



17799

27000

Översikt och aktuell status ISO/IEC 27000-serien

Lars Söderlund, Lüning Consulting





- Lars Söderlund
- Luning Consulting AB
- Uppsala
- Informationssäkerhet
- IT-säkerhet
- 7 Konsulter
- www.luning-consulting.se
- www.logeye.se



LÜNING
CONSULTING



Secure LogEye®





Ledningssystem för
informations-
säkerhet (LIS)
SIS TK 318

Ledningssystem för informationssäkerhet





LIS – Målsättning

- **Lättförståeligt**
- **Ej teknikberoende**
- **God sed**
- **Inte bara IT**
- **Marknadsdriven efterfrågan**





Organisationssalladen



International
Electrotechnical
Commission



International
organization for
standardization



International
Telecommunication
Union

...has built a strategic partnership with the WTO (World Trade Organization) with the common goal of promoting a free and fair global trading system.



World Trade
Organization



ISO



- Non Governmental Organization (NGO)
- Generalsekreteriat i Genève, Schweiz
- 157 medlemmar (en per land , i Sverige SIS)
- Har utvecklat 16000 standarder sedan 1947





SIS



SWEDISH
STANDARDS
INSTITUTE

- Medlemsbaserad, ideell förening
- 1450 företag och organisationer är medlemmar
- Är svensk representant i CEN och ISO
- Organiserar standardverksamheten i tekniska kommittéer (TK)
- TK 318 ansvarar för 27000-serien
- TK 456 ansvarar för IT-säkerhetsstandarder



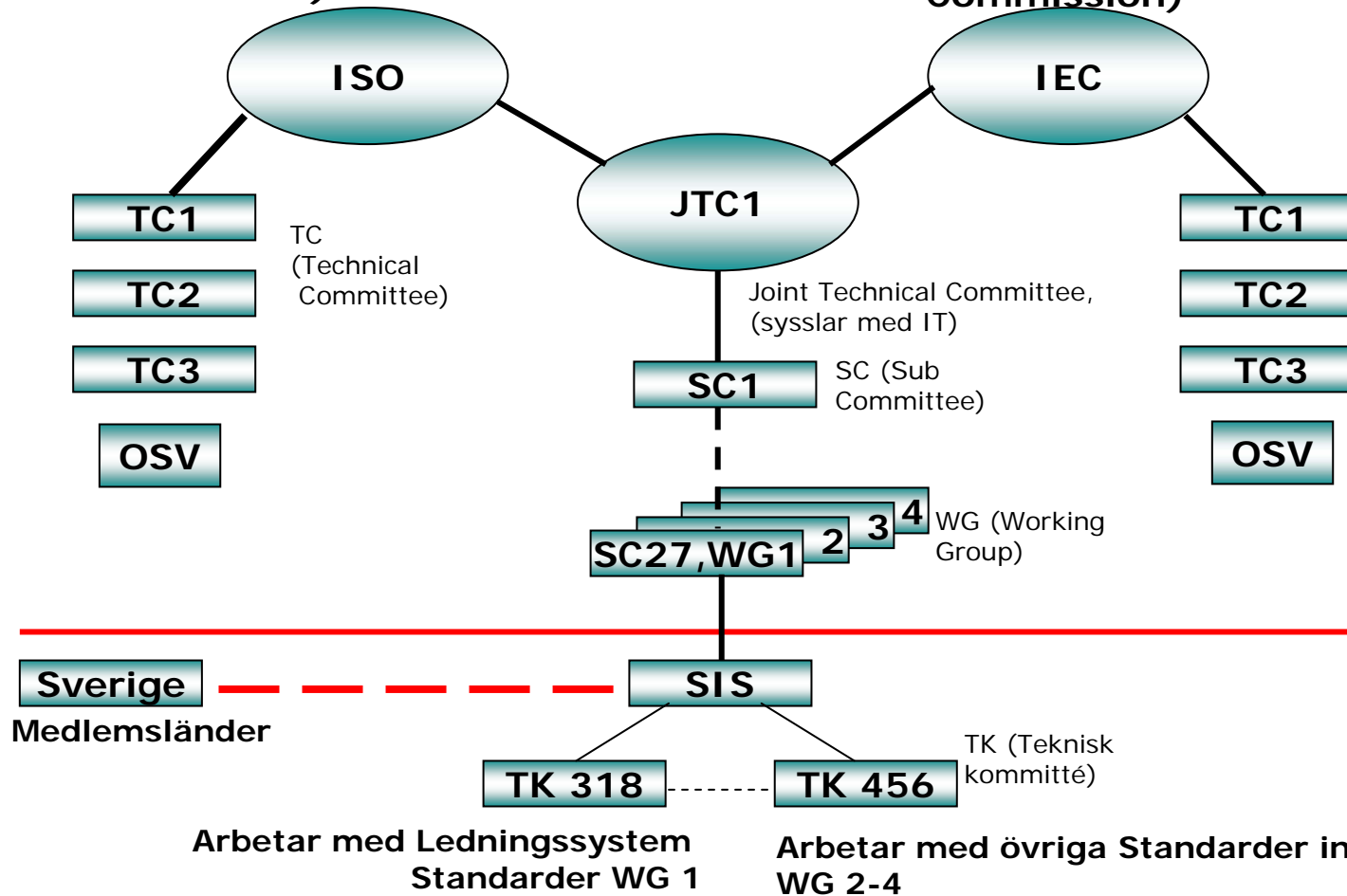
SWEDISH
STANDARDS
INSTITUTE



Skiss ISO/IEC-JTC1, SC 27/WG1

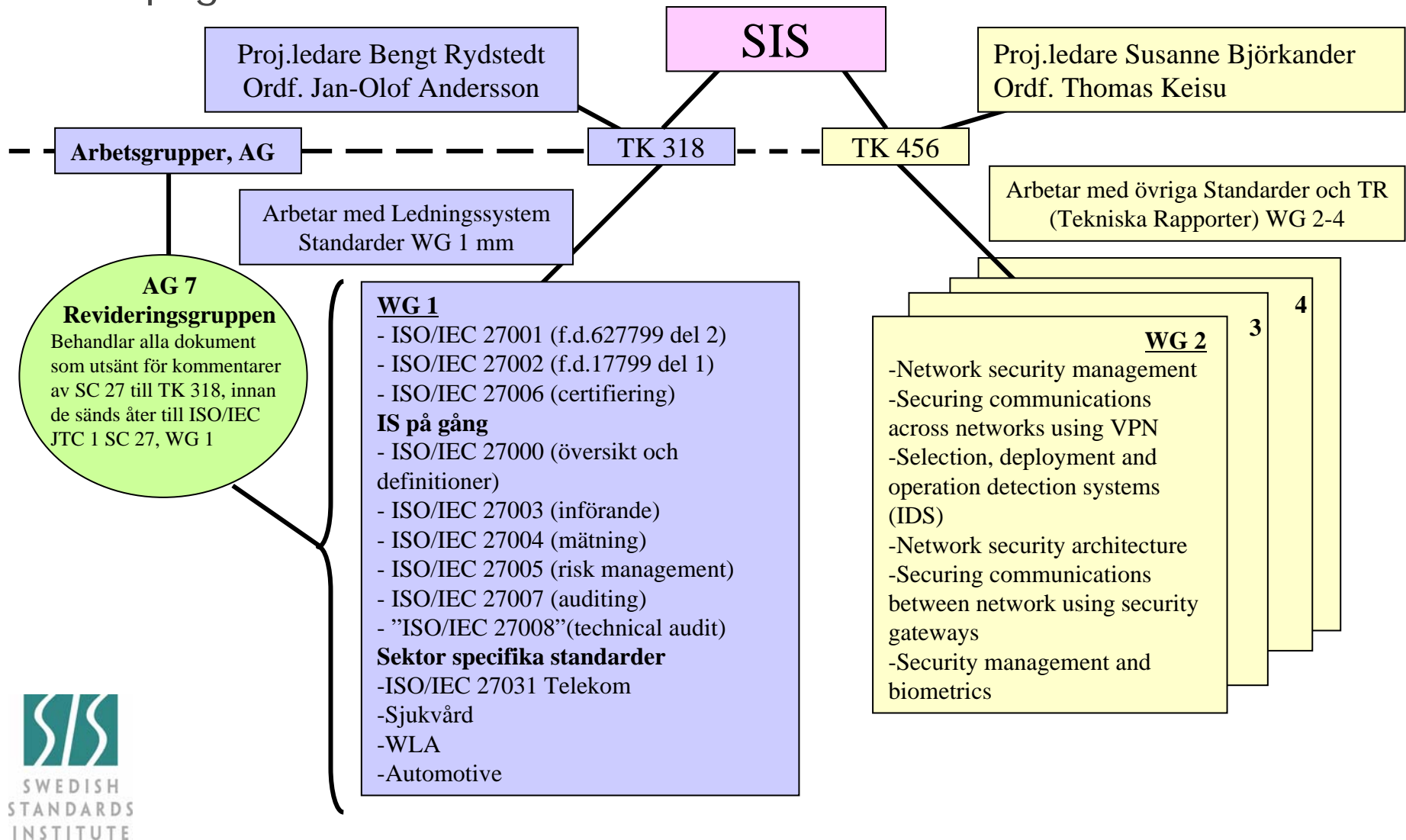
ISO (International Organization for Standardization)

IEC (International Electrotechnical Commission)



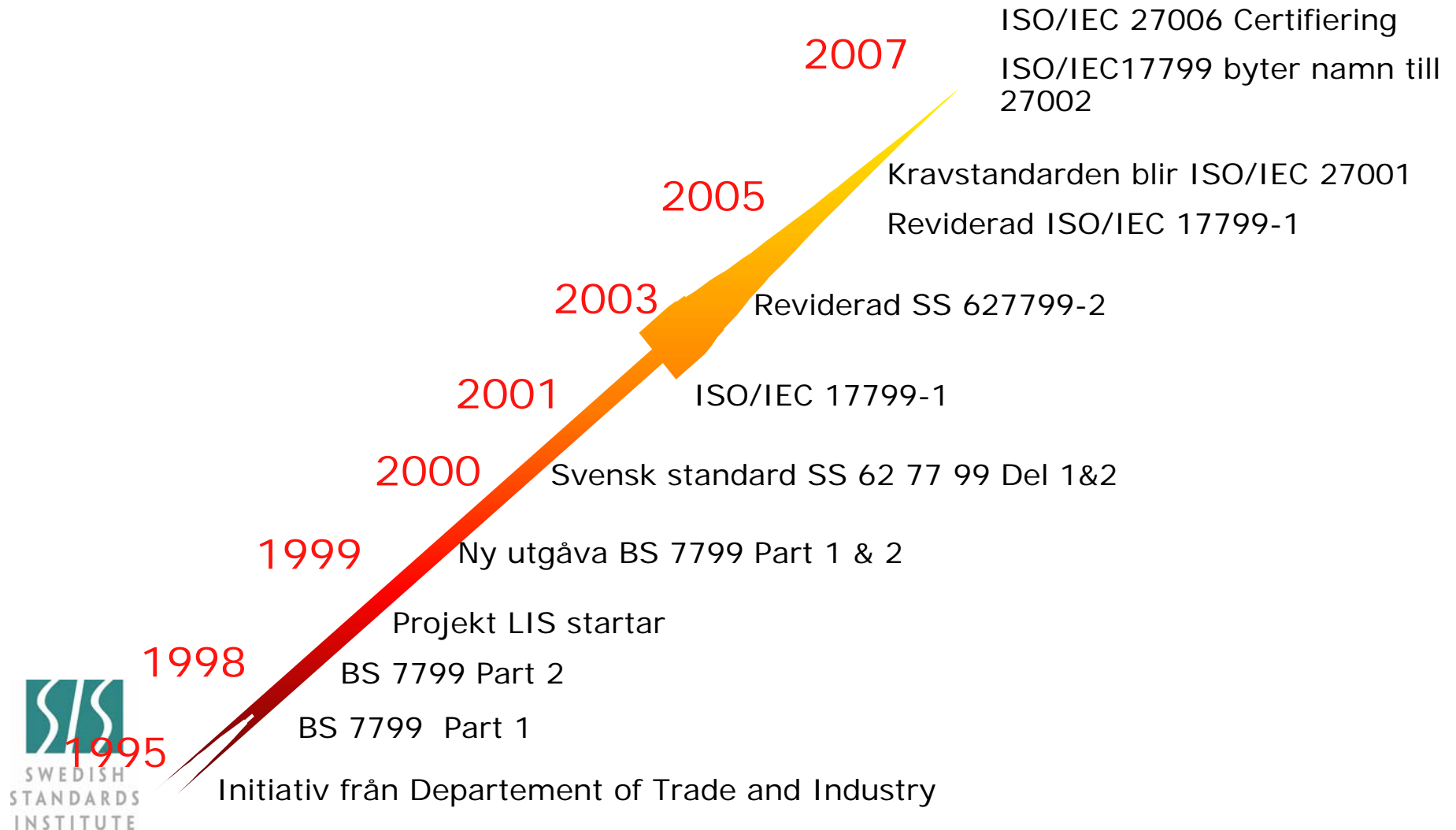


Hur speglar den svenska verksamheten den internationella?





Utvecklingen av 7799 - till idag





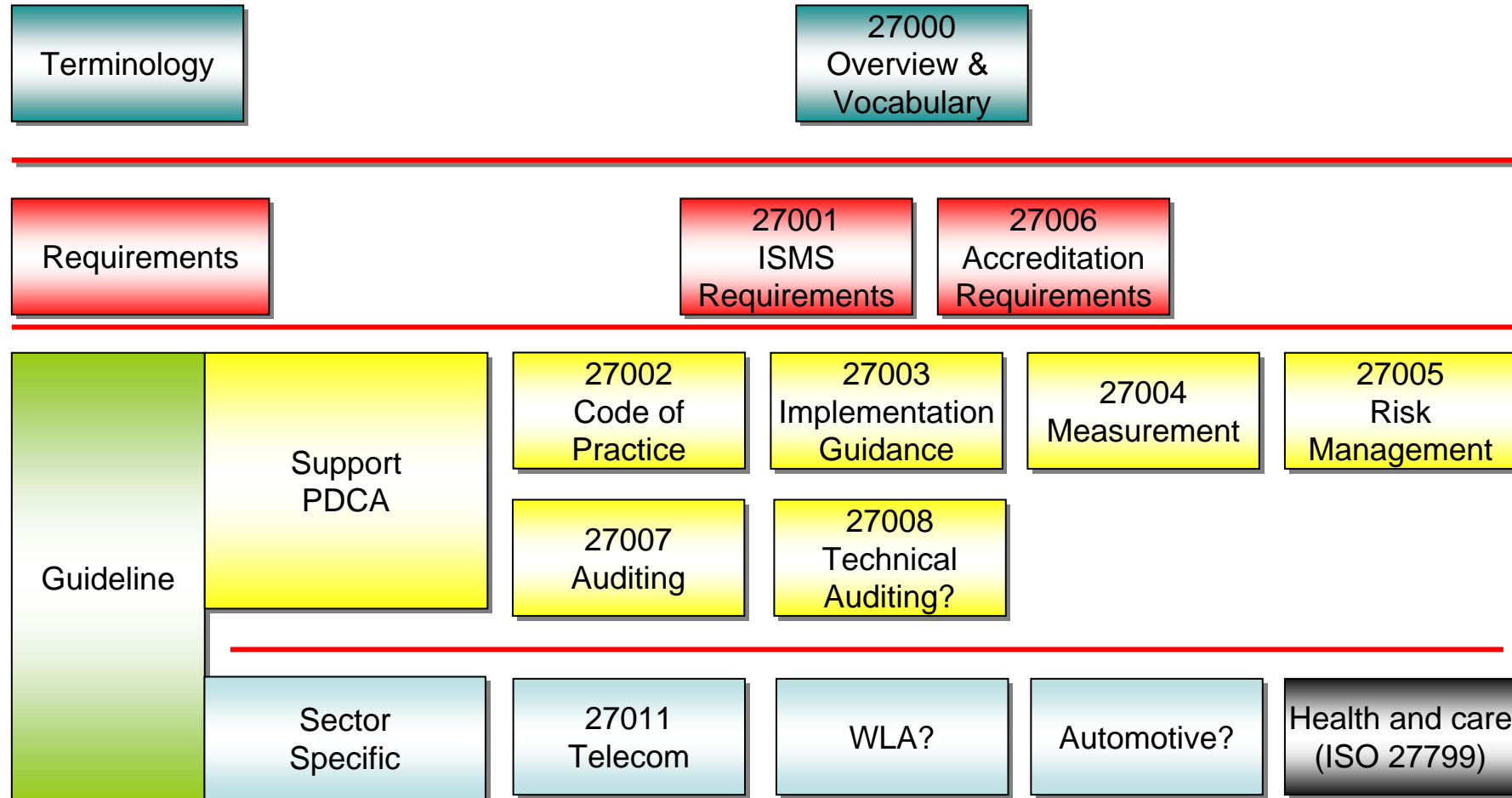
Hur lång tid tar det att utveckla en ny standard?

Status	Betydelse	Möten	Tid
Proposal new work item	Förslag	Omröstning på internationellt möte att gå vidare	0,5 år
WD Working draft	Första utgåva av förslag på standard, körs ofta i minst två omgångar (WD1 och WD2)	Synpunkter och beslut om status tas på internationellt möte	0,5-1 år
CD Committe Draft	Standarden har fått struktur men allt innehåll ej stabilt, körs ofta i två omgångar (CD1 och CD 2)	Synpunkter och beslut om status tas på internationellt möte	0,5-1 år
FCD Final Committe Draft	Sista utgåvan där man kan ändra innehållet eller strukturen	Synpunkter och beslut om status tas på internationellt möte	0,5 år
FDIS Final Draft IS	Sista utgåvan innan publicering, endast editorielle synpunkter tas emot	Synpunkter och beslut om status tas på internationellt möte	0,5 år
Publicering	Utgåvan fastställs att ges ut	Beslut tas på internationellt möte	0,5 år
SUMMA			3-4 år





ISO/IEC 27000-serien





ISO/IEC 27000

Overview and vocabulary

- Typ av standard: Terminology
- Innehåll: Definitioner samt övergripande beskrivning av området och ISO/IEC 27000-familjen
- Kommer att vara gratis
- Status: Revised text of 2nd CD ISO/IEC 27000





ISO/IEC 27001- Information security management systems – Requirements

- Typ av standard: Requirements
- Innehåll: Krav på Ledningssystem för informationssäkerhet
- Krav på processen
- 133 krav i Bilaga A som motsvarar ISO/IEC 27002 (tidigare ISO/IEC 17799:2005)
- Status: Utgiven sedan 2005-10-15, svensk översättning utgiven februari 2006





ISO/IEC 27002- Code of Practice for Information Security Management

- Typ av standard: Guideline
- F.d. ISO/IEC 17799
- Innehåll: Best Practice, Riktlinjer för styrning av informationssäkerhet
- Trots ny beteckning är det samma innehåll som i ISO 17799 som gavs ut 2005.
- Status: Utgiven 2007-07-01





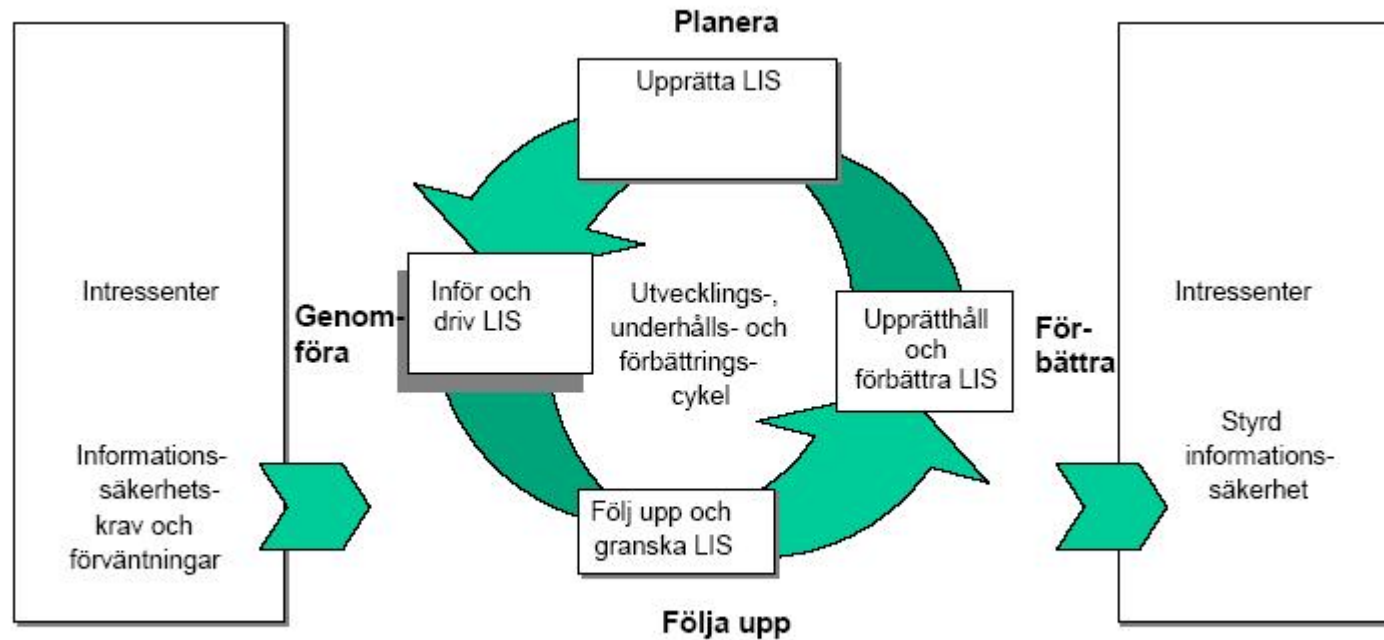
ISO/IEC 27003 - Information security management systems implementation guidance

- Typ av standard: Guideline
- Innehåll: Beskrivning av hur man inför ett ledningssystem för informationssäkerhet (ISMS)
- Kommer att beskriva införande i Plan och Do-fasen i (PDCA-processen) men ej i Check och Act
- Status: Revised text of 4th WD
(Working Draft) ISO/IEC 27003





LIS – införande

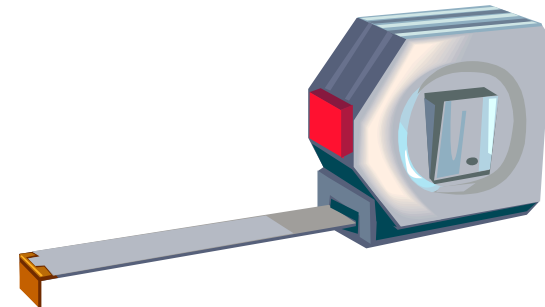


Figur 1 – PDCA-modellen tillämpad på LIS-processer



ISO/IEC 27004 - Information security management measurements

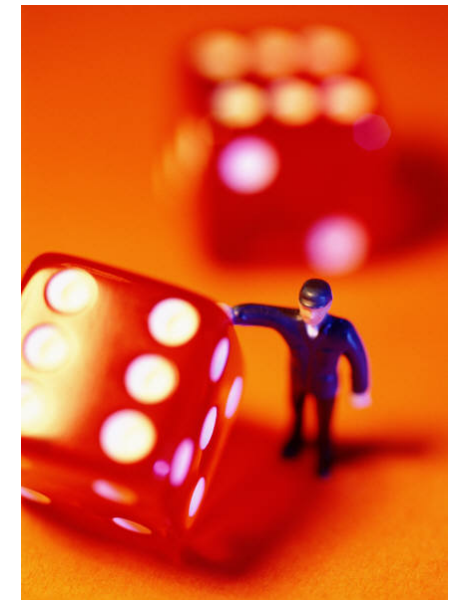
- Typ av standard: Guideline
- Innehåll: Beskriver program för mätning av ISMS och sammanställning av mätpunkter
- Beskriver VAD som ska mätas men INTE hur!
- Status: 3rd CD (Committe Draft) ISO/IEC 27004
- Beräknas bli klar under 2009





ISO/IEC 27005 - Information security risk management

- Typ av standard: Guideline
- Innehåll: Innehåller fördjupande information rörande användningen av riskanalyser och riskhantering i ett ISMS.
- Status: FDIS, Final Draft International Standard
- Kommer att ges ut under 2008!





ISO/IEC 27006 - Requirements for the accreditation of bodies providing certification of information management systems

- Typ av standard: Requirements
- Krav för certifieringsorgan som ska certifiera ISMS, tilläggskrav till ISO 17021 och ISO/IEC 27001
- Status: Utgiven 2007-03-01





ISO/IEC 27007 - Auditor ISMS guidelines

- Typ av standard: Guideline
- Innehåll: Komplettering till ISO 19011 (revision av ledningssystem) vad gäller revision av ISMS (intern eller extern).
- Status: New Work Item (NWI), 1st Working Draft (WD)





ISO/IEC 27011- Information security management guidelines for telecommunications

- Typ av standard: Guideline, Sector Specific
- Innehåll: Anpassad version av ISO/IEC 27002 med specifika tillägg för företag inom Telekom
- Ursprungligen framtagen som ITU-T X.1051
- Status: FDIS, Final Draft International Standard
- Kommer att ges ut under 2008!





Nya standardprojekt "Study Periods"





"ISO/IEC 27008" ISMS Technical Audit/Verification

- Typ av standard: Guideline
- Innehåll: Stöd för teknisk verifiering/revision av implementering av ISMS i IT-miljö
- Utvecklingen drivs huvudsakligen av Sverige+Japan
- Status: Study Period





"ISO/IEC 2703X" - ISMS standard for automotive industry

- Typ av standard: Guideline, Sector Specific
- Innehåll: Anpassad version av ISO/IEC 27002 med specifika tillägg för företag som verkar inom Automotive
- Status: Study Period





ISO/IEC JTC1 SC 27 WG 1

Information Security Road Map 2007-12-05

<u>Ongoing projects in SC27 WG1</u>	Oct 2007	April 2008	Oct 2008	April 2009	Oct 2009	April 2010	Oct 2010	April 2011
Information security management systems -- Fundamentals and vocabulary (IS 27000)	4th Committee Draft – April 2007 (FREE!)							
ISO/IEC 27001 – Information security management systems – Requirements (ISO/IEC 27001)	Published 15 October 2005							
ISO/IEC 27002 (17799) – Code of Practice for Information Security Management	Published 2005, transition to ISO/IEC 27002 July 2007							
IS 27003 – Information security management systems implementation guidance	4th Working draft– April 2008 (Swedish Editor!!)							
IS 27004 – Information security management measurements	3rd Committee Draft April 2008							
IS 27005 – Information security risk management	FDIS Final Draft International Standard - April							
IS 27006 – Requirements for the accreditation of bodies providing certification of information management systems	Published 1 March 2007							
IS 27007 Auditing	1st WD April 2008							
“IS 27008” ISMS Technical Auditing?	Study Period, New work item – April 2008					Commence–April 2008?		
IS 27011	Information security management guidelines for telecommunications					FDIS – April 2008		



Sector Specific Standards!

Telekom ITU-T X.1051



ISO/IEC 27011

World Lottery Association



ISO/IEC 2703X

Hälsa- och sjukvård ISO27799



ISO/IEC 2703X

Bilindustri



ISO/IEC 2703X

Samtliga bygger på ISO/IEC 27002 med vidareutvecklade branschspecifika tillägg!





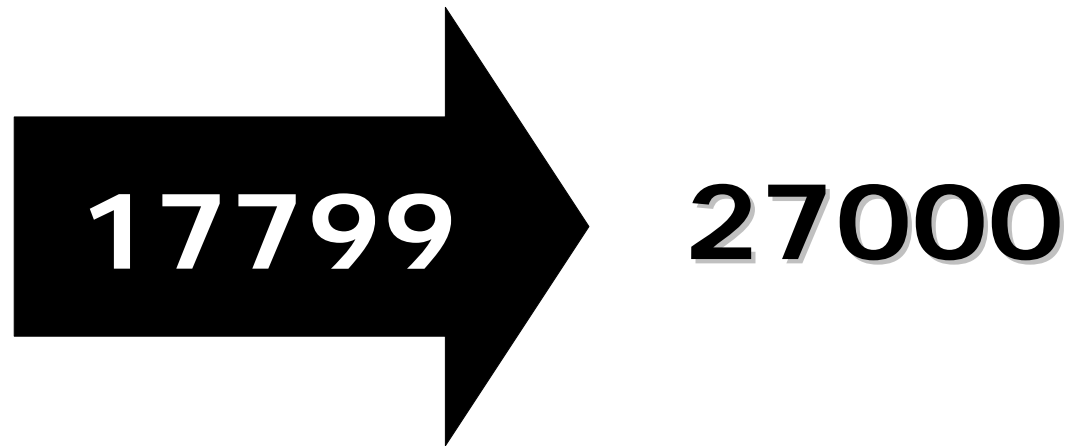
Översyn av ISO/IEC 27001 och ISO/IEC 27002!

- Bägge standarderna har nu några år på nacken
- Översynsarbete lär börja under 2008 eller 2009
- Framtagande av större förändringar eller helt nya koncept tar LÅNG tid!
- Slutsats: Det är dags att sätta igång under 2008 med att ta fram Svenska synpunkter och förslag på omarbetningar av ISO/IEC 27001 och 27002
- För deltagande, tag kontakt med Bengt Rydstedt, SIS (bengt.rydstedt@sis.se)





Nu är det slut!





ISO 27000-SERIEN
för informationssäkerhet