A special case of outsource:
on the security of cloud services
➔ requirements,
➔ tools for solving problems

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

Obuda University
John von Neumann Faculty of Informatics
szenes.katalin@nik.uni-obuda.hu

table of contents

table of contents

- on the one hand - my evergreen transparent on outsource
- what are my minimum requirements to a successful outsource?

- applying my methodology
  - operational excellence criteria
  - pillars of operations
  - my practice-based risk definition

- on the other hand - applying the methodology for the cloud problems
  - the operational excellence criteria and the pillars, serving the strategic goals

- the risks resulted in the specialities of the cloud services
  - **Students' HomeWork** how to contribute to their solution?

table of contents

- some IT security / audit aspects concerning cloud services

- cloud layers in the PCI PCI data security standards

- suggested control measures and objectives in the ISACA COBIT concerning
  - systems security - COBIT 4.1
  - helpdesk and incident amangement - COBIT 4.1
  - operations - ISO

- references
  - pieces from my research (methodology PCUBE-SEC)
  - some best professional practices
    - ISACA, NIST, ISO,
    - Cloud Security Alliance,
    - PCI Security Standards Council

what we hope to gain: advantages - from best professional practice

- ISACA - Information Systems Audit and Control Association
  - more effective, more agile enterprise
  - with more innovative, more competitive services
  - with cheaper operations

"Cloud governance: questions boards of directors need to ask"
© ISACA, 2013

- NIST - USA National Institute of Standards and Technology
  - more optimal server time, automatic store, without human intervention
  - broad range network access
  - resource pooling - service, which is independent from he location
  - and dynamic
  - and flexible
  - and measurable, supervised

NIST Special Publication 800-145 (Draft), 2011

Szenes 5.

a service model based on COBIT 5, and Cloud Security Alliance materials

- COBIT 5:
  Controls and assurance in the cloud: using COBT® 5
  © 2014 ISACA.

- here COBIT 5 quotes:
  Cloud Security Alliance, “Trusted Cloud Reference Architecture,”
  25 February 2013,

https://downloads.cloudsecurityalliance.org/initiatives/tci/TCI_Reference_Architecture_v2.0.

6.

quotation from: Cloud Security Alliance
“Trusted Cloud Reference Architecture” page 11
dimensions of a Cloud Computing Service Delivery and Deployment Model:

- "Cloud Trust:
  - Governance
  - Authentication
  - Auditabiity
  - Identity
  - Authorization
- Cloud Delivery:
  - Platform as a Service
  - Software as a Service
  - Infrastructure as a Service
- Cloud Operation:
  - Public
  - Hybrid
  - Private"

note: the dimension notion comes from me into this context- szk

7.

"Cloud Deployment Model" - COBIT 5 anyag, 4. ábra alapján

- "Private Cloud
  - Operated solely for one enterprise
  - May be managed by the enterprise or a third party
  - May exist on- or off-premise
- Public Cloud
  - Made available to the general public or a large industry group
  - Owned by an organization selling cloud services
- Community Cloud
  - Shared by several enterprises
  - Supports a specific community that has a shared mission or interest
  - May be managed by the enterprises or a third party
  - May reside on- or off-premise
- Hybrid Cloud
  - A combination of two or more cloud deployment models (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability,

    e.g., cloud bursting for load balancing between clouds"

8.

what about security? - releases from https://cloudsecurityalliance.org/

Latest In Research:

- September 25, 2014
  Survey Opportunitiy: Cloud Adoption in the Finance Industry
- September 23, 2014
  New Cloud Security Alliance Survey Reveals
  Emerging International Data Privacy Challenges
- September 18, 2014
  Cloud Security Alliance Releases New Big Data Taxonomy Report

Szenes 9.

on the one hand: my evergreen transparent on outsource

the ultimate truth - my favourite slogan

it does not matter, what we do and how we do it,
- involve partners into tasks
- get rid of human / material resources
- etc.

the responsibility stays inside

cloud is a good example for applying the methodology, as
- outsource is an ***operational*** process

➔
- that should be based on the ***strategic goals*** of the company

Szenes 10.

my minimum requirements to a successful outsource
(see the chapter on outsource in the Information Security Handbook)

- the SLA of the inside / outside service rpovider
  - is defined?
  - is supervised?
  - do the IT services take the goals of the company into account?
  - is capacity and performance monitored?
- cost supervision ≠ decrease costs !

improvement chance, if:

- the human material resources necessary to achieve the goals
  - are exactly identified
  - and are assigned
- to the activities serving the goals

Szenes 11.

now comes an example for applying the methodology
for supporting the evaluation, and even for the identification and implementation of cloud services

- excellence criteria
  supplementing and generalizing the
  ISACA and ISO IT criteria, to the scope of corporate operations
  (ISO - International Standard Organization)
- the pillars of operations
  for supporting the identification and classification of
  measures serving the strategic goals
- a novel risk notion: connected to a given goal and to its achievement

risk (goal) ~ distance (asset, goal)
probability of the attack (asset)
vulnerability (asset)

where asset is a human / material resource, *necessary* to achieve the goaL

Szenes 12.

my excellence criteria

can be used as operational objectives, contributing to strategic goals

↗ operational excellence criteria

↘ asset / resource handling excellence criteria

Szenes 13

operational excellence criteria

- effectivity,
- efficiency,
- compliance,
- reliability,
- strategy-driven goal & operational risk management excellence,
- functionality,
- order

Szenes 14

asset / resource handling excellence criteria

- operational confidentiality
- operational integrity
- operational availability

Szenes 15

order

The operations of an institution goes in so-called "order" - or, in other words, the *order of operations is* called to be *adequate*, if

- top management takes up the responsibility for the well-being of the institution.

This involves,

- from the one hand, the determination of the strategy, aligning it to the market success, and its continuous maintenance, and,
- from the other hand, to have the firm fulfill the strategic goals.

(Quoted from my PhD dissertation.)

16.

order for the IT special case

order
- IT serves the corporate order by the means of its IT-related tools,

thus

the head of the IT area
🛠 provides for the order of at least the followings:
- documentation,
- business continuity planning - operational & IT,
- change management,
- configuration management,
- incident management

🛠 the head has to provide for the 3 pillars for order,
regulational, organizational, technical

Szenes 17

the basic pillars of corporate operations: organization,,regulation, technics

this system of pillars = predefined chest of drawers
- for suggesting activities
- 3 drawers for info collected on goals, activities
- this stored info can be orde4ed according to relevant aspects, e.g. their range and domain, and
- for processing, this info can be retrieved according to these aspects
  this is very handy, e.g.
  - for risk assessment, and then
  - for risk management, too

thus the pillars are good for giving ideas on:
- the range /
- domain of the info to be collected
- the possible useful classifications of the collected info
- why, who, when, using what, who is the supervisor, who gives permission

Szenes 18.

on the other hand...
the other side of the problem

the cloud itself is also a security problem

19.

pillars / excellence criteria for clouds

strategic goal ← business goal

- immediate flexibility - availability according to the needs
- resource centralization - efficiency

seamless processing might be difficult because of the distance
between data sources / receiving points, e.g.
- VOIP telephone service
- frequent movement of small amount of data, e.g. mail, archiving

detective (preventive, corrective control measures, e.g.)
- organizational - appointing:
  - business area responsibe, who escalates problems
  - network administrator, who
- sets quality of service - technical

Szenes

20.

example - pillars / excellence criteria serving strategic goals

strategic **goal**: defense against inside attack

sub**goals** to this strategic goal:

- order
- confidentiality

regulational and then organizational control measure
- set the rules then obey them:

- regulation on separation of duties, then
- regulation on job descriptions, to be composed from role descriptions
- allocate access rights according to the roles

. / .

Szenes 21.

example - pillars / excellence criteria serving strategic goals

regulational, then technical:

- collecting the necessary permissions to the access rights, then
- have them set
- revocation of the unnecessary access rights

the process of access rights management
- and management of other type of users' request ***is to be organized***:

data- / business process owner

requestor ↗ ↘ security area

↖ ↙

the technician, who sets actually the modifications

22.

risks stemming from the specialities of cloud services
[reference: Vohradsky; my Outsource chapter in the Information security handbook]
- HW conribute the solving this problem, using citeria and pillars

- criminals exploit anonimity
- insecure interfaces
  - permit anonim access
  - non-encrypted authentication data, data transfer
- inside the cloud service provider - inside bad-will **! [disorder]**
  - human resource
  - handling security problems, incident management
  - controlling / supervising enterprise business processes (supply chain)

23.

risks stemming from the specialities of cloud services
[reference: Vohradsky; my Outsource chapter in the Information security handbook]
- HW conribute the solving this problem, using citeria and pillars

- one user against the other
- accountability of data handling
  - ownership
  - deletion
  - availability
  - data transfer, encryption
  - operational failures, etc.
- redirection
  - of user
  - of service

  by the means of cheating, - fraud, - exploiting vulnerabilities

24.

risks stemming from the specialities of cloud services
[reference: Vohradsky; my Outsource chapter in the Information security handbook] - HW conribute the solving this problem, using citeria and pillars

- there is almost**?** no transparency - between the participating actors
  - rules to be followed by customers are country-specific
    - e.g. different privacy requirements
  - security measurs, e.g. monitoring, logging
  - order, e.g.: configuration management, see the criteria
- user management
- customers' commitment **?** portability
- business continuity
  - problems arising during service - ***whose*** problems can we handle?
- the problems yielded by customers' activities
  - way of using facilities
  - customers' way of development, testing, etc

but: what if the hypervisor is infected?

25.

IT security / audit aspects for cloud services

↗ customers' requirements, because of e.g.
- the given profession
- strategic goals
- etc.

➔ requirements according to the type of the service - a possible classification: Software, Platform, Infrastructure, Security aaS

↘ according to sensitivity / security domains:
network - data transfer, data storing, service
(Chen, Wang, Wang: On-demand Security Architecture for Cloud Computing Computer, July 2012, IEEE Computer Society, p. 73-78)

to these dimensions my criteria can be assigned,
even weights can be given to the criteria according to business preferences

Szenes

26.

IT security / audit aspects for cloud services
example:
let's construct a matrix according to PCI Data Security Standard

- rows:
  cloud layer
- columns:
  service model
- in the matrix element:
  responsibility due to customer? supplier? both? ***or?***

PCI Security Standards Council:
Standard: PCI Data Security Standard (PCI DSS)
Version: 2.0 Date: February 2013
Author: Cloud Special Interest Group PCI Security Standards Council
Information Supplement: PCI DSS Cloud Computing Guidelines
https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Szenes 27.

Cloud layers: a copy from PCI DSS, ver. 2.0, February, 2013

Layer	Description
Application Program Interface (API) or Graphical User Interface (GUI)	The interface used by the client or their customers to interact with the application. The current most common API is RESTful HTTP or HTTPS. The current most common GUI is an HTTP or HTTPS based Web site.
Application	The actual application being used by one or more clients or their customers.
Solution stack	This is the programming language used to build and deploy applications. Some examples include .NET, Python, Ruby, Perl, etc.
Operating systems (OS)	In a virtualized environment, the OS runs within each VM. Alternatively, if there is no underlying hypervisor present, the operating system runs directly on the storage hardware.
Virtual machine (VM)	The virtual container assigned for client use.
Virtual network infrastructure	For communications within and between virtual machines
Hypervisor	When virtualization is used to manage resources, the hypervisor is responsible for allocating resources to each virtual machine. It may also be leveraged for implementing security.
Processing and memory	The physical hardware that supplies CPU time and physical memory.
Data Storage	The physical hardware used for file storage.
Network	This can be a physical or virtual network. It is responsible for carrying communications between systems and possibly the Internet.
Physical facility	The actual physical building where the cloud systems are located.

28.

proposed control objectives / measures supporting systems security
"DS5 Ensure Systems Security" quoted from ISACA COBIT 4.1

- "DS5.1 Management of IT Security
- DS5.2 IT Security Plan
- DS5.3 Identity Management
- DS5.4 User Account Management
- DS5.5 Security Testing, Surveillance and Monitoring
- DS5.6 Security Incident Definition
- DS5.7 Protection of Security Technology
- DS5.8 Cryptographic Key Management
- DS5.9 Malicious Software Prevention, Detection and Correction
- DS5.10 Network Security
- DS5.11 Exchange of Sensitive Data"

(quoted from:
COBIT ® 4.1 Framework, Management Guidelines, Maturity Models
Copyright © IT Governance Institute®, 2007)

Szenes 29

proposed control objectives / measures supporting systems security
"DS8 Manage Service Desk and Incidents" quoted from ISACA COBIT 4.1

"DS8 Manage Service Desk and Incidents

- DS8.1 Service Desk
- DS8.2 Registration of Customer Queries
- DS8.3 Incident Escalation
- DS8.4 Incident Closure (én: includes recording of resolution steps !)
- DS8.5 Reporting and Trend Analysis"

(quoted from: ***COBIT*** ® 4.1
Framework, Management Guidelines, Maturity Models
Copyright © IT Governance Institute®, 2007)

Szenes 30

proposed control measures and goals - supporting systems security
helpdesk, incident management - COBIT 5

"DSS01.02 **Manage outsourced IT services.**
Manage the operation of outsourced IT services to maintain

- the protection of enterprise information and
- reliability of service delivery."

suggested "activities"

- 1. Ensure that the enterprise's requirements for security of information processes are adhered to in accordance with contracts and SLAs with third parties hosting or providing services.
- 2. Ensure that the enterprise's operational business and IT processing requirements and priorities for service delivery are adhered to in accordance with contracts and SLAs with third parties hosting or providing services.

. / .

Szenes 31

proposed control measures and goals - supporting systems security
helpdesk, incident management - COBIT 5

"DSS01.02 **Manage outsourced IT services.**
suggested "activities" (cont'd)

- 3. Integrate critical internal IT management processes with those of outsourced service providers, covering, e.g., performance and capacity planning, change management, configuration management, service request and incident management, problem management, security management, business continuity, and the monitoring of process performance and reporting.
- 4. Plan for independent audit and assurance of the operational environments of outsourced providers to confirm that agreed-on requirements are being adequately addressed.

(**COBIT** ® 5: Enabling Processes - see references)

Szenes 32

proposed activities and goals to support operations -
International Standard Organization

- International Standard ISO/IEC 27001:
  - **version 2013:**
    - Annex A (normative) Reference control objectives and controls
      - A.14.2.7 Outsourced development:
      - A.15 Supplier relationships
        - A.15.1 Information security in supplier relationships
        - A. 15.2 Supplier service delivery management
  - **in version 2005,** also in Annex A
    - A.10.2 Third party service delivery management
    - A.10.2.1 Service delivery

(ISO standards - see references)

Szenes 33

some of my research & educational references

- on outsource - cloud is - *partially* - a special case
  Szenes, K.: Az informatikai erőforrás-kihelyezés auditálási szempontjai
  Hungarian - Auditing outsourcing of IT resources, Part I., Part II. (2010)
  in: Az Informatikai biztonság kézikönyve - Information Security Handbook
  Verlag Dashöfer, Budapest, ISBN: 963 9313 122

- some of the lots of publications on my methodology:
  Szenes, K.: Serving Strategy by Corporate Governance - Case Study:
  Outsourcing of Operational Activities; Procds. of 17th International
  Business Information Management Association - IBIMA November 14-15,
  2011, Milan, Italy, ed. Khalid S. Soliman, ISBN: 978-0-9821489-6-9

  K. Szenes: Operational Security - Security Based Corporate Governance
  Procds. of IEEE 9th International Conference on Computational Cybernetics
  July 8-10, 2013 Tihany, Hungary @2013 by IEEE

references - some of the best professional practices - ISACA

- COBIT® 4.0 Control Objectives, Management Guidelines, Maturity Models
  Copyright © IT Governance Institute® , 2005, editor: ISACA
- COBIT® 4.1 Framework, Management Guidelines, Maturity Models
  Copyright © IT Governance Institute® , 2007, editor: ISACA
- "Cloud governance: questions boards of directors need to ask"
  © ISACA, 2013
- Controls and assurance in the cloud: using COBT® 5
  © 2014 ISACA.
- COBIT ® 5: Enabling Processes
  Copyright © 2012 ISACA., ISBN 978-1-60420-241-0)

references - some of the best professional practices
NIST, Cloud Security Alliance

- NIST Special Publication 800-145 (Draft), 2011
  W. Jansen, T. Grance: Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology, January, 2011
- Cloud Security Alliance, “Trusted Cloud Reference Architecture,”
  25 February 2013,

https://downloads.cloudsecurityalliance.org/initiatives/tci/TCI_Reference_Architecture_v2.0.

references - some of the best professional practices
PCI Security Standards Council

- ***PCI Security Standards Council:***
  Standard: PCI Data Security Standard (PCI DSS)
  Version: 2.0 Date: February 2013
  Author: Cloud Special Interest Group PCI Security Standards Council
  Information Supplement: PCI DSS Cloud Computing Guidelines
https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

37.

references - some of the best professional practices
ISO - Internal Standards Organization

- International Standard Organization: International Standard ISO/IEC 27001
  First edition 2005-10-15
  International Standard ISO/IEC 27002 First edition 2005-06-15
  Information technology — Security techniques — Code of practice for information security management

present edition: 2013

  - there is a security family here: 27000, 27001, 2, 5
  - - but other numbers also deal with IT security aspectsa 27000-es

38.

references - some of the lots of publications in journals

- Chen, Wang, Wang: On-demand Security Architecture for Cloud Computing
  Computer, July 2012, IEEE Computer Society, p. 73-78

- David Vohradsky: Cloud Risk—10 Principles and a Framework for Assessment
  ISACA Journal Vol. 5, 2012, © 2012, ISACA, editor: ISACA