Vztah…???
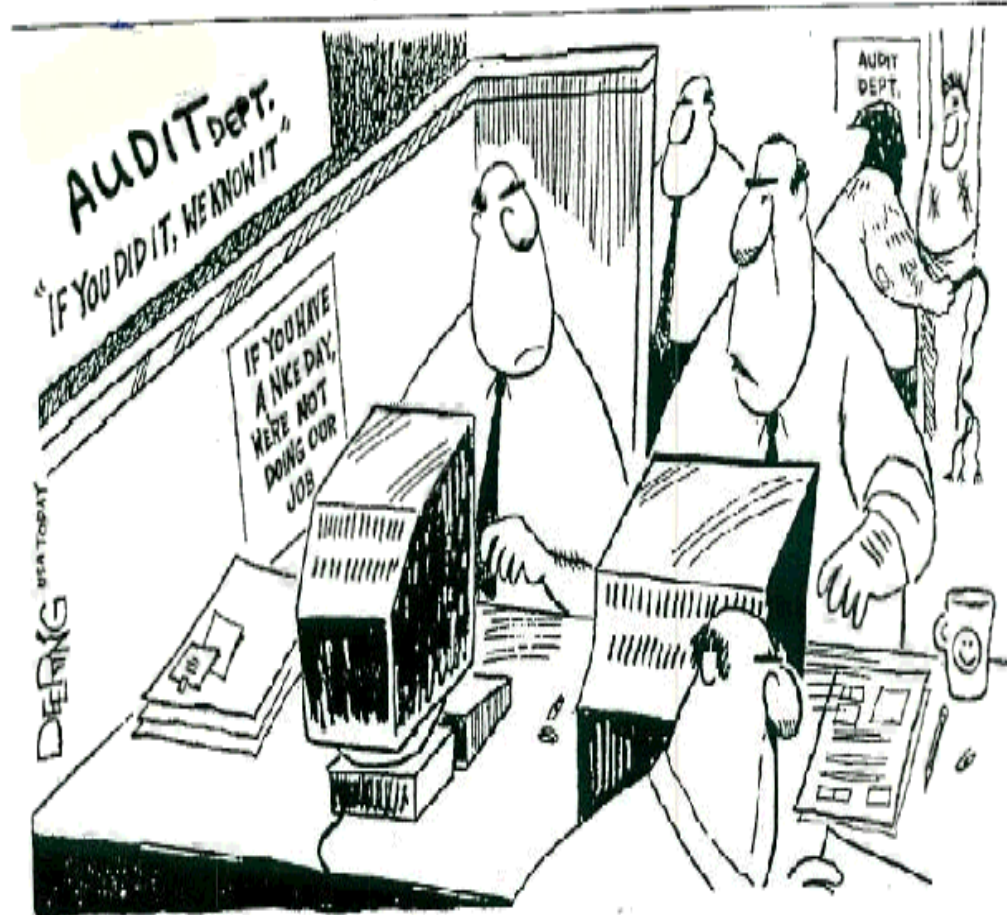
ISACA – organizace profesionálů

Bezpečnost a audit

17.2.2010

Luboš Klečka
lklecka@csas.cz

Obsah

❖ISACA
❖ITGI, Cobit 4.1
❖Strategie ISACA
❖Information Security Governance
❖Rizika

ISACA
Oblasti výzkumu

Information System Audit And Control Association

➢Certifications: IS Audit (CISA®) & Security (CISM™)
➢IS Audit, Control & Security - Specific Environments
➢IS Audit, Control & Security – Tools
➢IS Auditing
➢Net Centric (Intranet/Extranet/Internet) Control & Security
➢IS Security

➢IS Security Management
➢IS Control
➢IT Governance & Business Management
➢eBusiness
➢Telecommunications
➢Project Management
➢Professional Development

IT navazuje, plní , rozvíjí požadavky obchodu
IT podporuje, umožňuje plnit obchodní cíle a maximalizuje přínosy
Zdroje IT jsou využívány efektivně a odpovědně
Rizika IT jsou vhodným a optimálním způsobem řízena

ISACA
server, publikace....

- ❑ COBIT Mapping: Mapping NIST SP800-53 Rev 1 With COBIT4.1
- ❑ COBIT Mapping: Mapping ISO/IEC 17799:2005 With COBIT 4.0
- ❑ COBIT Mapping: Mapping of ITIL V3 With COBIT 4.1
- ❑ COBIT Mapping: Mapping SEI's CMM for Software With COBIT 4.0

- ▪ Windows
- ▪ NT/2000
- ▪ Windows 2003 Server
- ▪ OpenVMS
- ▪ SMF
- ▪ CGI
- ▪ MVS
- ▪ RACF
- ▪ Websphere
- ▪ UNIX
- ▪ Linux

- ▪ Netscape
- ▪ EDI
- ▪ OS/390
- ▪ SYS1.PARMLIB
- ▪ JAVA
- ▪ HP Openview
- ▪ ISA Server
- ▪ SQL Servers
- ▪ Active X
- ▪ Oracle Database
- ▪ AS/400

- ▪ Internet Explorer
- ▪ SAP R/3
- ▪ Novell NetWare
- ▪ Directory Services
- ▪ PeopleSoft
- ▪ Lotus Notes
- ▪ Tivoli TME10
- ▪ Desktop

- ▪ Apple
- ▪ CICS
- ▪ Oracle Financials
- ▪ Windows XP
- ▪ Vista
- ▪ Informix
- ▪ DB2
- ▪ IIS
- ▪ Windows ME
- ▪ Sybase
- ▪ ERP

GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

ISACA® eLibrary

ČESKÁ SPOŘITELNA
Jsme Vám blíž.

ISACA
Klíčová témata

❖Security, Control and Assurance
❖Accounting, finance and Economics
❖Business, Management and Governance
❖Contingency Planning, Disaster Recovery
❖IT
❖Risk Management

ITGI

- – 1998
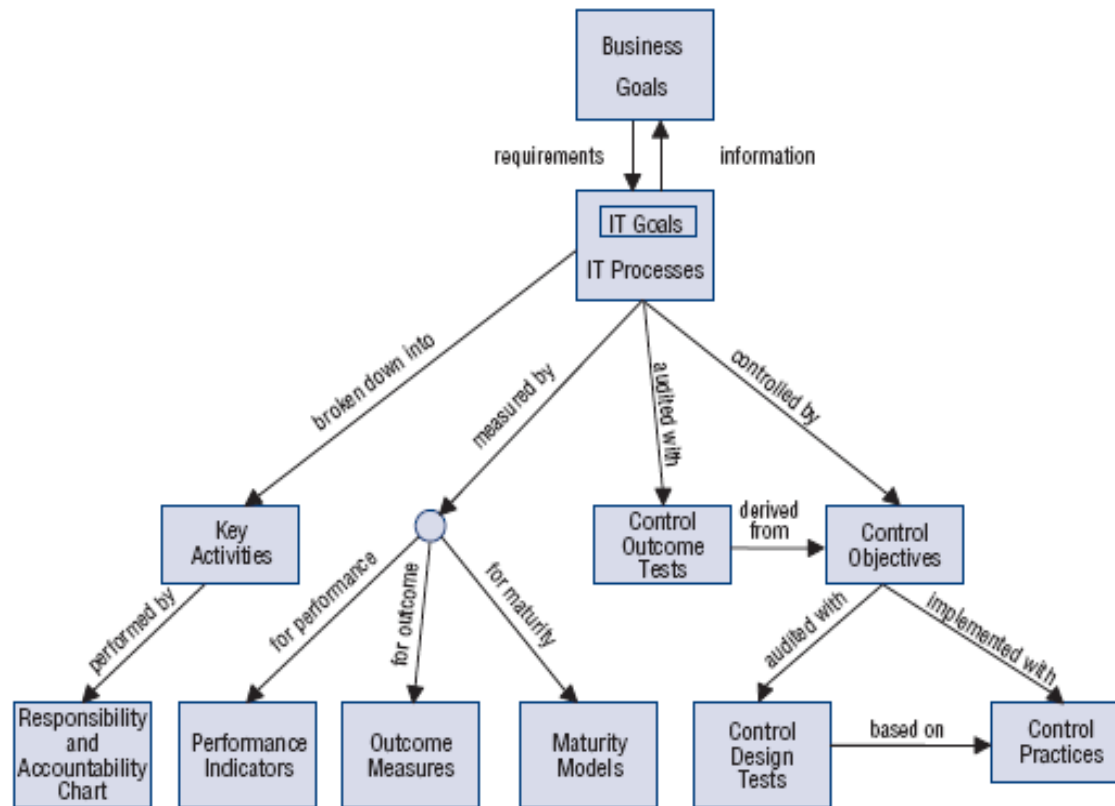- – Sjednocení norem a standardů v oblasti kontroly, řízení a směřování IT
- – Sjednocení pojmů

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

Figure 4—Interrelationships of CobiT Components

ITGI
Cobit 4.1

K zajištění potřebných informací a dat, která jsou vyžadována k dosažení obchodních cílů, organizace investuje, řídí a kontroluje zdroje IT, přičemž používá celou množinu procesů. Prostřednictvím či s pomocí těchto procesů se realizují a nastavují služby, návody, standardy, směrnice……, jejichž cílem je zpracovat, uchovat, poskytnout, třídit informace potřebné pro splnění obchodních cílů.

Figure 5—Basic CobiT Principle
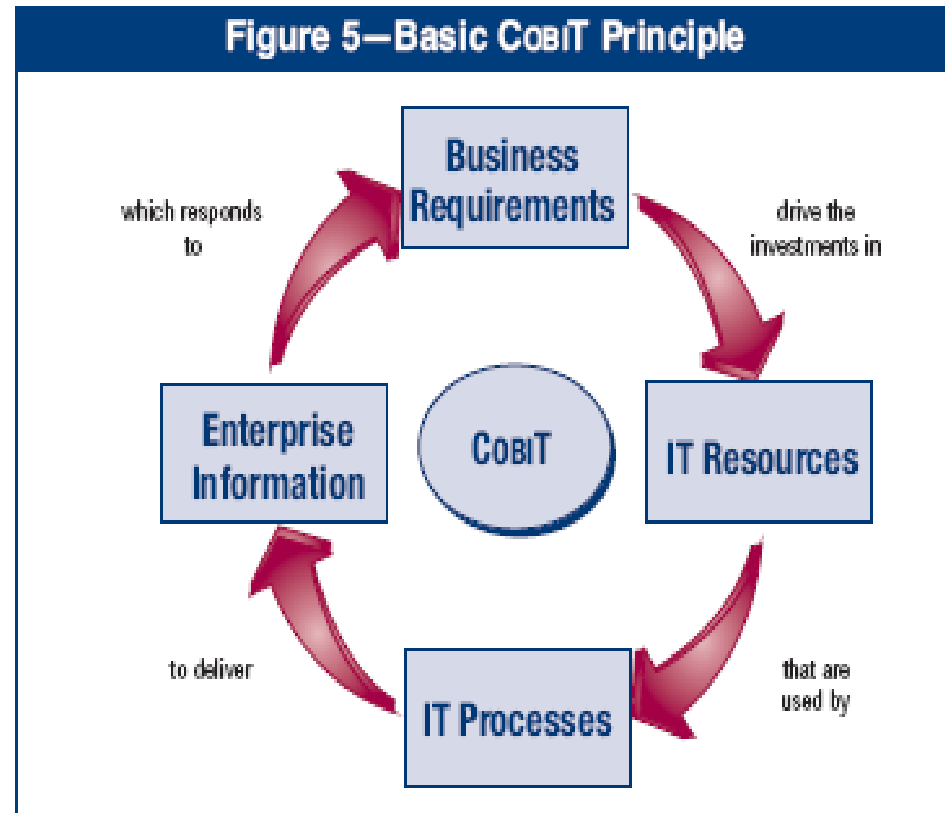
Strategie ISACA

- Nová strategie představena v polovině loňského roku
- Založena na průzkumech trhu, hodnocení stávajících prostředí IS a budoucích požadavcích
- Mise a vize

Vision
Trust in, and value from, information systems

Mission
For professionals and organizations be the leading global provider of knowledge, certifications, community, advocacy and education on information systems assurance and security, enterprise governance of IT, and IT-related risk and compliance

Rok 2010

Context
Information systems environments are continuing to increase in complexity and impact, bringing unprecedented value opportunities along with significant risk. While enterprises need to manage the risk, they also need to maximize value. This requires active governance and management of internal and external information systems.

Enterprise-wide Value
Given the growing complexities of global competition, ever-increasing risk and the need to demonstrate compliance, enterprises must take a systemic approach to governing their information systems. ISACA certifications, education, research, standards, frameworks and professional communities help enterprises balance the risks and rewards from their information systems.

Member Value
Members rely on ISACA for resources that enhance their skills, expand their professional knowledge and connect them with a vibrant community of peers. Many professionals worldwide consider membership in ISACA essential to their ongoing education, career progression and value delivery to their enterprises.

Key Message
As an independent, nonprofit, global membership association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA helps its members achieve individual and organizational success, resulting in greater trust in, and value from, information systems. Its members and certification holders are qualified and skilled professionals who make a difference.

Global Value
With members residing in more than 100 countries, ISACA is internationally recognized as a high-performing organization that addresses global, national and local information systems and business issues. Subject matter experts from around the world contribute to the development of ISACA's thought-leading knowledge, certifications, education and research.
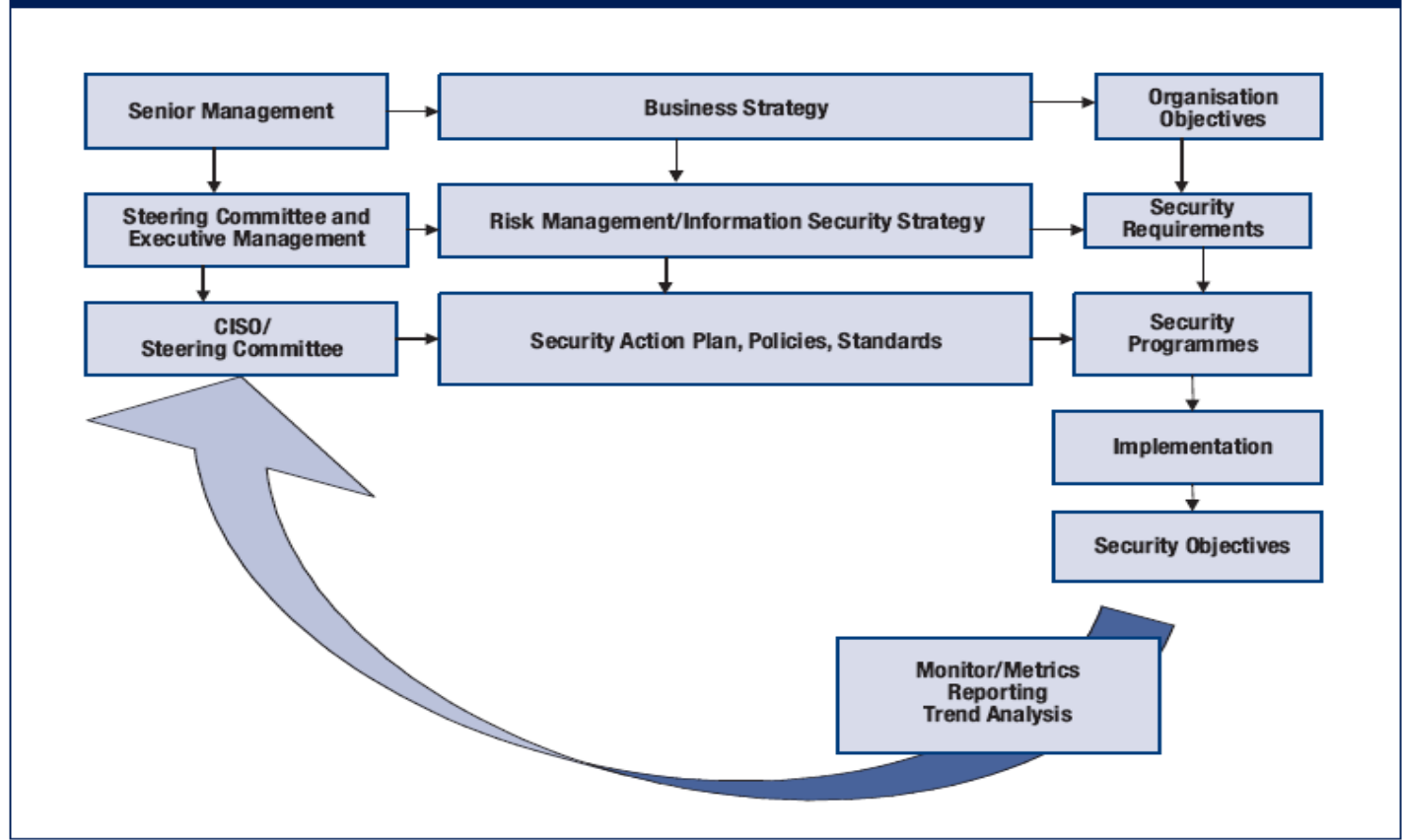
Industry Value
ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide. The COBIT, Val IT and Risk IT governance frameworks and the CISA, CISM and CGEIT certifications are ISACA brands respected and used by these professionals for the benefit of their enterprises.

www.isaca.org/strategy

IT GOVERNANCE INSTITUTE®
LEADING THE IT GOVERNANCE COMMUNITY

ČESKÁ SPOŘITELNA
Jsme Vám blíž.

Information Security Governance

Figure 1—Conceptual Information Security Governance

Rámec řízení a organizace informační bezpečnosti:

➢ Metodologie řízení rizik

➢ Komplexní bezpečnostní strategie – propojená s obchodními i IT cíli

➢ Efektivní organizační struktura bezpečnosti

➢ Strategie bezpečnosti zpracovávající informace, jej hodnotu a způsoby ochrany informace

➢ Bezpečnostní politiky – strategie, kontrolní a řídící mechanismy a regulace

➢ Bezpečnostní standardy, vycházející a podporující každou z politik

➢ Proces, který zajistí průběžné hodnocení a obměnu bezpečnostních politik, standardů, procedur a rizik……

Něco o rizicích

ENTERPRISE RISK:
IDENTIFY, GOVERN AND
MANAGE IT RISK

The Risk IT Framework

Závěr

Otázky??

www.isaca.org
www.isaca.cz
www.itgi.org

Luboš Klečka

lklecka@csas.cz

ISACA, Bezpečnost a audit
28. 12. 2015 – strana 15