
o	IA	Identification and Authentication	SC	System and Communications Protection
o	IR	Incident Response	SI	System and Information Integrity
o	MA	Maintenance	PM	Program Management"

(the families of the security control [objective groups] with their identifiers)

"old" requirements - SEC www.SEC.gov

world crisis in 1933 ➔ regulation

SEC: US Securities and Exchange Commission
founded in: 1934 to promote the compilance to

- Securities Act of 1933 and
- Securities Exchange Act of 1934

Securities Act of 1933:

- to provide for financial and other important info to the investors
- to prohibit different kind of cheating

Securities Exchange Act of 1934:

- to regulate the trade of securities

SOX: Sarbanes - Oxley Act of 2002

later, to promote SOX.

- PCAOB: US Public Company Accounting Oversight Board
  for supervising the auditors

"old" requirements - SOX
an example for SOX-related pentest requirements

pentest for investigating **Sarbanes-Oxley (SOX) compliance:**
the goal is to detect

threats to

- digital data integrity,
- data access auditing,
- accountability,
- availability

as mandated in

- Section 302 ("Corporate Responsibility for Fiscal Reports"),
- Section 404 ("Management Assessment of Internal Controls"),
- Section 409 ("Real Time Issuer Disclosures")

source: a pentest standard, see pentest section

the "official" best practice sources; 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

Europe, and, of course, overseas, too: ISO standards

ISO / IEC 27000 family:

- 27000 - overview of the ISMS family, and terms
- 27001 - ISMS (information security management system) requirements
- 27002 - IT security practice, control measures
- 27003 - ISMS implementation project
- 27005 - risk

other security-related:

- ISO/IEC GUIDE 73:2002(E/F) [risk terms + on their connections - guidelines for use +
- ISO GUIDE 73:2009(E/F) Risk management — Vocabulary
  Management du risque — Vocabulaire [list of risk terms]
- etc.

on some other ISO standards

- 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

corresponds to: ISO/IEC 12207:1995 *what a pity! that old*

but:

- ISO/IEC 27034:2011+ Information technology — Security techniques — Application security (parts 1, 2 & 6 published, remainder in DRAFT)

there are lots of others:

- on business continuity planning (24762),
- governance (38500), etc.

other useful sources

- 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
- www.securityfocus.com

one of the most important knowledge base: COBIT

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

the basic terms - alapvető fogalmak:

control objectives + control measures
ellenőrzési célok + ellenőrzési intézkedések

(hopefully this differentiation will be required - at last
remélhetőleg ez egy megkívánt megkülönböztetés lesz - végre)

COSO, one of the predecessors - egy elől
a source of some basics in the ISACA materials
néhány alapvető dolog forrása az ISACA anyagaiban

- The Committee of Sponsoring Organisations of the Treadway Commission - a Treadway bizottságot szponzoráló szervezetek bizottsága.
- A COSO a magánszektor egy önkéntes szervezete, amely a pénzügyi jelentések minősége fejlesztéséhez kíván hozzájárulni, az üzleti etika, a hatékony belső ellenőrzési intézkedések, és a vállalatirányítási módszerek segítségével.
- 1985-ben alakult, a pénzügyi jelentésekkel kapcsolatos csalások nemzeti bizottságának (National Commission on Fraudulent Financial Reporting) támogatására. Ezt a bizottságot röviden gyakran csak "Treadway bizottságnak" nevezik, első elnökéről, James C. Treadway, Jr.-ról.
- A Treadway bizottság a magánszektor kezdeményezésére alakult. Annak alapján készít ajánlásokat a tőzsdei társaságok, azok auditorai, a SEC, és más szabályozó szervezetek, és oktatási intézmények részére is, hogy tanulmányozzák a csaló pénzügyi jelentések sajátosságait.

COSO, one of the predecessors - egy elöd
organizations supporting COSO - támogató szervezetek

A Treadway bizottságot támogató további szervezetek:

- az AICPA (American Institute of Certified Public Accountants - a Könyvszakértők Amerikai Intézete),
- az AAA (American Accounting Association - Amerikai Számviteli Szövetség),
- az FEI (Financial Executives International - a Pénzügyi Vezetők Nemzetközi Társasága),
- az IIA (Institute of Internal Auditors - a Belső Ellenőrök Intézete), és
- az IMA (Institute of Management Accountants).

Hungarian source – forrás English: on the web:
Szenes Katalin: 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.

example for *practical* problem solving:
classifying the problems to be handled

- ways of classifications
- viewpoints of classifications
- ways for problem solving or rather:
  ways of exploring, identifying the problems

(+ see some important aspects of defense in ISAFI lecture)

a (proposed) dimension for classifying the problems to be handled
- 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

subject for discussion / homework:

what do we think about these viewpoints?

classifying the problems to be handled
- classification according to the *characteristics* of the problem, e.g.:
according to the excellence criteria

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

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

I suggest the excellence criteria as subgoals to strategic-level goals

practical problem solving, using:
ISACA asset classification & 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

problems

? ∃ state against state? or:state against enterprises ?

- ? North Korea ⇆ Sony (information)
- ? Russia ⇆ US election (information)
- ? China ⇆ Philippines (DDos) "of course":
  the parties involved in South China Sea ...

- ? Israel ⇆ Iran (Stuxnet)

or was it somebody else? enthusiastic patriots?
or?

... on the Hungarian defense facilities ...
Hungary, 2021: Pegasus scandal
(forbidden stories; NSO Group; ***shalev*** hulio)

homework: enumarate the related official bodies of the above foreign states

examples for problems to be handled
typical problem: mobile, e.g. Android mobile

a typical GOVCERT alarm notice

- 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

- homework find something e.g. about android vulnerability, ransomware or anything
  - for Hungarian students: http://tech.cert-hungary.hu/vulnerabilities/
  - for everybody: http://www.androidcentral.com/, securityfocus, or anywhere

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

examples for problems to be handled /
social hacking: social media, e.g. a LinkedIn invitation - a dangerous army-related matter

"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

great fright: 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*

. / .

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

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)

some of the old classics

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 **optional homework: details**

examples / Moonlight Maze

around 2000:

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

targets:
- government sites,
- systems at the Pentagon, NASA , US Department of Energy,
- universities, research labs, doing military research

stealing tens of thousands of files:
- maps of military installations
- troop configurations
- military hardware designs

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

NASA - https://www.nasa.gov

NASA: National Aeronautics and Space Administration

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

Topics:
- international space station
- journey to Mars
- Earth
- technology
- etc.

Note: sometimes hackers mix NSA, NASA, NIST

examples / Titan Rain

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

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

a combined, well-researched social engineering attack on *targeted* individuals
- stealthy Trojan horse attacks
- using malware techniques bypassing contemporary security countermeasures.

➔ government secrecy ➔ ? choosing targets from industry:
- aerospace, defense, energy, financial services, manufacturing, pharmaceutical

optional homework: details

examples / Sykipot

2006:
- spear-phishing emails with malicious attachment or
- link to an infected web site,
- zero-day exploits

➔ found later, and then:

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

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

servers mostly China, belonging perhaps to an intelligence agency

optional homework: details

examples / Operation Aurora

2009:
- o used a zero-day exploit to install a malicious Trojan horse, Hydraq

➔ :

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

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

- o Adobe, Juniper, ...
- o banks, defense
- o contractors, security vendors, oil and gas companie
- o + Chinese human rights activists **!**

optional homework: details + collect more **!**

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 - kind of

protection targets / levels - a *possible* but not distinct view

- endpoint
- network
- border
- users' activities
- corporate

etc.

on defense levels & measures

endpoint protection:

- **local desktop** - malicious code
  - virus, trojan, stealthy watching - e.g. keystroke, and *more*

  infrastructural elements here:
  - machine itself - physical, bootsrtap / executive / monitor level, operating system, database, applications

  application - related security:
  - already at development phase!
  - user identity and authentication management
  - data checking
  - data encrypting

- **special endpoints**, e.g.:
  - webserver ➔ special defense tools

  infrastructural elements here:
    - webserver Microsoft / Apache - measures: banner, hardening, etc.
    - databases: disciplined development phase,
    - etc.

on defense levels & measures - mix

protection inside the network

- intrusion detection / prevention - endpoint too !
- etc.

protection on the corporate border + inside (firewalls, etc.)

- see screens on border . / .
- flood - DDos
- site-to-site connection
- site-and-employee connection (VPN, SSL, IPSec, etc.

database for the authorized ! AAA

- Radius, TACACS, or ISE (Identity Services Engine)?

- proxy for web applications
- sandbox
- etc.

once upon a time: stateful inspection

on defense levels & measures

users' activity-related measures: detective, preventive, corrective
on all the 3 pillars (regulate + organize, technics)

- data leak prevention
  - endpoint: mostly removable devices
- border:
  - internet - screening the usage
  - mail - different ways for screening the contents
- non-compliance to requirements of excellent operations, e.g.
  - missing integrity checks
  - non-functional applications +
- developing other ways unsafe applications

- enterprise mobile management
- wireless

etc.

turning to corporate level:: what is the fashion? - buzzwords

buzzwords

- digitalization
  according to Software AG
  - transformation - streamlinig multi-sys.related processes
  - integration - building consequent relations in the IT envir. of the firm
  - data - understanding data models describing enormous amount of data
  - visibility - of the operations real-time, facilitating responses to risks/ possibilities
  - applications - monitoring automatizing
    multi-sys. and multi-appl. related processes
  - scale utilizingbig data by processes with sophisticated analytic capabilities
  - connectivity - facilitating inside/ outside data sharing serving effectivity

explanation and measurement tool see: http://digital.softwareag.com/

- big data

- cloud

turning to corporate level: an other view on the needs

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
- means of attaining these goals
- means of avoiding / managing risks meanwhile
- monitoring performance
- etc.

solution: adequate governance

a *usable* corporate governance definition - from my practice

corporate - enterprise governance

- is the responsibility of the whole staff, top management included
- top management has to
  - direct the company onto the best possible way towards
    - continuous improvement, and
    - market success
  - taking every kind of environmental aspects into consideration as far, and in such a way, as it is in the interest of the enterprise, based on the strategy of the institution
  - to define and maintain this strategy belongs to the responsibility of the top management, while the staff is responsible for supporting the top management in these issues

notes to my corporate governance definition

- no hidden details are "involved".
- 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
- these have to be kept constantly under surveillance, and
- 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

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 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:

- an effective and efficient support of enterprise strategy by derivating
  - concrete everyday improving goals and
  - actions from strategic goals
- a possibility of tailoring and
- tuning the strategy

based on a *direct,* and *operations-related* feedback
- 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

- without customers there is no success in the market,
- 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.

! all of these will come

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***,

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

Risk management excellence

- a strategy-driven managing of risks,
- that are related to given goal, asset and effort
- the importance of the excellence criteria should always be evaluated
  - by the top management / business delegates,
  - with respect to each other ← there is no stand-alone risk

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

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

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

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

operational excellence criterium order

to operational excellence criterium: *order* belong:

- 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 /
- **...**

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

the pillars of operation: organization - regulation - technics

the { pillars } can be considered as:
= 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
(the distance from the strategy)

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:

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

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

- a code of ethics defining the principles of staff behaviour

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

Technics covers

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

Example for technical elements are:

- the elements of the physical infrastructure,
- together with the buildings and other facilities,
- machines,
- actually the elements of the inventory belong here,
- together with their ***descriptive*** technical features,
- 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.

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

their relation to the problem:
- detective - preventive - corrective
  vizsgálati - megelőző - javító

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.

on the "to do" details according to the best practice of ISACA and ISO

their important subjects:

- governance, IT governance

- special goals - "evaluative" goals -
  the predecessors of my excellence criteria:
  - ISO requirements / e.g. control objectives in Annex A of 27001
  - COBIT ➔ COBIT 4.1 (1998 - 2007) information criteria
  - COBIT 5 - ? the metrics
- "more general" goal: the control objective
- activity: operational measure, control measure
- domain of activity - similar to my pillars:
  - COBIT ➔ COBIT 4.1: ? resources
  - COBIT 5 enablers (- are they similar?)
  - ISACA risk management areas

governance

in the best professional practice

corporate governance - OECD
(Organisation for Economic Co-operation and Development)

corporate governance - corporate wellness, market success, growth
OECD:

➔

- "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]

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

2.4.1 Best Practices for IT Governance

Exhibit 2.2—IT Governance Focus Areas

- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.
- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

stakeholders role in IT governance

IT governance implies a system where
all stakeholders
provide input into the decision making process:

- Board
- Internal customers
- Finance

source: CISA® Review Course transparents, ISACA

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

homework: 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 predecessors of my operational ! excellence criteria:

the ! quality ! of the information

in the best professional practice

COBIT till 4.1 and ISO

Control Objective for Information Technology
- információ kritériumok - information criteria

- 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]

ISO (first CCITT, then BSI, and then ISO)
- availability
- integrity
- confidentiality

special goals - "evaluative" goals in COBIT 5

taking these as goal is ! my interpretation !

- percent of e.g.
  - IT-enabled investments
  - IT services where expected benefits are realised
  - IT-enabled investments where claimed benefits are met or exceeded
- coverage of
- level of
- number of
- cost of
- ...?

source:
Enabling Processes - COBIT 5 ... / Figure 7. IT-related Goal Sample Metrics
(see references)

the information [quality] criteria in COSO

COSO requirements:
quality + fiduciary + security

where:

- quality: quality - cost - delivery

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

- security:
  availability - confidentiality - integrity

in Hungarian: . / .

az informatikai [minőségi] kritériumok a COSO-ban

a COSO követelményei :
minőség + bizalmi fedezet + biztonság

ezek jelentése itt :

- minőségi szempontok: minőség - költség - kiszállított eredmény

- bizalmi fedezet ("kibocsátó" iránti bizalmon alapuló):
  a műveletek célravezetőek és eredményesek
  a pénzügyi jelentések megbízhatóak
  a törvényeknek és szabályozásnak való megfelelés

- biztonság:
  rendelkezésre állás - bizalmasság - sértetlenség

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

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 [the geffective 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
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.

ellenőrzési alapfogalmak - ellenőrzési cél

hivatalos

ellenőrzési cél: legjobb szakmai gyakorlatot követő általános cél, amit az IT-nek tűz ki a legfelső vezetés

IT ellenőrzési cél: az a kívánt eredmény v. szándék, amit az adott IT tevékenységre vonatkozó ellenőrzési eljárással lehet elérni. Az informatikai folyamatok hatékony irányításához a COBIT ellenőrzési céljait kell teljesíteni.

saját értelmezés

általános ellenőrzési cél: a legfelső vezetés az intézményi stratégiából levezetett, a legjobb szakmai gyakorlatnak megfelelő ellenőrzési célja

IT ellenőrzési cél: általános ellenőrzési célból levezetett, az informatikai működésre vonatkozó ellenőrzési cél. A kívánt eredményt kifejező állítás. Az informatikai tevékenységekre vonatkozó ellenőrzési intézkedésekkel / eljárásokkal érhető el.

basic audit notions - control objective - COSO - ellenőrzési cél

COSO control objectives:

(fiduciary)

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

ellenőrzési célok a COSO szerint:

(a v.mit nyújtó fél iránti bizalmon alapuló - pl. fiduciary loan: fedezet nélküli kölcsön)

- az [üzleti] céloknak megfelelő és eredményes működés
- a pénzügyi jelentések megbízhatósága
- az adott esetre alkalmazható törvényeknek és szabályozásnak való megfelelés

basic audit notions - control measure / procedure

private

control measure / procedure: series of measure: procd.

- 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

ellenőrzési alapfogalmak - ellenőrzési intézkedés / eljárás

magán

ellenőrzési intézkedés / eljárás: intézkedés sorozat: eljárás

- a szervezeti struktúrák, működési gyakorlatukkal és eljárásaikkal
- az irányelvek és szabályzatok ≠ politika!
- a technikai fejlesztések és intézkedések

amelyeket ésszerű mértékű biztosítéknak alakítottak ki

- az üzleti célok elérése,
- a nem kívánt események megakadályozása / észrevétele / kijavítása

céljából

megakadályozó - vizsgálati - javító ∃ hatás csökkentés

basic audit notions - internal control [measure] - COSO
ellenőrzési intézkedés

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

COSO belső ellenőrzés[i intézkedés]:
az igazgatótanács
a vezetőség
a többi dolgozó folyamata,
amelyet arra terveztek, hogy

ésszerű mértékben meg lehessen bizonyosodni
a COSO ellenőrzési célok eléréséről

what kind of assurance is reasonable?
- mi az ésszerű mérték?

az ellenőrzési intézkedés / eljárás ésszerűségéről
on the reasonability of the control measure / procedure

reasonable assurance
what is reasonable?
that is efficient;
we spend effort, money, HR, etc., while it is worth to spend it

ésszerű mértékű biztosíték
mi az ésszerű?
ami eredményes, hatékony;
addig költünk, amíg megéri

example for control objective and control measure
példa ellenőrzési célra és ellenőrzési intézkedésre

a COBIT 34 informatikai folyamatából egy - 4.1-ig

AI2 Acquire and Maintain Application Software
Alkalmazói rendszerek beszerzése és karbantartása

egy COBIT szerinti ellenőrzési cél az ehhez rendelt 10-ből:
AI2.6 Major Upgrades to Existing Systems

hozzá van fűzve a 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.

example for control objective and control measure
példa ellenőrzési célra és ellenőrzési intézkedésre

példa fejlesztési ellenőrzési intézkedésekre:

- a fejlesztés minden fázisában jóváhagyandó:
- a rendszer funkcionalitása megfelel
  - a tervezési specifikációnak,
  - a fejlesztési és a dokumentációs szabványoknak, és
  - a minőségi követelményeknek
- a változtatási igények jóváhagyása
- outsource esetén: jogi, szerződési követelmények kezelése

example for the 3 types of "control" measures
példa a 3-féle "ellenőrzési" intézkedésre

warning: the type depends on the interpretation
vigyázat: kiszerelés kérdése, hogy melyik fajta

preventive - detective - corrective control measures:

order, discipline, maintenance,
testing, scanning,
logs, preventive reviews,
encryption, digital signature - PKI

megakadályozó – vizsgálati – kárenyhítő intézkedések:

rendezettség, fegyelem, karbantartás,
tesztelés, szkennelés,
naplózás, megelőző vizsgálatok,
titkosítás, digitális aláírás - PKI

- Q: why the "quotes" in the title? kérdés: miért van idézőjel a címben?

COBIT history: the relationship of the 4 "old" COBIT domains
COBIT történelem: a 4 "régi" tartomány összefüggései

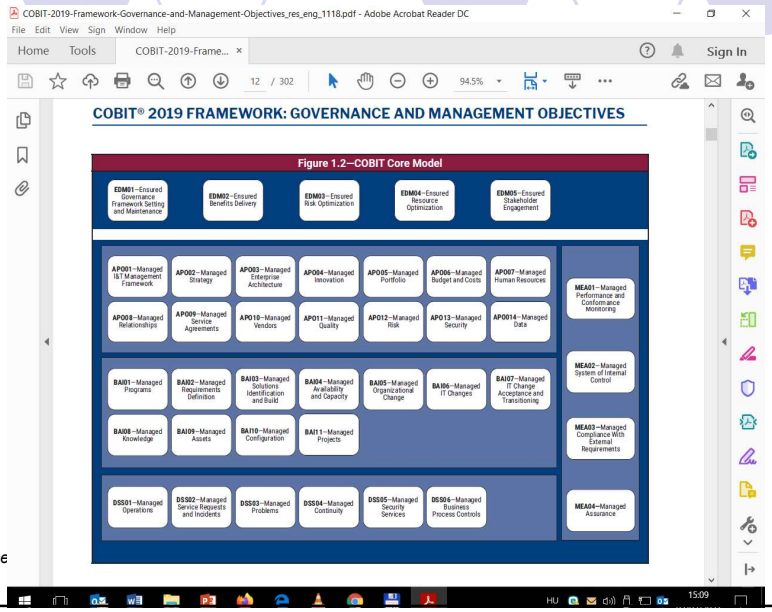
- Tervezés és szervezet (PO)
  a megoldás- és a szolgáltatás kiszállításnak, azaz a "Beszerzéshez és megvalósításhoz", illetve a "Kiszállításhoz és támogatáshoz" az útmutatást a "Tervezés és szervezés" adja.
- Beszerzés és megvalósítás (AI)
  a megoldásokat "beszerzésből" vagy "megvalósításból" nyerjük, AI támogatja a megoldások létrehozását, és továbbadja [DS-nek], hogy szolgáltatásokká alakítsák ezeket
- Kiszállítás és támogatás (DS)
  megkapja a megoldásokat, és a végfelhasználók számára felhasználhatóvá alakítja át ezeket, a megoldásokat "szolgáltatássá" a "Kiszállítás és támogatás" csiszolja, hiszen ezek a fázisok teszik hozzá a már kész megoldáshoz azt, aminek eredményeképpen a végfelhasználó már valódi terméket fog kapni.
- Felügyelet és értékelés (ME)
  felügyeli a folyamatokat, hogy biztosítsa, a megadott irányt [PO] követik, A "Tervezési és szervezési" folyamat során született specifikációk betartását pedig a " Felügyelet és értékelés" biztosítja

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

a COBIT alap ➔ 4.1 domain-eknek megfelelő
COBIT 5 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

COBIT 2019 Framework: Governance and Management Objectives
ISBN 978-1-60420-728-6



take care ! best practices are not omnipotent!

even if my favourite excellence criterium

➔ documentation

➔ etc.

one of the possible common mistakes adopting COBIT 5:

- **"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."

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 | ISACA

PART - II