Intézményi biztonság tervezés
- problémák és megoldások

Corporate security - design I.
- problems & ways to solve them

Dr. Katalin Szenes, CISA, CISM, CGEIT, CISSP, PhD
szenes.katalin@nik.uni-obuda.hu

Obuda University
John von Neumann Faculty of Informatics

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

My English formulation doesn't always follows the original either

Angol fogalmazásom 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

Insertion to quotations enclosed in braces [ ] also denotes my comments

Idézetnél is az én kommentemet jelöli a szögletes zárójel [ ]

Enforcing English / bilinguality is to support the related vocabulary of the Hungarian students

Az angol eróltetése / kétnyelvűség célja a magyar hallgatók ide tartozó szókincse fejlesztése

Szenes Katalin

tartalomjegyzék

NÉHÁNY "KURRENS" PROBLÉMA

- globális gazdasági kérdések
- nagyvállalati kérdések
  - GDPR (2016/679) : hangsúlyozottabb adatvédelem + biztonsággal ízesítve
  - fenyegetések versus a jelenlegi fejvadász HR problémák
    felvetések egy Frost & Sullivan tanulmányban
- ~~AI, felhő, big data, IoT..~~
- "új" módszerek a rendszerfejlesztésben
  - e.g.: DevOps + agile

Beal, Helen; “DevOps: The Past, the Present and the Future—Part One,” MidVision, 15 November 2012, *www.midvision.com/resources-blog/bid/275507/DevOps-The-Past- The-Present-and-the-Future-Part-One*

Beck, K.; et al.; “Manifesto for Agile Software Development,” 2001, *www.agilemanifesto.org/*

- rendszerfejlesztés új környezeti feltételek között - pre DevOps
- pénzintézeti problémák
  - PSD2 - a kényelmi szolgáltató
  - kripto: bizalomvesztés?

table of contents

SOME OF THE "CURRENT" PROBLEMS

- global economic issues
- corporate issues
  - GDPR (2016/679) : a more emphasized privacy + a flavour of security
  - threats versus the present head-hunting HR problems
    - concerns in a Frost & Sullivan study
- ~~AI, cloud, big data, IoT...~~
- "new" methodologies in the systems development
  - e.g.: DevOps + agile

Beal, Helen; "DevOps: The Past, the Present and the Future—Part One," MidVision, 15 November 2012, *www.midvision.com/resources-blog/bid/275507/DevOps-The-Past- The-Present-and-the-Future-Part-One*

Beck, K.; et al.; "Manifesto for Agile Software Development," 2001, *www.agilemanifesto.org/*

- system development in new environmental conditions - pre Devops
- issues in financial institutions
  - PSD2 - the service provider
  - crypto: losing the trust?

tartalomjegyzék

NÉHÁNY, AZ ÖRÖKZÖLD PROBLÉMÁK KÖZÜL

- kapcsolattartás ügyfeleinkkel az interneten keresztül
- advanced persistent threats
  (rendszerünkben tartósan jelenlévő veszélyes tényező(k))
- biztonságtudatosság
- pénzintézetek: PCI DSS (kapcsolatos a kiszervezéssel is)

table of contents

SOME OF THE EVERGREEN PROBLEMS

- customer relations through the internet
- advanced persistent threats
- security consciousness
- financial institutions: PCI DSS (related to the outsource, too)

tartalomjegyzék

A MINDENNAPI GYAKORLATBAN MÁR BEVÁLT MEGOLDÁSI MÓDSZERTANOM

- intézményi kormányzás, informatikai kormányzás

➔

- az intézményi-
  - stratégia és
  - biztonság kölcsönös kapcsolata
- kiterjesztett alapfogalmak
  - az intézményi működés alappillérei:
    - szervezet, szabályozás, és technika
  - az intézményi stratégia és biztonság kölcsönös kapcsolata alapján:
    - működési cél
    - elérését támogatja: működési tevékenység
  - az erőforrások kiváló kezelését jellemző kritériumok

- kritérium történet
- a célok ("control objective") - intézkedések ("control measure") összefüggése

table of contents

MY PROBLEM MANAGEMENT METHODOLOGY HAVING BEEN PROVED ALREADY IN THE EVERYDAY PRACTICE

- corporate governance, IT governance

➔

- the mutual relation between corporate-
  - strategy
  - security
- extended basic terms
  - the basic pillars of institutional operation:
    - organization, regulation and technics
  - based on the mutual connection between corporate strategy and security
    - operational objective
    - contributes to its fulfillment: operational activity
  - operational excellence criteria

- the history of the criteria
- the relation between the goals (control objectives) / activities (control measures)

tartalomjegyzék

KOCKÁZAT

- az intézmény stratégiai kockázata
  - stratégia ➔ egy hasznos kockázatdefiníció, és következményei
  - egy lehetséges kockázatkezelési ciklus fő lépései

PÉLDA MÓDSZERTANOM ALKALMAZÁSÁRA

- működési célok, működési tevékenységek, és a működési alappillérek a GDPR-nek való megfelelésben

IRODALOM

- módszertanok, szabványok, irányelvek és más hasznos tanács lelőhelye
- egy lehetséges best practice lista - választott források

(who am I)

table of contents

RISK

- strategic corporate risk
  - strategy ➔ a useful risk definition, and its consequences
  - a possible risk management cycle - phases

EXAMPLE TO MY METHODOLOGY

- operational objectives, operational activities and pillars of operation in the GDPR compliance

REFERENCES

- a chosen list of best practice sources
- where to find: methodologies, standards, guidelines and other advice

(who am I)

NÉHÁNY, AZ ÖRÖKZÖLD PROBLÉMÁK KÖZÜL

SOME OF THE "CURRENT" PROBLEMS

Frost & Sullivan - global economic issues

" Virtually all companies today are going through a cycle of disruption, collapse and transformation. Some companies are actively working on strategies to overcome the challenges of disruption while others are simply unaware."

https://ww2.frost.com/about/

20th Sept. 2018

some of the current issues in their market research reports:

.

- The Emerging Threat Profiles, Defence Cooperation, Spending and Industry Evolution Shape the European Security Strategies:
  - slow recovery of the European economy
  - Cyprus, Italy, Greece, Spain, Portugal, and Ireland needs further nsupport
  - Brexit
  - NATO, US pressure on defence spending

➜ additional pressure on defense spending

https://www.reportbuyer.com/product/5567620/an-overview-of-european-national-defence-strategies-2018.html

let's continue with other issues, and with the question: who will handle them? **./.**

threats (a reformulation of those in the study)

according to the Frost & Sullivan

- The 2017 Global Information Security Workforce Study
  © 2017 Frost & Sullivan

staff to solve problems like these are needed:

- hacking
  - stealing identification
  - DDOS attacks
  - and other attacks exploiting the errors of the IT operations
- malware
  - virus
  - ransomware
  - exploitation of the gullible customers
    probably no longer lies the old chief of tribe
    under an oak-tree buried with valuable treasures

- social engineering - I am John, HelpDesk, tell me your password

emphasized in the Frost & Sullivan study: the present head-hunting HR problems

the problems of the head-hunters in **finding staff to handle the threats:**

- "qualified personnel difficult to find
- security workers difficult to retain
- requirements not understood by leadership
- business conditions can't support additional personnel
- no clear information security career path" (quoted from the study)

towards solution:

- "Clearly, new recruitment practices are needed "
- increase the HR staff
- attract young people
- attract women
- improve skills

  my personal opinion: this is the key!

I do not see:

- lack of interest

I do see:

- improper education + its improper regulation ➔ its results you can see

A GDPR-ből következő alapvető változások az EU adatvédelmében (2016 / 679 EU)

- a személyes adatok beszerzéséhez való ***beleegyezés*** követelményeinek szigorítása
- a beegyező korát ***13-ról 16-ra emeli***
- köteles az adatgyűjtő az adatot ***törölni,*** ha a gyűjtés oka megszűnik
- köteles az adatgyűjtő az adatot ***törölni,*** ha az érintett a beleegyezést visszavonja
- a vállalatok kötelessége, hogy, ha értesülnek, adatvédelmi incidensben érintettek, ehhez képest ***72 órán belül értesítsék*** az EU hatóságait
- a GDPR-rel kapcsolatos panaszok felügyeletére és kezelésére nemzeti hivatal létrehozása.
- adatvédelmi felelőst kell kinevezniök azoknak a vállalatoknak, amelyek vagy jelentős mennyiségű érzékeny adatot kezelnek, vagy sok ügyfelük viselkedését monitorozzák
- ***a bírság korlátja 20m €,*** vagy a vállalat ***bevételének 4%-a***

mik ennek a vonzatai számítástechnikai rendszerünk kezelésében?

Key changes to EU data protection introduced by the GDPR (2016 / 679 EU)

- More rigorous requirements for obtaining ***consent*** for collecting personal data.
- Raising the age of consent for collecting an individual's data from 13 to 16 years old.
- Requiring a company to ***delete data if*** it is no longer used for the purpose it was collected.
- Requiring a company to ***delete data if*** the individual revokes consent for the company to hold the data.
- Requiring companies to ***notify*** the EU government of data breaches in ***72 hours*** of learning about the breach.
- Establishing a single national office for monitoring and handling complaints brought under the GDPR.
- Firms handling significant amounts of sensitive data or monitoring the behaviour of many consumers will be required to appoint a data protection officer.
- ***Fines up to € 20m or 4%*** of a company's global revenue for its non-compliance.

what are the consequences of these in the corporate computer system management?

CURRENT PROBLEMS in systems development: "new" methodologies

DevOps:

- integrates the operations side of software deployment into the development itself
- combines the concepts of
  - agile development,
  - agile infrastructure,
  - flexible operations

  in order to enable rapid and continuous releases

- goals (as usual)
  - improve business
  - meet market requirements
  - efficiency
  - resilience in adapting to users' requirements + in operations ?
  - to enable rapid and continuous releases and ongoing improvement in IT value creation

information on DevOps see e.g.: ISACA Knowedge Center / DevOps Series White paper
contributing: 2 columns of **Expert Reviewers** (in COBIT 5 we were of some pages)

CURRENT PROBLEMS in systems development: "new" methodologies

DevOps:

at the integration

➜ the separation (segregation) of duties principle can, and IS TO BE kept

- requirements for the introduction of DevOps:
  - cultural change
  - improve communication towards a "bridge" between development - operations
  - apply agile principles to every phases of the systems development life cycle
  - practical advice (of ISACA)
    - use CMMI or ! COBIT 5

see: ISACA Knowedge Center / DevOps Series White paper

- what comes to one's mind:
  - everything is agile (development, infrastructure) and operations are flexible ➜
  - immutable infrastructures

CURRENT PROBLEMS in systems development: "new" methodologies

DevOps / immutable

immutable servers:

- can not be changed, once set up, they are set
- in the case of ANY change requirement, the server is to be taken out, and a new one is put in
- should a server fail, we have to roll back to the previous one

immutable servers in cloud environment:

- everything is done once for the master image, and then refresh the server population as needed

➜

- core security functions can be automated ➜ unnecessary
  - patching
  - updating thousands of servers
- statements of the immutable fans:
  - stronger security
  - stronger compliance
  - saving of administration time

CURRENT PROBLEMS in systems development: new environmental conditions

methodological requirements pre DevOps

- **[** mutual relations between: strategy, governance, risk management, security **]**
- define success factors
- identify expectable benefits - is the (considerable) effort worth at all?
- identify training requirements
  - for IT
  - **&** the business area

to the ***success factors*** belong:

- according to ISACA:
  - collaboration across disciplines
  - cloud
  - virtualization
  - repeatable processes [see ! CMM] ➔ rigor, discipline; I think: documentation
  - version control
  - configuration management
  - [above all these:] culture

CURRENT PROBLEMS - issues in financial institutions - PSD2

these duties of the banks were accepted by the EU authorities

the no problem part: the security requirements

- regular risk & vulnerability management
- improving the quality of IT operations
  - operational security, e.g. authentication, encryption, etc.
- improving the quality of IT infrastructure
- business continuity management
- monitoring
- incident reporting (already regular to the Hungarian National Bank)
- audit, etc.

but

CURRENT PROBLEMS - issues in financial institutions - PSD2

disadvantages in relations with different service providers:

AISPs - Account information service providers

- are subject ***only to registration instead of authorisation***
- have many exemptions, e.g.
  - requirements related to AML,
  - to statutory audits,
- etc.

see: EBA/GL/2017/09 11/07/2017 final report

TPP (third-party payment service providers) ➔➔ Banks
experts' opinion in 2017 March:

customers' - TPP - bank relation:
does not matter, who made the mistake,
it is the risk of the bank, TPP has the advantage

CURRENT PROBLEMS - issues in financial institutions - PSD2

TPP ➔➔ Banks examples:

- if the customer complains, then the bank has to credit ***immediately*** the questioned amount onto the customer's account,
- and ***only afterwards*** can the ***bank begin proving***, it was not a mistake of the bank
- the bank is the one, that ***has to notify the TPP***, that the latter has to commence an investigation to prove its faultlessness
- the way of notification - investigation - result processing is not detailed

(I wonder if the TPPs will admit any fault)

- should the TPP admit its mistake, then it is obliged to pay back the money of the bank

(what if it does not?)

- should the customer be mistaken, then the bank has to find a way to get its money back
- the bank may be obliged to compensate even the TPP

solution:

- to prove, which organization did, what:

  offer app as a connection point

pénzintézeti kurrens problémák - kripto - bizalomvesztés?

- bank:
  - ismert: az ügyfél
  - titok: az egyenleg
- crypto:
  - a vevőt egy privát kulcs "jelképezi"
  - az egyenleget mindenki láthatja, sőt, látnia kell

ez az átláthatóság biztosítja, ha biztosítja, hogy megvan a pénzünk

  - alap: blokklánc (lényegében gráfszerű, a szögpontokban vagyonok, és ...)

- az adat valódiságának elfogadása az ügyféltől függ, hiszi-e

- EU: habozás és zűrzavar
  szabályozni, vagy nem szabályozni, ez itt a kérdés
- vannak tervek a szabályozásra, kell is, névtelenség → pénzmosás, terrorizmus, stb.

egész EU-t árfogó blockchain adatbázis?

- megbízhatóan kell szabályozni az adat, és a tranzakciók környezetét

https://www.coindesk.com

CURRENT PROBLEMS - issues in financial institutions - crypto - losing he trust?

- banks:
  - the customer is known
  - the balance is secret
- crypto:
  - the customer is "represented by" a private key
  - everybody can see the balance

this transparency is believed to ensure the existence of this property

  - base: blockchain more-or-less graph-like, info on wealts in the nodes, and ...)

- acceptance of the data validity: depends on the given user's taste

- EU: hesitation and disturbance
  to rule, or not to rule - that is the question
- plans to regulate, because of anonymity ➔ money laundering, terrorists, etc

EU-wide blockchain?

- a reliable, transparent and EU law compliant "data and transactional environment."

https://www.coindesk.com/european-commission-to-assess-potential-of-eu-wide-blockchain-infrastructure/

(URLs: February 2018).

CURRENT PROBLEMS - issues in financial institutions - crypto

USA: SEC against, while NYSE for

- Public Statement of the SEC Chairman, Jay Clayton,
  11 Dec. 2017:

  "A number of concerns have been raised regarding the cryptocurrency and ICO markets, including that, as they are currently operating, there is substantially less investor protection than in our traditional securities markets, with correspondingly greater opportunities for fraud and manipulation."

  https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11
  (URL: February 2018)

💣 *but:*

- New York Stock Exchange launches bitcoin pricing index NYXBT
  https://bitcoinmagazine.com/articles/new-york-stock-exchange-launches-bitcoin-pricing-index-nyxbt-1432068688/ (URL: February 2018)

CURRENT PROBLEMS - issues in financial institutions - crypto

the science fiction based on blockchain:

- as everything will have a digital "trace"
- everything -
  intangible property, agreements, ...
  will be stored in such a way, that everybody can see it
- integrity + confidentiality will be assured by digital signatures [integrity: hash]
- no lawyers (???)
- no bookkeepers
- etc.

will be needed

💣 *but:*

- lots of hackers', stealing, etc. frightening stories
- generation of this money: crypto miners

- anyway: a general, basic change can not be introduced too fast

technical base: the blockchain, a special "database" structure

- what is blockchain?
  distributed ledger for recording transactions
  public: e.g. Bitcoin, Ethereum, private: e.g. Ripple

- the basic features
  the followings are quoted from:
  https://hbr.org/2017/01/the-truth-about-blockchain?referral=03758&cm_vc=rr_item_page.top_right
  Harward Business Review (URL: February 2018)

  - "Distributed Database

    Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary."

EVERGREEN PROBLEMS

CUSTOMER RELATIONS THROUGH THE INTERNET
CUSTOMERS' INTERFACE REQUIREMENTS AND ADVICE

- contribute to + try to preserve customers' trust
  - discourage trolls
  - stop misinformation
  - certification possibilities
  - + ∞ possibilities

- 2-factor authentication
  - 3rd party
  - in Hungary: password in SMS

- "about this account"-type access attempts:
  - verification & !
  - logging

- of course: secure platform for communication with the customers
  - e.g. website

EVERGREEN PROBLEMS

ADVANCED PERSISTENT THREATS

my favourite old definition:

- *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*

from year to year new definition, then . / .

EVERGREEN PROBLEMS

ADVANCED PERSISTENT THREATS

NIST Releases

Draft NIST Special Publication 800-160 Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems

March 21, 2018

https://csrc.nist.gov/News/2018/draft-sp-800-160-vol-2-released

(21 Sept. 2018)

- APTs "have the capability
  - to breach our critical systems,
  - establish a presence within those systems (often undetected), and
  - inflict immediate and long-term damage to the economic and national security interests of the Nation."

my personal opinion:
"Nation" can be substituted by "institution"

EVERGREEN PROBLEMS

- ISACA / ADVANCED PERSISTENT THREATS:

  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

- The Highest Risk to Enterprises From an APT Attack
  [from strategic point of view the most important risks]:

  - Reputation Damage
  - Financial Loss (Tangible)
  - Contractual Breach or
  - [other] Legal Issues
  - Loss of Personal Information
  - Loss of Intellectual Property
  - Loss of Availability

EVERGREEN PROBLEMS

security consciousness

- Twitter: 1.4 million people interacted with Russian trolls during 2016 presidential campaign - January 31, 2018 - https://techcrunch.com

  bots promote fake advertisements
  Russian bot activity in the Brexit referendum in 2016?
  150 million people contacted on Face by troll accounts
  https://techcrunch.com

  bot: "*software* application that runs automated tasks (scripts) over the Internet. Typically, *bots* perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone"
  https://en.wikipedia.org/wiki/Internet_bot

- *another use of the bots:*

  the crypto

financial institutions: PCI DSS - related to the outsource, too

- PCI DSS: Payment Card Industry Data Security Standard

common data security requirements by the

PCI Security Standards Council

- Visa
- Mastercard ? 1st?
- American Express
- Discover: DFS Services LLC (100% US-based customer service)
- JCB: credit card, but not a network, US-based service

responsibilities of the actors in the payment card industry:

security of the cardholder data in

- processing
- transmitting
- storing

PCI Security Standards Council
helps with "specifications, tools, measurements and support resources"

- https://www.pcisecuritystandards.org/

"Who We Serve

- We serve those who work with and are associated with payment cards. This includes: merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers who create and operate the global infrastructure for processing payments.

What We Do

- There are two priorities for our work:
  - Helping merchants and financial institutions understand and implement standards for security policies, technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data.
  - Helping vendors understand and implement standards for creating secure payment solutions."

PCI DSS

- the actors:
  - cardholder
  - merchant
  - service provider - qualification

- organizations, who can / could improve the situation by regulations:
  - international organizations with regulational power e.g.
    - EU organizations, e.g. EBA - European Banking Association
  - government administration offices
  - financial institutions

- [means of qualification:]
  - PCI DSS Self-Assessment Questionnaire - SAQ

PCI DSS and the outsource

on *some* of the different, sophisticated qualifications:

- SAQ A
  - Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced
    - to validated 3rd parties - at the merchant : only papers

- validated 3rd parties: PCI DSS compliant service providers

  the services can be e.g.:
  - website design
  - different hosting services
  - payment processing

! important: do not mix merchants with service providers

! if the service provider is certified to do a given service,

- then it has an Attestation of Compliance - AoC

A MINDENNAPI GYAKORLATBAN
MÁR BEVÁLT MEGOLDÁSI MÓDSZERTANOM

MY PROBLEM MANAGEMENT METHODOLOGY, HAVING BEEN PROVED ALREADY IN THE EVERYDAY PRACTICE

THE SOLUTION IS THE STRATEGIC EXCELLENCE: PASSPORT FOR SECURITY TO CORPORATE GOVERNANCE

intézményi kormányzás - governance, informatikai kormányzás - IT governance

Az intézmény kormányzása:

- annak piaci versenyképességét szolgáló irányítása,
  - a technológiai
  - gazdasági
- környezethez
- lehető legjobban alkalmazkodó stratégia alapján, amelynek
  - meghatározása,
  - betartatása, és
  - rendszeres karbantartása
- az első számú vezető felelőssége

  - ez a "hivatalos" definíciók egyfajta javítása és kiterjesztése

az intézmény informatikai kormányzása:

- a sikeres vállalati kormányzás egyik szükséges feltétele

- az IT (részleg + tevékenységek + ...) olyan irányítása,amely
  - a vállalati kormányzást
  - a felső vezetés szándékai szerint szolgálja

az intézményi stratégia és biztonság kölcsönös kapcsolata

the task of the whole staff, management and security included:

- to *support* corporate strategy, by contributing to the strategic goals, by
  - the fulfillment of useful subgoals
  - useful activities

strategic goals can be supported by security goals
security goals are to be justified by strategic goals

corporate governance ↔ security / audit mutual relation

➜ security methodologies, ideas can be used in / extended to support
  - corporate governance
  - excellent corporate operations
  - risk management

(➜ informatikai biztonsági és ellenőrzési módszerek, módszertanok, ötletek kiterjeszthetőek
  - a vállalatirányítás,
  - a vállalati működés,
  - a kockázatkezelés támogatására) ➜ ./.

the mutual relation between corporate strategy and corporate security

➜ érdemes a biztonság / audit alapdefinícióit
stratégiai szintre emelni

azaz:
informatikaiból legyen ➜ működési, intézményi

tehát
legyen:
➜ ellenőrzési célból működési cél;
➜ ellenőrzési intézkedésből működési tevékenység

a hivatalos név control objective / measure
- mármint azokban a módszertanokban,
ahol ezek a fogalmak nem szűntek meg

ISO szabványokban időnként a control objective-k megjelennek,
a COBIT 5-ben már nincs, *így* a COBIT 2019-ben sincs, de reménykedjünk

a useful risk definition, and its consequences
egy hasznos kockázatdefiníció, és következményei

my proved solution:
strategy-based security ↔ supporting strategy by security

risk (impact) ↗ strategic value of the asset * probability of the threatening

➔ weighting the criteria
- according to the current requirements of the strategy
- actually to their importance in the strategy

risk: is to be managed:
according to the strategic importance of the "things"
= assets serving strategy
risk management, based on
business process / organizational units /data / systems classification

➔ easier to introduce important requirements, e.g.:

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

the 3 pillars of operation

3 pillars of operation:

- organizational
- technical
- regulational

organizational pillar elements are, e.g.:

- the whole organizational structure, and its parts

regulational pillar elements are, e.g.:

- the procedural rulebooks, the role-, the job descriptions

but preparing job description is an organizational activity

technical pillar elements are, e.g.:

- all physical, /

infrastructural property assetsthat are necessary to perform operational activities,

- together with the technical conditions, that determine their use.

extended basic terms

extension of the control 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.

Let's define the

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

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

This importance is not a single value
it *has meaning only in comparisons*.

↓

The *more* important goal is *closer* to the given strategic goal.

extended basic terms

extension of the control measure:

- The *operational* activity is 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.

using the elements of the 3 pillars,
to the strategic goals
  lower-level operational objectives & activities
can, and are to be found

then these are more exact
➜ can be more easily be assigned to the staff, than a general task

operational excellence criteria

suggested "subgoals" to the strategic goals
the criteria of excellent governance:

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

asset handling excellence criteria:

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

kritérium történet - the history of the criteria

a vagyontárgy - erőforrás kezelési kritériumok az intézményi kormányzás minőségében

- a vagyontárgyak *kezelésének* kiválóságát jellemzik

ez a 3 kritérium a legrégebbi, és a legismertebb:

evergreen - örökzöld CCTA, BSI 7799, ISO 177999, ISO 27001,2

ISACA CISA Review Manual, COBIT

CCTA - Central Computer and Telecommunications Agency

BSI - British Standards Institution

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

a vagyontárgy

- rendelkezésre állása -
  - előre jelezhető mértékben
  - mérhető mértékben
- integritása,
- bizalmassága

Hf.: miért pont ezek a legrégebbiek az ISACA+COSO 7-ből, ill. az én 10-emből?

the relation between the goals (objectives) / activities (measures)
a célok - intézkedések összefüggése

nem feltétlenül diszjunkt gráfokból álló erdő,

az egyes fák az erdőben:

a stratégiai célokból kiindulva (gyökerek, vagy végpontok - ízlés kérdése)

↓

- az eseket ***támogató***, egyre gyakorlatibb célok,
  illetve

- egyre gyakorlatibb intézkedések

amelyek ***hozzájárulnak*** legalább egy magasabb szintű, akár stratégiai cél teljesüléséhez

↓

a kiválósági kritériumok bármelyik szinten alkalmazhatóak részcélnak

a *stratégiai,*
ráadásul intézményi stratégiai kockázat definíció célja:

☺ az intézményi *stratégiai* célok szolgálata
☺ proaktív megközelítéssel, a szokásos defenzív helyett

➔

the reason behind our definition of *strategic*, and, what is more, strategic *corporate* risk:

☺ the support of the *strategic corporate goals*
by
☺ a proactive approach, instead of the usual defensive one

➔

az intézmény stratégiai kockázata

stratégia - stratégiai célok
ezeket a vezetőség értékelése alapján osztályozzuk
↓

üzleti folyamatok - üzleti célok
! osztályozni a stratégiában betöltött szerepük értékelése szerint
↓

üzleti célok ➜ ... ➜ működési kiválósági célok /
működési intézkedések ➜ ...

➜ teendő:

- folyamat - szervezet - adat, stb. mátrixok
  (egy hasznos segédlet: kérdőívek)
- ahogy a Business Process Reengineering !

ld.: kockázatbecslés / felmérés fázis !

the strategic corporate risk

strategy - strategic goals
these goals are to be classified
according to the evaluation of the management

↓

business processes - business goals
these are to be classified according to their strategic role

↓

- business goals → … → operational excellence goals /
operational activities → …

→ to do:

- process - organization - data, etc. matrices
(useful accessory: questionnaires)
- just as in Business Process Reengineering !

see: risk assessment / overview - survey !

a useful risk definition, and its consequences
egy hasznos kockázatdefiníció, és következményei

my proved solution:
strategy-based security ↔ supporting strategy by security

risk (impact) ↗ strategic value of the asset * probability of the threatening

➔ weighting the criteria
- according to the current requirements of the strategy
- actually to their importance in the strategy

risk: is to be managed:
according to the strategic importance of the "things"
= assets serving strategy
risk management, based on
business process / organizational units /data / systems classification

➔ easier to introduce important requirements, e.g.:

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

tehát:
a kockázat ≠ bármiféle érték * valamilyen valószínűség - a népszerű buzzword
(a dimenziók amúgyse stimmelnének)

és egyáltalán: hogy lehetünk ebben ennyire biztosak?!?

sajnos, csak 

azaz csak "arányosság" az, amit állíthatunk

thus:
risk ≠
any kind of value *
any kind of probability, and especially not any kind of likelihood

- as the popular buzzword says
(the dimensions would not match, anyway)

anyway: how can we be that sure?!?

unfortunately, only 

that is, only "proportionality" can be stated

az intézmény stratégiai kockázata

az intézmény stratégiai kockázatának definíciója legyen:

- egy olyan, *skálázható* érték, amelyet
- egy adott intézményi emberi / tárgyi *erőforráshoz rendelünk*, és amely
- egyenesen arányos
  - az erőforrás stratégiai / üzleti jelentőségével / értékével
  - annak valószínűségével, hogy
    - bekövetkezik egy olyan esemény, amely veszélyezteti azt, hogy az erőforrás az üzleti folyamat rendelkezésére álljon, mégpedig
    - az előírt mértékben

      (ilyenkor lehet %-ozni)
  - az erőforrás (a vizsgálat időpontjában feltárt / feltárható) sérülékenysége mértékével

! ∃ az erőforrás fontossága / értéke szerinti karbantartás, és egyéb, az aránypárt (↗) megfordító megfontolások

the strategic corporate risk

let's define the strategic corporate risk as:

- such a *scalable* value, that
- is assigned to a given corporate human / material resource, that is
- directly proportional to its
  - strategic / business importance / value
  - to the probability of the
    - occurrence of an event, endangering the availability of the resource for the business process,
    - according to the prescribed measure

    (now the % might be of interest)
  - the degree of the vulnerability of the resource (observed / assessed at the time of the assessment)

! ∃ maintenance depending on the importance / value of the resource, and other considerations, that might result in turning the relation (↯) upside down

egy lehetséges kockázatkezelési ciklus fő lépései

- a vezetés, és az üzleti szakterület elkötelezettségének biztosítása
  - egyébként reménytelen

- módszertan:
  - kiválasztjuk az adott helyzetre alkalmas részeket különféle best practice-kből
  - rászabjuk az adott helyzetre, és
  - kialakítjuk a kiinduló verziót, majd ezt
  - folyamatosan fejlesztjük, a
    - környezeti, és a
    - belső változások szerint

a *possible* risk management cycle - phases

- ensure management & business commitment
  - otherwise hopeless

- methodology:
  - pick the appropriate parts of the many best practice source
  - tailor them to the given situation
  - develop a starting version
  - develop it further continuously, according to the change of
    - environment
    - inside situation

egy lehetséges kockázatkezelési ciklus fő lépései

- előkészítés:

  a sorrend (/1, /2, /3) az adott helyzetnek megfelelően,

  lehet első ciklus, vagy ismételt

  ne spóroljunk a munkával, mindjárt jön a következő:

  az adatszerkezeteket eleve eszerint kell felállítani

/1? Adatbázisok kialakítása, aztán folyamatos fejlesztése, pl.:

- azonosítani: stratégiai célok ➔ fő üzleti folyamatok ➔ ezek fő céljai - ld. IBM BPR
- a kezelendő (ld. a risk aránypárjában a "fontosság"-ot)

  emberi / tárgyi erőforrások azonosítása
- a fontos infrastruktúrális elemek leltára

+ ! e leltár update-jének megszervezése

- etc.

/2? a vizsgálandó célterület kiválasztása, definiálása

/3? az épp alkalmazandó irányelvek kialakítása / felülvizsgálat

a *possible* risk management cycle - phases

- preliminaries:

  the ordering (/1, /2, /3) depends on the current situation; 1st cycle or repeated

  do not take it simple, defining the data structures do not forget:

  to prepare for the next task, coming soon

/1? databases: initialization, then continuous development, e.g..:

- identify: strategic goals ➜ main business processes ➜ itheir most important goals

  see: BPR (e.g. IBM)

- identify the human / material resources to be managed

  (see the part of the risk relation, using the "importance" of the subject)

- inventory of the important infrastructural elements

+ ! provide for its update in case of need

- etc.

/2? choose the area ➜ vulnerabilities, etc., to be currently investigated

/3? identify the current appropriate basic principles / update them

egy lehetséges kockázatkezelési ciklus fő lépései

- kockázatbecslés
  - ciklus ismétlésnél

    az információk felújítása:

    ld. előkészítés lépés / /1, /3,

    a kiválasztott célterület figyelembe vételével
  - a védelmi igények meghatározása

    ⊃ **!** sérülékenységek
  - összefüggések meghatározása, azaz pl.
    - különféle mátrixokba rendezése
      - másik dimenzió: pl. alk. rendszerek, szervezeti egységek, stb.

a vállalati stratégia szerepe, haszna itt, a kockázatbecslési fázisban

- az erőforrások / vagyonelemek (pl. infrastrukturális elemek) osztályozása,
- majd ellenőrző szerepe a kockázatkezelési ciklus újraindításakor

ld. pl., üzletmenet folytonosság **!**

a *possible* risk management cycle - phases

- risk assessment
  - repeated cycle

    info update:

    see preliminaries: step /1, /3,

    taking the chosen present scope into consideration
  - identify the defense requirements

    ⊃ ! vulnerabilities
  - identify relations using, e.g. by:
    - ordering them into different matrices
      - other dimensions e.g.: appl. systems, org. units, etc.

role & importance of corporate strategy in this risk assessment phase

- classification of the resources / property assets (e.g. infrastr. elements),
- then: strategy-based check at reinitializing the risk management cycle

see e.g., business continuity planning !

egy lehetséges kockázatkezelési ciklus fő lépései

- védelmi lehetőségek *keresése*
  - támadni könnyebb:

  infrastruktúrális, fizikai, emberi, stb. tényezők
    - feltárása
    - rendszerezése
    - felkészítése
    - használható összefüggések meghatározása:

      (vigyáznom kell, hogy kerüljem a határozott névelőket):
      - az igények ≠ szükségletek,
      - veszélyeztetett ≠ elemek,
      - veszélyek ≠ sérülékenységek,
      - védelmi lehetőségek

      egymáshoz rendelése

sose keverjük a "szükségeset" az "elégségessel" **!**

a *possible* risk management cycle - phases

- *looking for* defense measures
  - attack is easier:

    infrastructural, physical, human, etc. considerations
    - identification
    - ordering
    - turning them to working state

    - identifying usable relations between

      (I keep checking myself to avoid definite articles):
      - requirements ≠ needs,
      - endangered ≠ vulnerable elements,
      - dangers ≠ threats,
      - ***possible*** ← see the difference above - defense measures

never mix "necessary" with "sufficient" and vice versa **!**

egy lehetséges kockázatkezelési ciklus fő lépései

- az eredményül kapott biztonsági intézkedési rendszer dokumentumai alapján:
  - a védelmi
  - védelem ellenőrzési
  - védelmi rendszer auditálási
  - feladatok pontos meghatározása
  - a feladatokra megoldási terv készítése, és
  - ahol kell: kockázat elfogadási nyilatkozat(ok) felvétele

a *possible* risk management cycle - phases

- based on the documentation of the resulting security arrangements:
  - giving an exact definition of the tasks related to
    - defense
    - checking of defense
    - auditing of defense system
  - solution planning together with
  - risk acceptance declaration(s), if necessary

egy lehetséges kockázatkezelési ciklus fő lépései

- az eredmények értékelése, legalább ezek szerint:
  - az elvárások
  - a javasolt megoldások elfogadhatósága
  - a kockázatbecslésnél alkalmazott szempontok
  - stb.

- szabályzatok készítése ill. módosítása, szükség szerint - nem politika **!**

- a vizsgált célterület következő felülvizsgálatának beütemezése

- oktatás:
  - Az informatikai szolgáltatásoktól való függés mértékének tudatosítása
    a vezetőkben és a munkatársakban,
    veszély / védelem tudatuk fejlesztése

- a módszertan felújítása, az adatbázisok kiegészítése / újak létrehozása a ciklus folyamán szerzett új információk alapján

a *possible* risk management cycle - phases

- minimal set of aspects for evaluating the results:
  - the original requirements
  - the acceptability of the proposed solutions
  - the aspects of the risk assessment
  - etc.

- **!** in case of need preparing / updating the procedural rulebooks ≠ policy

- A vizsgált célterület következő felülvizsgálatának beütemezése

- Oktatás:
  - Az informatikai szolgáltatásoktól való függés mértékének tudatosítása
    a vezetőkben és a munkatársakban,
    veszély / védelem tudatuk fejlesztése

- A módszertan felújítása, az adatbázisok kiegészítése / újak létrehozása a ciklus folyamán szerzett új információk alapján

PÉLDA MÓDSZERTANOM ALKALMAZÁSÁRA

operational objectives, activities and pillars of operation in the GDPR compliance
működési célok és tevékenységek és a működés alappillérei a GDPR megfelelésben

objectives / activities (measures) on the pillars of operational excellence:

- organizational, regulational, technical

organizational operational objectives & activities (measures):

- privacy officer appointed
- identification of related business processes ➔ related organizational units
  - where: customer data, or outsourced support are involved,
  - privacy-sensitive applications, etc.
- join efforts with those dealing with regular obligatory / BCP-related risk assessment

  ➔ business process & business data privacy classification ➔ encryption**?**

regulational operational objectives & activities (measures):

- procedural rulebook
  - handbook-like — policy is not enough **!**
  - rules for the involved organizational units:
    how to handle / what / who / permission / acknowledgment / when

operational objectives, activities and pillars of operation in the GDPR compliance
működési célok és tevékenységek és a működés alappillérei a GDPR megfelelésben

technical control objectives & measures:

- monitor the activities of the staff / access to sensitive systems / data

already at development phase, ***systems analysis knowledge is needed everywhere***

organizational, regulational, and technical control objectives & measures:

- incident handling
- identity management
- access right management / **!** by business processes

joining efforts with PO (Privacy Officer) where needed:

- introduce ***usable*** metrics for qualifying the level of enterprise privacy protection
  (e.g. number of privacy-sensitive applications - join efforts with risk assessment
  % of systems affected by incidents,
  average time to recover, etc.)
- tailoring incident handling to satisfy privacy issues, too
  (special contact rules, communications plans & procedures, etc.)

where to find: methodologies, standards, guidelines and other advice

- ISACA - Information Systems Audit and Control Association
  founded in: 1969 - the knowledge center of ISACA: ISACF
  - ISACA Journal
    időként változik a címe
  - reference manuals: CISA, CISM, stb.

1999-től évente, a CRM 2011 kivételével
*expert reviewer-ként szolgálok, a **Quality Assurance Team**-ben:*
1998 - 2019 CISA Review Technical Information Manual
published yearly; editor: ISACA

a legutóbbi CISA kézikönyv verzió:

CISA Review Manual 27th edition
Updated for 2019 Job Practice

1700 E. Golf Road, Suite 400, Schaumburg IL 30173 USA
ISBN 978-1-60420-767-5

where to find: methodologies, standards, guidelines and other advice

- ISACA - cont'd
  - the ISACA methodology: COBIT - Control OBjectives for IT
    - életciklus:
      COBIT 1998 indulás - 2019 update

      2011-től szolgálok, expert reviewer-ként,
      a COBIT 5-nél: SME: Subject matter Expert csoport
      a COBIT 2019-nél:Expert Reviewer munkacsoport

- [COBIT 5, 2012, Proc.] Enabling Processes COBIT® 5:An ISACA Framework

  ISBN 978-1-60420-239-7

- [COBIT 5, 2012, Gov.] COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT

  ISBN 978-1-60420-237-3

where to find: methodologies, standards, guidelines and other advice

- ISACA - cont'd

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

2019-től, ebben a könyvben az ISACA-nak már ÚJ CÍME VAN:
1700 E. Golf Road Suite 400
Schaumburg, IL 60173, USA

- [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

ISACA bookstore!

where to find: methodologies, standards, guidelines and other advice

- ISO

régiek, de fontosak:

- ISO/IEC TR 133354, First edition, 1996-I 2-15, Information technology - Guidelines

- ISO/IEC 15408 család
  Information technology — Security techniques — Evaluation criteria for IT security -

mai divat:

- 27000-es család
  - 27000 az informatikai biztonsági irányítási rendszer áttekintése és szótár
  - 27001 az informatikai biztonsági irányítási rendszer követelményei
  - 27002 gyakorlati útmutató a biztonsági célokhoz ["controls" ejnye]
  - 27003 az irányítási rendszerhez implementálási útmutató
  - 27005 risk management
  - 27035 biztonsági incidens kezelése - biztonság a másmilyen is!

. / .

where to find: methodologies, standards, guidelines and other advice

- ISO - cont'd

- Guide 73 risk management vocabulary
- 24762 disaster recovery
- 22301 business continuity management
- 38500 IT governance

- [alkalmazásfejlesztés]
  - a jó öreg 12207, és, ami nemrég még mindig részben draft volt:
  - 27034 information security to those specifying, designing and programming or procuring, implementing and using application systems

- stb., stb., ...

egy lehetséges best practice lista - választott források
a chosen list of best practice sources

- NIST: National Institute of Standards and Technology, USA, Department Commerce

  https://www.nist.gov
  - guides,
  - policies,
  - security notices,
  - information quality standards,

  ... from the nanoscale, and neutron research

  to the manufacturing and transportation

létezik: NASA - National Aeronautics and Space Administration:

https://www.nasa.gov

a hackerek időnként összekeverik: NSA, NASA, NIST

NIST - National Institute of Standards and Technology

- **the so-called NIST Cybersecurity Framework**

(Framework for Improving Critical Infastructure Cybersecurity
version 1.0, National Institute of Standards and Technology
February 12, 2014 - kiterjedt magyar felhasználás)

Framework for Improving Critical Infastructure Cybersecurity
version 1.1, National Institute of Standards and Technology
April 16, 2018

NIST - National Institute of Standards and Technology - cont'd

- **NIST Special Publication 800-53**

Revision 4

Security and Privacy Controls for Federal information Systems and Organizations, April 2013

INCLUDES UPDATES AS OF 01-22-2015

U.S. Department of Commerce

National Institute of Standards and Technology

itt figyelembe vették: Federal Information Processing Standard (FIPS) 200

cél volt a FISMA bevezetésének támogatása

FISMA: Federal Information Security Modernization Act of 2014

where to find: methodologies, standards, guidelines and other advice

- Cloud Security Alliance
- consequences of jurisdiction & other obligations
  - USA
    - SOX
  - EU
    - GDPR (2016 / 679) :
  - others
    - PSD2

materials on immutable servers, e.g.

- Security Magazine:

  Nick Piagentini, Senior Solutions Architect, CloudPassage:

  How Immutable Servers Can Revolutionize Cloud Security [as old as]: August 12, 2014

  https://www.securitymagazine.com/authors/2030-nick-piagentini

egy lehetséges best practice lista - választott források
a chosen list of best practice sources

további hasznos anyagok:

- PCI DSS - Payment Card Industry Security Standards
  https://www.pcisecuritystandards.org/security_standards/

- OWASP - Open Web Application Security Project

- OASIS-OPEN - advancing open standards for the information society
  https://www.oasis-open.org/
  ős: SGML (Standard Generalized Markup Language) Open, 1993.

who am I?

CISA – Certified Information Systems Auditor	designator: ISACA
CISM - Certified Information Security Manager	designator: ISACA
CGEIT - Certified in Governance Enterprise IT	designator: ISACA
CISSP - Certified Information Security Professional	designator: ISC2

ISC2: International Information Systems Security Certification Consortium,
founded in the USA, www.isc2.org

ISACA: information Systems Audit and Control Association, founded in the USA
www.isaca.org

- lectures at the Hungarian CISA Review Course from 1999
- 1999-2019 member of the Quality Assurance Team as Expert Reviewer of the CISA Review Technical Information Manual © ISACA
- member of the Subject Matter Expert Team, as Expert Reviewer
  - COBIT 5
  - COBIT 2019