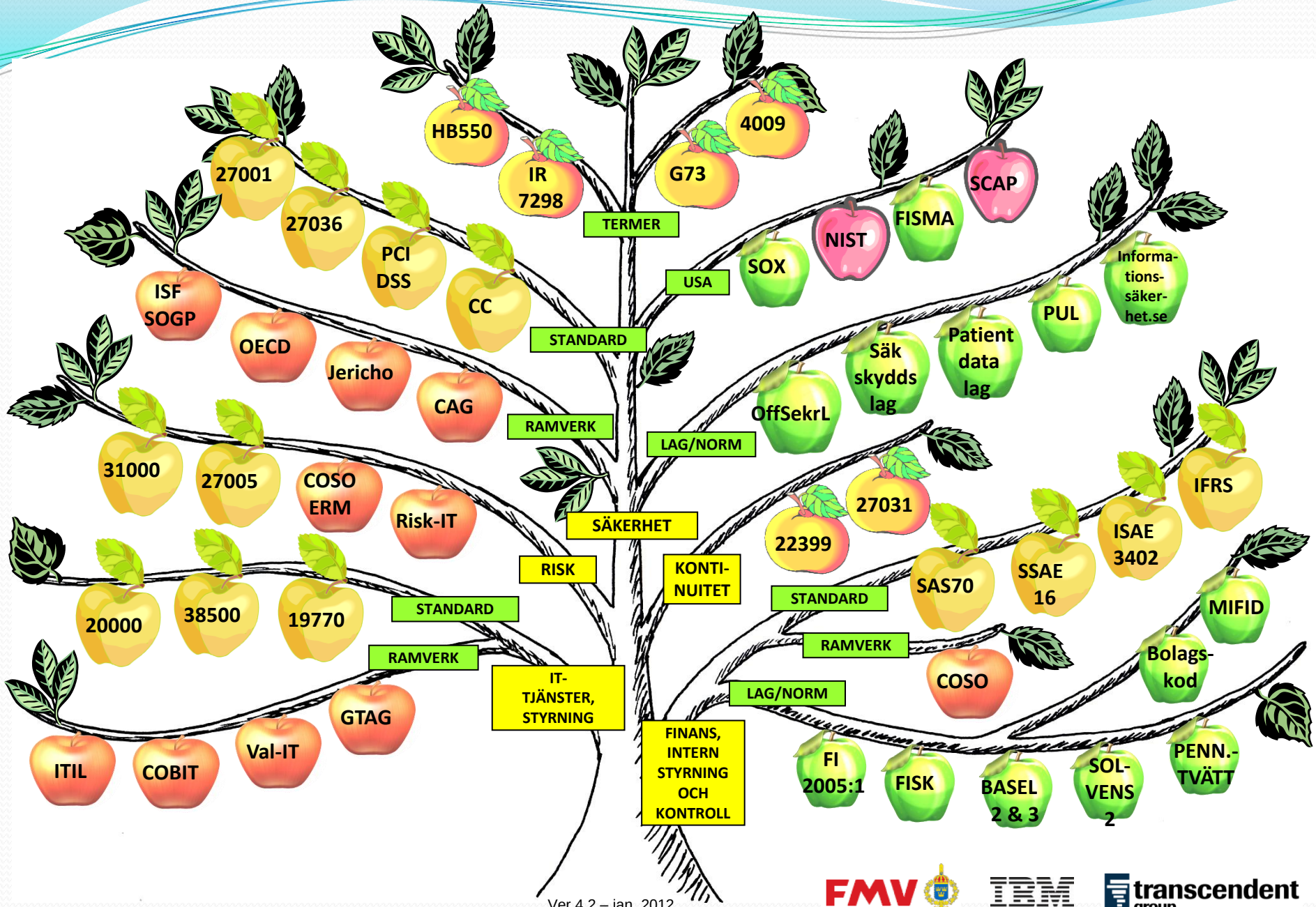
Standarder och regelverk inom informationssäkerhet



Standarder och regelverk inom informationssäkerhet (del 1)

FI 2005:1

Finansinspektionens allmänna råd om styrning och kontroll av finansiella företag (2005:1). Råden följer principen ”följ eller förklara”. De behandlar även riskhantering och säker-ställan av regelefterlevnad. Råden bygger på ramverket COSO.

- fi.se/Regler/FIs-forfattningar/Samtliga-forfattningar/20051/

FISK

Med förordningen för intern styrning och kontroll, 2007:603, (”FISK”), stärker regeringen sin styrning av statliga myndigheter. Därigenom förtydligas kravet på myndigheterna att fullgöra sitt förvaltningsansvar.

- riksdagen.se/sv/Dokument-Lagar/

Basel 2 & 3

Kapitaltäckningsregler för organisationer som står under Finansinspektionens tillsyn. Reglerna innebär att institut ska ha fungerande riskhanteringssystem för att hantera riskerna i verksamheten.

- fi.se/Regler/Kapitaltackning/

Solvens 2

”Försäkringsbolagens Basel 2”. Namnet kommer från engelskans solvency, betalningsförmåga. Syftet är att skydda de direkta försäkringstagarnas och andra ersättningsberättigades intressen. Hösten 2012 ska de nya reglerna vara införda i svensk lagstiftning.

- fi.se/Regler/Solvens/

Penningtvättslagen

Penningtvättslagen, SFS 2009:62. Förkortningen AML används också i samman-hanget, Anti Money Laundering. Penningtvätt är när pengar från brottslig verksamhet förvandlas till tillgångar som kan redovisas öppet. Lagen omfattar alla finansiella institut, men även andra bolag tex. finansiella rådgivare och kasinon.

- penningtvatt.se

Kod för svensk bolagsstyrning

Svensk kod för bolagsstyrning (”Koden”), är en norm för bolagsstyrning och gäller alla svenska aktiebolag vars aktier är upptagna till handel på en reglerad marknad i Sverige. Syftet är att stärka förtroendet för de svenska börsbolagen.

- bolagsstyrning.se/koden

SAS 70

Amerikansk revisionsstandard för tredjepartsgranskning, som möjliggör för en revisor att förlita sig på resultatet av ett arbete som en annan revisor har genomfört. Standarden är utgiven 1992 av AICPA (American Institute of Certified Public Accountants). Viktiga rapport-typer: typ 1 resp. typ 2.

- sas70.com
- aicpa.org

SSAE 16

Statement on Standards for Attestation Engagements (SSAE) No. 16 är utgiven av AICPA 2010 och avser ersätta SAS70 i USA. Den ska överensstämma med ISAE 3402.

- ssae16.com
- aicpa.org/soc

ISAE 3402

International Standards for Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, gäller sedan 15 juni 2011. Det är den första globala standarden för tredjepartsgranskning av serviceorganisationer. Standarden har mycket gemensamt med SAS70.

- isae3402.com
- web.ifac.org

IFRS

International Financial Repor-ting Standards, ett regelverk för finansiell rapportering. Från 2005 ska svenska bolag med värdepapper noterade på en reglerad marknad inom EU ha en koncernredovisning enligt IFRS. Syftet med IFRS är att ge aktieinvesterarna bättre information om företagens verkliga värde vid redovisningstillfället.

- iasb.org

COSO

Committee of Sponsoring Organizations of the Treadway Commission. COSO är ett internationellt ramverk för intern styrning och kontroll, vilket är definierat som en process utförd av en organisations styrelse, ledning och annan personal, utformad för att ge rimlig försäkran om att målen uppfylls.

- coso.org

MIFID

Directive on Markets in Financial Instruments. 2007 infördes ett gemensamt regel-verk för alla EU-länder avse-ende värdepappershandeln. Regelverket ska göra det enk-lare att handla med värde-papper över nationsgräns-erna, öka konkurrensen på europeiska marknaden och stärka investerarnas skydd.

- fi.se

ITIL

Ramverket ITIL ("IT Infra-structure Library") är en sam-manställd praxis för IT service management. ITIL beskriver ett systematiskt arbetssätt som hjälper organisationer att leverera välskötta IT-tjänster. Fem delar i ITIL version 3: Strategy, Design, Transition, Operation, Continual Improvement.

- itil.org
- Itsmf.se

ISO/IEC 20000

Standard för ledningssystem för IT- tjänster (IT Service Management), nära knuten till metodiken inom ITIL-konceptet. Del 1 anger de krav en organisation måste uppfylla för att erhålla en certifiering. Del 2 ger en vägledning om hur kraven kan uppfyllas.

- sis.se

COBIT

Control Objectives for Infor-mation and related Technology är ett internationellt accepterat ramverk för IT-styrning och IT-revision. COBIT överbryggar gapet mellan styrande regelverk, tekniska frågor och affärsrisker och ökar värdet av IT-leveransen. Aktuell version: 4.1. COBIT 5 planeras utkomma 2012.

- isaca.org, isaca.se

Val-IT

Val-IT från IT Governance Institute (ITGI) är mer än ett ramverk. I Val-IT finns ett antal processer utformade inom tre områden – värdestyrning, portföljhantering och hantering av investeringar. Val-IT kommer att integreras i COBIT 5, vilken planeras utkomma 2012.

- isaca.org
- itgi.org

GTAG

Global Technology Audit Guidelines (GTAG) är ett ramverk för att underlätta för internrevisorn att identifiera och bedöma IT-risker. GTAG hänvisar till redan etablerade ramverk, som COBIT, ITIL, 27000-serien. Idag finns 13 olika GTAG, som kan användas av alla, dvs inte bara för revisorn!

- theiia.org/guidance/technology

ISO/IEC 38500

Internationell standard för IT-styrning - ISO/IEC 38500:2008 - Corporate governance of information technology. Standarden definierar sex principiella ansvarsområden för styrelsen; ansvar, strategi, anskaffning, prestanda, efterlevnad och mänskligt beteende.

- sis.se

Standarder och regelverk inom informationssäkerhet (del 2)

ISO/IEC 27001

Den mycket centrala standarden ISO/IEC 27001 (f.d.17799) anger kraven för certifiering av ett ledningssystem för informationssäkerhet i en organisation. 27002 ger riktlinjer och vägledning för arbetet. Flera andra delar i 27000-serien finns eller är under framtagning.

- sis.se, swedac.se
- iso27001security.com

ISO/IEC 27036

Ett exempel på ett pågående standardarbete, i detta fall med titeln "IT Security - Security techniques - Information security for supplier relationships". Flera delar tas fram, där del nr 4 och 5 kan komma att handla om Outsourcing resp. Cloud Computing.

- www.iso27001security.com/html/27036.html

PCI DSS

Payment Card Industry Data Security Standard – reglerar hur företag ska hantera bank- och kreditkortsinformation på ett säkert sätt. Standarden anger detaljerade tekniska krav, baserade på tolv grundkrav. Version 2.0 kom i okt -10.

- pcisecuritystandards.org

Common Criteria

Internationell standard ISO/IEC 15408, "Common Criteria", anger hur IT-produkter kan evalueras och certifieras. Granskningsresultat anges med assurans-nivå (EAL1-EAL7), som anger graden av tilltro till en produkts eller ett systems säkerhetsfunktioner. Viktiga begrepp: Protection Profile, Security Target.

- csec.se,
- commoncriteriaportal.org

OffSekrL

Offentlighets- och sekretesslagen (2009:400) reglerar bl.a. myndigheters hantering av allmänna handlingar och ger bestämmelser om sekretess till skydd för bl.a. rikets säkerhet, rikets centrala finans- och valutapolitik, in-tresset av att förebygga brott samt sekretess till skydd för enskilds förhållanden.

- riksdagen.se/sv/Dokument-Lagar/

Säkerhetsskyddslagen

Lagen (1996:627) gäller i princip för alla vars verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Säkerhetsskyddsförordningen (1996:633) kompletterar lagen med detaljerade bestämmelser.

- riksdagen.se/sv/Dokument-Lagar/

ISF SOGP

Information Security Forum:s "Standard of Good Practice" har uppdaterats 2011. En omfattande standard utifrån sex aspekter, nedbrutna i areor och sektioner, var och en med princip och syfte.
Följer ISO 27001, COBIT v4.1 and PCI/DSS. En "Executive Summary" kan laddas ner gratis.

- securityforum.org

OECD

OECD-rådets "Riktlinjer för säkerheten i informationssystem och nät – på väg mot en säkerhetskultur" antogs som en rekommendation inom EU i juli 2002. Anger nio principer i syfte att skapa en säkerhetskultur, förenlig med demokrati, ett öppet och fritt informationsflöde och skydd avseende personlig integritet.

- oecd.org/dataoecd/42/57/32494705.PDF

Jericho

Open Group anger elva nätverksprinciper för att möta utmaningen med "utsuddade gränser". COA Framework v2.0 är ett ramverk för att forma sin egen arkitektur. Även exempel på arkitekturer ges. Publ. 2008. Andra dokument anger en "Cloud Cube Model" samt 14 "identitetsprinciper".

- opengroup.org/jericho/publications.htm

CAG

SANS har publicerat ver.3.1 av Consensus Audit Guide-lines, innehållande 20 riktlinjer för en kraftigt förbättrad kostnadseffektivitet i informationssäkerhets-arbetet. Viktigt är att skyddet kan skapas och övervakas av automatiska verktyg. En mappning finns till NIST SP 800-53.

- sans.org/critical-security-controls

Patientdatalagen

(2008:355) Patientdatalagen ska öka patientsäkerheten och inflytandet för patienterna. Lagen ställer krav på säkerhet, dokumentation och regler för sekretess och åtkomst. Den gör det möjligt för fler vårdgivare att lättare ta del av en patients journal.

- riksdagen.se/sv/Dokument-Lagar/

PUL

Personuppgiftslagen kom 1998 och ska skydda människor mot kränkning av den personliga integriteten. Anger regler för hur person-uppgifter får behandlas. Lagen bygger i hög grad på s.k. samtycke.

- datainspektionen.se

ISO 31000

ISO 31000:2009 är en internationell standard som tillhandahåller principer och generella riktlinjer för riskhantering. Begreppet risk definieras som "the effect of uncertainty on objectives". Standarden kan tillämpas på alla typer av risker, oavsett karaktär, och oavsett om de har positiva eller negativa konsekvenser.

- sis.se

ISO/IEC 27005

ISO/IEC 27005:2011 innehåller riktlinjer för hantering av informationssäkerhetsrisker. Standarden stödjer de allmänna koncept som specificeras i ISO/IEC 27001 och den är utformad för att stödja ett lyckat införande av informationssäkerhet med utgångspunkt från riskhantering.

- sis.se

COSO ERM

COSO ERM (Enterprise Risk Management) publicerades 2004 och är en andra generation av COSO. COSO ERM består av åtta olika komponenter och används som en företagsövergripande process för riskhantering. COSO ERM framställs, liksom COSO, ofta i form av en kub.

- coso.org

RISK-IT

Risk-IT är ett ramverk utgivet av ITGI (ISACA). Risk-IT, som är ett komplement till Cobit, bygger på vägledande principer för effektiv hantering av IT-risker. Risk-IT hjälper organisationer att etablera en modell för att identifiera, styra och hantera sina IT-risker. RISK-IT kommer att integreras i COBIT 5, vilken planeras utkomma 2012.

- isaca.org

informationssäkerhet.se

Ett ramverk för systematiskt informationssäkerhetsarbete är framtaget under ledning av MSB och publicerat på informationssäkerhet.se. Ramverkets processkarta ger en översikt av alla de processer och stöddokument som ingår, bl.a. för informationsklassning och riskanalys.

- informationssäkerhet.se

ISO/IEC 19770

Internationell standard för Software Asset Management (SAM) Programvaruhantering. Syftet med standarden är att skapa bättre möjligheter att kontrollera kostnaderna för programvarulicenser. Med en enklare hantering och bättre kostnadskontroll följer även en bättre riskhantering.

- iso19770.com
- iso.se

Standarder och regelverk inom informationssäkerhet (del 3)

SOX

Den amerikanska lagen Sarbanes-Oxley Act (SOX) gäller alla företag som är noterade på amerikansk börs. I Sverige direktberörs ett tiotal företag. Lagen fastställer företagsledningens ansvar avseende en tillfredsställande intern kontrollstruktur i syfte att säkerställa den finansiella rapporteringen.

- sv.wikipedia.org/wiki/Sarbanes-Oxley_Act

NIST

National Institute of Standards and Technology i USA ger ut ett stort antal olika typer av standarder och guidelines:

- FIPS – Federal Information Processing Standards
- Special Publications (”800-serien”)
- NISTIR - Interagency eller Internal Reports.

- csrc.nist.gov/publications

FISMA

Federal Information Security Management Act - ett regelverk för hur amerikanska myndigheter kontrolleras. I processen används många NIST-standarder.
Exempel: FDCC (Federal Desktop Core Configuration) anger hur myndigheters PC-klienter ska konfigureras.

- csrc.nist.gov/groups/SMA/fisma/

SCAP

Security Content Automation Protocol (SCAP) är en metod där specifika standarder an-vänds för att skapa automatisk sårbarhets-hantering, säkerhets-bedömning och policy-efterlevnad.
Beskrivning ges i NVD – National Vulnerability Database.

- scap.nist.gov
- nvd.nist.gov

ISO/PAS 22399

Societal security - Guidelines for incident preparedness and operational continuity management. Dessa riktlinjer ger allmän vägledning för alla typer av organisationer vid framtagning av egna kriterier för incidentberedskap och operationell kontinuitet, samt vid utformning av lämpligt styrningssystem.

- sis.se

SIS HB 550

Handbok 550 Terminologi för informationssäkerhet - svenskt referensverk inom informationssäkerhet.
Utgåva 3, 2007.
Svenska och engelska termer, inkl kvalitetsbegrepp.

- sis.se

IR 7298

NIST-rapporten IR 7298 Glossary of Key Information Security Terms utkom reviderad i februari 2011.
Dokumentet är en sammanställning av säkerhetstermer i NIST:s säkerhetsrelaterade dokument.

- csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

ISO Guide 73

ISO Guide 73:2009 är en ordlista som ger definitioner av generella termer inom riskhantering, i syfte att skapa en enhetlig terminologi. Den refererar även till ISO 31000.
Den internationella titeln är: ”Risk management – Vocabulary”.

- sis.se

CNSSI 4009

CNSS Instruction No. 4009 har rubriken “National Information Assurance (IA) Glossary” och är en ordlista med både ord och förkortningar, utgiven av amerikanska CNSS – The Committee on National Security Systems. Reviderades april 2010.

- www.cnss.gov/Assets/pdf/cnssi_4009.pdf

ISO/IEC 27031

I mars 2011 publicerades Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity. Standarden ger vägledning kring koncept och principer för hur IT-stödet bör utformas för att säkerställa kontinuitet i en verksamhet.

- iso27001security.com

Disclaimer: alla modeller utgör en tolkning av verkligheten – så även detta äppelträd! Urvalet av regelverk och den valda strukturen är vårt sätt att åskådliggöra en del av alla de regelverk och relationer som finns inom området.

Ett tack för bidrag i arbetet till:
- Dag Ströman, FMV
- Margareta Lindahl, Transcendent Group
- Helena Andersson, MSB

Martin Bergling
070-982 4730
martin.bergling@fmv.se

Hans Darenberg
070-793 4298
hans.darenberg@se.ibm.com

Karin Winberg
0730-98 60 49
karin.winberg@transcendentgroup.com