Regelverk, Standarder och Riktlinjer

Erik Ravinder, CISA

Kim Haverblad, CISM

2009-02-10

Varför behövs detta?

- Struktur
- Tydlighet
- Målsättning
- Spårbarhet
- Mätbarhet
- Rapportering
- Externa krav
- Interna krav

- Interna målsättningar
- Budget
- Kvalitet
- Lönsamhet
- Nöjd kund
- Rapportering
- Intressenter

Vilka olika typer finns?

Lagstiftning

- Aktiebolagslag (ABL) (2005:551)
- Arkivlag (1990:782)
- Bokföringslag (1999:1078)
- Elektroniska signaturer (2000:832)
- Elektronisk kommunikation (2003:389)
- Företagshemligheter (1990:409)
- Personuppgiftslag (PUL) (1998:204)
- Sekretesslag (SekrL) (1980:100)
- Samhällsviktiga anläggningar (1990:217)
- Skydd mot olyckor (LSO) (2003:778)
- Smittskyddslag (2004:168)
- Upphovsrättslagen (URL) (1960:729)

Statliga

- Basel II
- Bits (Basnivå för informationssäkerhet)
- Riktlinjer för extern rapportering för företag med statligt ägande (N7042)
- Statens ägarpolitik 2007 (N6090)
- Styrelseansvaret i företag med statligt ägande (N8020)
- Myndighetstillsyn såsom FFFS (FI:s författningssamling)

Kommersiella

- Cobit
- Coso
- ISO/IEC 15408 (Common Critera)
- ISO/IEC 25999 (Business Continuity)
- ISO/IEC 27001 (ISMS)
- ISO/IEC 27002 (Code of practice)
- ISO/DIS 31000 (Risk Management)
- ISO/IEC 38500 (IT Governance)
- Itil
- PCI DSS
- Svensk Bolagskod
- Uppförandekod

Lagstiftning

- Aktiebolagslag (ABL) (2005:551) – Former och revision …
- Arkivlag (1990:782) – Att lagra, men inte hur länge …
- Bokföringslag (1999:1078) – Hur får man spara bokföring …
- Elektroniska signaturer (2000:832) – Certifikat …
- Elektronisk kommunikation (2003:389) – Mycket mer än e-post …
- Företagshemligheter (1990:409) – Vad är hemligt…
- Personuppgiftslag (PUL) (1998:204) – Personuppgiftsombud …
- Sekretesslag (SekrL) (1980:100) – Att lämna ut eller inte …
- Samhällsviktiga anläggningar (1990:217) – Vad är skyddsobjekt …
- Skydd mot olyckor (LSO) (2003:778) – Utförande av arbete …
- Smittskyddslag (2004:168) – Informations spridning…
- Upphovsrättslagen (URL) (1960:729) – Pirate bay och fildelning …

Statliga

- Bits (Basnivå för informationssäkerhet) – Från KBM, samhällsviktiga funktioner …
- Riktlinjer för extern rapportering för företag med statligt ägande (N7042) – Informationsspridning från statliga bolag …
- Statens ägarpolitik 2007 (N6019) – Ansvar och rapportering …
- Styrelseansvaret i företag med statligt ägande (N8020) – Mycket om information …
- Myndighetstillsyn såsom FFFS (FI:s författningssamling) – En mängd regler från FI…

Kommersiella

- Basel II – Minskat kapitalbas
- Cobit – Övergripande styrningsmodell för IT
- Coso – Finansiellt styrverktyg
- ISO/IEC 15408 - Common Critera
- ISO/IEC 20000 - IT Service Management
- ISO/IEC 25999 - Business Continuity
- ISO/IEC 27000 - Overview & Vocabulary
- ISO/IEC 27001 - IS Management System
- ISO/IEC 27002 - Code of practice
- ISO/DIS 31000 - Risk Management
- ISO/IEC 38500 - IT Governance
- Itil – För optimera drift organisation
- PCI DSS – Säkra korttransaktioner
- Svensk Bolagskod – Intern kontroll
- Uppförandekod – Etiska riktlinjer

Internationella standarder och regelverk

- California Cyber Security Laws (SB1386, SB355, AB1950)
- Director of Central Intelligence Directives (DCID 6/3)
- Department of Defence (DoD / 8500.1, 8500.2)
- EU:s 8:e direktiv (2006/43/EG)
- Family Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FIPS 199 / 200)
- Health Insurance Portability & Accountability (HIPAA)
- North American Electric Reliability Council (CIP-001 - > CIP-009)
- National Institute of Standards and Technology (SP800 serien)
- Sarbanes-Oxley Act 2002 (Sarbox / SOX / Section 404)

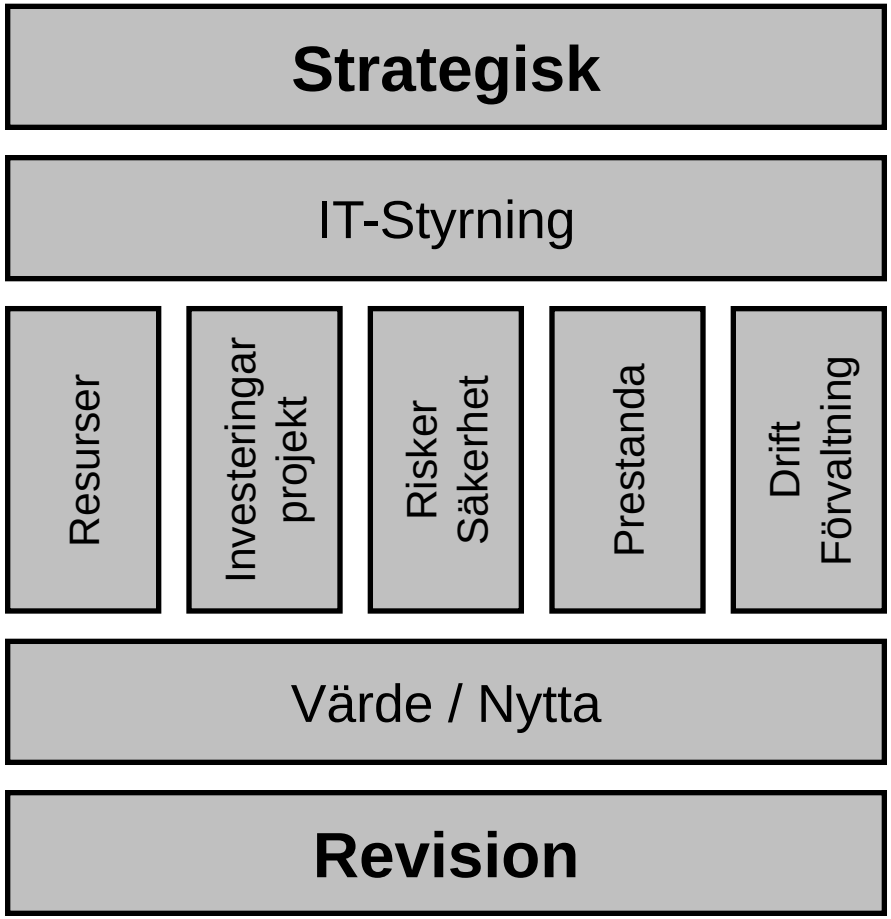
Externa / Interna krav

Tvingande	Reglering	Riktlinjer	Policys	Procedurer
ABL PUL osv.	FFFS 2005:1 (Styrning och kontroll av finansiella företag)	Branschnormer Tex. FAR SRS regelverk Statliga Organisatoriska	Säkerhetspolicy Internetpolicy IT-policy	Nedbruten och tillämpbar policy. Tex. Rutiner för lösenordshantering

Externa krav

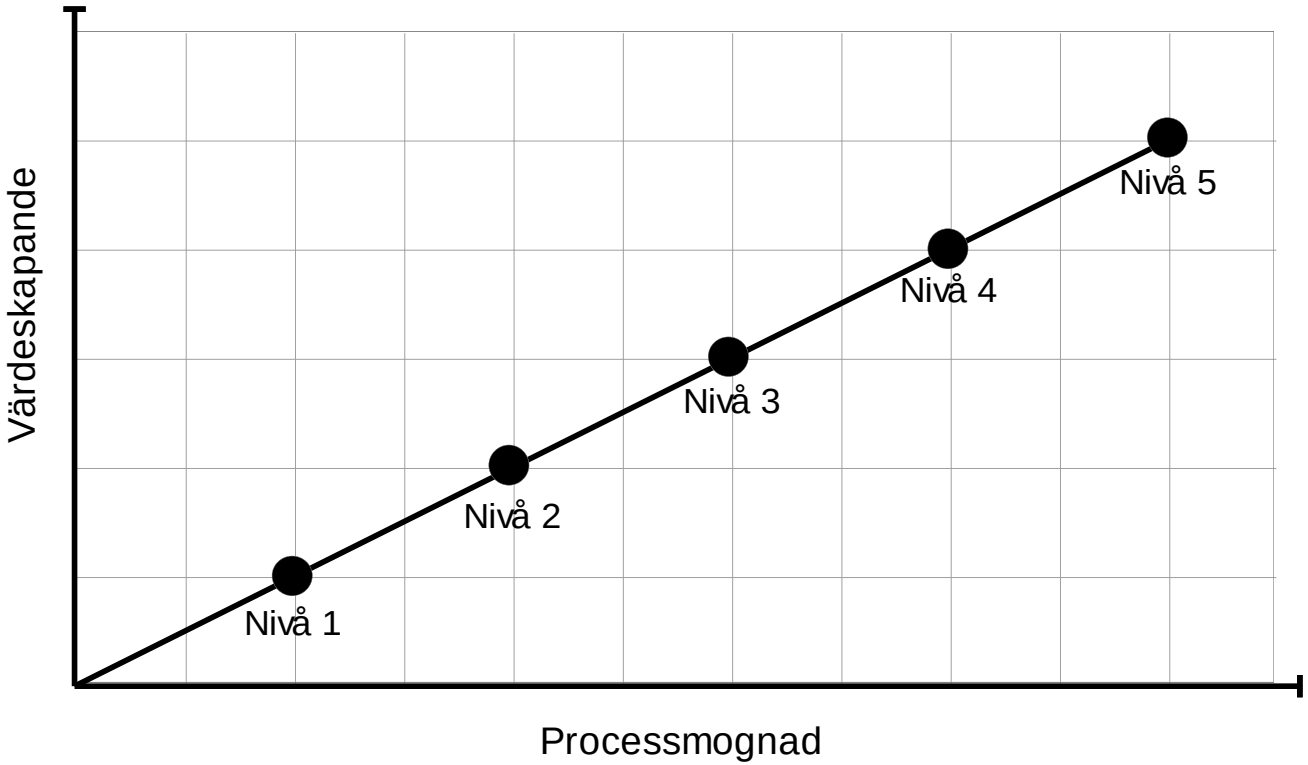
Interna krav

Organisatorisk helhetsbild



Källa: IT ur ett affärsperspektiv

Mognadsnivå



Exempel på mognadsnivå

Nivå 0 - Existerar inte

- Ledningen har inte uppmärksammat behovet för en process för servicenivåer. Ansvar för att mäta servicenivåer är inte definierat.

Nivå 1 - Initial

- Det finns en medvetenhet om behovet för att hantera servicenivåer men processen är informell och reaktiv. Ansvar för att definiera servicenivåer är inte definierat.

Nivå 2 - Upprepande

- Det finns överenskomna servicenivåer men de är informella och granskas inte. Rapportering är bristande och kan vara irrelevant och missledande för kunderna. En servicenivå koordinator är utsedd men har begränsade befogenheter. Det är upp till den enskilde individen om processen följs eller inte.

Nivå 3 - Definierat

- Processen är dokumenterad och förankrad. Ansvar är tydliga. Tjänster är definierade. Servicenivåer är definierade och överenskomna men speglar inte alltid affärsbehovet.

Nivå 4 - Kontrollerat och hanteras

- Servicenivåer definieras redan vid kravspecifikation för nya system. Kundnöjdhet mäts kontinuerligt och prestandamätning reflekterar affären. Vid missade servicenivåer genomförs en granskning för att identifiera orsaken. Det finns ett formellt system för mätning av nyckeltal.

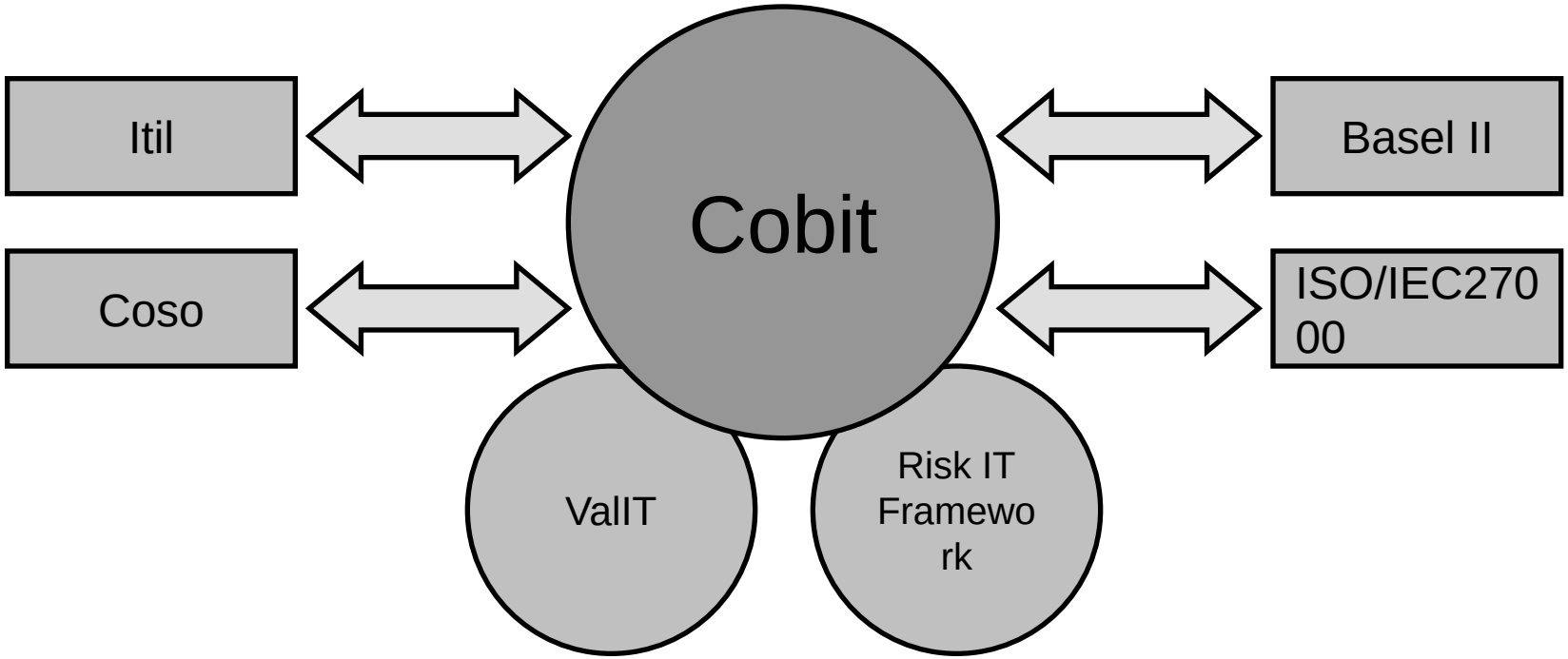
Nivå 5 - Optimerat

- Servicenivåer utvärderas kontinuerligt för att säkra att dessa är kopplade till affärsmål. Processen förbättras ständigt och kundnöjdhet mäts och hanteras kontinuerligt. Belöningar är kopplade till servicenivåmål.

Varför IT-revision?

- Legala krav
- Statliga krav
- Kommersiella krav
- Intern osäkerhet (internkontroll)
- Extern osäkerhet (revisionskontroll)

Mappat till Cobit



Frågor?

Länkar för mer information

www.coso.org
www.fi.se
www.iso.org
www.isaca.org/cobit
www.msbmyndigheten.se
www.ogc.gov.uk
www.pcisecuritystandards.org
www.riksdagen.se
www.sis.se

iase.disa.mil
www.dtic.mil
www.iatrp.com
www.fas.org
csrc.nist.gov
www.hhs.gov
www.nerc.gov
www.awwa.org
www.ed.gov

Tack för oss!

Erik Ravinder, CISA
040-614 25 55 / erik.ravinder@set-revision.se
Kim Haverblad, CISM
070-728 37 86 / kh@haverblad.se