# Livet med sikkerhed

Bent Poulsen

# Tilbageblik

- Mainframe
  - Central datalagring og -administration
  - Central sikkerhedsadministration
  - Central netværksadministration
  - Terminaladgang
- Decentral/distribueret edb-anvendelse
  - + decentral lagring, datatransmission…
- Modem'er bliver "hver mands eje"
  - + bagdøre, uautoriseret anvendelse…
- Internet => +++
- Outsourcing => +++
- Cloud => +++
- Håndholdte enheder / BYOD => +++

- Uanset platform
  - Krav om sikkerhed er ledelsens ansvar
    - Politikker
    - Bestemmelser
    - Forretningsgange

    - Risici >< kontroller
    - Dokumentation
    - Rapportering
    - Opfølgning

# Den spæde start for sikkerheden

- Edb-afdelingen havde teten
- Brugerne levede på edb-afdelingens nåde
- Edb-afdelingen ejede systemerne
- Sikkerhed var alene relateret til driftssikkerhed

- Fysiske dokumenter var alligevel de vigtigste i edb-alderens begyndelse

- Det blev revisorerne, der udfordrede de autonome edb-afdelinger
  - Revisionsvejledninger
  - Revisionsstandarder
  - Revisionsrapporter og –protokoller

- Ledelsen indså behovet for at ændre situationen og blive proaktive, så det ikke længere var revisorerne (alene), der satte dagsordenen.

# Generelle edb-kontroller

- FSRs Revisionsvejledning nr. 14
- Revisors praktiske anvendelse af FSRs Revisionsvejledning nr. 14
- EDB-revision (Heilbuth & Tjagvad)
- Bogføringslov m.v.

# Generelle edb-kontroller – V14

- Edb-politik/-strategi
- Organisatoriske forhold
- Systemudvikling/-vedligeholdelse
- Driftsafvikling (+ adgang til systemer og data)
- Dokumentation af systemer, metoder og procedurer
- Fysisk sikkerhed
- Sikkerhedskopiering og nødplaner

# System-, data- og driftssikkerhed

- Systemsikkerhed
  - Resultatet af de foranstaltninger, der sikrer
    - pålidelige systemer
    - systemer og edb-udstyr er dokumenteret, godkendt, aftestet og sikret mod ødelæggelse
- Datasikkerhed
  - Resultat af de foranstaltninger, der sikrer
    - pålidelig registrering, opbevaring og brug af data
    - ændring, sletning eller brug af data er godkendt og dokumenteret
- Driftssikkerhed
  - resultatet af de foranstaltninger, der sikrer
    - rettidig og pålidelig gennemførelse af databehandlingen
    - håndtering af fejl og mangler
    - kontinuerlig databehandling

# Generelt om trusler/scenarier

| Hændelse | | Brutto risiko | Rest risiko |
|---|---|---|---|
| Utilstrækkeligt personale | | | |
| Manuelle fejl | | | |
| Systemer og data | Datalækage | | |
| | Systemnedbrud | | |
| | Hardware nedbrud | | |
| | Tab af data | | |
| Eksterne angreb | IT angreb | | |
| | Terror | | |
| Domicil | Ubrugeligt | | |
| | Ikke adgang | | |
| | Strømsvigt | | |
| Nye produkter og services | | | |
| Netværk m.v. | Web-adgang ikke tilgængelig | | |
| | Netværk ikke tilgængeligt | | |

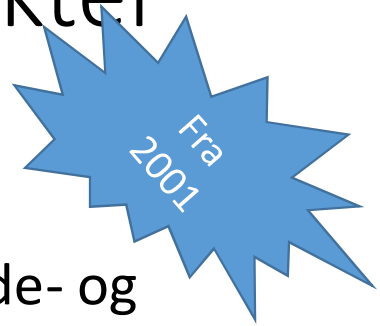
# Lidt om udviklingen i Danmark

- CISA-certificering
  - Blev første ”uddannelse” på området omkring informationssikkerhed
- God edb-skik
  - FSR
  - EDPAA (nu ISACA)
  - IIA
- God edb-skik og revisor
  - (som ovenfor)

- ESL-uddannelsen
  - Institut for Datasikkerhed
  - Længere kursusforløb
  - Flere eksaminer + hovedopgave
  - (multiple choice eksamen blev senere erstattet af CISM)
  - Rådgivende uddannelsesudvalg

  - Varetages nu af ESL-foreningen og Ezenta

# IT-sikkerhed – udfordringens karakter




- Globalisering
- Krav om åbenhed, samarbejde og alliancer
- Øget regulering – lovgivning, standarder, kunde- og ejerkrav.
- Medierne bevågenhed – tilgængelighed og privacy
- Krav om effektivitet
- Digital økonomi og øget anvendelse af Internet/netværks-teknologi
- Alle har adgang til alt …. og til alle
- Elektronisk, anonymt og 24x7
- Øget kompleksitet og udviklingstakt

# Sikkerheds målsætning


- *Ledelsen BØR benytte de nødvendige kontroller, mekanismer, værktøjer og overvågning der sikre at virksomheden kan :*
  - Autentificere identiteten af alle brugere af applikationer eller kommunikations forbindelser;
  - Beskytte trafikken imod modifikation, destruktion, opsamling;
  - Beskytte trafikken imod upassende eller unødvendig afsløring;
  - Sikre at virksomheden kan fortsætte driften på trods af teknologi fejl;
  - Kunne demonstrere for en uvildig part, at virksomheden kan gøre rede for alle forretningstransaktioner i detaljer;
  - Opdage afvigelser fra den forventede anvendelse, drift eller ”system opførsel” og betids foretage effektive og korrigerende handlinger

# Tillid eller ej

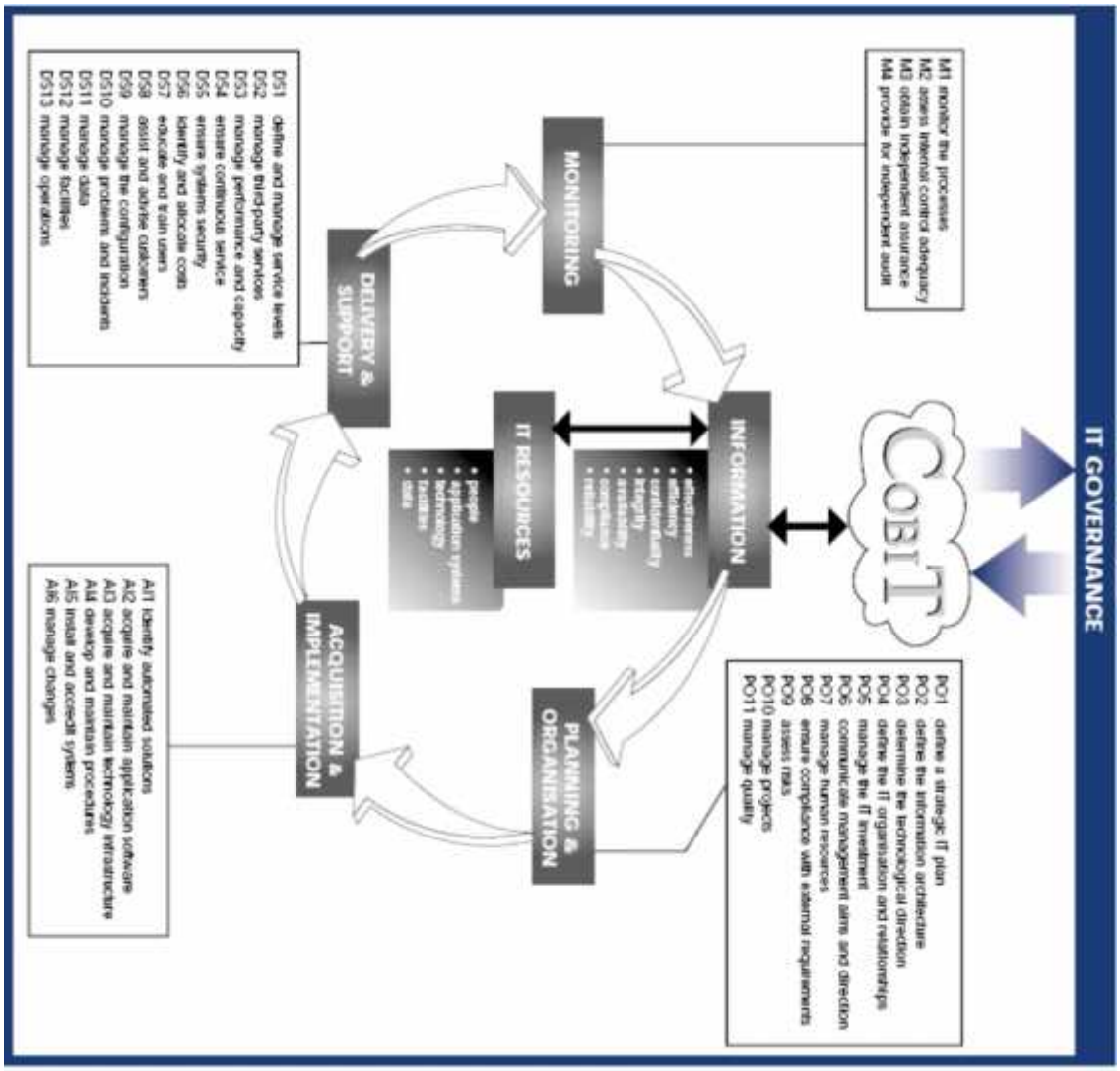
Fra 2002

| Tillid | Reaktion |
|---|---|
| Jeg stoler slet ikke på dig | Al adgang nægtes |
| Jeg tror kun du vil udføre harmløse aktiviteter | Kun adgang til offentligt tilgængelige informationer |
| Jeg ville stole på dig, hvis jeg kendte dig | Skaf identificerende information, derefter adgang til funktioner, som er tilgængelige for ”kendte” personer |
| Jeg ville stole på dig, hvis jeg kendte dig og din information kan verificeres | Skaf information – check off-line. Indtil bekræftet kun adgang som en af de ovenstående kategorier. |
| Jeg stoler på dig fordi jeg kender dig | Skaf identificerende information og sammenlign med lagret information |
| Jeg stoler på dig, fordi du har en bestemt status i systemet | Skaf information og sammenlign med lagret information om personen og om ”privilegeret” adgang |
| Jeg stoler på dig, fordi du har betalt for at blive ”stolt på” | Skaf information og sammenlign med lagret information om personen og betalingsstatus |
| Jeg stoler på dig, fordi jeg er en tillidsfuld (naiv) person, eller der ikke er nogen risiko | Lad alle gøre alting  |

# Security recommendations for e-Business

- Internet Security Task Force (ISTF):
  Focus on
  - authentication
  - privacy of information
  - detection of security events
  - defence of the corporate perimeter
  - intrusion detection
  - malicious content
  - access control
  - administration
  - incident response

Kilde: http://www.cai.com/press/2000/03/ebiz_taskforce.htm



# Hjælp fra myndighederne ex 1

# Hjælp fra myndighederne ex 2

## National Infrastructure Protection Center
## CyberNotes: 2001 Year End Summary

*Issue #2001-26* *December 31, 2001*

**CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.**

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, D.C., 20535.

# Hjælp fra myndighederne ex 3 (FT-afgørelse)

- Kontrolfunktioner kan kun i begrænset omfang outsources
- Ansvaret for kontrollernes gennemførelse kan ikke outsources
- Isolerede ledelseserklæringer til kontrol af leverandørens overholdelse af outsourcede virksomheders it-sikkerhedspolitik kan ikke erstatte deres egen kontrol
- Systemrevisionens erklæring vedrører den samlede data-, system- og driftssikkerhed
- Erklæringen vedrører datacentralens generelle it-sikkerhedsmæssige forhold, som ikke direkte kan kontrolleres ude fra de tilsluttede virksomheder
- Erklæringen kan ikke omfatte samtlige kontroller af overholdelsen af de tilsluttede PI'ers it-sikkerhedspolitik

# Økonomisk Ugebrev nr. 27 2003

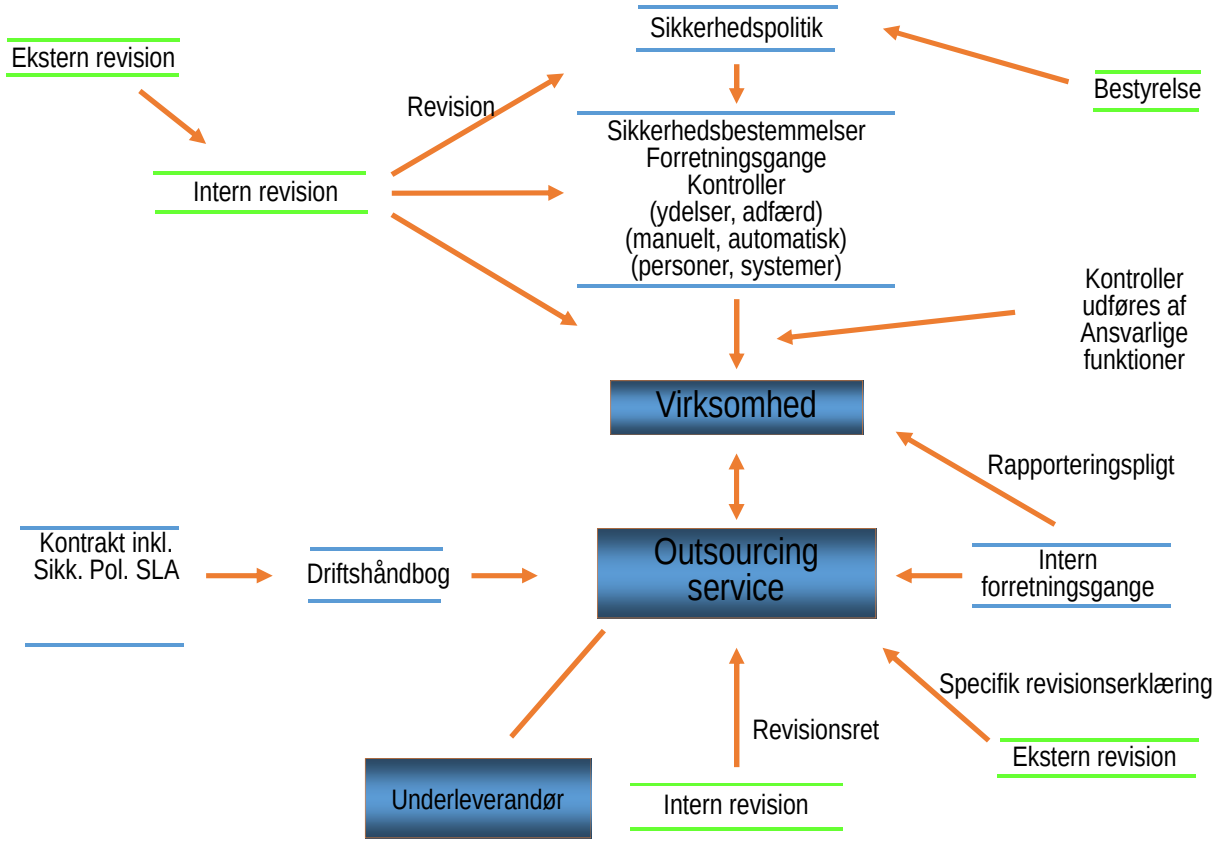

Karakter af marketingsgimmick
- laveste fællesnævner, kvalitetssikringen bliver sat efter

Partner Birgitte Mogensen, PwC

Man kan frygte, at mange af de penge, der bliver brugt på f.eks. ISO 9000 bliver smidt ud af vinduet

Professor Bøje Larsen, Handelshøjskolen

# Security compliance - overblik



# Risiko-kontrol matrix

- Risici
  - Oplistning af relevante risici
  - Afstemning med ejer
- Kontroller
  - Udpegning af egnede kontroller
  - Gennemgang af dokumentation og beskrivelser mv.
  - Afstemning med ejer
- Samlet overblik
  - Udækkede risici
  - Residuale risici
  - Overflødige kontroller / kompenserende kontroller

# Risici versus kontroller

| | Risici | | | | | | |
|---|---|---|---|---|---|---|---|
| **Kontroller** | R1 | R2 | R3 | R4 | R5 | R6 | R7 |
| K1 | 1 | 1 | | 1 | | | |
| K2 | 2 | | | | 2 | | |
| K3 | | | | | | | |
| K4 | | 3 | | | | 3 | |
| K5 | 2 | | | | 2 | | 2 |
| K6 | 1 | | | | 1 | 1 | |

Manglende kontrol

Nøgle-kontrol

Residual risiko ???

Risiko uden kontroller

Risiko med ringe kontroller

# ISA 315 Intern Control

## Internal control components

- The control environment
- The entity’s risk assessment process
- The information system, including related business processes
- Control activities
- Monitoring controls

# ISA 315 General IT Controls

Policies and procedures that support the effective functioning of application controls, and include

- Data centre and network operations
- System software acquisition, change and maintenance
- Access security
- Application system acquisition, development and maintenance

To deal with IT risks

- Reliance on inaccurate processing
- Unauthorised access to data
- IT personnel gaining inappropriate privileges
- Unauthorised changes
- Failure to make necessary changes
- Inappropriate manual intervention
- Potential loss of data
- Inability to access data

# ISA 315 Application Controls

Manual or automated procedures

- Ensure that transactions are
  - Authorised
  - Completely and accurately recorded and processed

- Typically operating at the business process level
- Relate to procedures used to initiate, record, process and report transactions etc.

# Ledelsesbekendtgørelsen

Bestyrelsens opgaver og ansvar

- IT-sikkerhedspolitik
  - Organisering af it-arbejdet, herunder funktionsadskillelse
  - Regelmæssig risikovurdering
  - Beskyttelse af systemer, data, maskinel og kommunikationsveje
  - Systemudvikling og vedligeholdelse af systemer
  - Driftsafvikling
  - Backup og sikkerhedskopiering
  - Beredskabsplaner, der indeholder målsætning og planer for genetablering af normal drift
  - Kvalitetssikring
  - Principper for implementering af politikken i uddybende retningslinjer
  - Forholdsregler i tilfælde af brud på it-sikkerhedspolitik og sikkerhedsregler
  - Overholdelse af relevant lovgivning
  - Rapportering, kontrol og opfølgning
  - Eventuelle dispensationer fra it-sikkerhedspolitikken

# Ledelsesbekendtgørelsen (2)

Direktionens opgaver og ansvar

- Sikre, at it-sikkerhedspolitikken efterleves
  - Ansvarsplacering og ejerskab
  - Overvågning af funktionsadskillelsen
  - Kontrol med opretholdelse af ønsket it-sikkerhedsniveau
  - Klassificering og prioritering af systemer og data
  - Systemer dokumenteres
  - Sikkerhedskopiering af systemer og data, herunder opbevaring af sikkerhedskopierne.
  - Tilstrækkelige it-ressourcer
  - Systemudvikling og afprøvning af nye og ændrede systemer sker betryggende
  - Test og anden kvalitetssikring
  - Ændringshåndtering og problemstyring
  - Adgangskontrol til systemer og data
  - Tilstrækkelig fysisk sikkerhed, herunder fysisk adgangskontrol
- Beredskabsplan – vedligeholdelse og test