Business Continuity & Resilience Services

Beredskab til iSeries

- For en sikkerheds skyld

Peter Nittegaard
IBM
IT-katastrofeberedskab

E-mail: peter_nittegaard@dk.ibm.com

Agenda

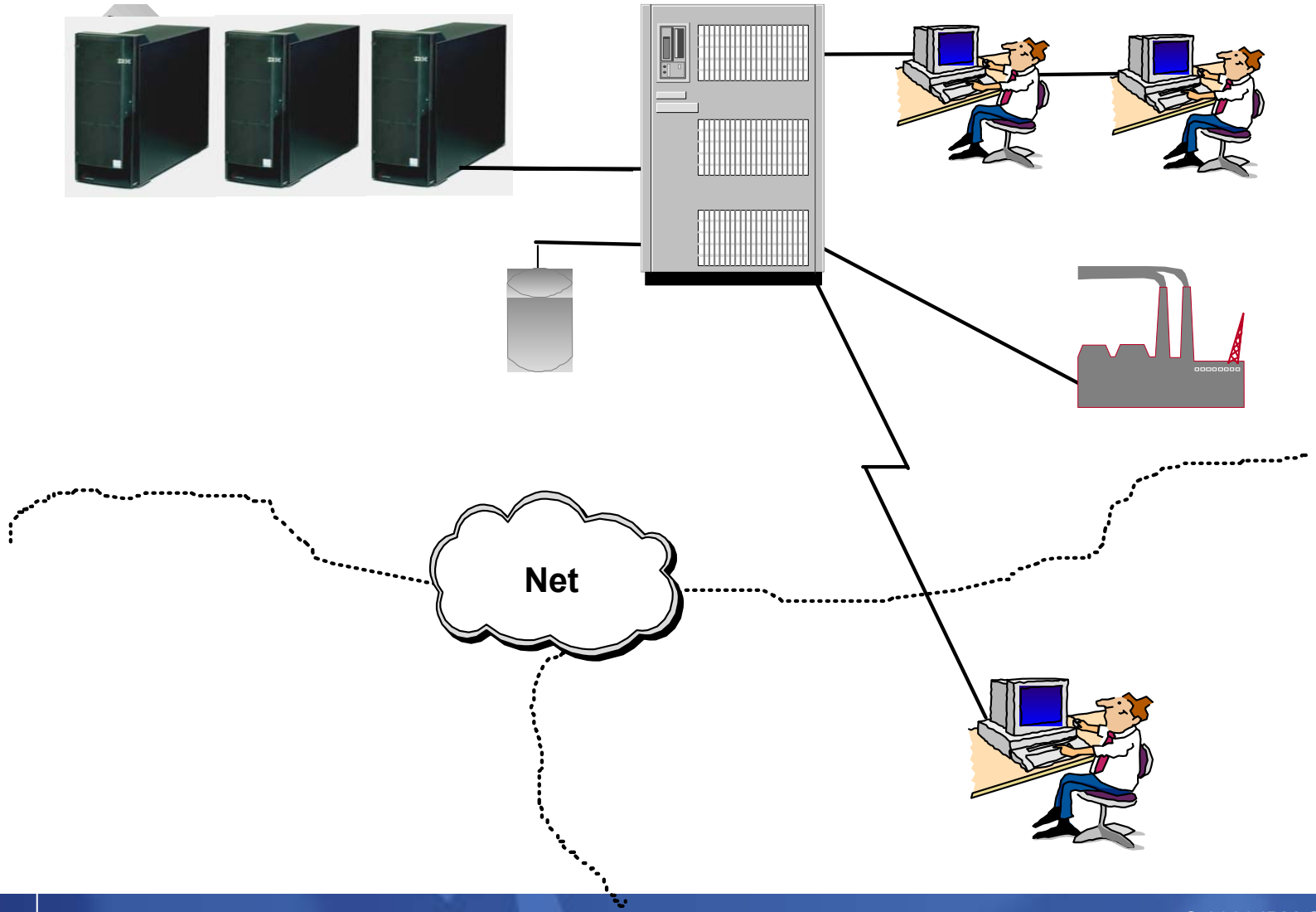
- **Hvorfor skal virksomheden have et beredskab**
- **Hvilke krav er der**
- **Hvilke muligheder**
- **Hvorfor skal man teste**
- **Hvordan kommer man i gang**

Hvorfor skal virksomheden have beredskab?

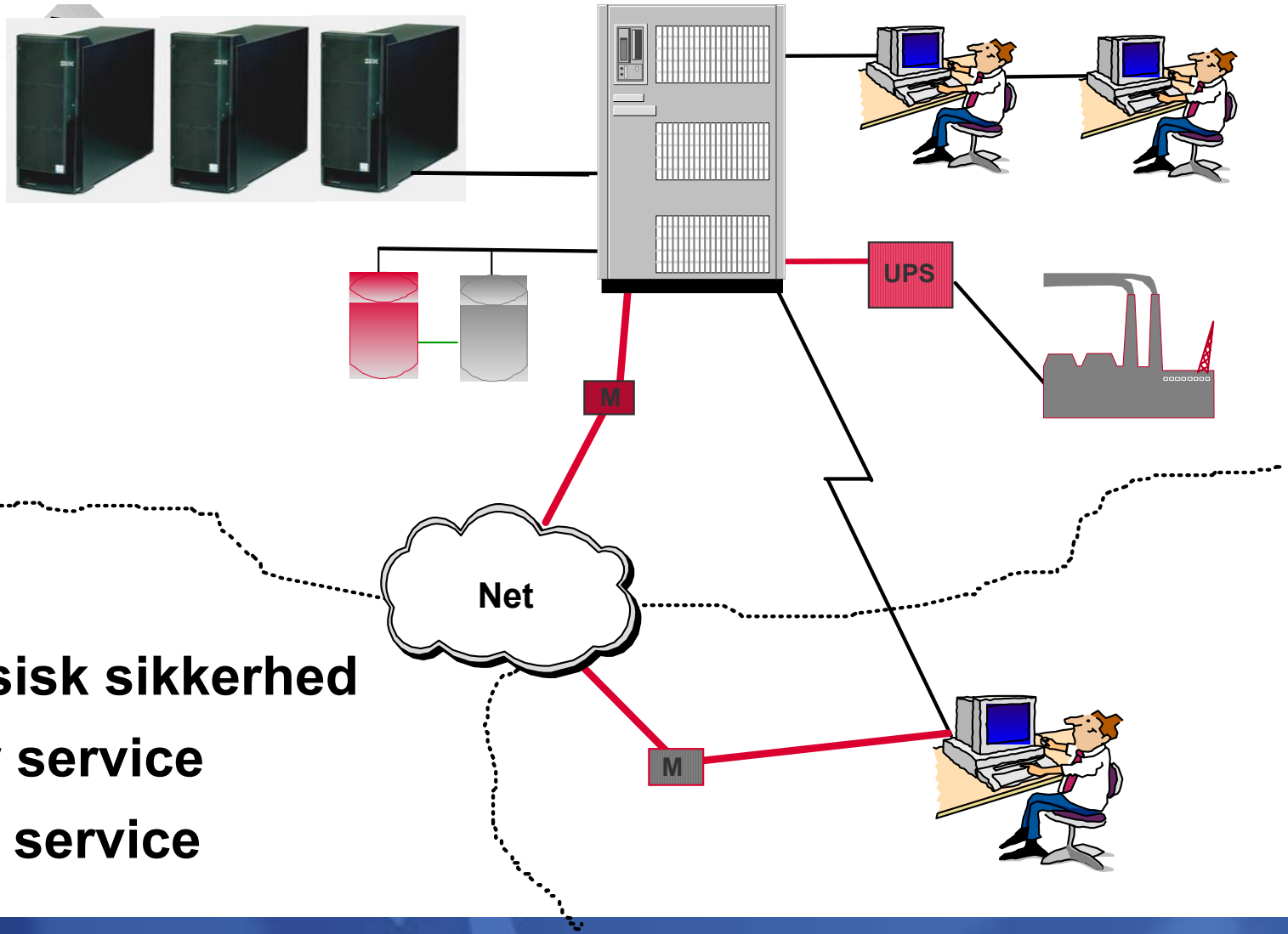
Værdi

- **For at forberede sig til afbrydelser**
  - Analysere risikoen og reducere den
  - Kende effekten og omkostningerne ved nedetid
  - Holde beredskabsplanen opdateret
  - Teste (øve) beredskabsplanens effektivitet
- **Compliance**
  - Leve op til krav fra lovgivning og industristandarder
  - Krav fra revision
  - Sikkerhed - ISO 17799, Code of practice for information security management
- **Finansielt begrundet**
  - Beskyttelse af investorer
  - Begrænse finansielle tab både på kort sigt (order, lager, produktivitet, …) og lang sigt (brand, kunder, markedsandel og tillid)

IT-infrastruktur



Risikoanalyse – reduktion af risiko

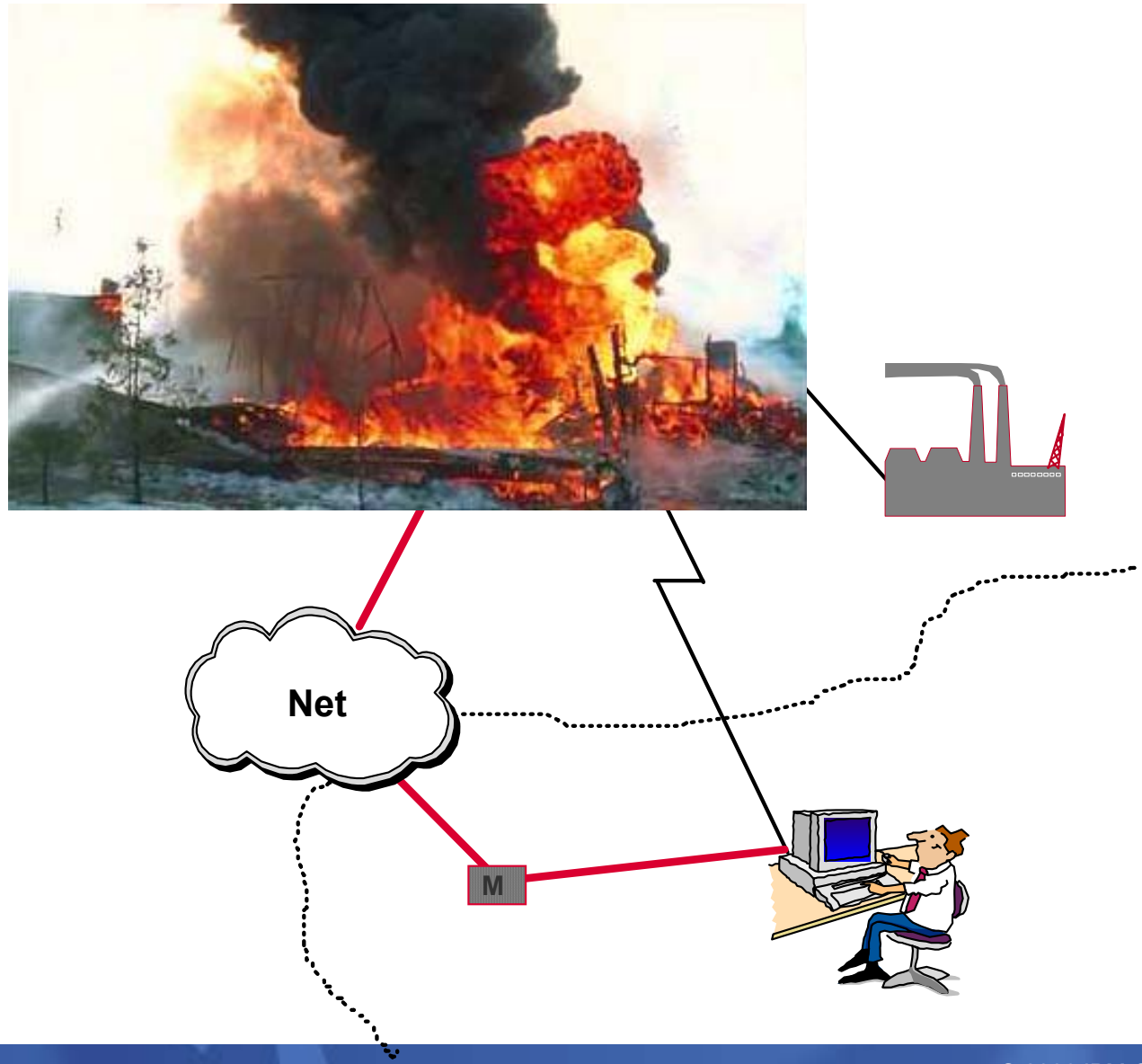


Fysisk sikkerhed

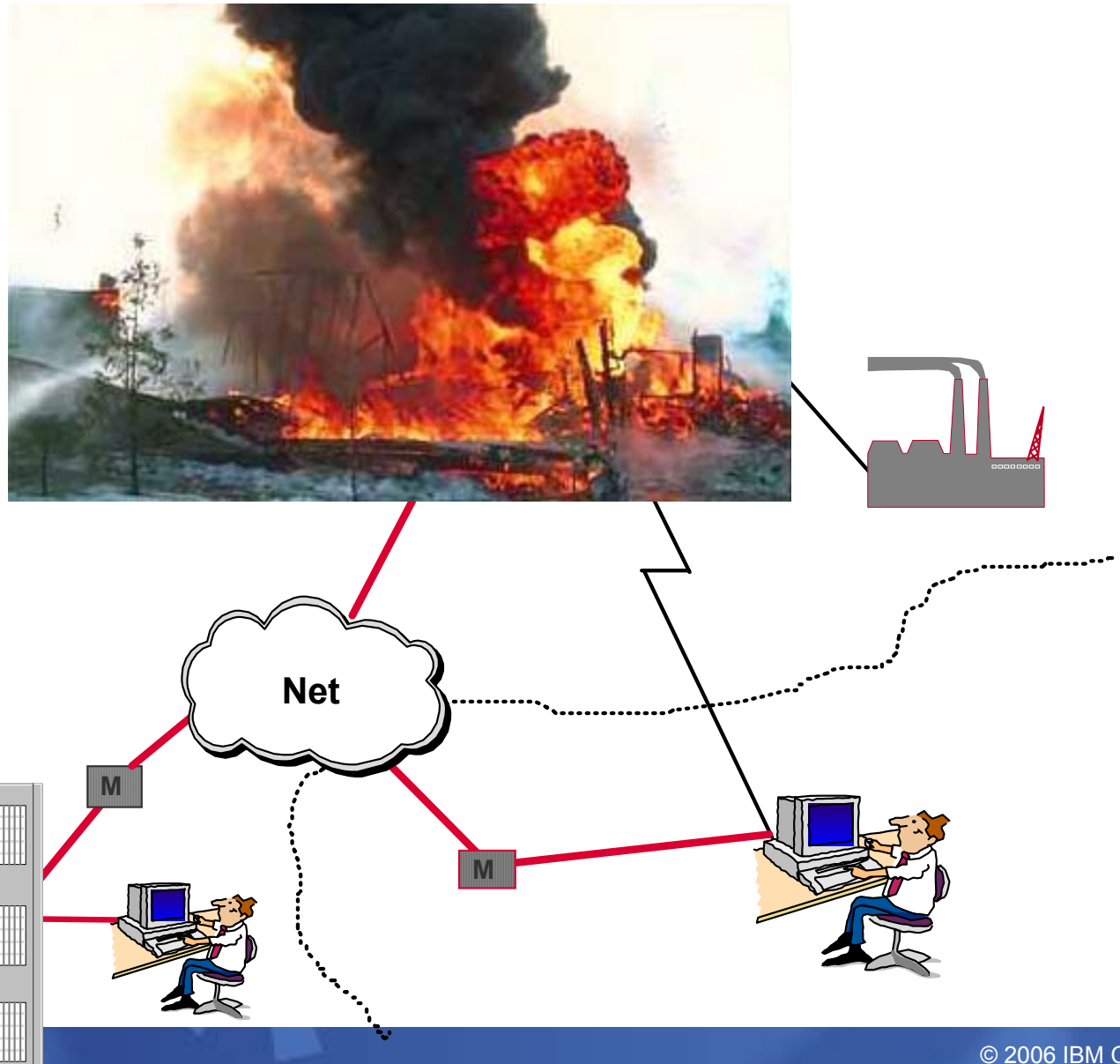
Hw service

Sw service

En katastrofe – måske mindre brand



IT-infrastruktur for katastrofeberedskab



Analyse af aktuelle trusler

Hvordan er trusselsbilledet – evt. scenarier

- **Strømsvigt**
- **Hw / sw**
- **Strejke / lockout / blokade**
- **Brand**
- **Sabotage**
- **Netværk**
- **Vandrør**
- **Naturkatastrofer**
- **Virus**
- **Hacking**

Risikoanalyse – eksempel baseret på DS484

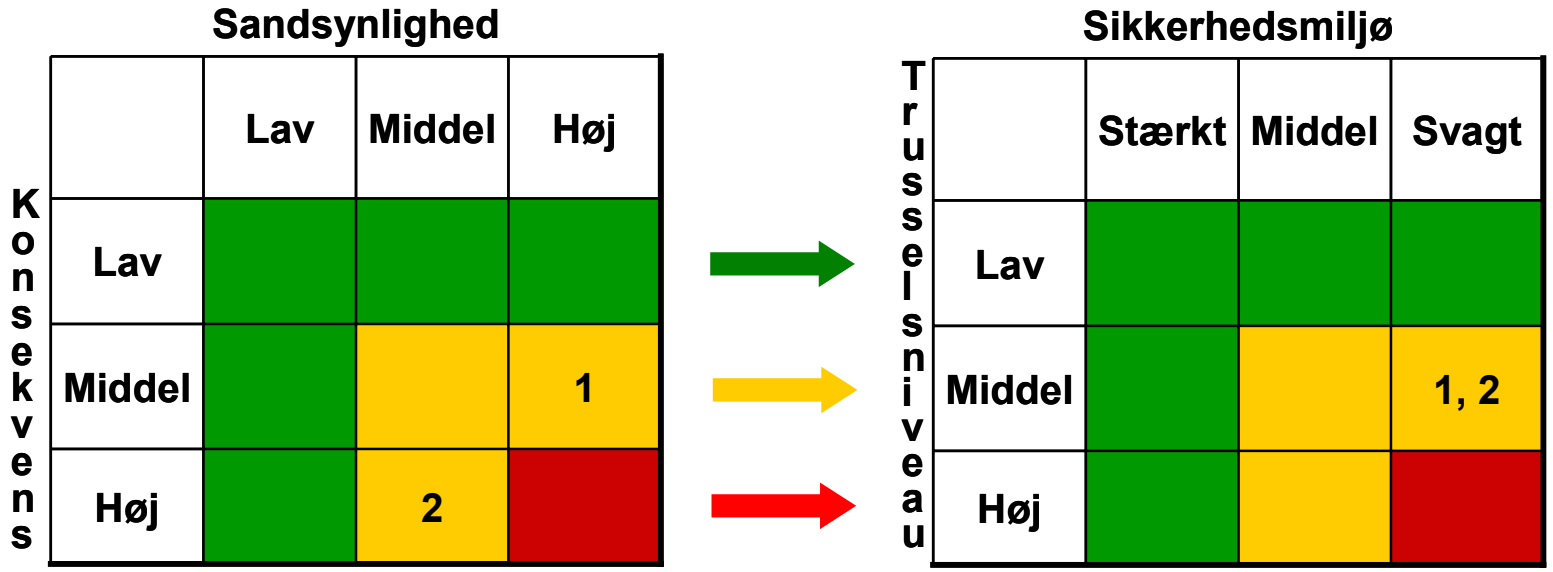
Trusler

1. Brand i eller omkring IT-rum
2. Katastrofe

Sikkerhedsmiljø

Mangler sikret IT-rum

Mangler adgang til backup-systemer og test



Risikoniveauet for de to trusler er middel, og kan reduceres ved etablering af sikret IT-rum, adgang til backup-systemer og årlig test af beredskabet.

Start sikkerheden med et sikkert IT-rum

Sikker brand- og varme beskyttelse iht. EN1047-2

- **Modulopbygget - gulve, vægge og loft**
- **Gas- og fugttæt**
- **Slukningsvand beskyttet**
- **EMC beskyttet – ”Faradays bur”**
- **Tæt kabelgennemføringssystem**
- **Mekanisk beskyttelse – ”building-deformation”**
- **Indbrudssikkert**

Demo: TITE/Enaco, Malmö

Eksempel:

IT-rum på 90 m2, installationsgulv, køleanlæg, UPS, dieselgenerator

HI-FOG brandsikring, projektledelse, afleveringstest

Elementer i et sikkert IT-rum

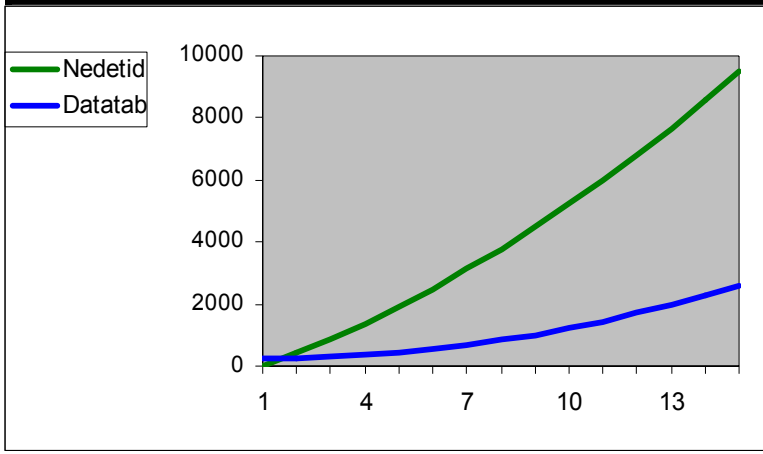
- **Sikkert underlag**
  - **installationsgulv**
- **Strømforsyning og strømkvalitet**
  - **UPS / generator**
- **Konstant lufttemperatur**
  - **Køling / installationsgulv**
- **Konstant luftfugtighed**
  - **Køling**
- **Brand**
  - **Alarmering og slukning (f.eks. HI-FOG)**
- **Sikker forsyning**
  - **dublering**

Sårbarhedsanalyse (Business Impact Analysis)

- **Hvilke systemer er kritiske**
- **Hvad er tabet ved nedetid**
- **Hvad er tabet ved datatab**

- **Tab stammer f.eks. fra**
  - Tabt omsætning og profit
  - Manglende økonomistyring
  - Skadet image
  - Kontraktlige forpligtelser og bod
  - Tabte markedsandele
  - Mistet tillid hos investorer

System A	Tab ved nedetid	Tab ved datatab
1 min.	0	250.000
1 time	10.000	250.000
12 timer	150.000	250.000
24 timer	420.000	262.000
1 uge	3800.000	840.000
2 uger	9500.000	2600.000



Katastrofe - definition

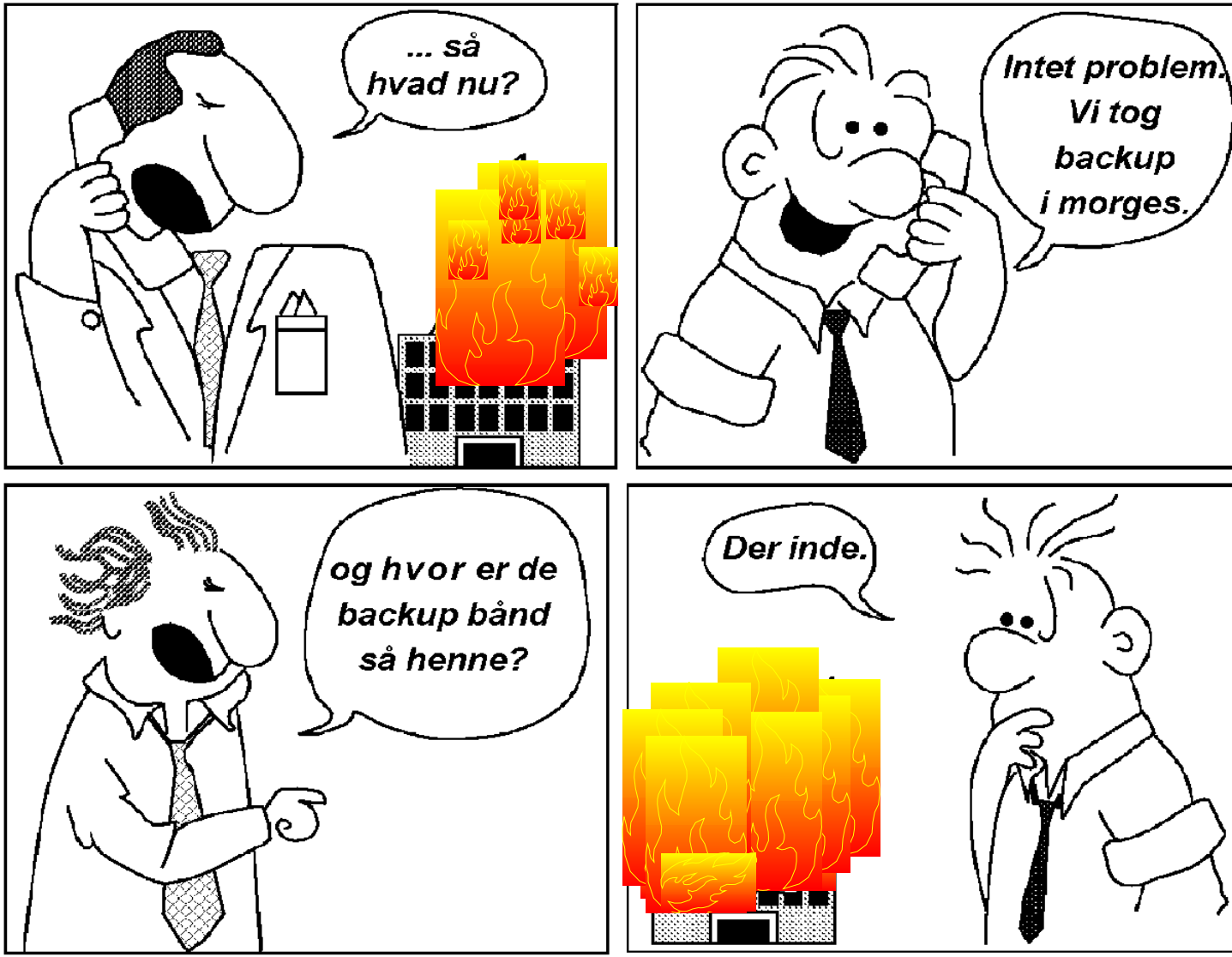
Definition, f.eks:

- En hændelse, der forhindrer driften af IT-systemerne i mere end 48 timer
- Datatab svarende til 36 timer - fra seneste backup
- Omfanget er begrænset til lokaler, bygninger eller et område

Backup – en særlig risiko ... – og hvad med datatabet

Backup i sikkerheds-arkiv er basis for beredskabet

7 % af danske virksom-heder mistede data i 2002

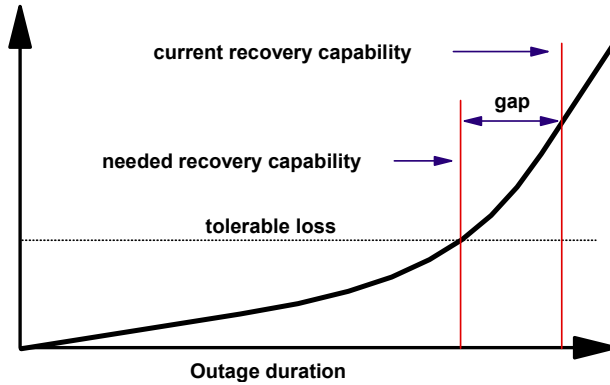


sikkerheden i Danmark 2002 (3. juli 2003)

Analyse af retableringsevne

Lever infrastruktur og processer op til kravene

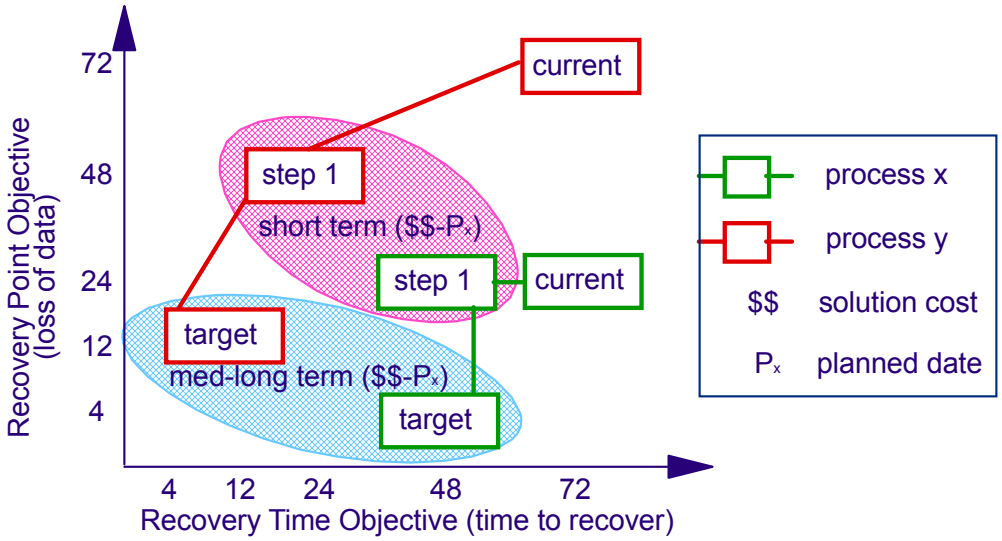
- **Er infrastrukturen kendt og dokumenteret ?**
- **Er netværket dokumenteret ?**
- **Skal backup være synkroniseret ?**
- **Er backup i eksternt arkiv ?**
- **Hvem har adgang til at hente backup i eksternt arkiv ?**
- **Hvordan retableres arbejdspladser ?**
- **Er beredskabsplanen testet ?**
- **Er beredskabsplanen opdateret ?**
- **...**



Strategi for retablering

Udarbejdelse og evaluering af alternative muligheder

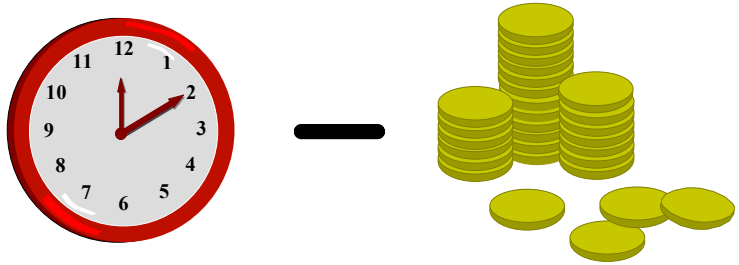
- **Backup-systemer, netværk, alternative IT-rum**
- **Alternative arbejdspladser og/eller hjemmearbejdspladser ?**
- **Integration af tilgængelighed og beredskab ?**



- **Nøglepersoner og kvalifikationer**
- **Omfattet af ændringsstyring**
- **Økonomi**

Hvad er mulighederne ?

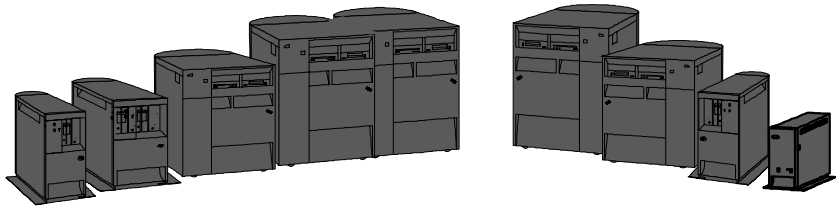
Behov	Anbefaling
IT kan undværes i 2-6 uger :	Check med ledelse og revision
IT kan undværes i 24-48 timer:	Adgang til backup-system
Data er meget værdifulde :	Spejling af data
IT kan højst undværes 1 time :	Spejling af systemer



Katastrofeberedskab består af 3 elementer

Et beredskab (infrastruktur) sikrer, at kritiske forretningsprocesser kan videreføres efter en katastrofe

- **backup i sikkerhedsarkiv**
- **backup-system**
- **netværk**
- **...**



En beredskabsplan

- **beskrivelse af aktivering og anvendelse af beredskabet**

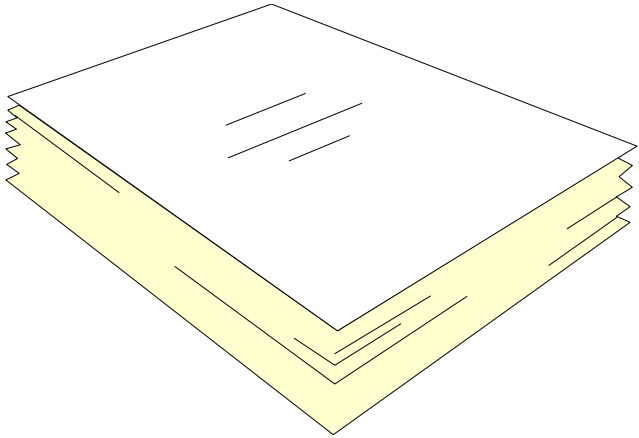
Årlig retableringsøvelse

- **træning i retablering eller verifikation af beredskabet**
- **...**

IT-katastrofeberedskabsplan

Beskrivelse af beredskabets anvendelse

- **alarmering**
- **klassifikation - ulykke/katastrofe**
- **afhentning af backup fra sikkerhedsarkivet**
- **retablering**
- **bygningsfaciliteter**
- **maskiner**
- **programmel**
- **netværk**
- **backup-aftale og andre aftaler**
- **rapport fra sidste retableringsøvelse**



Retableringsøvelser er et nødvendigt onde

Retableringsøvelser er besværlige

- **planlægning - specielt infrastruktur til øvelsen**
- **dyrt – adgang til backup-center med testspecialister**
- **tidskrævende – ofte flere dage**
- **rapportskrivning og opfølgning**

men også en overset kunst

- **kan de rigtige bånd findes ?**
- **kan backuppen læses ?**
- **indeholder backuppen alle data ?**
- **kender jeg mit system (hw, sw, tape, backup-sw, ...) ?**
- **har jeg retableringsprocedurer ?**
  - **til retablering på andet hw (specielt WinTel) ?**
  - **også drivere og rettelser fra nettet ?**

Simpelt katastrofeberedskab: Beredskabs-Service

Beredskabs-Service består af 3 elementer:

- **Adgang til Backup-System ved katastrofe (transporteres til kunden – normalt inden 6 timer)**
- **Adgang til årlig test hos IBM**
- **Oplæg til simpel beredskabsplan**

Backup-Systemer:

- **iSeries**
- **pSeries**
- **xSeries**
- **Tape Units**
- **Storage Units**

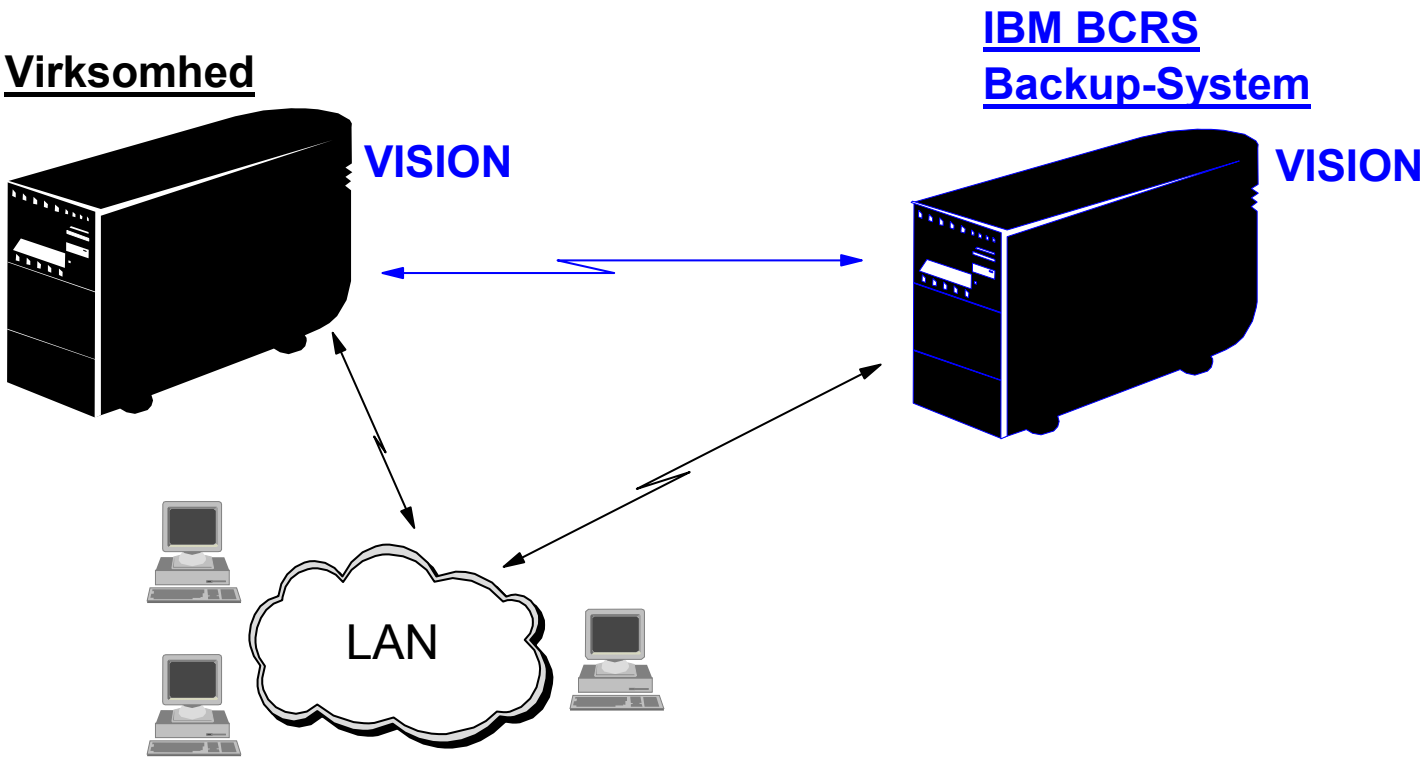
Support:

- **Alarmering 24/7/365**
- **Lokaler**
- **Consulting**
- **IBM testspecialister**
- **IT Sikkerhed**

Spejling - Rapid Recovery eller HAS

Spejling af iSeries data kan udføres med sw fra Vision Solutions

- **Rapid Recovery – spejling til IBM, drift af IBM**
- **HAS – intern spejling og drift**



Tillid hos kunder og i samfundet kan let mistes – tillid er kostbar

Virksomheder og myndigheder må holde kritiske forretningsprocesser kørende:

- **når de rammes af fejl**
- **når de bliver hacket**
- **når de rammes af virus**
- **hvis de rammes af brand eller naturkatastrofe**
- **hvis de rammes af hærværk**
- **hvis de bliver udsat for terror**

skal katastrofeberedskabet levere varen – også i tilfælde af (e-)terror.

Katastrofeberedskab er et af de 11 basale krav i DS 484, Standard for informationssikkerhed