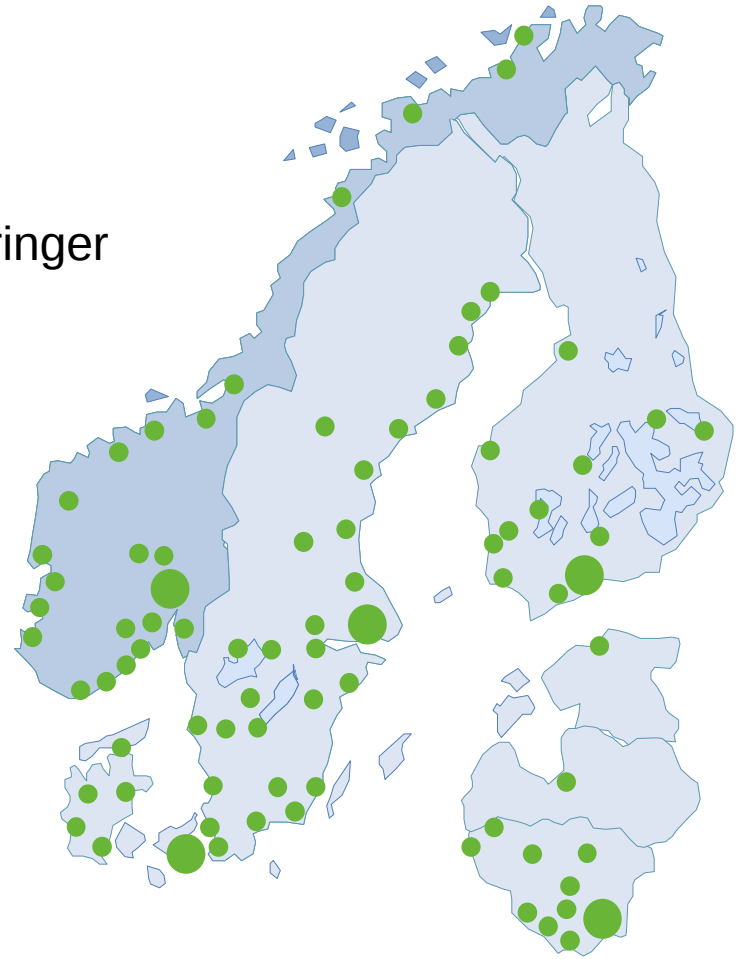


Gjennomføring av arkitekturprinsipp nr 4 Business Continuity – et forslag til TOGAF-modell

Arild Steen Birkelund
Bjørn A. Tveøy
IT-arkitekter
Atea AS

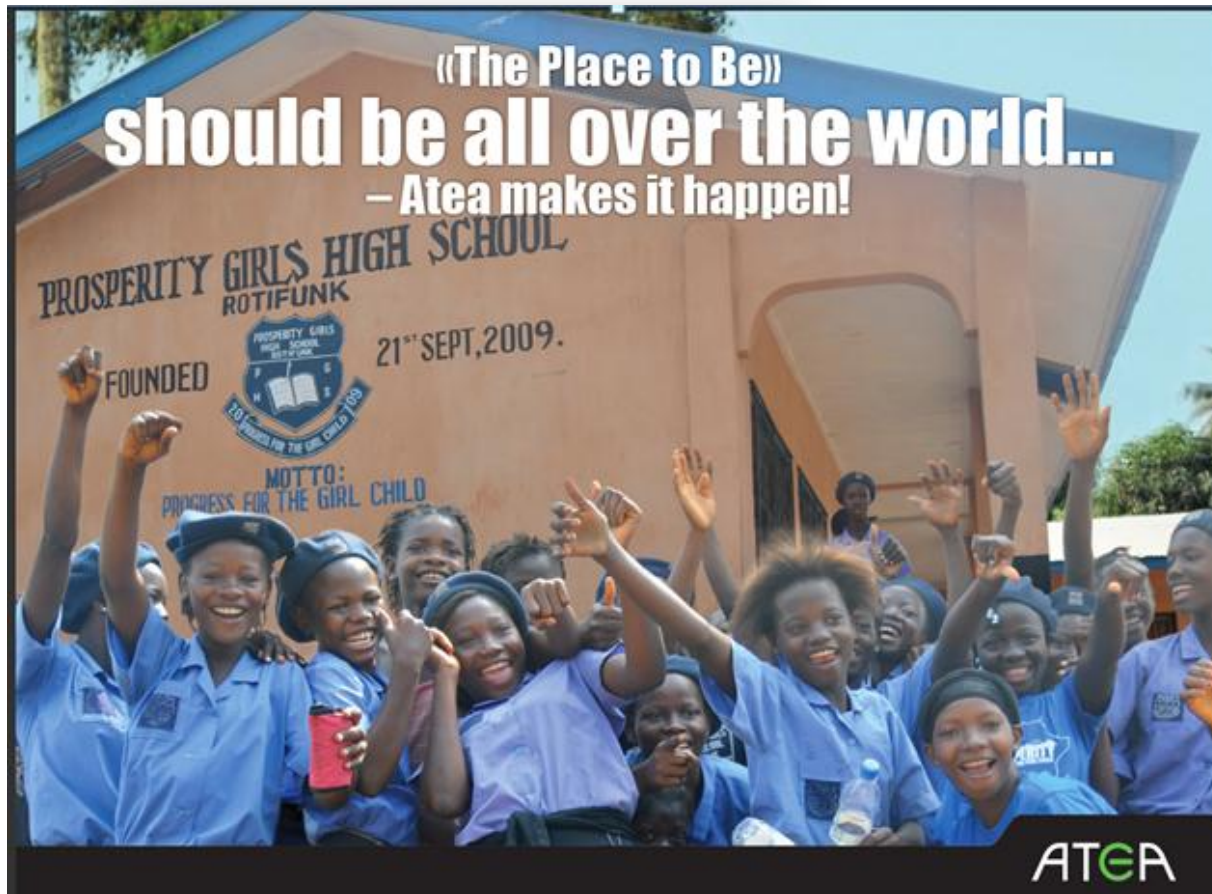
Atea

- Ledende nordisk og baltisk IT-infrastrukturleverandør
 - Nordens største, og 2. størst i Europa
 - Nr. 1 posisjon i alle markedene
 - Ca. 21 mrd. i omsetning 2012
- Den leverandøren i Europa med flest sertifiseringer
 - Over 7 500 teknologisertifiseringer
- Sterk lokal tilstedeværelse
 - 82 lokasjoner i 7 land
 - Ca. 6 300 ansatte
- En unik mulighet til å kombinere lokal tilstedeværelse med europeisk størrelse



Atea

Visjon - The place to be

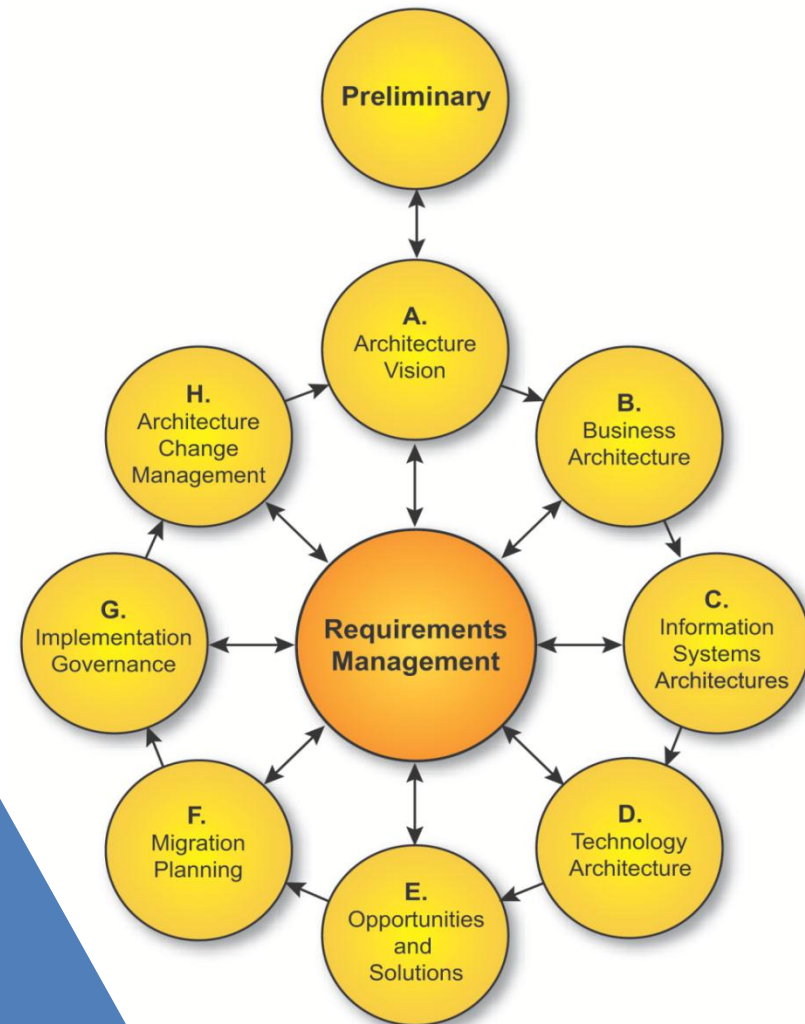


Together Towards the Top



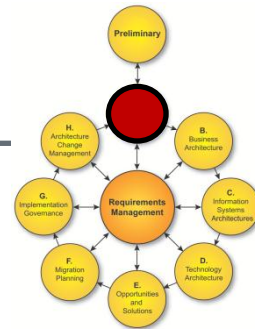
ATEA

Atea og TOGAF



Business Continuity- MNT og MDT

Normal driftssituasjon og/eller ved katastrofe



MDT – Maks Datatap

Akseptabelt Datatap

MNT – Maks Nedetid

Tid for gjenoppretelse av tjenesten

Siste
konsistente
datakopi

Hendelse
inntreffer

System
tilbake i drift

Uker Dager Timer Min. Sek.

Sek. Min. Timer Dager Uker

Hvor lang tid tilbake?

Hvor lang tid for gjenoppretelse?

MNT inkluderer:

- Feildetektering/feilretting
- Recovery av data
- Ta applikasjoner online

Business Continuity – utfordringer og løsninger

Våre lokaler i Havnegata er ikke tilgjengelig, og byggets infrastruktur og IKT/telefoniløsninger er satt ut av drift. Det fryktes at tilstanden blir langvarig.....Hva gjør vi?



DN 25. juli 2011:

- Vi har vært operative her siden 22. juli kveld, sier finansråd Svein Gjedrem i Finansdepartementets reservelokaler
- Alle våre viktigste funksjoner vil kunne opprettholdes
- Plan for beredskapslokaler i krisetid gjorde at dette ble mulig.
- Arbeidet med Statsbudsjettet blir ikke forsinket, sier Gjedrem

Business Continuity – Ateas modell

Plan

1. BIA - forretningsmessigekonsekvenser "langvarig" IT-avbrudd
2. Kravsetting, kartlegging og klassifisering av IT-systemer
3. Kartlegging av status dagens IT-løsning (teknologi, drift, ressurser/kompetanse)
4. Mulige løsninger (måloppfyllelse, egenskaper, økonomi, risikovurdering)
5. Innstilling til ledelsen
6. Utarbeide policy for IT-kriseberedskap

DO - planlegge

7. Risikoreduserende tiltak dagens løsning
8. IT-beredskapsplan
9. Teknisk IT-beredskapsløsning
10. Informasjon, opplæring og trening



Architecture principles i TOGAF

Principle 1: Primacy of Principles

Principle 2: Maximize Benefit to the Enterprise

Principle 3: Information Management is Everybody's Business

Principle 4: Business Continuity

Principle 5: Common Use Applications

Principle 6: Service Orientation

Principle 8: IT Responsibility

Principle 9: Protection of Intellectual Property

Principle 10: Data is an Asset

Principle 11: Data is Shared

Principle 12: Data is Accessible

Principle 13: Data Trustee

Principle 14: Common Vocabulary and Data Definitions

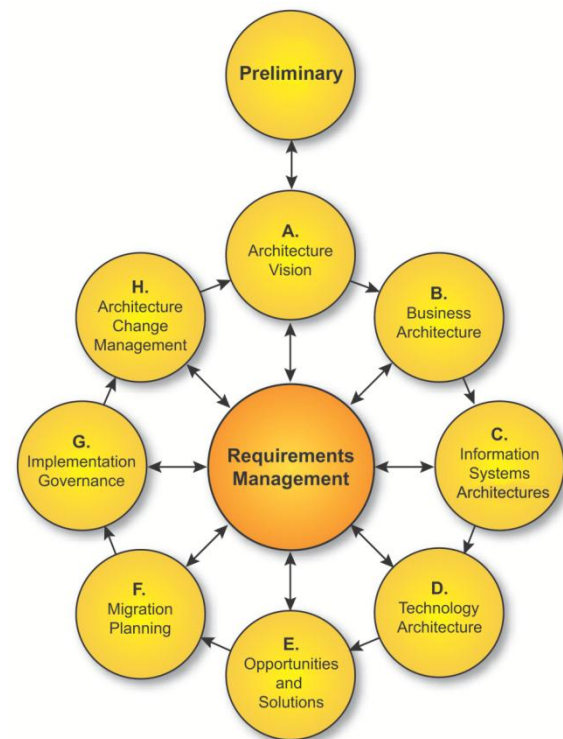
:

Principle 21: Interoperability

Architecture principle # 4 – Business Continuity

Statement	Enterprise operations are maintained in spite of system interruptions.
Rationale:	As system operations become more pervasive, we become more dependent on them; therefore, we must consider the reliability of such systems throughout their design and use. Business premises throughout the enterprise must be provided with the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop enterprise activities. The enterprise business functions must be capable of operating on alternative information delivery mechanisms.
Implications:	Manage risks Recoverability, redundancy, and maintainability Applications must be assessed for criticality and impact on the enterprise mission, recovery requirements

Business Continuity – Ateas modell i TOGAF ADM



ATEA

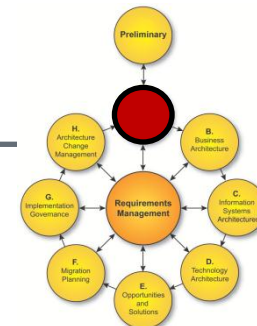


- A. Visjon: IT-beredskap
- B. Forretningsarkitektur: BIA
- C. Informasjonssystemer: Krav og klassifisering
- D. Teknologi
 - Alternative løsninger
 - Kontinuitetsvurdering
- E. Muligheter: Innstilling og beslutning
- F. Migrasjonsplanlegging
 - Policy
 - IT-beredskapsplan
 - Teknisk løsning

Artifakter

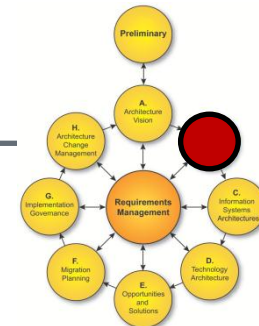
Visjon: Business Continuity - Fase A

- Avbruddstid (MNT) og datatap (MDT) i tråd med virksomhetsledelsens informerte beslutning
- Optimal økonomi og ressursbruk – forbyggende og gjennomføring
- Optimal risikoreduksjon for hendelser
- Fungerer når den skal



Forretningsarkitektur - Fase B

BIA – Business Impact Analysis

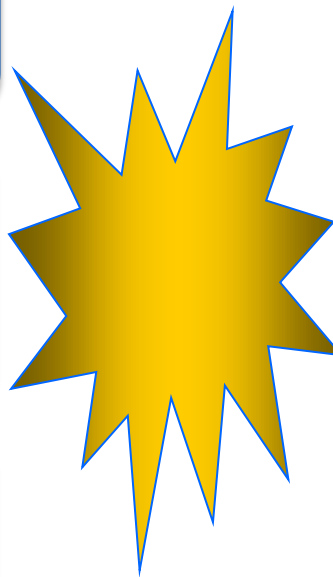


Tjenesteproduksjon stanser
Ekstern produksjon går

Produksjonssystemene
Kundestøttesystemene
Datakommunikasjon
Personlig IT-utstyr
Lokaler

MNT 1 – 2 (3) dager
P > 5 år

MDT 1 døgn
P = 1 - 5 år



1 ukes IT-driftsavbrudd

- 3000 saker
- 800 vedtak
- 300 nye saker
- 800 kundehenvendelser
- 800 bestillinger

Blir forsinket en uke

1 ukes IT-driftsavbrudd

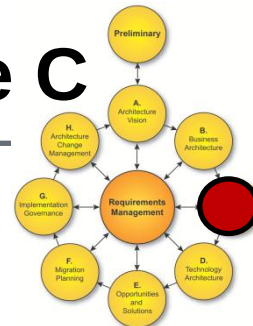
- Inntektstap inntil 4 MNOK
 - Overtidskost 2 MNOK
- Tall vel begrunnet og forankret

Omdømme

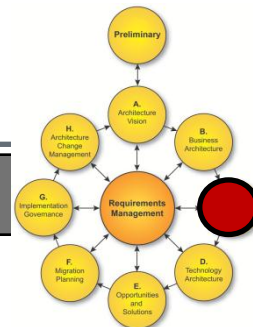
- I dagspressen etter 1 – 2 dager
- Negative oppslag
- Overordnet myndighet
- Direktør

Informasjonssystemer: Klassifisering - Fase C

- **Virksomhetskritisk** – IT Systemer som vil medføre at virksomhetens hovedprosesser stopper opp dersom de ikke er tilgjengelige. Kan få store økonomiske og/eller virksomhetsmessige konsekvenser
- **Svært viktig** - Manglende tilgang på IT systemet gir negative konsekvenser av økonomisk eller omdømmemessig art.
- **Normal** - IT Systemer som er viktig ut i fra enkeltmedarbeideres effektivitet, men ikke nødvendigvis kritisk for avdelinger eller enheters produksjon
- **Mindre «viktig»** - Manglende tilgang gir minimale konsekvenser.

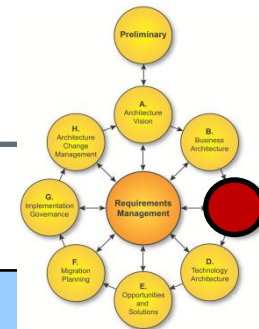


Krav til de enkelte klasser - Fase C



Klasse	Parametere
A. Virksomhetskritisk	MNT: 1 time MDT: 0 timer Tilgjengelighet/oppetid: 99,9% Ytelse: Høy Åpningstid (tidsrom tjenesten er tilgjengelig): 24/7/365 Vedlikeholdsvindu: Ikke relevant
B. Svært Viktig	MNT: 4 timer MDT: 1 time Tilgjengelighet/oppetid: 99,6% Ytelse: Høy Åpningstid: 24/7/365 Vedlikeholdsvindu: Søndag 22:00 – 24:00
C. Normal	MNT: 8 timer (1 dag) MDT: 8 timer (1 døgn – dvs. 8 timers arbeidsdag) Ytelse: Middels Åpningstid: 08.00-16.00/mandag-lørdag Vedlikeholdsvindu: Hverdager 17:00 – 07:00 og søndager
D. Mindre "Viktig"	MNT: 16 timer (2 dager) MDT: 8 timer (1 døgn – dvs. 8 timers arbeidsdag) Ytelse: Middels Åpningstid: 08.00-16.00/mandag-fredag Vedlikeholdsvindu: Hverdager 17:00 – 07:00 og helg

Kartlegging: IT-Systemer - Fase C

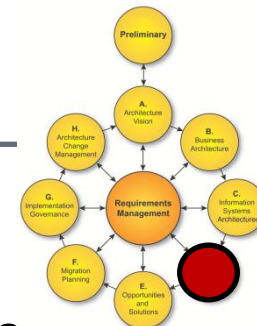


Tjeneste	Krav / Klasse	Antall berørte brukere	Plattform Fysisk/ Virtuell	Lagring (Volum, SAN/NAS)	Avhengighet/ Merknad
Exchange	B	750	Virtuell	SAN	
Filtjener	B	750	Fysisk	NAS	
Oracle DB	A	750	Fysisk	SAN	Kjernesystem
CRM	B	750	Virtuell	SAN	
Lønn	C	3	Virtuell	SAN	

Når krav er utarbeidet og klassifisering gjennomført, bør følgende klarlegges:

- Tilfredsstiller tjenesten kravet i dagens løsning?
- Hvordan kan/bør tjenesten implementeres i en eventuell reserveløsning?
- Hvordan er driftsrutinen for sikkerhetskopiering/gjenoppretting og den nåværende IT-beredskapsplanen

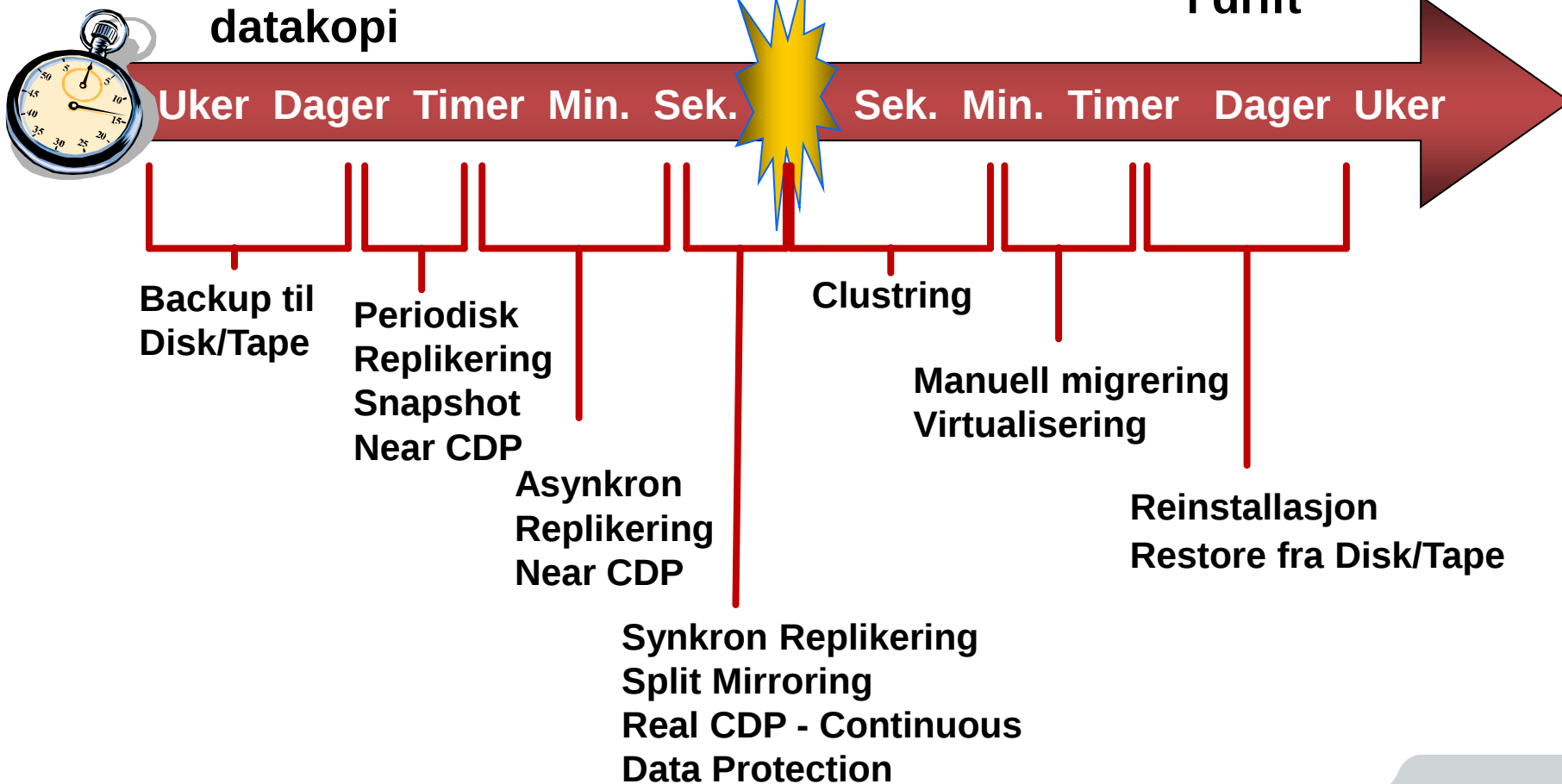
Løsninger / Teknologier - Fase D



**Siste
konsistente
datakopi**

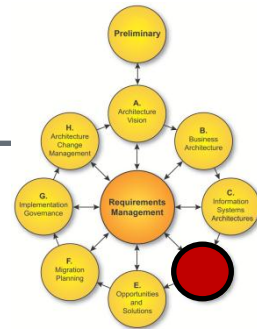
**Hendelse
inntreffer**

**System tilbake
i drift**



Teknologi: Alternative løsninger - Fase D

- Housing
- Leie IT-beredskapsløsning
- To-romsløsning
- Bombe- og strømsikker lokal løsning
- Akseptere risiko ved dagens løsning – gjøre forebyggende tiltak



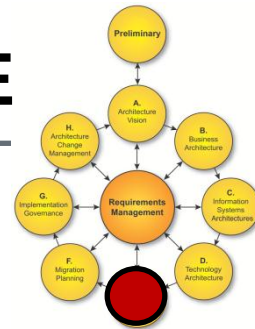
Hvilken løsning
skal vi velge?



Mulighetene: Innstilling til ledelsen - Fase E

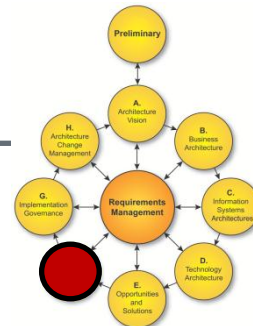
Oppsummering – inntil to sider
Vedlegg – inntil fem til sju sider

1. Anbefaling og begrunnelse
2. Problemstilling
3. Hva sier forretningsenhetene?
4. Konsekvenser for virksomheten – og kundene – ved en ukes driftsavbrudd (produksjon, kunder, økonomi, omdømme etc)
5. Alternative IT-beredskapsløsninger – nytte, kostnader, risiko
6. Mer om risikovurdering
7. Kompetanse, ressurser og dokumentasjon
8. Trusler og hendelseshåndtering



Migrasjonsplanlegging - Fase F

- Policy for IT-beredskap
- IT-beredskapsplan
- Risikoreduserende tiltak i dagens IT-løsning
- Teknisk IT-kriseløsning
- Opplæring, øving, informasjon

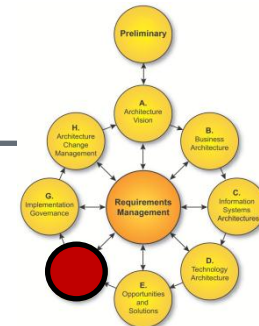


Policy for IT-kriseberedskap - Fase F

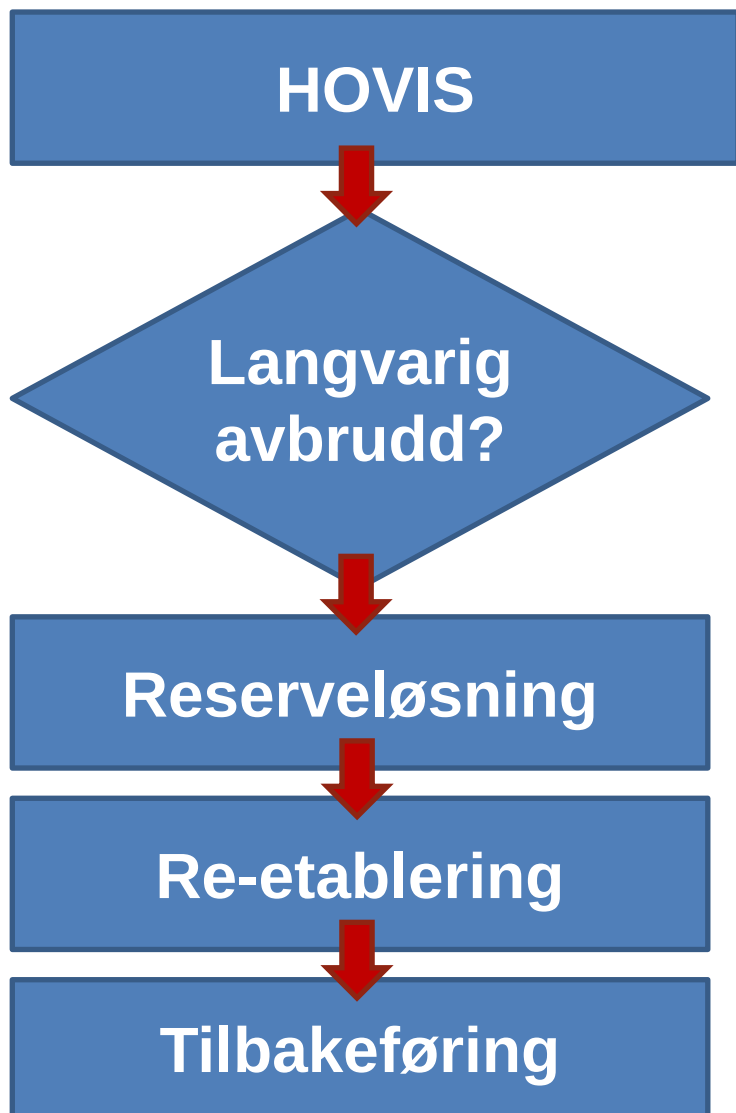
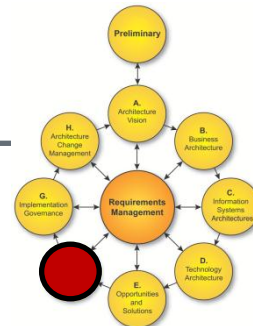
ISO 22301

Policy (overordnede retningslinjer) for IT-beredskap basert på ledelsens beslutning - underordnet virksomhetens policy for beredskap

- Scope
- Mål og rammer
- Organisering og ansvar
- Planlegging
- Implementering og drift
- Oppfølging
- Forbedring



Business Continuity, er en plan! Fase F

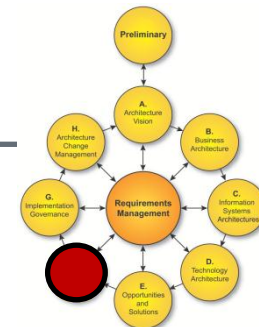


- Backup/gjenoppretting
- Datarom
- Dataromutstyr
- IT-utstyr/sw/appl
- Kabling, nettverk, trådløst
- Datakommunikasjon
- Brukerutstyr
- Ressurser

-
- Ansvarlig
 - Change
 - Tilgjengelig
 - Opplæring
 - Øving
 - Informasjon



Risikoreduserende tiltak - Fase F



➤ Datarom

- fysiske ressurser, strøm, kjøling, kabling

➤ Sentral IT løsning

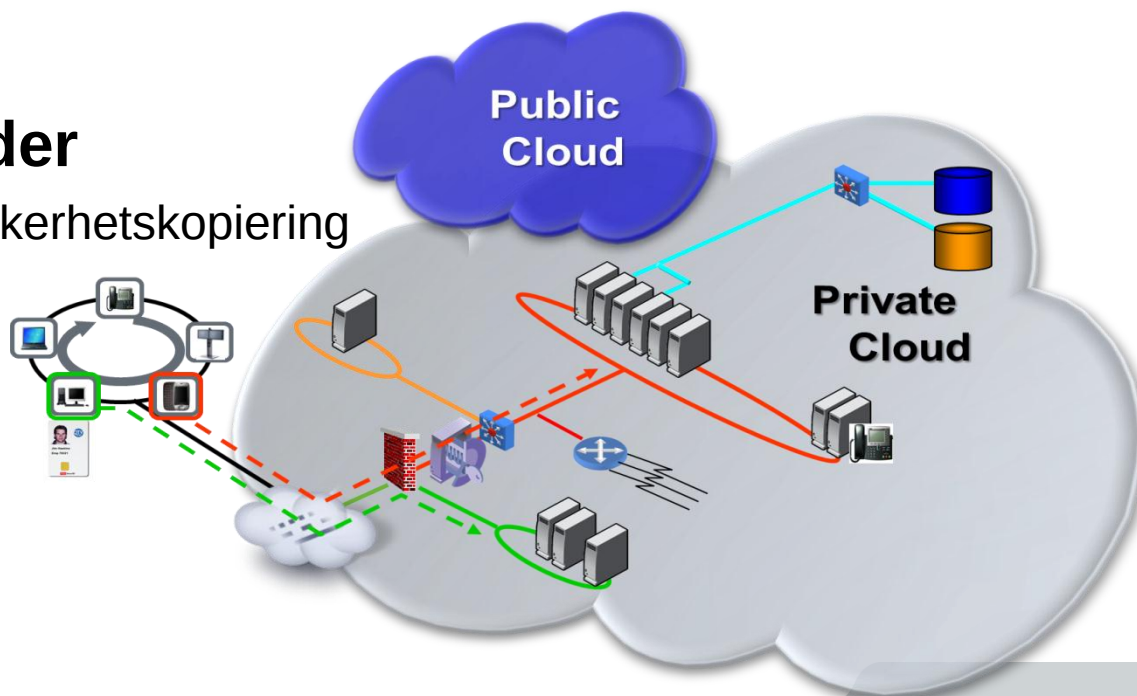
- kommunikasjonslinker (LAN, WAN), lagring, server

➤ IT personalressurser

- kompetanse, tilgjengelighet

➤ Sentrale IT driftsområder

- Rutiner og prosesser rundt sikkerhetskopiering og gjenoppretting

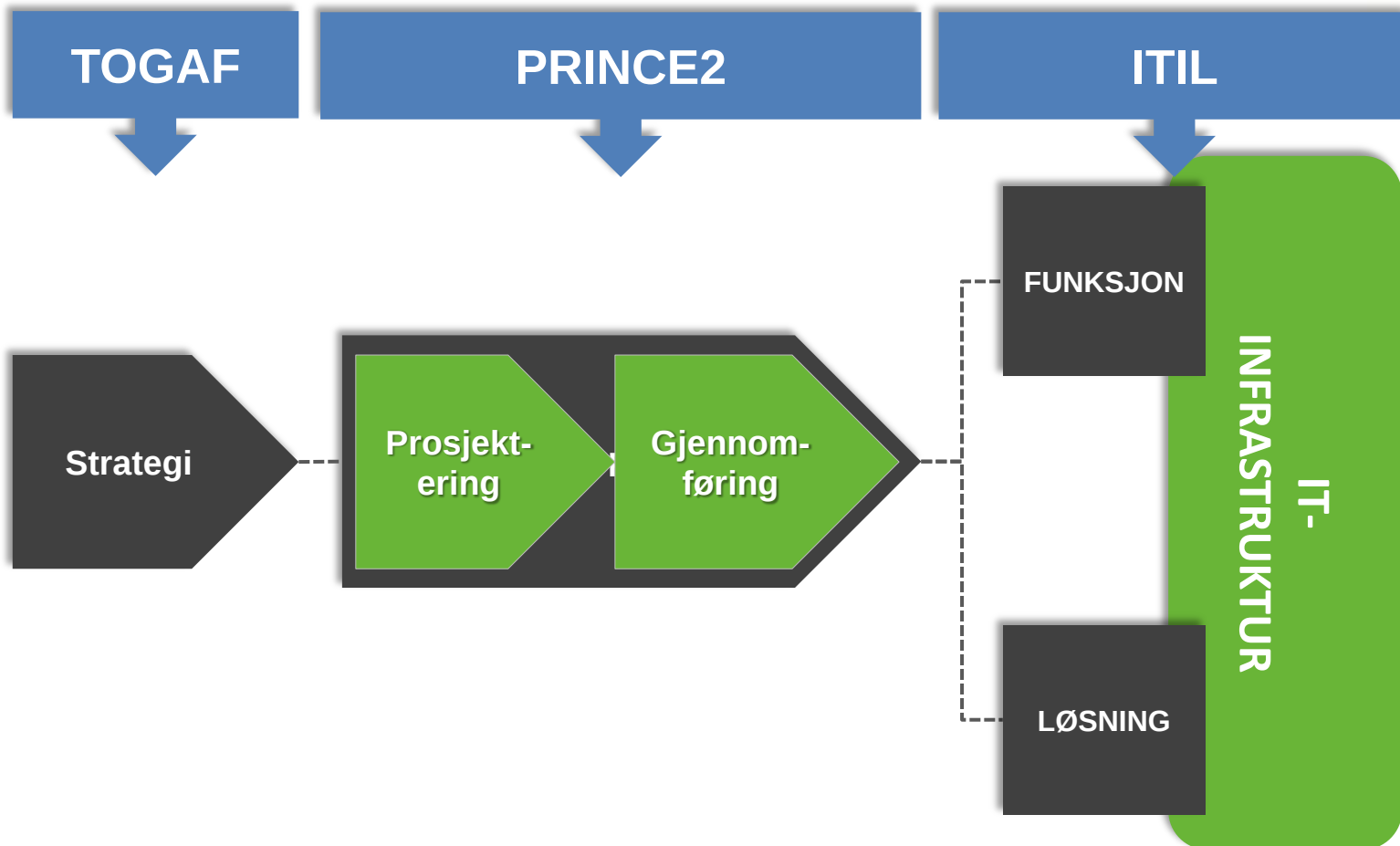
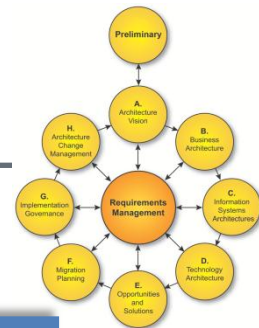


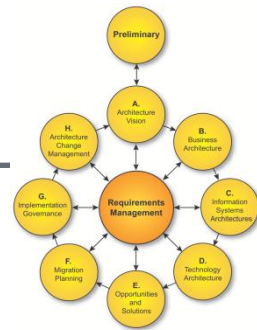
TOGAF - artifakter



- **Metodedokument BC** – 25 sider
- **Metodedokument ROS** – 25 sider
- **BIA** – prosess, resultater
- **Systemer** – krav og klassifisering, prosess, resultater
- **Kontinuitetsvurdering** – prosess, resultater
- **Innstilling til ledelse** – eksempler
- **ROS-vurderinger** – eksempler
- **IT-beredskapsplaner** - eksempler
- **Reserveløsninger** - eksempler

Realisering





Takk for oppmerksomheten

Arild Steen Birkelund

Bjørn A. Tveøy

IT-arkitekter

Atea AS