IT GRC versus ? Enterprise GRC
but: IT GRC is a Basis of Strategic Governance

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

Obuda University

Faculty John von Neumann

Institute Software Technology

szenes.katalin@nik.uni-obuda.hu

contents

1 corporate ***governance*** - IT governance
what are these? and what is their purpose?
2 how to manage corporate governance?
requirements, should we want to buy a supporting tool
3 how to achieve our goals?
- let's start from the requirements of the company!

4 derived requirements - ***compliance***
regulatory bodies, Acts
5 benefit of compliance: the story of "my" internet banks
6 how to manage compliance?
7 compliance example: the benefits of SOX in practice

contents

8 ***risk*** - audit basics - control objective, control measure / procedure

9 success ➔ derived requirements that are the base of risk management

10 a possible risk management processes from my practice

steps from the assessment to the implementation of the necessary measures

then: go to step1 !

11 risk management in USA: what did NIST do with FISMA

12 ***to do***: find key control objectives & measures - where?

- use COBIT to formulate our goals and evaluate our information

13 we have a plus! what is it?

o important duties to do to succeed

o there are things that high performers never let their staff do

contents

corporate governance - IT governance

corporate governance - corporate wellness, market success, growth

➔

- "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"

[CRM] - OECD

corporate governance - IT governance

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.

corporate governance - IT governance

COBIT on IT Governance:

"The need for assurance about the value of IT, the management of IT-related risks and increased requirements for control over information are now understood as key elements of enterprise governance. Value, risk and control constitute the core of IT governance. "

"IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives. "

my private experience shows:

the new interpretation of "IT governance" might be:

IT-*based* management (without IT can we survive?)

corporate governance - IT governance

IT governance is:

- the responsibility of the board of directors and executive mgmt.
- an integral part of the enterprise governance
- leadership + organisational structures + processes

☞

ensure that IT sustains and extends
the strategy & objectives of the organisation

ITGI - IT Governance Institute: Board Briefing on IT Governance
2nd Ed., USA, 2003

how to manage corporate governance?

governance requirements for tools
when buying a tool

see Sing, Lilja article

some of the most important requirements:

business alignment + strategy development support
management of the communications media
decision support data
acquisition & processing

let's see the details!

how to manage corporate governance?

governance requirements for tools - details

business alignment + strategy development support

- assistance to the governance support system (e.g. MIS, DW);
- methods & readiness to moderate strategic planning
- alignment of governance with business objectives

- operational support

  document management

  procedural rulebooks, financial! reports - SOX

  workflow to manage work and progress

how to manage corporate governance?

governance requirements for tools - cont'd

management of the communications media

policy - procedures, guideline, standards

expressing the intentions and commitment of management

control facilities, supervision mechanism for the management such as e.g.

- static: IT tools - dashboard, reporting tools - template & maintenance
- continuous: audit tools
- development, testing, maintenance facilities for these

how to manage corporate governance?

governance requirements for tools - cont'd

decision support data

- acquisition & processing

- express the proposed control measures in an understandable way
- prove their business use
- risk data to justify spending
- cost / benefit info

how to achieve our goals?

let's start from the requirements characteristic to the company

and: what are the consequences of the current economic situation?

now governance is:

- IT-based fight for success
- for continuously improved production and its realization
- in compliance with every "restriction" (law, rule, ...) affecting the institutions

based on a *solid* operation + IT

in order to achieve these -

let's translate the requirements into the terminology of a best practice methodology ISACA, COSO, ISO/IEC

how to achieve our goals?

most generic (control) objective: success

↓ ... drilling down ...

... + operational support, e.g. IT of good quality + ...+ compliance + ...

↓ ... drilling further down ...

information [evaluation quality] criteria ← we'll come back to these

↓ ... drilling further down ...

...

↓ ... drilling further down ...

requirements on the level of the individual infrastructure elements

derived requirements - compliance

where are the compliance requirements to be found?

- o legislative materials
- o special sectoral regulatory enactment
- o in the expressed / implied intentions of the mother company
- o etc.

regulatory bodies:

USA: Congress, SEC, PCAOB, OSHA, ...

Hungary: parliament, government, Supervisory Authority for Financial Institutions, other sectorial level administration

popular examples in the USA: GLB, SOX, HIPAA, ...

derived requirements - compliance

Hungary keeps up quite well:

- Act on Credit Institutions & Financial Enterprises of 1996 CXII
- Data Protection Act of 1992 LXIII.
- 196, 200/2007 government decrees on credit / operational risk
- Data Protection Act of 1992 LXIII.
- Act On The Recording of the Personal Data and Home Address of Citizens 1992 LXVI.

and we have others as well: marketing, digital signature, etc.

derived requirements - compliance

what are these regulatory bodies and acts? - some of them:

- SEC: US Securities and Exchange Commission, founded in 1934!
- PCAOB: US Public Company Accounting Oversight Board (founded: 2002-SOX)
- OSHA: Occupational Safety and Health Administration Office
- NIST: National Institute of Standards - FIPS Publication Series

GLB

The Gramm-Leach Bliley Act 1999 - The Financial Modernization Act of 1999 contains provisions on

- the privacy of financial matters
- the confidentiality of customers' information
- the collection of financial information on customers

derived requirements - compliance

SOX: Sarbanes - Oxley Act of 2002

its predecessors:

the Securities Act of 1933 and the Securities Exchange Act of 1934

there are lots of legends spread by the suppliers

but positive examples can and will be shown on its proper application

HIPAA: Health Insurance Portability and Accountability Act, 1996

regulates healthcare insurance companies and providers

- in order to improve the US health insurance system
- ours is: Title IV: defines rules for protection of patient information

benefits of compliance - "my" i-banks

the story of "my" internet banks:

1 board of the bank wants internet bank

➔

I get budget for the technical information security architecture, safe nw topology

2 the special interest of the year at
Supervisory Authority for Financial Institutions includes internet bank

➔

I get resources to ethical hacking
(and a nice logging feature is sponsored)

note: against customers' weaknesses there is no defense

how to manage compliance?

compliance requirements recommended to the organizations

being well-versed + continuous follow-up
authoritatve collection of the requirements, control measures to be followed
regulatory changes

being able to correlate the requirements of different authorities
e.g. PCI DSS + SOX

being able to track the progress of control measures

reporting according to any kind of requirements to be taken into account

compliance example: the benefits of SOX in the practice

what follows here is:

"Expanding Business Horizons Through IT" - ISACA® Journal front page

+ a practical example to the business value in SOX related IT investments

what is SOX about?

according to suppliers:

- identity management
- activity monitoring

but what does SOX *really* provides?

compliance example: the benefits of SOX in the practice

compared to its predecessors in 1933, 34
multiplication of the penalties - $, length of imprisonment

and !

in internal reporting:

- due diligence
- discipline
- regularity
- CEO and CFO periodically has to sign reports
- auditors shall preserve every note

compliance example: the benefits of SOX in the practice

Spears 2007 Thesis verifies all of these:

10 organizations / 20 persons research shows:

- reduction in risk to financial reporting
- improved internal control measures
- improvements in governance

HOW?

compliance example: the benefits of SOX in the practice

my favourites:

- obligation to **document**

➔ maturity - see SEI CMM and, of course, COBIT

- control measures are aligned to business objectives
- while helping to manage security risk
  to financial reporting.

"functional business users *routinely* contribute
business perspective to IT"

I do think that there is no business - following IT *without* IT security and vice versa

risk - audit basics

basic audit notions:

what is the control objective? how can they be achieved?

using control measures - procedures

official definition of control objective*:*

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 can be taken as:

the minimum requirements needed to control effectively the IT processes.)

risk - audit basics

my *private* interpretation:

generic control objective:
generic best practice top management obj. derived from corporate strategy

IT control objective: IT operation objective derived from generic ctrl. obj. in the form of a statement expressing a desired result. It can be achieved by implementing control measures / procedures concerning IT activities.

management responsibility: to determine the generic control objectives

internal audit responsibility: support the management doing so

IT + information security responsibility: to achieve the objectives

risk - audit basics

the question was:

what is the control objective? how can they be achieved?

the answer:

using control measures - procedures

bad short form: "control"

these are to be 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

derived requirements - risk management

what is the goal?

corporate wellness - market success, growth

the quality of the information

compliance

let's take the fiduciary formulation of the Treadway Commission - COSO :

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

derived requirements - risk management

what do we need to actually achieve all of these?

remember:

to fulfill the control objectives we have: the control measures / procedures

where do these measures act?

- the organisational structures with their operational procedures and practices
- the guidelines and procedural rulebooks - ¬ policy!
- the technical developments and measures

here are the 3 pillars of IT - IT security

a possible risk management process

this is what I use in the real life

- assessment of the situation
- choosing the target of the review
- choice of the appropriate methodology & tools (ideal order)
- determination of the presently *available*
  institutional preconditions for improvement
- determination of the required level
- assessing the difference between the levels
- cost/effectively determining the control measures to be introduced
- implement them
- cycle

a possible risk management process

some details:

assessment of the situation:

- requirements (business, compliance, ...)
- business process / operation / organization / assets relations

choosing the target of the review:

- scope definition
- guidelines definition / revision

choice of the appropriate methodology & tools

- control objectives from the usual sources - for goals

a possible risk management process

details - cont'd

determination of the presently available improvement tools
institutional preconditions for improvement

- corporate IS security infrastructure
- organizational & procedural defense
  e.g. organizational operational rule system
- built – in control measures
- 3rd party agreements
- etc.

a possible risk management process

details - cont'd

determining the necessary control measures + cost / effectivity evaluation
=>

- implementing the control measures
- OR accepting risks in a documented way

implement:

- **documentation**, procedural handbooks, etc., prepare / update these
- organizational (security) measures

scheduling the next review and goto step 1

risk management - USA

risk management in the way of the Information Security Management Act

E-Government Act (Public Law 107-347):

"passed by the 107th Congress and signed into law by the President in December 2002 recognized the ***importance of information security to the economic and national security interests*** of the United States"

its Title III: Federal Information Security Management Act (FISMA):

the federal agencies shall "**develop, document, and implement** an agency-wide **program** to provide information security for the information and information systems that support the **operations and assets of the agency**, including those provided or managed by another agency, contractor, or other source"

http://csrc.nist.gov/groups/SMA/fisma/overview.html

risk management - USA

steps *after* FISMA - NIST Risk Management Framework:

- categorize

the IS based on impact

- select

an initial set of control measures & minimum security requirements

- tailor these

to the risk assessment, to the local conditions

- implement the measures
- assess them
- authorize

IS operations based upon organizational, asset dependent, personal...risks

monitor and assess selected security control measures

to do: find key control objectives & measures

so what we can do is - going back to the drilling down from the top level goal to FIND key control objectives & measures - for the SUCCESSFUL enterprises

➔ for the SUCCESSFUL IT governance

➔ for the COMPLIANT enterprises

1 the control objectives can be derived from the strategy

top: most general control objective: successful institution

🡻

bottom: requirements on the quality of the infrastructural elements

2 using info quality requirements from best practice: COSO, COBIT, ISO / IEC

3 using + !

4 using education

let us formulate our goals

COBIT components - control objectives - will help us:

quality + fiduciary + security

quality: quality + cost + delivery

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

security: availability + confidentiality + integrity

our goal definitions: how to evaluate info

COBIT components - cont.'d

information [evaluation / quality] criteria

- effectiveness
- efficiency
- confidentiality
- integrity
- availability
- compliance
- reliability of Information

+ non-repudiation, accountability, authenticity, QoS (technics), **...**

and what is the + ?

the findings of a 2007 article of Melancon from the IS Control Journal

control measures bringing success:

- change management
- configuration management

(6 years long IT Process Institute Study)

surprise?

what do we need to configuration management?

inventory, asset classification, data classification, data owner / custodian

and what is the + ?

if

NO change management

NO configuration management

➔

NO tracking of

- unauthorized
- unsuccessful configuration and other changes

➔

NO understanding of

- production environment
- past mistakes ...

and what is the + ?

change management control measures
used by the ***high performers*** of the Melancon ITPI study
these are discriminant control measures:

all of the low performers lack them

- to monitor the systems in order to identify unauthorized changes
- to define the consequences of the unauthorized changes

➔ practically:

the change management procedures should be included
into the IS Security Procedural Rulebook
to write a security policy is not enough

and what is the + ?

configuration management control measures
used by the ***high performers*** of the Melancon ITPI study
these are discriminant control measures:

all of the low performers lack them

- to define the configuration management process
  automatization where possible
- track change success (changes that cause no mishaps)
- continuous info on the current state to those who need to know

and what is the + ?

the never let-s

the ***high performers NEVER LET***

- developers make changes in the production systems
- change management process get bureaucratic
- users exceed their role in the change management process

another key control measure: education

every employee should be educated

- at the working places - regularly
- at the schools already

our University Obuda (former College Kando, Budapest Tech)

1998 Introduction to IS Audit

2002 Information Security - at the students' request
+ state exam

now: 3 - term specialization in Information Security

basic requirements of IS:strategy support, ACI, documentation, functionality

to do: find the minimum security requirements

Minimum Security Requirements for Federal Information and Information Systems (FIPS PUB 200, March 2006)

sample - some of my favourites from the little bit more than 17

- configuration management
- contingency planning - this is the BCP / disaster recovery
- audit & accountability
- maintenance - systems,
  - control measures for personnel, tools, mechanisms, techniques
- media protection (protect the info, limit the access)
- systems, communications protection ...

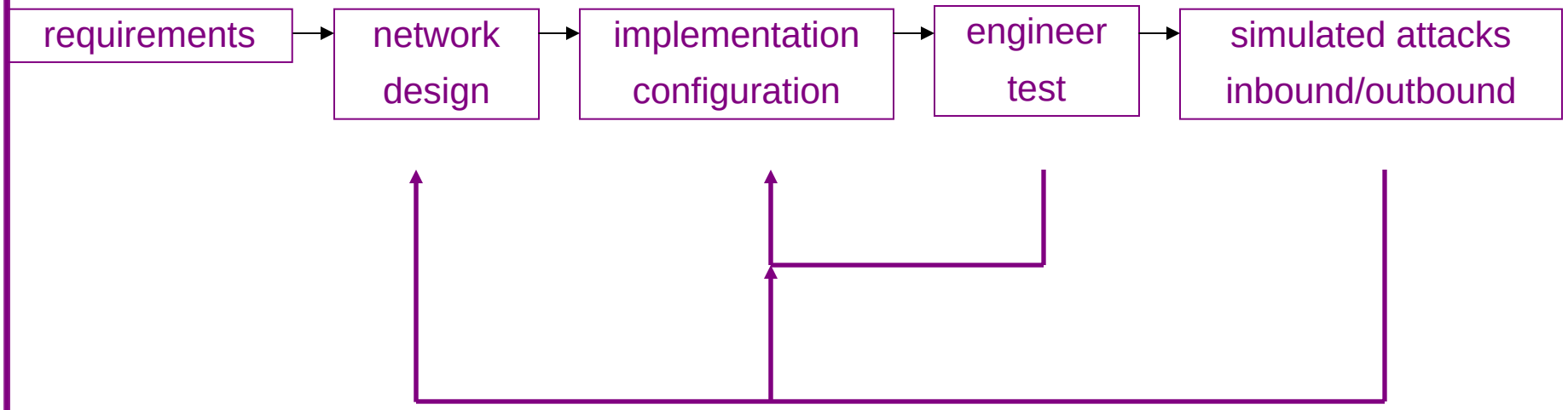
exactly how do we implement proper IT & ! security?

to satisfy all of these control objectives and the risk management requirements
we have the 3 basic pillars of IT - IT security
proper IT and IT security works hand in hand
this one important key of any kind of success

- **organization**
- **rule**
- **technics**

organization - segregation of duties, identity management, etc.
rulebooks - SDLC, BCP, IT BCP, information security rulebook
and what about the technics?

technical example: to do-s when creating secure networks



technical example: tests, simulated attcks

every test should be regular + after every approved ! change

engineer test - the control objectives are to be tested by:

- IT
- information security
- IS audit

specifics e.g.: customers' requirements, incident handling, scalability, QoS, **...**

simulated attacks to test e.g.:

strength of authentication, open ports, unecessary services, state of patching **...**

references

the favourite +

Dwayne Melancon: Security Controls That Work
IS Control Journal, Vol. 4, 2007
pp. 29-32
ITPI - IT Process Institute
http://www.itpi.org/home/default.php

IT Controls Performance Benchmark - the present:
http://www.itpi.org/home/controls_benchmark.php
(12 March, 2010)

references

Anand Singh, David J. Lilja:
Criteria and Methodology for GRC Platform Selection
ISACA® Journal, Vol. 1, 2010
pp. 32-37

Janine L. Spears:
How Has Sarbanes - Oxley Compliance Affected Information Security?
ISACA® Journal, Vol. 6, 2009
pp. 33-36

references

COSO

http://www.coso.org/

The Committee of Sponsoring Organisations of the Treadway Commission - was founded in 1985 to support the National Commission on Fraudulent Financial Reporting.

- "a voluntary private-sector organization"
- "dedicated to guiding executive management and governance entities toward the establishment of more effective, efficient, and ethical business operations on a global basis"
- contributes to the quality of the financial reports by the means of business ethics, effective internal control measures and enterprise governance methods

references

COSO - cont'd

COSO materials support the companies of the stock exchange and their auditors, the SEC, other institutions having regulational duties, educational organizations in the recognition of the specifics of the fraudulent reports

Sponsors of COSO:

- AICPA - American Institute of Certified Public Accountants
- AAA - American Accounting Association
- FEI - Financial Executives International
- IIA - Institute of Internal Auditors
- IMA - Association for Accountants and Financial Professionals in Business

references

CRM 2010 CISA Review Technical Information Manual

editor: Information Systems Audit and Control Association

Rolling Meadows, Illinois, USA, 2009

COBIT Executive Summary

April 1998 2nd Edition

Released by the COBIT Steering Committee and the Information Systems Audit and Control Foundation

COBIT® 3rd Edition, July 2000

Released by the COBIT Steering Committee and the IT Governance Institute™

editor: Information Systems Audit and Control Association - ISACA

references

COBIT - cont'd

***COBIT*® 4.0**
Control Objectives, Management Guidelines, Maturity Models

***COBIT*® 4.1**
Framework, Management Guidelines, Maturity Models

references

ISO 27001 International Standard ISO/IEC 27001 First edition 2005-10-15

Information technology - Security techniques - Information security management systems - Requirements

Reference number: ISO/IEC 27001:2005 (E)

ISO 27002 International Standard ISO/IEC 27002 First edition 2005-06-15

Information technology — Security techniques — Code of practice for information security management

Reference number: ISO/IEC 27002:2005(E)

references

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

European Union Law:
http://eur-lex.europa.eu/en/index.htm
12 March, 2010

Summaries of EU Legislation:
http://europa.eu/legislation_summaries/index_en.htm
12 March, 2010

references

NIST - National Institute of Standards and Technology
FIPS - The Federal Information Processing Standards (FIPS) Publication Series
official series of publications due to
FISMA - Federal Information Security Management Act of 2002

FIPS PUB 200, March 2006
Minimum Security Requirements for Federal Information and Information Systems
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
http://csrc.nist.gov/publications/PubsFIPS.html (12 March, 2002)