

Internetdagarna

24-25 oktober 2006, Rica Talk Hotel vid Stockholmsmässan **2006**

Spårbarhet och Koncernsäkerhet

Sarbanes-Oxley i ett
industriföretag



Åke Wedin

Senior IT Audit Project Manager, CISA, CISSP
Group Internal Audit IT
Member of IIA, ISACA, (ISC)², RCK



ABB AB

Kopparbergsvägen 2
SE-721 83 Västerås, Sweden

Phone: +46 (0)21 325846

Fax: +46 (0)21 140212

Mobile: +46 (0)70 6304000

e-mail: ake.wedin@se.abb.com

Sarbanes-Oxley i ett industriföretag

-  - ett industriföretag !
- Vad är Sarbanes-Oxley, eller “SOX” ?
- Införande av kontrollmekanismer
 - Erfarenheter, test,
 - Finns det några verktyg ?



Sarbanes-Oxley i ett industriföretag

-  - ett industriföretag !

- Vad är Sarbanes-Oxley, eller “SOX” ?
- Införande av kontrollmekanismer
 - Erfarenheter, test,
 - Finns det några verktyg ?



Fakta om ABB

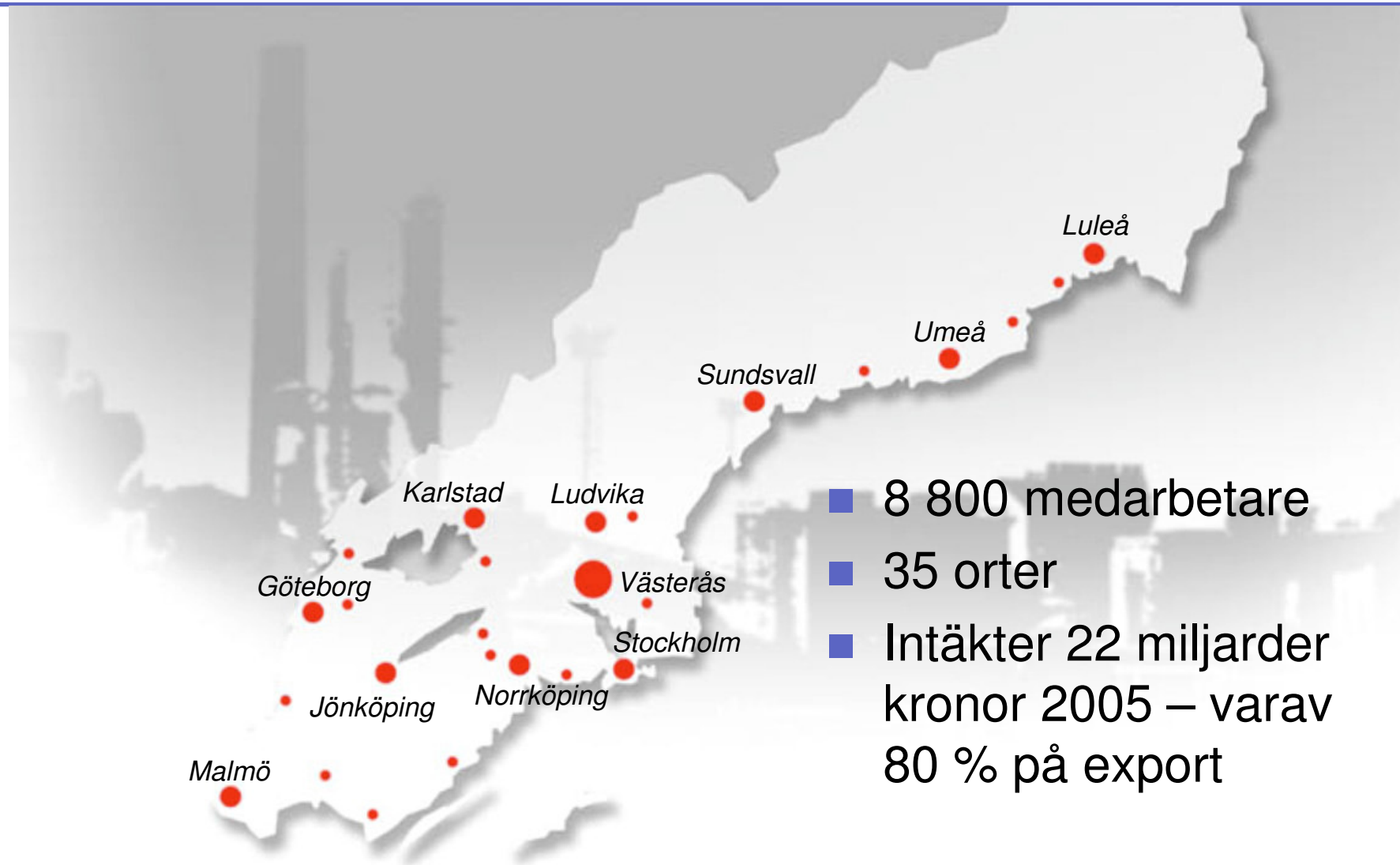


Världsledande inom kraft- och automationsteknik

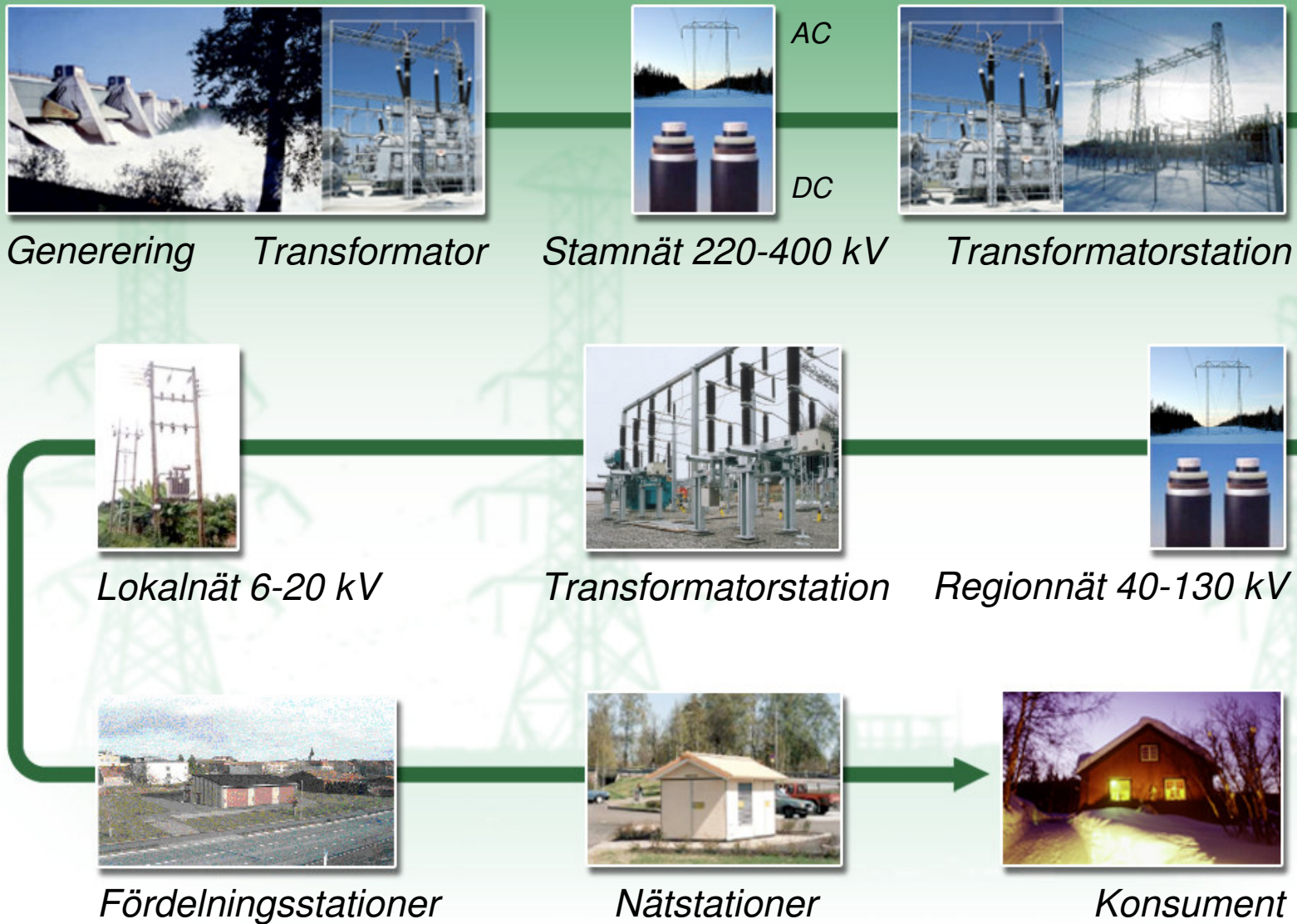
- Huvudkontor i Zürich, Schweiz
- Ungefär 104 000 medarbetare i 100 länder
- Orderingång 2005: 23,6 miljarder USD
Intäkter 2005: 22,4 miljarder USD



ABB Sverige



Kraft – från generering till konsument



Sarbanes-Oxley i ett industriföretag

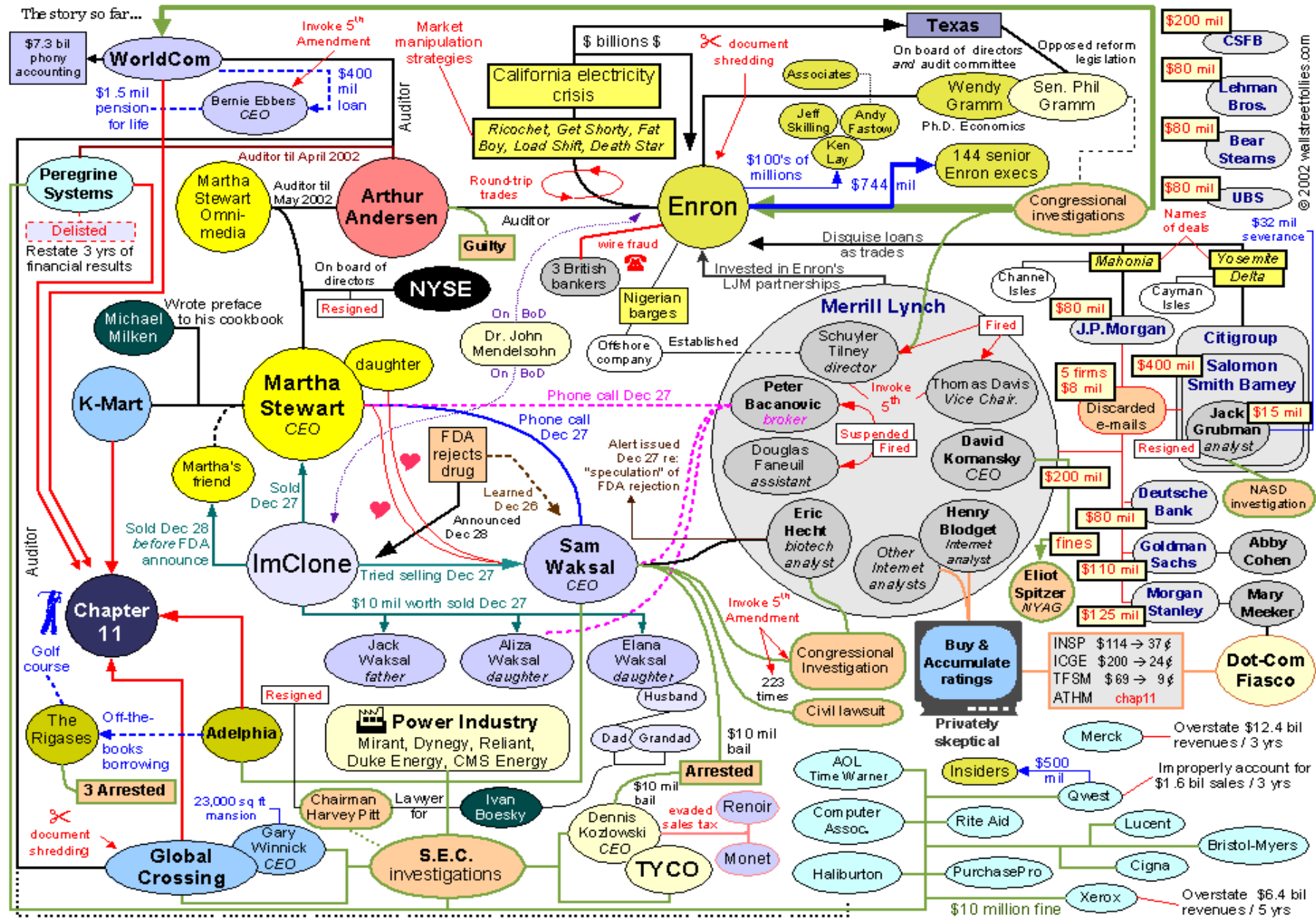
-  - ett industriföretag !

- Vad är Sarbanes-Oxley, eller “SOX” ?

- Införande av kontrollmekanismer

- Erfarenheter, test,
- Finns det några verktyg ?

Bakgrunden till Sarbanes-Oxley Act 2002 - Enronskandalen



Sarbanes-Oxley Act 2002, eller "SOX" – syftet

- Syftet med lagen är primärt att bolag noterade på NYSE eller Nasdaq-börserna skall införa ett regelsystem för intern kontroll för att återställa allmänhetens förtroende för stora börsnoterade bolag efter den rad av företagsskandaler som inträffat i USA
- Säkerställa att den finansiella rapporteringen är tillförlitlig
- Hindra eller försvåra avsiktliga fel eller bedrägerier i redovisningen



United States Senator

Paul S. Sarbanes

from Maryland



Congressman
Michael G. Oxley
Fourth Ohio District

SOX – Hur kommer IS/IT in i bilden

- Finansiell rapportering – Informationshantering
- System- och Informationssäkerhet är en förutsättning för att säkerställa den finansiella rapporteringen

Vad innebär SOX för ett företags ledning

- Ledningen måste kunna demonstrera att man har ett fungerande ramverk på plats för att säkerställa riktigheten / tillförlitligheten i den finansiella rapporteringen (*kräver **spårbarhet***)
- Vilket då inkluderar:
 - Att kunna demonstrera att man upprätthåller en ändamålsenlig säkerhet i de informationssystem och den infrastruktur som stödjer den finansiella rapporteringen
 - system som processar, lagrar, överför finansiell information
- Långtgående krav och personliga ansvar åläggs nu ledningen för att upprätthålla en betryggande informationssäkerhet

Straffskalan – ett mått på allvarlighetsgraden

NYA BENHÅRDA REGLER

■ Straffskala för olika brott i USA.

Rymning	1–2 år
----------------	--------

Kidnappning	3–5 år
--------------------	--------

Mord av andra graden	11–14 år
-----------------------------	----------

FALSKT SARBANES-OXLEY-INTYGANDE	10–20 år
--	----------

Flygplanskapning	20–25 år
-------------------------	----------

Vilka aspekter på informationssäkerhet ligger i SOX fokus ?

- **Integritet** Ja, informationens riktighet och skydd mot otillbörlig förändring är fokus
- **Tillgänglighet** Till viss del
 - Finansiell information skall (oförvanskat) kunna göras tillgänglig, men tiden det tar att få fram informationen är inte kritisk
- **Konfidentialitet** Ytterst begränsat

Regelverk liknande SOX ("SOX-inspirerade")

- EuroSOX (ett uppdaterat Direktiv 8) från 2008
- Den nya Svenska Koden för Bolagsstyrning
- M.fl. . . .

Vilka företag påverkas ?

- I första hand påverkas amerikanska börsnoterade bolag
- Dessutom påverkas utländska företag som är noterade på amerikanska börser
 - (t.ex. ABB, Ericsson, Electrolux m.fl.)
- Företag som gör affärer med USA kan indirekt komma att påverkas

Externrevisorernas förändrade rapporteringsskyldighet

- Före SOX – skyldighet att rapportera
 - Revisorernas bedömning av företagets finansiella redovisning
- Efter SOX – skyldighet att rapportera
 - Revisorernas bedömning av företagets finansiella redovisning - som tidigare . . .

Dessutom, nya SOX-krav från 2006 och framåt:

- Bedömning av företagslednings eget intygande när det gäller upprätthållandet av interna kontroller för att säkerställa riktigheten i den finansiella rapporteringen
- Revisorernas egen bedömning av företagets interna kontroller för att säkerställa riktigheten i den finansiella rapporteringen



Externrevisorernas förändrade rapporteringsskyldighet

- Före SOX – skyldighet att rapportera
 - Revisorernas bedömning av företagets finansiella redovisning
- Efter SOX – skyldighet att rapportera
 - Revisorernas bedömning av företagets finansiella redovisning - som tidigare . . .

Dessutom, nya SOX-krav från 2006 och framåt:

- Bedömning av företagslednings eget intygande när det gäller upprätthållandet av interna kontroller för att säkerställa riktigheten i den finansiella rapporteringen
- Revisorernas egen bedömning av företagets interna kontroller för att säkerställa riktigheten i den finansiella rapporteringen

Sarbanes-Oxley i ett industriföretag

- **ABB** - ett industriföretag !
- Vad är Sarbanes-Oxley, eller “SOX” ?

- **Införande av kontrollmekanismer**

- Erfarenheter, test,
- Finns det några verktyg ?

Ett ramverk för SOX Intern Kontroll

- ***Implementation kit for Dummies***
- Identifiera SOX relevanta (finansiella) processer
- Design och dokumentation av processer och kontroller
 - Kontroller skall kunna efterlämna bevis
- Implementation av överenskomna processer/kontroller
 - Efter implementationsdatum skall processer vara operativt i drift och genomförda kontroller efterlämna bevis (***spårbarhet***).
- Upprätta detaljerade testplaner, för att genom test kunna verifiera att processer / kontroller fungerar och efterlevs
- Genomföra tester (t.ex. årligen)
- Rapportera
 - brister – måste åtgärdas – testa igen
 - klartecken – rapportera uppåt i näringskedjan
- Stödjande verktyg är en nödvändighet

Ett ramverk för SOX Intern Kontroll

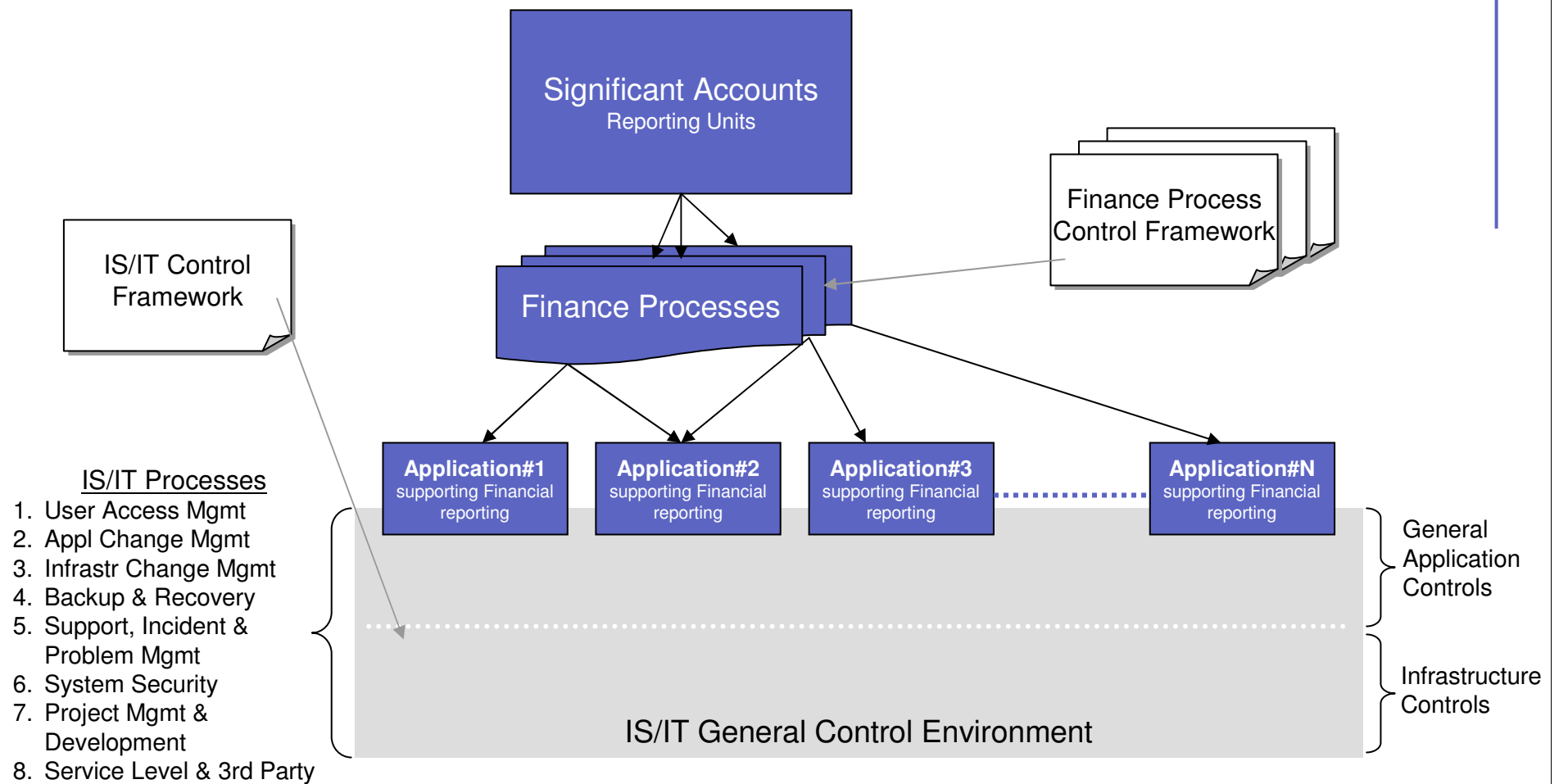
■ *Implementation kit for Dummies*

- Identifiera SOX relevanta (finansiella) processer
- Design och dokumentation av processer och kontroller
 - Kontroller skall kunna efterlämna bevis
- Implementation av överenskomna processer
 - Efter implementationsdatum skall processer vara i drift och genomförda kontroller efterlämnas bevis (spårbarhet).
- Upprätta detaljerade testplaner, för att genomföra test och verifiera att processer / kontroller fungerar och efterlämnas bevis (spårbarhet).
- Genomföra tester (t.ex. årligen)
- Rapportera
 - brister – måste åtgärdas – testa igen
 - klartecken – rapportera uppåt i näringskedjan
- Stödjande verktyg är en nödvändighet

När det kommer till IS/IT

- Identifiering av applikationer och infrastruktur som understödjer dessa processer
 - d.v.s. behandlar, lagrar eller överför "finansiell information"
- Design, dokumentation . . .
- Implementation . . .
- Testplaner . . .
- Genomföra tester ... o.s.v.

Ett ramverk för SOX Intern Kontroll



Ett ramverk för SOX Intern Kontroll

■ Erfarenheter

- Tröghet i förändringsprocesser
- Förståelsen för begreppet **kontroll** är inte medfött . . .
- När processer och kontroller är implementerade är man inte ens halvvägs igenom projektet . . .

Då gäller det att se till att alla medarbetare gör det vi dokumenterat att vi skall göra !

- Testresultaten blir i många fall brutala påminnelser om att vi varit okunniga, slarvat eller tagit ”praktiska” genvägar

Ett ramverk för SOX Intern Kontroll

■ Erfarenheter

- Tröghet i förändringsprocesser
- Förståelsen för begreppet **kontroll** är inte medfött . . .
- När processer och kontroller är implementerade är man inte ens halvvägs igenom projektet . . .

Då gäller det att se till att alla medarbetare gör det vi dokumenterat att vi skall göra !

- Testresultaten blir i många fall brutala påminnelser om att vi varit okunniga, slarvat eller tagit ”praktiska” genvägar

Spårbarhet



Sarbanes-Oxley i ett industriföretag

-  - ett industriföretag !
- Vad är Sarbanes-Oxley, eller “SOX” ?

- Införande av kontrollmekanismer

- Erfarenheter, test,
- Finns det några verktyg ?

Internet, Verktyg, SOX ?

- Vad finns det för behov av verktyg ?
- Är man en händig snickare så kan man lösa det mesta med en hammare



Behov av verktyg – underlag till “försäkran”

- Från 2006 och framåt skall företagslednings kunna leverera en försäkran angående upprätthållandet av interna kontroller för att säkerställa riktigheten i den finansiella rapporteringen
- Antingen Ja eller Nej
- Som sedan skall bedömas / kommenteras av revisorerna

		Företaget	
		Ja	Nej
Revisor	Ja	(a)	(b)
	Nej	(c)	(d)



Behov av verktyg

- Försäkran skall vara baserat på trovärdigt underlag
 - Företagsledningen skall kunna redovisa hur man kommit fram till sitt ställningstagande.
- Det är ett tungt ansvar

FALSKT SARBANES-OXLEY-INTYGANDE 10-20 år

- Kan man som de yttersta ansvariga (koncernens CEO och CFO) delegera detta hot ??
- Man måste göra den underliggande ledningskadern personligen ansvariga för:
 - inte bara "sin del" av den finansiella rapporteringen
 - även intyga att "motsvarande delmängd" av den interna kontrollen fungerar
- Det behövs ett verktyg för att hantera underlag och "sign-off" att kontroller är på plats och fungerar





Nätet [Bilder](#) [Grupper](#) [Kategori](#)

Internet Security Tool

Sök

[Avancerad sökning](#)
[Inställningar](#)

Sök: ☒ webben ☐ sidor på svenska ☐ sidor från Sverige

Nätet

Resultat **1 - 20** av ungefär **181 000 000** vid sökning efter

[Center for Internet Security - Standards](#)

The Center for **Internet Security** The Center for **Internet Security** · Site Map · Contact Us ...
CIS Benchmarks/Scoring **Tools** - Now available, free of charge! ...

www.cisecurity.org/ - [23k](#) - [Cachad](#) - [Liknande sidor](#)

[Internet/Network Security on About.com](#)

Sign Up Now for the **Internet / Network Security** newsletter! ... Anti-spyware has become
somewhat of a standard **security tool** that most people run on their ...

netsecurity.about.com/ - [35k](#) - [Cachad](#) - [Liknande sidor](#)

[Internet Security: The Computer Security Tool for your Internet ...](#)

The Computer **Security Tool** has recommendations & useful information to keep your
computer secure against **internet security** threats.

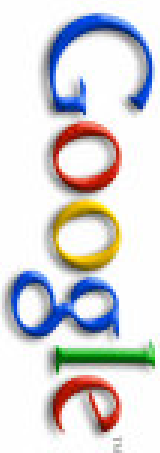
www.computersecuritytool.com/ - [12k](#) - [Cachad](#) - [Liknande sidor](#)

[Microsoft Security Home Page](#)

Tools and Tips. **Security** for Home Computers ... Learn about the Microsoft **Security**
Response Center (MSRC). ·, Read the MSRC blog ...

www.microsoft.com/Security/ - [25k](#) - [Cachad](#) - [Liknande sidor](#)

[Home of Gibson Research Corporation](#)



Nätet [Bilder](#) [Grupper](#) [Kategori](#)

SOX control tool

Sök

[Avancerad sökning](#)
[Inställningar](#)

Sök: ☒ webben ☐ sidor på svenska ☐ sidor från Sverige

Nätet

Resultat **1 - 10** av ungefär **11 700 000** vid sökning

[Reuters: Graduate Opportunities: SOX Project and Control Co-ordinator](#)

Development of **SOX control** compliance Reports using the **SOX tool** and controls data loaded to automate the production of **SOX** quarterly sign-off certificates. ...

[about.reuters.com/careers/graduate/opportunities/internships/jobspecs/soxprojectspec.asp](#) - 12k - [Cachad](#) - [Likhande sidor](#)

[Sidebar: What's a Sarbanes-Oxley Control?](#)

April 10, 2006 (Computerworld) -- In **Sarbanes-Oxley**, a **control** is a practice established ... Download Microsoft's latest Data Protection Management **tool** ...

[www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=110292](#) - 113k - [Cachad](#) - [Likhande sidor](#)

[Paisley Consulting to Co-Sponsor Sarbanes-Oxley Control Deficiency ...](#)

Sept. 14, 2006 New Version of Leading Audit Automation **Tool** is Now Available ... Paisley Consulting to Co-Sponsor **Sarbanes-Oxley Control** Deficiency Training ...

[www.paisleyconsulting.com/website/pwweb.nsf/wv_ContentByDocID/DCOS-6A5Q98?OpenDocument](#) - 57k - [Cachad](#) - [Likhande sidor](#)

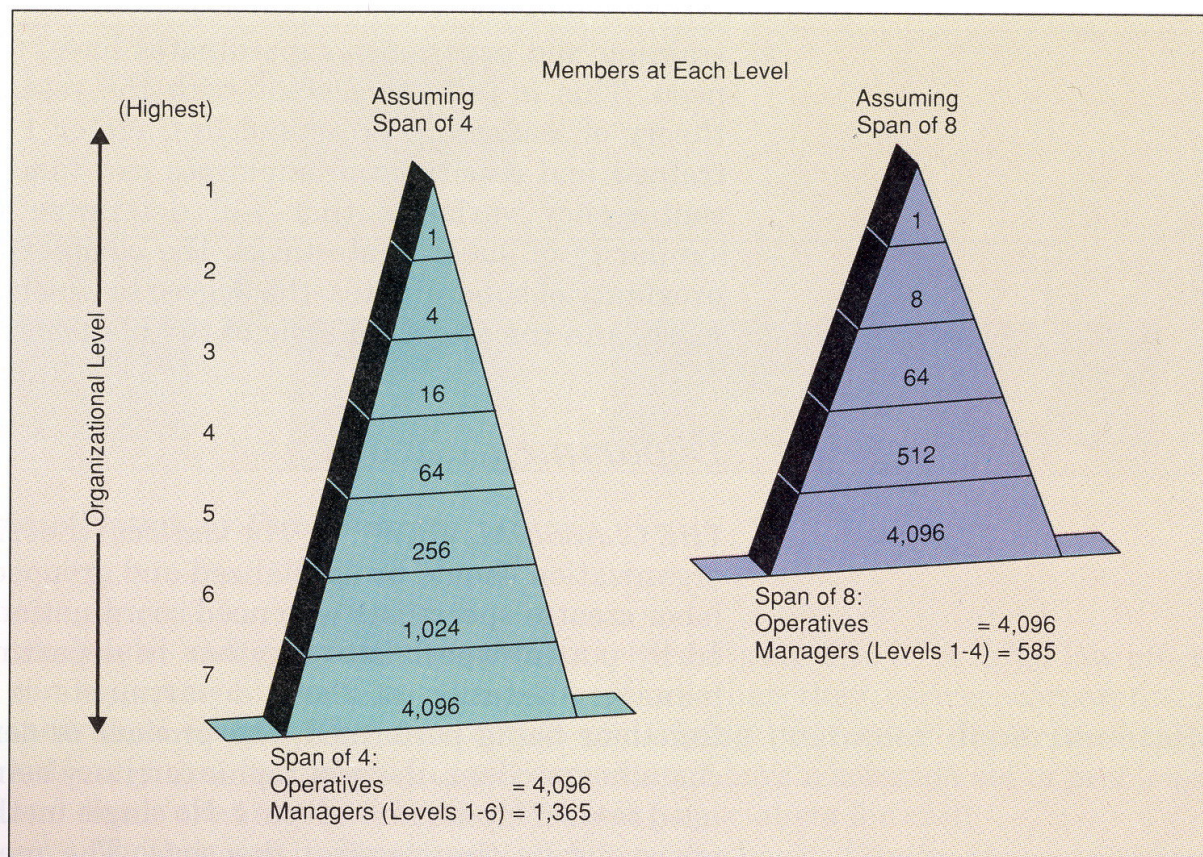
[Paisley Consulting Sponsors Sarbanes-Oxley Control Deficiency ...](#)

14, 2006 New Version of Leading Audit Automation **Tool** is Now Available ... Paisley Consulting Sponsors **Sarbanes-Oxley Control** Deficiency Training Workshops ...

[www.naislawconsulting.com/website/pwweb.nsf/wv_ContentByDocID/DCOS-6A5Q98MM?](#)

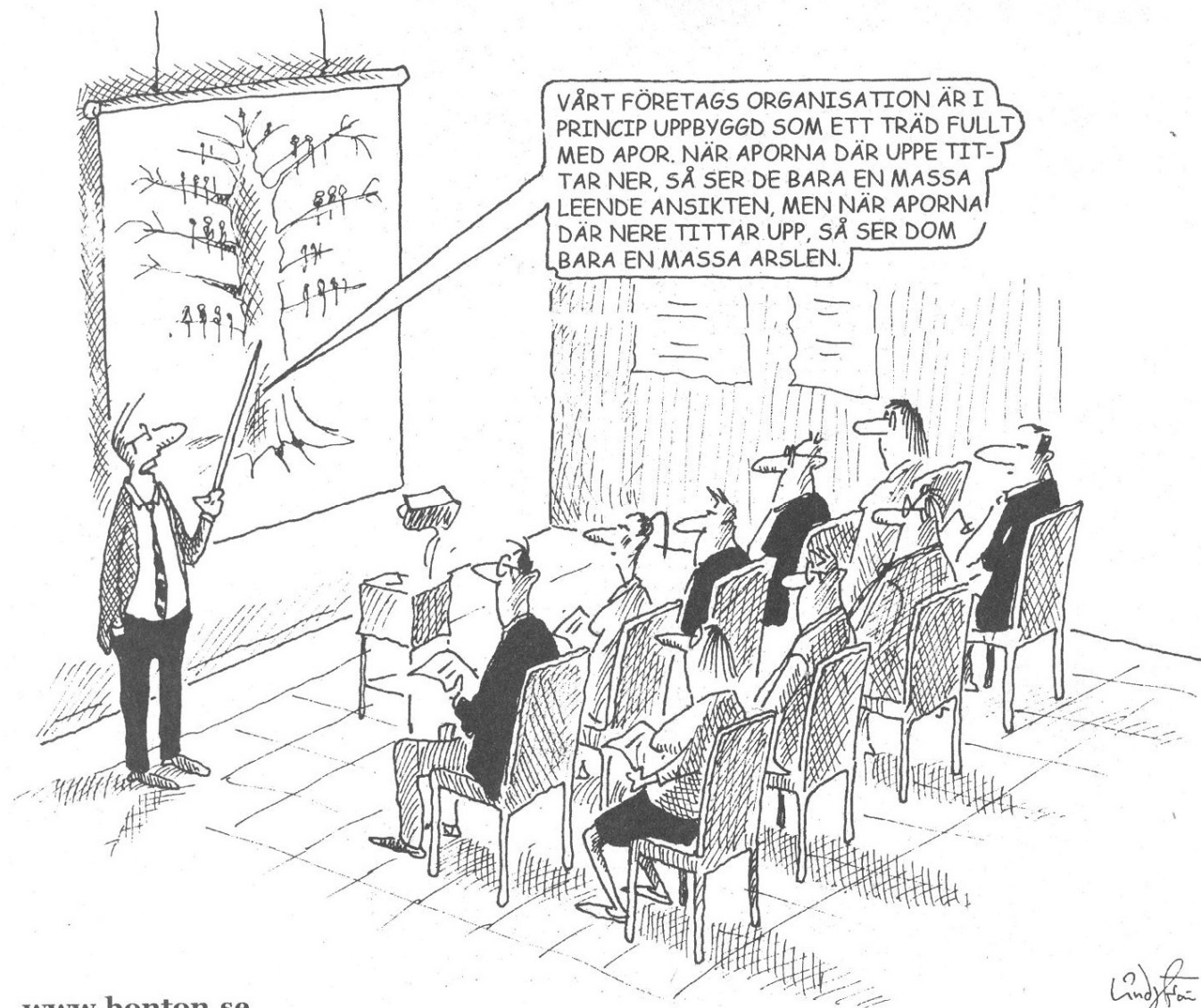
Verktyg för att hantera underlag och "sign-off"

- Betydelsen av organisationens djup
- ABB-medarbetare
 - 8800 i sverige
 - 104000 totalt
- Även med en genomsnittlig enhetsstorlek på 10 blir det 6 nivåer



Organisationens djup

- Hur kan man skapa trovärdighet i “rapporteringen uppåt” ?



www.bonton.se

Verktygen

- Det viktigaste ”verktyget” är medarbetarna som medverkar operationellt i processerna !!
 - Att göra rätt och inte slarva eller skapa genvägar . . .
- Verktyg för att samla underlag inför slutgiltig ”sign-off” av koncernens CEO och CFO
- Underlag i form av
 - Dokumentation av ”implementerat kontrollramverk”
 - Godkända testplaner
 - Godkännande av Testare
 - Godkännande av kombinationen Testare och Enhet/Process att testa
 - Genomförda test
 - Analys av testresultat – uppfyller processen som sådan (med kontroller) uppställda krav på intern kontroll ?
 - ”Sign-off” av testresultat av
 - Processägare (normalt lokal IT-ansvarig)
 - Lokal ledning (enhetens Chef och Controller)
 - Landsledning (CEO och CFO)



Verktygen

- Det viktigaste ”verktyget” är medarbetarna som medverkar operationellt i processerna !!
 - Att göra rätt och inte slarva eller skapa genvägar . . .
- Verktyg för att samla underlag inför slutgiltig ”sign-off” av koncernens CEO och CFO
- Underlag i form av
 - Dokumentation av ”implementerat kontrollramverk”
 - Godkända testplaner
 - Godkännande av Testare
 - Godkännande av kombinationen Testare och Enhet/Process att testa
 - Genomförda test
 - Analys av testresultat – uppfyller processen som sådan (med kontroller)
 - ”Sign-off” av testresultat av
 - Processägare (normalt lokal IT-ansvarig)
 - Lokal ledning (enhetens Chef och Controller)
 - Landsledning (CEO och CFO)

Spårbarhet



Verktygen

- Det viktigaste "verktyget" är medarbetarna som medverkar operationellt i processerna !!
 - Att göra rätt och inte slarva eller skapa genvägar . . .
- Verktyg för att samla underlag inför slutgiltig "sign-off" av koncernens CEO och CFO
- Underlag i form av
 - Dokumentation av "implementerat kontrollramverk"
 - Godkända testplaner
 - Godkännande av Testare
 - Godkännande av kombinationen Testare och Enhet/Process att testa
 - Genomförda test
 - Analys av testresultat – uppfyller processen som sådan (med kontroller) uppställda krav på intern kontroll ?
 - "Sign-off" av testresultat av
 - Processägare (normalt lokal IT-ansvarig)
 - Lokal ledning (enhetens Chef och Controller)
 - Landsledning (CEO och CFO)
- Sedan är det dags för slutgiltig "sign-off" av koncernens CEO och CFO

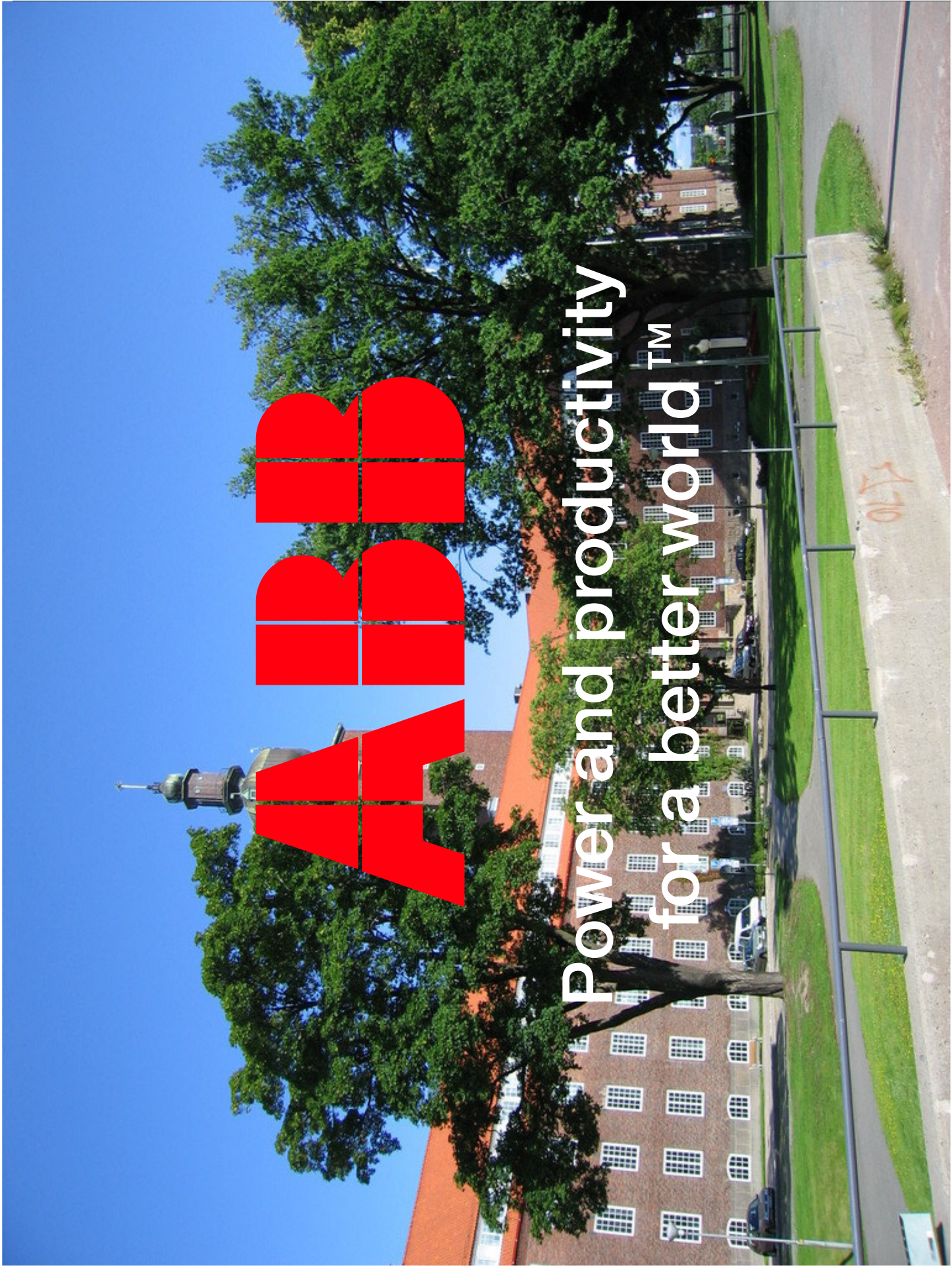
Spårbarhet



Sarbanes-Oxley i ett industriföretag

-  - ett industriföretag !
- Vad är Sarbanes-Oxley, eller “SOX” ?
- Införande av kontrollmekanismer
 - Erfarenheter, test,
 - Finns det några verktyg ?
- Tack för ordet – Frågor ??





ABB

Power and productivity
for a better world™

ABB Sverige – Nyckeltal 2005



Power Products

Intäkter:
5 800 MSEK
Medarbetare:
2380



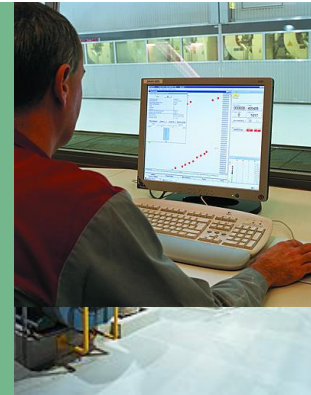
Power Systems

Intäkter:
5 900 MSEK
Medarbetare:
1500



Automation Products

Intäkter:
3 700 MSEK
Medarbetare:
1690



Process Automation

Intäkter:
4 090 MSEK
Medarbetare:
1490



Robotics

Intäkter:
4 550 MSEK
Medarbetare:
1100

varav Service:

intäkter: 1 130 MSEK, Medarbetare: 720

