Verifica

Revision af IT anvendelsen -revisionsmæssige udfordringer

af Seniorrådgiver Hans Henrik Berthing,
Statsautoriseret Revisor, CIA, CGEIT, CRISC, CISA

Agenda

- God IT Skik
- Forstå informationssystemer og tilhørende forretningsprocesser
- Virksomhedens reaktion på IT relaterede risici
- Kompetencer – anvendelse af specialist, herunder Intern Revision
- Revisionsmæssige overvejelser i forbindelse med kunden anvendelse af serviceleverandør
- Erklæringer i forbindelse med IT Anvendelsen

Verifica

- Nationalt og internationalt netværk indenfor IT-revision, herunder service bureauer (ISAE 3402, IT Assurance, Business Risk Services)
- Specialiseret indenfor IT Governance, IT Risk Management, IT Sikkerhed
- IT Revisor og rådgiver for mindre og mellemstore virksomheder
- Pengeinstitutter – finansielle virksomheder
- IT serviceleverandører
- Medlem af FSR, ISACA, IIA – interne revisorer, DJØF
- CISA og CRISC instruktør
- Samarbejde med Beierholm
- FSR's informatikudvalg

Hans Henrik Berthing

- Statsautoriseret revisor, CRISC (IT Risikostyring), CISA (IT revision), CGEIT (IT Governance) og CIA (Intern Revision)
- 7 år finansiel revision og 17 år IT assurance og Risikostyring
- Compliance reviews (ISO 9000; ITIL; ISF; ISO 27001/ISO27002)
- Internationalt projekt forsikringsvirksomhed
- IT risikoworkshop
- Intern revision
- Revisionserklæring for IT servicebureauer
- Projekt reviews & Systemgennemgange
- ISACA Assurance Task Force
- Underviser og foredragsholder
- FSR Informatikudvalg
- Associate professor og Senior rådgiver Aalborg Universitet
- Forsker i revision, risikostyring og Compliance

NemID

- 15 okt 23:08: Problemer med seneste java opdatering
- 18 okt 20:55 Al drift er OK. NemID kører uden driftsproblemer

- NemID nede i tre døgn.

- Onlinespiludbyderne anslår, at de seneste dages NemID-rod koster seks millioner kroner om dagen
- Sikkerhedsekspert kritiserer NemID for at være for sårbart og for usikkert
- Helt almindelig standardopdatering (Java), har vist sig at skabe problemer

- 18 april: Ustabilitet som følge af DDoS-angreb

Forebyggelse af hackerangreb

- Rigsrevisionens beretning oktober 2013
- Stigende digitalisering af forvaltning øger behovet for, at statslige virksomheder beskytter sig mod hackerangreb
- Senere år været angreb på flere statslige virksomheder
- 3 centrale sikringstiltag
  - Teknisk begrænsning af download af programmer fra internettet
  - Begrænsning af brugen af lokaladministratorer
  - Systematisk sikkerhedsopdatering af programmer.

- Undersøgelsens resultater om utilstrækkelig sikring af data er af principiel betydning.
- Alle statslige virksomheder bør forholde sig til anbefaling om at håndtere risikoen for hackerangreb.

Forebyggelse af hackerangreb Konklusion

- Data ikke tilstrækkeligt beskyttet
- Unødig stor risiko for hackerangreb og misbrug af IT-systemer og fortrolige data pga sikkerhedsniveauet.
- Ingen af de undersøgte virksomheder havde i deres risikovurderinger håndteret den risiko, de udsatte sig for.
- Ikke klart opgavesplittet mellem Statens It og virksomhederne
- Ikke systematisk forebygget hackerangreb ved teknisk at begrænse download af programmer og brugen af lokaladministratorer
- Kun 2 ud af 4 virksomheder sørgede for sikkerhedsopdatering
- Ikke dokumentation i risikovurderinger for, at ledelsen taget stilling til risikoen ved ikke at have implementeret de 3 sikringstiltag
- Statens It ikke tilstrækkeligt undersøgt risikoen for, at et hackerangreb et sted kunne sprede sig til andre
- Udbredt brug af domæneadministratorer øgede risikoen for spredning af et angreb

Bedre systemer kan mindske fejl i kræftforløbet

- Den Nationale Arbejdsgruppe for Patientsikkerhed i kræftforløb anbefaler bl.a. bedre IT-systemer som en måde at forbedre patientsikkerheden
- Kræftens Bekæmpelse anbefaler, at arbejdet med IT-systemer foregår på nationalt niveau

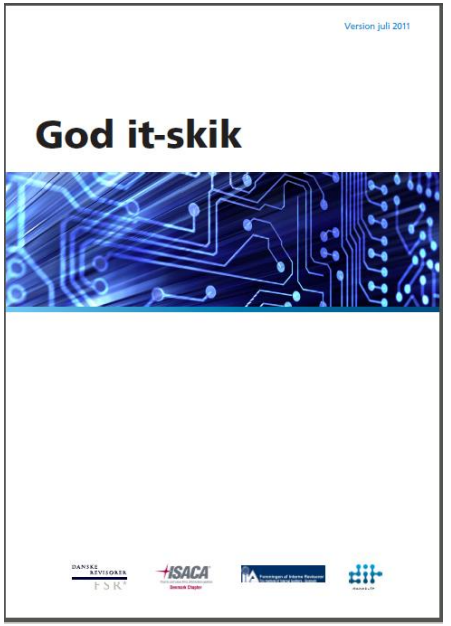
- Mange har stået med nogle forkerte koder i det gamle IT-system.
- Fejlagtige koder overført til nyt system -> set ud som frameldt screeningsundersøgelserne på grund af en IT-teknisk fejl.

- Brev til 19.000 kvinder. Ved en fejl frameldt screeningsprogrammet for livmoderhalskræft (1981- 2007)
- Ca. 400 med uopdaget behandlingskrævende forstadier til kræft

Randers Reb

- Beretningen for 2002-regnskabet: Nyt standard-system skulle være i drift i moderselskabet 1. april i 2003. Fra januar næste år skulle datterselskaberne kobles på.
  - IT-systemet dyrt og så fejlbehæftet, at det har kostet vareleverancer for reb-producenten.
  - Flere dage ad gangen var det slet ikke i drift.
- Juni 2003: Beder fondsbørsen om handlen med aktie i bero
  - Bestyrelse har indledt en gennemgang af forudsætningerne for selskabets budgetter og herunder forventningerne for indeværende regnskabsår.
  - Aftale med administrerende direktør, at han fratrådte. Begrundelsen var blandt andet en utilfredsstillende implementering af et nyt it-system
- Juni 2004 Betalingsstandsning
- Marts 2005 Konkurs

God IT skik 2011



Temaer som er drøftet

- Porteføljestyring
- Compliance
- Outsourcing
- KPI'er
- SWOT
- Organisering
- Forretningsforståelse
- Risk Management
- Awareness
- Information
- Processer

Definition

God IT-skik er som norm de branchemæssige sædvaner og den praksis, der til enhver tid efterleves af kyndige og ansvarsbevidste fagfolk med henblik på, at IT-anvendelsen baseres på forretningsmæssige mål, krav og ønsker samt at den er i overensstemmelse med lovgivningen og interne regler.

Definition - underforstået

God IT-skik er en del af god ledelse med fokus på informationsteknologi, systemer og deres resultater og risikostyring. Der er et særligt behov for ledelsens fokus på god it-skik som følge af øgede krav om overholdelse af initiativer og regler samt en erkendelse af, at IT-projekter har stor indflydelse på en virksomheds succes.

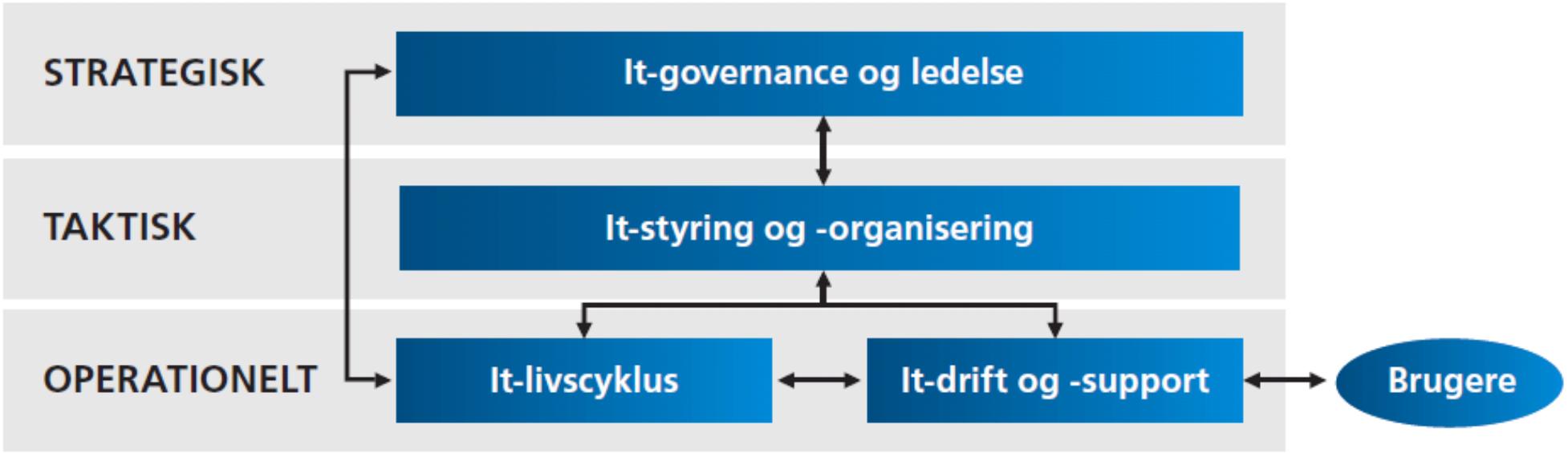
God IT-skik indebærer, at ledelsen ikke kan betragte it-området som værende en sort boks. Topledelsen bør involveres i vigtige it-beslutninger og kan ikke delegere dette ansvar til virksomhedens it-fagfolk, men skal selvfølgelig inddrage dem i beslutningsprocessen. God IT-skik forudsætter en proces, hvor alle interessenter, herunder ledelse og brugere, har det nødvendige input til beslutningsprocessen.

It-anvendelsen skal tilrettelægges på en klar, overskuelig og verificerbar måde, blandt andet skal der implementeres tilstrækkelige og effektive sikkerhedsforanstaltninger.

Ledelsens ansvar

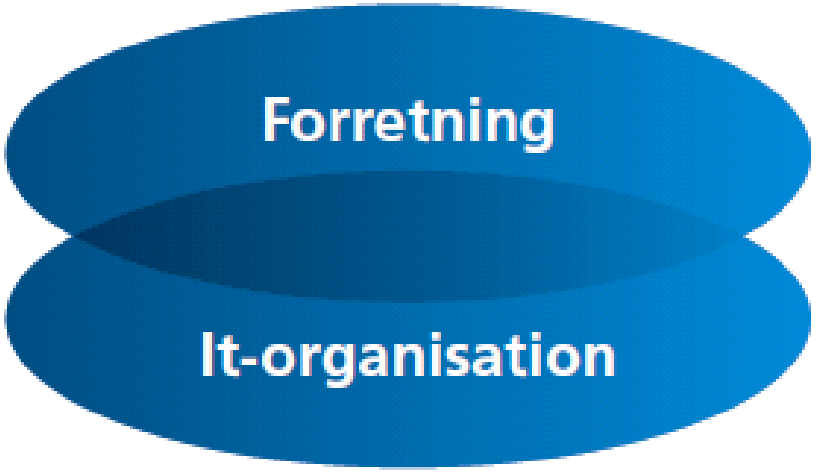
En forudsætning for god it-skik er, at der på det øverste ledelsesniveau træffes beslutning om de muligheder, it-anvendelsen indebærer for forretningsstrategien. It er i dag et naturligt emne på dagsordenen i forbindelse med ledelsesmøder – i såvel den øverste ledelse som den daglige ledelse.

Opdeling af it-aktiviteter i processer



Interaktion forretning og it afdeling

INTERAKTION MELLEM FORRETNING OG IT-AFDELING



Samspil

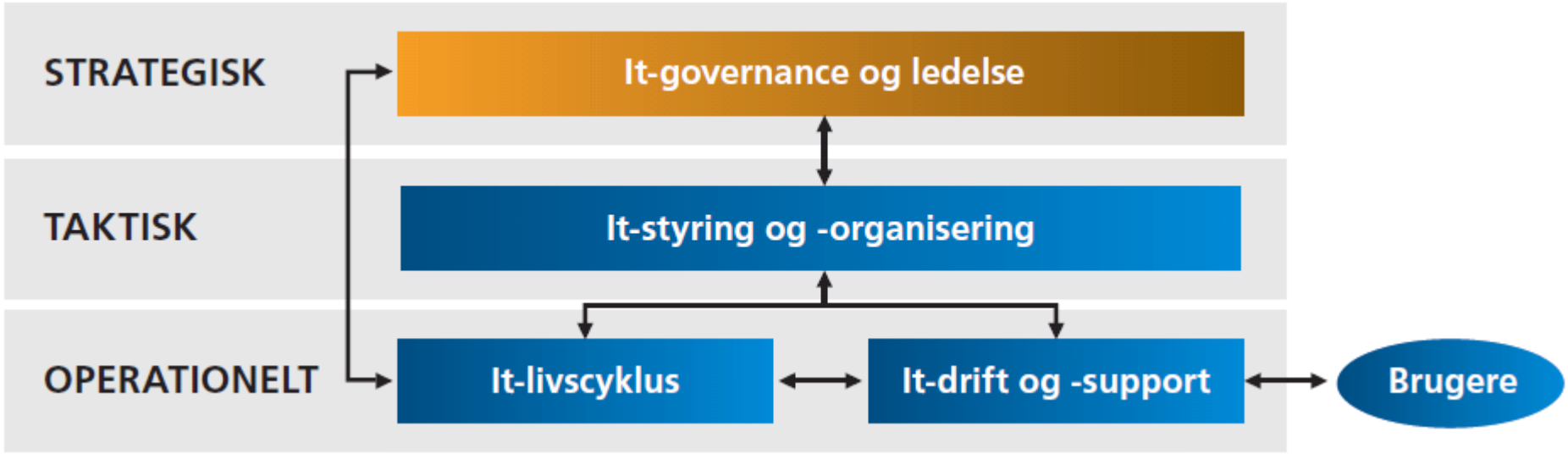
Forretningsforståelse

Understøttelse

Fleksibilitet

Prioritering

It-Governance og ledelse



5.1 It-strategisk planlægning

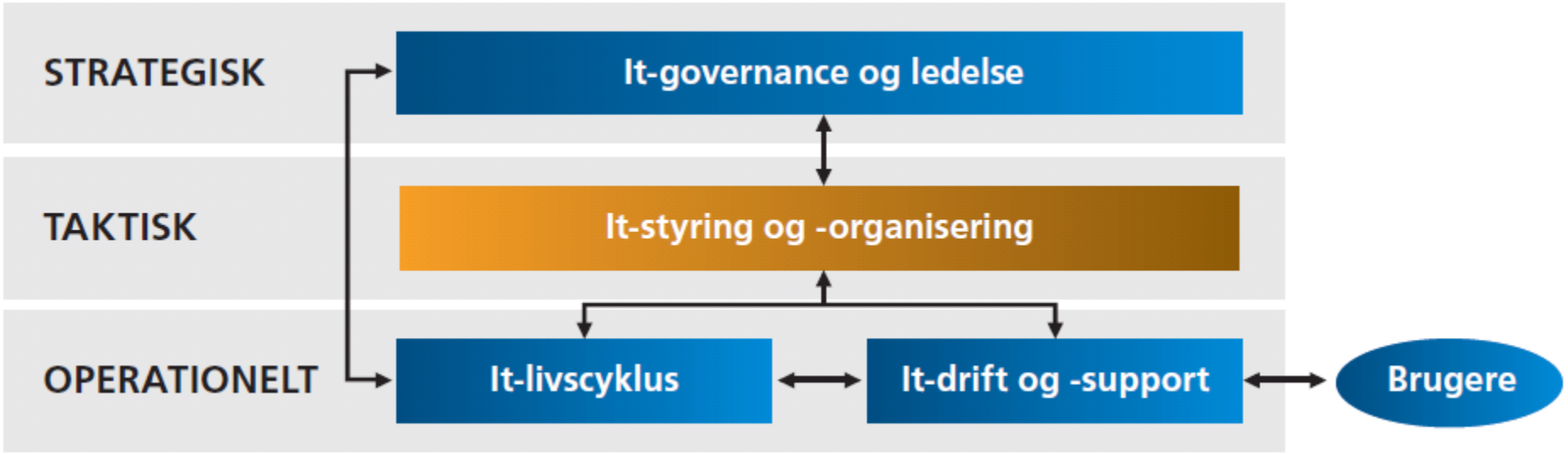
5.2 Analyse af muligheder og risici

5.3 Beslutning og planlægning

5.4 Implementering

5.5 Overvågning og opfølgning

IT-styring og organisering

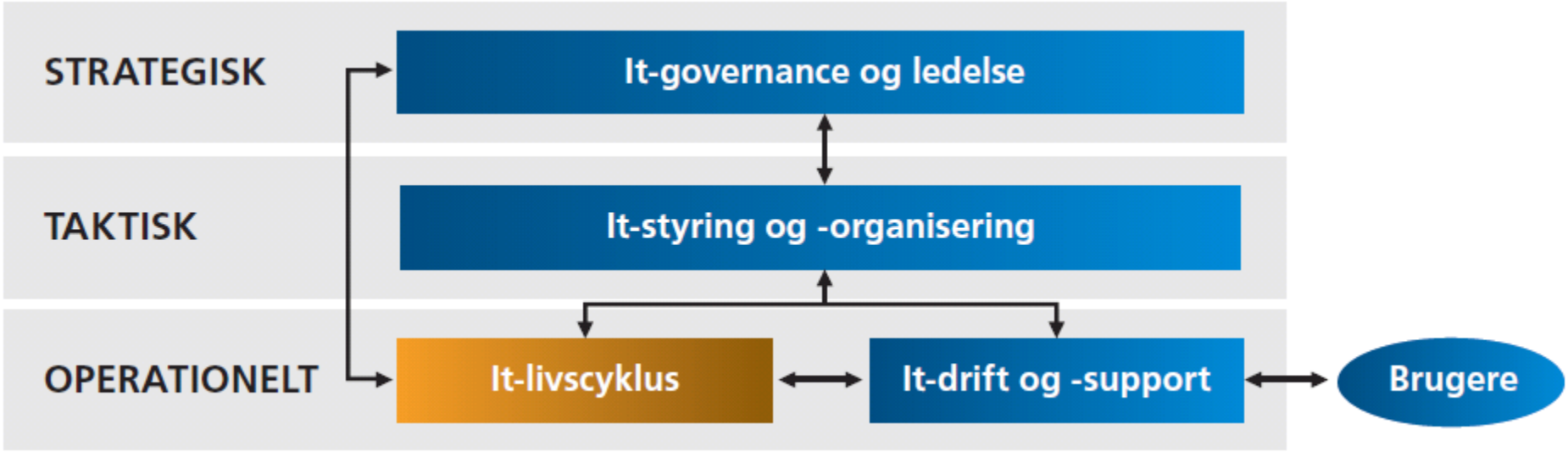


6.1 Styringsprincipper og -modeller

6.2 Organisering

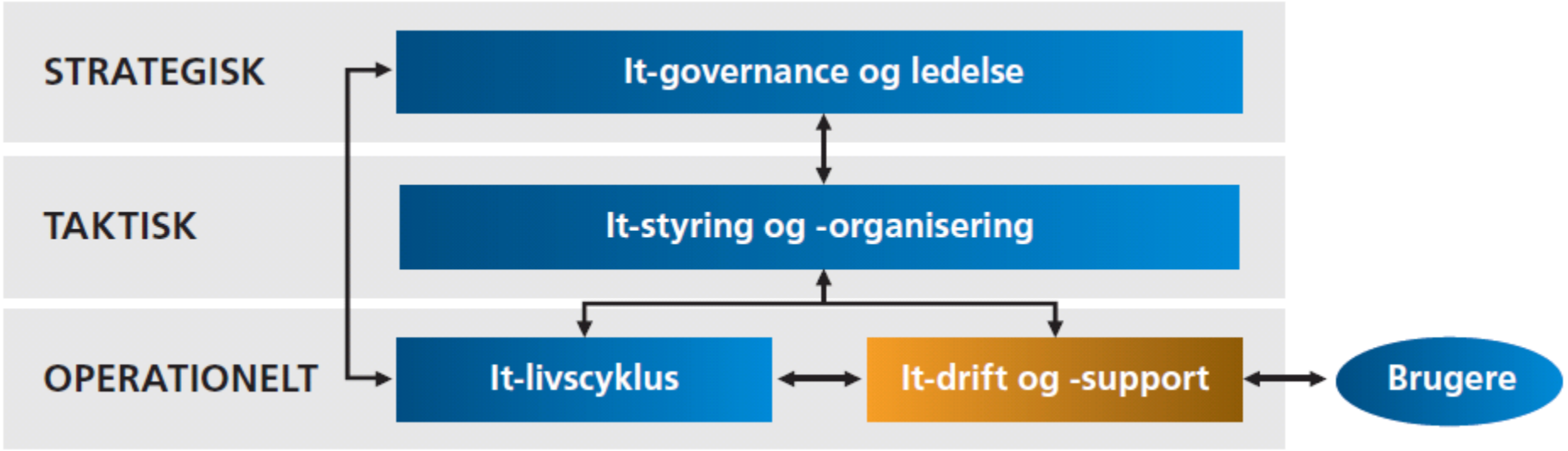
6.3 Styring af risici og eksterne krav

IT-styring og organisering



7.1 Behovsanalyse og afdækning af løsningsmuligheder
7.2 Anskaffelse af brugersystemer
7.3 Etablering og vedligeholdelse af it-infrastruktur
7.4 Udfasning

IT-drift og -support



8.1 It-drift og service management

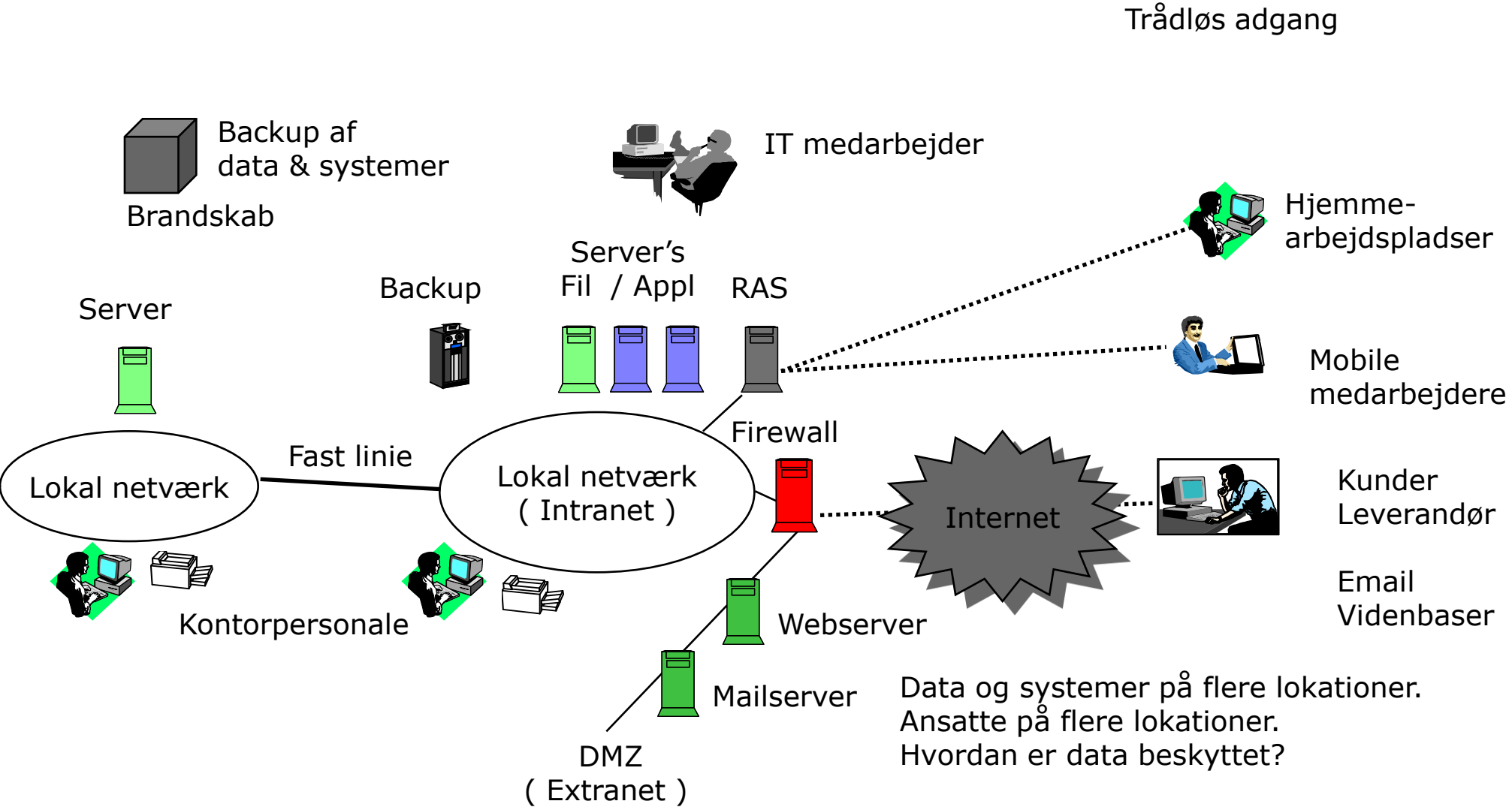
8.2 It-support og brugeradministration

Forstå informationssystemer og tilhørende forretningsprocesser

Hvorfor er IT vigtig?

- Alle forretningsprocesser er understøttet af IT
- Procedurer og kontroller udføres ved hjælp af systemer
- IT driften påvirker kvaliteten og tilgængeligheden af ledelsesinformation
- Krav til høj tilgængelighed
- Data dannes, udveksles og opbevares ved hjælp af systemer
- Dokumentation og godkendelse af transaktioner erstattes af elektroniske transaktioner og godkendelse
- Ledelsen skal vurdere risici og kontroller
- IT er outsourcet

IT infrastruktur



IT-udfordringer

- Lav (stigende) involvering af ledelsen
- 8 direktiv og bogføringsloven (dokumentation af kontroller)
- Formel IT-strategi til at understøtte virksomheden
- Udarbejdelse af risiko- og konsekvensanalyse
- Retningslinjer for IT-sikkerhed
- Beskrivelse af udviklingsprocessen
- Udarbejdelse af IT-driftsmanualer
- Manglende eller utilstrækkelige nødplaner/beredskab
- Utilstrækkelig fysisk sikkerhed
- Manglende dokumentation af udviklingsarbejde og systembeskrivelser
- Manglende procedure for tildeling og gennemgang af rettigheder
- Manglende overholdelse af projektbudgetter
- Stigende IT-omkostninger (især indirekte og projekter)

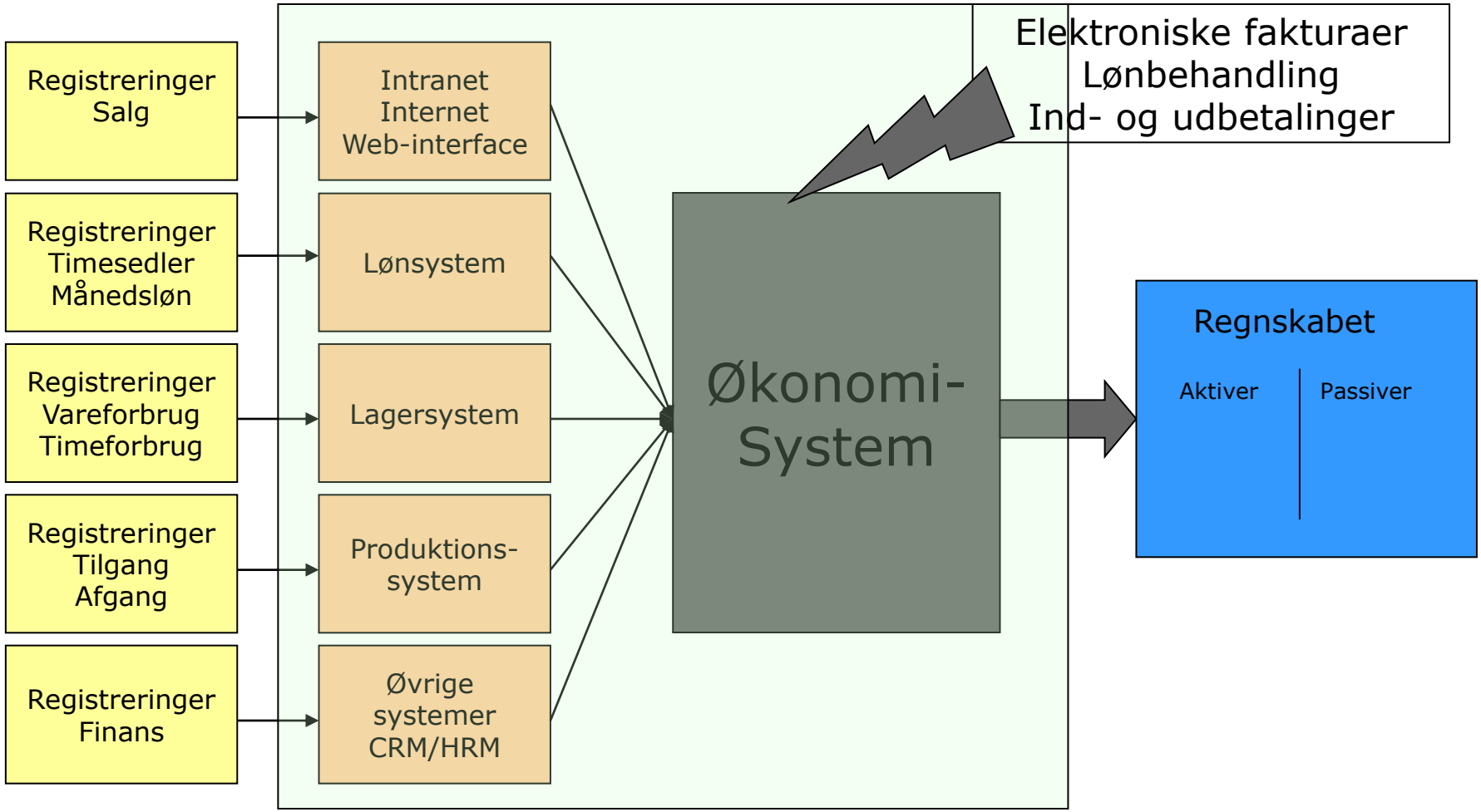
IT-procesmodel

IT-revision i revisionsprocessen

- Revisionsprocessen
- Planlægning – strategi
- Udførelse – eksperter
- Dokumentation – særlig rapport
- Kontrolmiljø
- IT-anvendelse

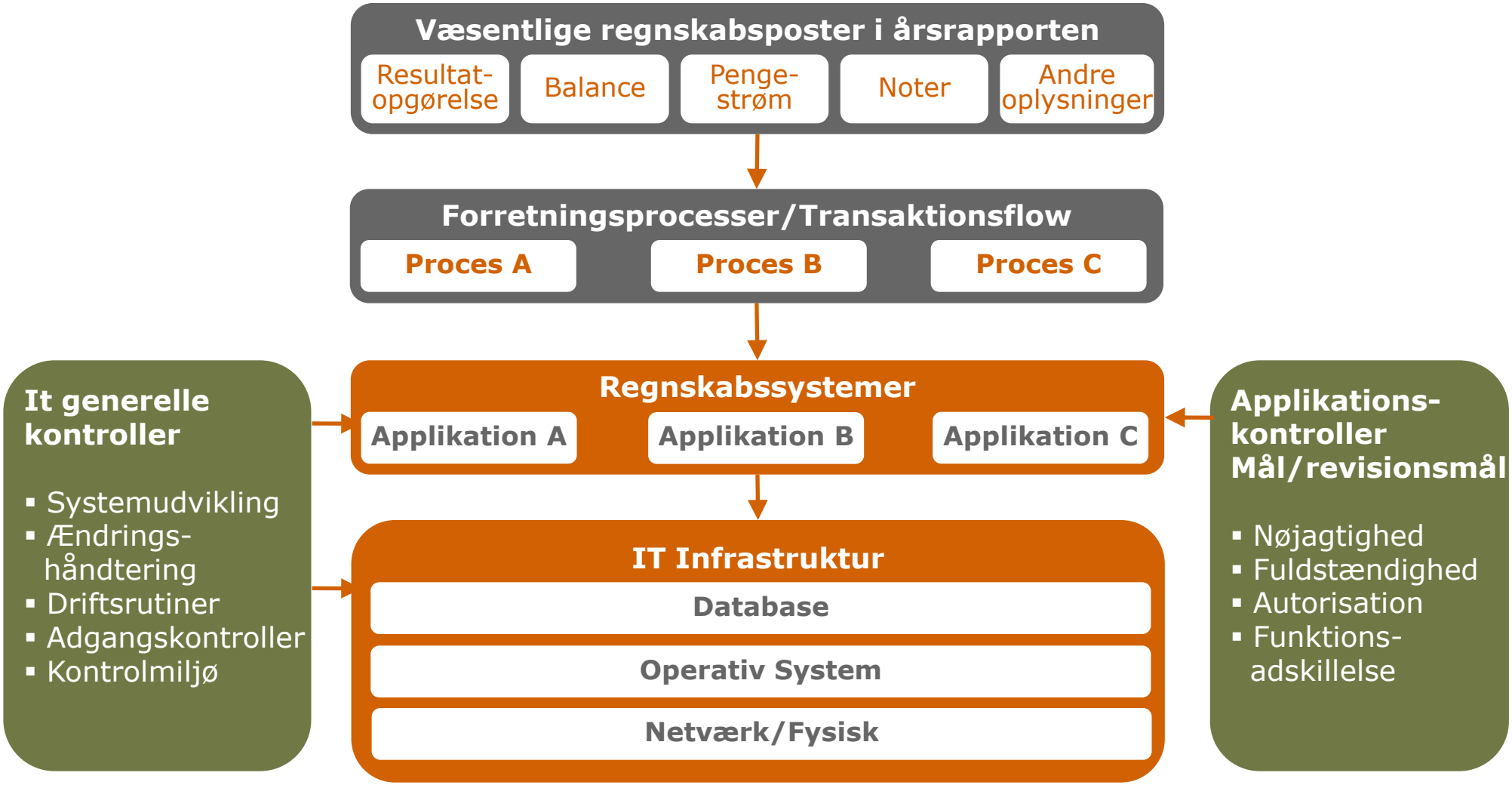
- Revisor skal være i stand til at vurdere selskabets IT-anvendelse

Virksomhedens informationssystem



Kilde: Inspi nr. 9-2005

Cobit i finansiel revision



Hovedformål med IT-revision

Gennemgå, vurdere og eventuelt teste virksomhedens IT-ressourcer, forretningsgange og IT-baserede registreringssystemer med henblik på at fastslå, om disse er tilstrækkeligt sikre og kontrollerede til at opfylde virksomhedens behov for sikkerhed og til at understøtte revisionen ved at basere denne på kontrollerne.

- Sædvanlig finansiel revision er ikke tilstrækkelig
- Opnå en anden form for revisionsbevis
- Opnå den nødvendige hurtighed som loven kræver
- Øget anvendelse af IT, ERP-systemer, Dynamics, SAP og lign.
- Internationale og dermed større og komplekse virksomheder
- Cloud, outsourcing, hosting

Revisor skal være i stand til at:

- Vurdere risikoen ved virksomhedens IT-anvendelse
- Fastlægge revisionsstrategien
- Afgrænse gennemgangen af de generelle IT-kontroller
- Konkretisere de overordnede revisionshandlinger
- Vurdere resultatet af den foretagne gennemgang

Vurdering af selskabets IT-anvendelse

- Indledende vurdering af omfanget af virksomhedens IT-anvendelse.
- I ISA forudsættes, at virksomheder er afhængige af IT-anvendelsen
- Outsourcede IT ydelser
- Spørgsmål man bør stille:
  - Kan virksomheden risikere væsentlige økonomiske tab ved reduktion eller bortfald af IT
  - Kan ødelæggelse af elektroniske data medføre, at regnskaber ikke kan aflægges og/eller revideres
  - Kan virksomhedens IT medføre åbenbare fejl, mangler eller usikkerheder i regnskaber

Lovgivning

- SL § 130 – Forretningsorden
- Årsregnskabsloven § 135 - revisionspligt
- Bogføringsloven og bogføringsbekendtgørelse
- Revisorloven § 16 - Opgaver udføres med fornøden omhu, nøjagtighed og den hurtighed, som deres beskaffenhed tillader, samt i overensstemmelse med god revisorskik.
- Erklæringsbekendtgørelsen § 1 - Revisor skal tage stilling til alle forhold, medmindre de er uvæsentlige for formålet med erklæringen eller rapporten

- Systemrevisionsbekendtgørelsen § 3 – Revisor skal påse betryggende kontrol- og sikringsforanstaltninger ved udvikling, vedligeholdelse og drift af datacentralens systemer
- Lov om finansiel virksomhed § 71 – En finansiel virksomhed skal have betryggende kontrol- og sikringsforanstaltninger på IT-området

Lovgivning

SL § 115 og 116

I kapitalselskaber, der har en bestyrelse, skal denne ud over at varetage den overordnede og strategiske ledelse og sikre en forsvarlig organisation af kapitalselskabets virksomhed påse, at

(I kapitalselskaber, som har et tilsynsråd, skal tilsynsrådet påse, at)

1) *bogføringen og regnskabsaflæggelsen foregår på en måde, der efter kapitalselskabets forhold er tilfredsstillende,*

2) *der er etableret de fornødne procedurer for risikostyring og interne kontroller,*

3) *bestyrelsen/tilsynsrådet løbende modtager den fornødne rapportering om kapitalselskabets finansielle forhold,*

4) *direktionen udøver sit hverv på en behørig måde og efter bestyrelsens retningslinjer og*

5) *kapitalselskabets kapitalberedskab til enhver tid er forsvarligt, herunder at der er tilstrækkelig likviditet til at opfylde kapitalselskabets nuværende og fremtidige forpligtelser, efterhånden som de forfalder, og kapitalselskabet er således til enhver tid forpligtet til at vurdere den økonomiske situation og sikre, at det tilstedeværende kapitalberedskab er forsvarligt.*

SL § 118

Direktionen skal sikre, at kapitalselskabets bogføring sker under iagttagelse af lovgivningens regler herom, og at formueforvaltningen foregår på betryggende måde.

SL § 130 – Forretningsorden

Revisionsstandarder

ISA 315 + 330

ISA 402

ISA 265

ISA 240

ISA 620

ISA 610

ISAE3000/ISAE3402 handler om erklæring

God IT-skik

Cobit Framework

Særlig IT-standards

Systemrevisionsbekendtgørelse

Bogføringsloven - Transaktionsspor, §4 stk. 1

- Den sammenhæng, der er mellem de enkelte registreringer og den bogføringspligtiges årsrapport, skatte- eller afgiftsopgørelse, tilskudsregnskab eller tilsvarende regnskabsopstilling, der skal udarbejdes i henhold til lovgivning.
- Kontrolsporet er defineret som: ”de oplysninger, der dokumenterer registreringernes rigtighed”
- Oplysningerne kan være interne og eksterne underbilag, afstemninger, analyser
- Verificering af registreringerne

Systembeskrivelse

- Systembeskrivelse af registrering af transaktioner – § 14
- Beskrivelse skal sikre fuldstændighed og nøjagtighed af bogføring - Forretningsgange
- Beskrivelse af det materiale, der danner grundlag for registreringer
- Beskrivelse af registreringerne – konteringsinstruks, systemer
- Beskrivelse af automatiske registreringer, beregningsgrundlag og beregningsformler
- Undtagelsesregel for standardsystem (stk. 4)
  - Ikke væsentlige ændringer
  - Leverandøren udarbejdet beskrivelser, som virksomheden opbevarer

Opbevaring af regnskabsmateriale

- Opbevaring af regnskabsmateriale - § 10
- Betryggende vis i 5 år
- Hele opbevaringsperioden muliggør en selvstændig og entydig fremfinding
- Elektronisk medie mv kunne udskrives i klarskrift (uden bearbejdning, beregninger eller tilpasninger)
- Beskrivelsen af systemer til at fremfinde og udskrive regnskabsmaterialet i klarskrift skal opbevares i klarskrift
- Opbevares her i landet (indeværende og forrige måned kan opbevares i udlandet)
- Norden accepteret
- EU og tredjelande?

Dispensation

Opnås dispensation til opbevaring udenfor Danmark og Norden:

1. Udelukkende elektronisk regnskabsmateriale
2. Direkte online adgang til det elektroniske regnskabsmateriale fra Danmark
3. Begrundet i et ønske om at opnå iøjnefaldende besparelser
4. Ingen formodning for, at ansøger vil misbruge en dispensation til skade for danske skatte- og efterforskningsmyndigheder
5. De hørte myndigheder har ikke i deres udtalelse anført noget, der konkret taler imod, at der meddeles dispensation

Dispensation gives med vilkår om at:

- Regnskabsmateriale opbevares efter BFL's krav
- Udelukkende findes i fysisk form skal opbevares i Danmark/Norden
- Dispensationens gyldighed begrænses til tre år.
- Fornyet vurdering af ansøgningen ved ændringer forhold/overtrædes

Erhvervsankenævnet

- 16/6-2006: Server i Tyskland
- 1/7-2009: Server i USA– Henv til 16/6-06
- 14/7-2011: England, Tyskland og 5 i USA
- 10/10-2011: USA
- 6/12-2012 ((16/6-8; 1/7-09 og 14/7-11):
  - Koncern SAP R/3 & Central B-system i Schweiz (4 i alt)
  - En ØS på Server i Tyrkiet og en Database i Mexico
- 6/12: 2 kendelser til Fornyet behandling af 14/7-11. Angående dispensationsvilkårene (SAP i USA)

  Den foreliggende sag er indbragt for Erhvervsankenævnet, da Erhvervsstyrelsen, uanset Erhvervsankenævnets førnævnte kendelser ikke ses at have følt sig forpligtet af den ved nævnets kendelser udstukne praksis og således har nægtet dispensation.

  Nævnet finder afslutningsvis anledning til at bemærke, at de problemer, som efter myndighedernes opfattelse rejser sig ved denne forståelse af lovens betingelser, er egnet til regulering ved særlige bestemmelser.

Lovgivning – sammenfatning

- Lovgivning i form af revisionsstandarder har været kendt i de seneste 10 år.
- Revisionsstandarder er meget detaljerede og strukturerede målt i forhold til andre standarder. De vil fremover fortsat præge dansk praksis.
- Et område med færre holdninger end anden traditionel revision.
- God revisionsskik understøttes også af FSR´s blå notathæfter med tilhørende eksempler.
- ISA 315 og 330 (gen)indfører Coso-begrebsrammen
- Grundloven indenfor bogføring, der ofte overses, men indeholder flere af de grundlæggende regler for bogføring.
- Transaktionsspor er sammenhæng af den enkelte transaktion fra bogføring til regnskab eller skatteopgørelse. Fra fødsel til grav.
- Kontrolspor sikrer en nøjagtig registrering af alle bilag fra bogføring til regnskab. Transaktionsspor kan gå begge veje.
- Systembeskrivelse, herunder forretningsgange for it-anvendelse, så en fremmed bruger kan anvende systemet.
- Overtrædelse af bogføringsloven påvirkede tidligere revisionspåtegningens konklusion. Det er senere ændret.

Supplerende oplysninger - Opbevaring

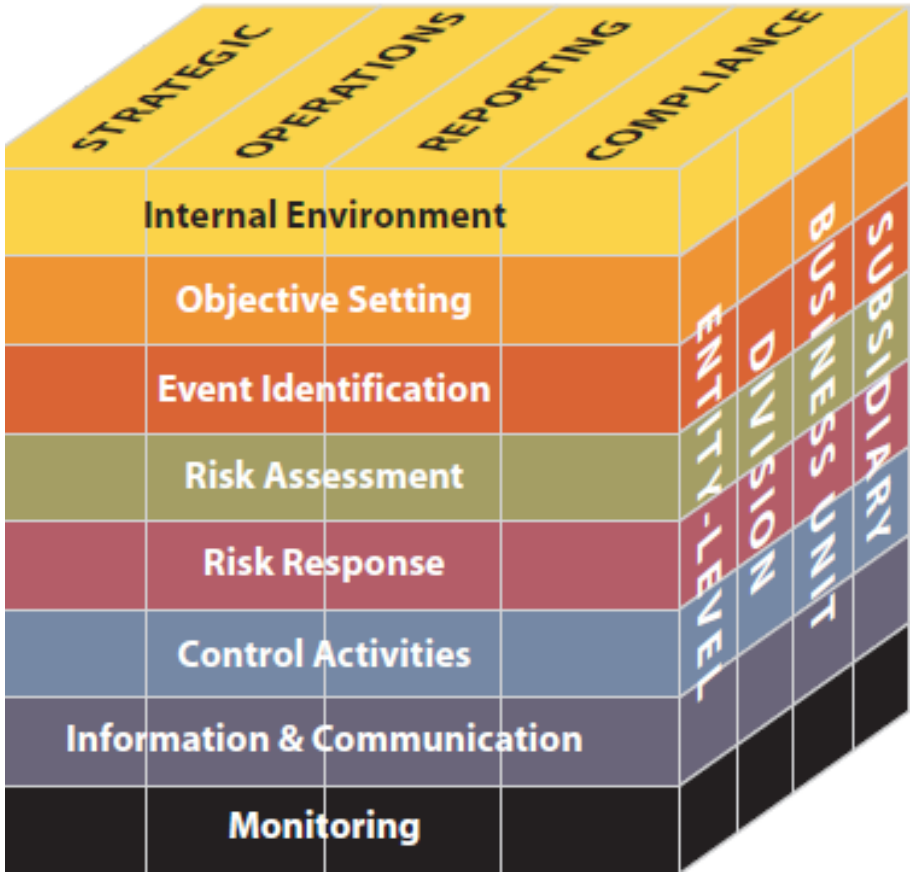
Supplerende oplysninger vedrørende andre forhold

Uden at det har påvirket vores konklusion, skal vi oplyse, at selskabet ikke har overholdt bogføringslovens krav om, at regnskabsmateriale skal opbevares i Danmark, hvorved ledelsen kan ifalde ansvar.

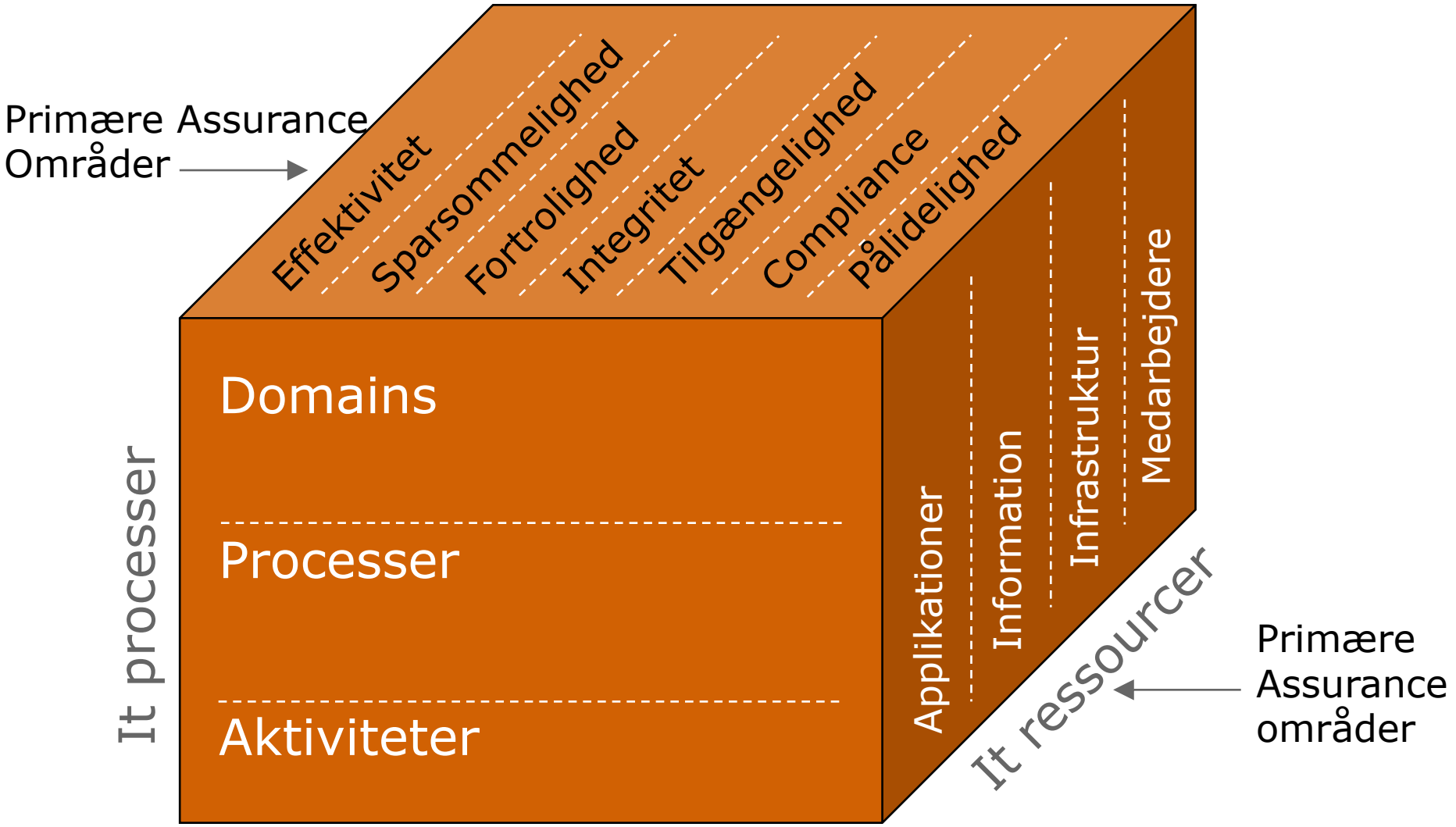
Virksomhedens risikostyring - Generelt

COSO kuben

1. Intern kontrolmiljø
2. Målsætning
3. Identificering af begivenheder
4. Risikovurdering
5. Risikohåndtering
6. Kontrolaktiviteter
7. Information og kommunikation
8. Overvågning



IT Assurance – Cobit kuben



Interne IT-kontroller

- Generelle kontroller, der omfatter sikring af data, systemer og drift
- Applikationskontroller, er omfatter systematiske IT-baserede kontroller og manuelle kontroller på et givent område
- Programmerede kontroller

Opgave – er IT-anvendelsen væsentlig

- SAS – flyselskab omsætter 54 mio., Egenkapital 17 mio., Balance 48 mio.
- Danske Bank, 25 mia. renteindtægter, Egenkapital 125 mia., Balance 3.400 mia.
- Voldslev Autoophug, omsætning 7 mio., Egenkapital -0,2 mio., Balance 4,2 mio.
- XX Holding, Omsætning 0 kr, Egenkapital, 200 tkr., Balance 400 tkr.
- Stålproduktion Jylland A/S, Omsætning 24 mio., Egenkapital 2,3 mio., Balance 18 mio.

Generelle IT kontroller

Interne kontroller

- COSO-begrebsrammen
  - Kontrolmiljøet
  - Risikovurderingsproces
  - Informationssystemet
  - Kontrolaktiviteter
  - Overvågning af kontroller
- Opfylde bogføringsloven og anden lovgivning
- Formelle forretningsgangsbeskrivelser
- Interne kontroller opdeles i generelle og applikations-kontroller

Forhold og begivenheder, der kan indikere risici for væsentlig fejlinformation (ISA 315 bilag 2)

- Uoverensstemmelser mellem virksomhedens it-strategi og dens forretningsstrategier
- Ændringer i it-miljøet
- Installation af nye betydelige it-systemer der vedrører regnskabsaflæggelse

Informationssystemet (ISA 315 – afsnit 18)

Revisor skal opnå en forståelse af det informationssystem og tilhørende forretningsprocesser, der er relevante for regnskabsaflæggelsen, herunder følgende områder:

b) de procedurer i både it-systemer og manuelle systemer, der anvendes til at igangsætte, registrere og behandle disse transaktioner samt rette dem efter behov, overføre dem til finansbogholderiet og rapportere dem i regnskabet

Kontrolaktiviteter (ISA 315- afsnit 20)

Ved forståelsen af virksomhedens kontrolaktiviteter skal revisor opnå en forståelse af, hvordan virksomheden har reageret på it-relaterede risici (jf. afsnit A103-A105).

Kontrolaktiviteter (ISA 315 Bilag 1 afsnit 9)

Informationssystemets kontrolaktiviteter:

- Applikationskontroller,
  - Vedrører behandlingen i individuelle applikationer
    - Efterregning af nøjagtigheden af registreringer,
    - Vedligeholdelse og gennemgang af balanceposter og råbalancer,
    - Automatiserede kontroller, f.eks. inddatavalidering og kontrol af nummerrækkefølge
    - Manuel opfølgning på afvigelsesrapporter.
- Generelle it-kontroller,
  - Politikker og procedurer, der vedrører mange applikationer og understøtter, at applikationskontroller fungerer effektivt ved at hjælpe med til at sikre, at informationssystemer til stadighed fungerer behørigt.
    - Kontroller af programændringer,
    - Kontroller, som begrænser adgangen til programmer eller data,
    - Kontroller af implementering af nye udgaver af standardsoftwareapplikationer og
    - Kontroller af systemsoftware
- Se afsnit i bilag 1 bl.a. afsnit 2, 4, 5, 6, 7 og 8

IT specifikke risici (ISA 315 A63)

- IT medfører specifikke risici for en virksomheds interne kontrol:
- Tillid til systemer eller programmer, som behandler data unøjagtigt, og/eller behandler unøjagtige data
- Uautoriseret adgang til data
- Mange brugere har adgang til en fælles database,
- IT-medarbejderes adgangsrettigheder
- Manglende funktionsadskillelse
- Uautoriserede ændringer af data i stamfiler eller af systemer eller programmer,
- Manglende nødvendige ændringer af systemer eller programmer,
- Upassende manuel indgriben,
- Tab af data eller manglende mulighed for at få adgang til data

Generelle IT-kontroller (ISA 315 A104)

Generelle IT-kontroller er politikker og processer

- Mange applikationer
- Understøtter, at applikationskontroller fungerer effektivt

Generelle IT-kontroller, som bibeholder informationers integritet og sikkerheden af data, omfatter normalt kontroller med:

- Drift af datacentre og netværk
- anskaffelse, ændringer og vedligeholdelse af systemsoftware
- programændring
- adgangssikkerhed
- anskaffelse, udvikling og vedligeholdelse af applikationssystemer.

Generelt er de implementeret for at imødegå de risici omtalt i afsnit A63 i ISA 315

Generelle IT kontroller

Generelle IT kontroller

CobiT Control Objective Heading	PCAOB IT General Control Heading			
	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire or develop application software.	●	●	●	●
2. Acquire technology infrastructure.	●	●	●	
3. Develop and maintain policies and procedures.	●	●	●	●
4. Install and test application software and technology infrastructure.	●	●	●	●
5. Manage changes.		●		●
6. Define and manage service levels.	●	●	●	●
7. Manage third-party services.	●	●	●	●
8. Ensure systems security.			●	●
9. Manage the configuration.			●	●
10. Manage problems and incidents.			●	
11. Manage data.			●	●
12. Manage operations.			●	●

Anskaffelse, ændringer og vedligeholdelse af systemsoftware og applikationer

- **Kontrol med systemudviklingsaktiviteterne**
  - Standarder og procedurer eller formaliseret metode
- **Procedurer til styring af og kontrol med rettelser og ændringer (versionsstyring mv.)**
- **Fyldestgørende, dokumenterede og bruger-godkendte specifikationer**
  - Krav til funktioner og kontroller
  - Hensyntagen til relevant lovgivning,
- **Kvalitetssikret via reviews, test mv.**
  - Godkendelse af brugerne og systemejer inden frigivelse til produktion

Driftsafvikling

Effektiv drift

- Forebygger og opdage fejl
- Forebygger og opdage besvigelser
- Forebygger og opdage skader og ødelæggelse

Kontrolleret miljø med godkendte programmer og data

Driftsvejledning – realtime eller batch

Kontrol af fuldstændighed og nøjagtighed af data

Retningslinier for rettelser, tilføjelser eller sletning

Arkivregistrering

Vedligeholdelsesplaner

Drift af datacentre og netværk

- Dokumenterede og godkendte driftsplaner
- Overførsel af programmer til produktion sker efter procedurer, som sikrer, at der kun driftsafvikles autoriserede programmer.
- Kontroller, som sikrer, at driftsfejl og afvigelser opdages og behandles.
- Regler og retningslinier for rettelser udenfor den normale driftsafvikling
- Datakommunikationen- og transmission er hensigtsmæssigt sikret i relation til integritet og afsløring af indholdet.
- Adgangen til IT-lokaliteterne er sikret mod uønsket og uautoriseret adgang
  - Skalsikring og
  - Adgangskontrolsystemer
- Adgangen til IT-lokaliteterne administreres
- Rumsikring af IT-lokaliteterne til imødegåelse af brand, vand og overophedning
- Foranstaltninger til sikring af vedvarende forsyninger.

Drift af datacentre og netværk (Fysisk sikkerhed)

Observation	1	2	3	Anbef.	Ændr.
Anonymt IT-lokale				**Ja**	
Vinduer i IT-lokalet				**Nej**	
Aflåst dør til IT-lokalet				**Ja**	
Adgangskontrolsystem (kode/kort)				**Ja**	
Hvor mange har nøgle til IT-lokalet				**IT-afd.**	
Serverne aflåste og fastspændte				**Ja**	
Tyverisikring				**Ja**	
Branddør til IT-lokalet				**Ja**	
Branddetektorer i IT-lokalet				**Ja**	
Brandslukningsudstyr				**Inergen/ argonite**	

Drift af datacentre og netværk (Fysisk sikkerhed)

Observation	1	2	3	Anbef.	Ændr.
Test af brandudstyr				**Ja**	
Brandsikring udenfor IT-lokalet				**Ja**	
Koblet til alarmcentral (indbrud/brand)				**Ja**	
Aircondition i IT-lokalet				**Ja**	
Vandrør i IT-lokalet				**Nej**	
IT-gulv				**Ja**	
Vanddetektorer i IT-gulv				**Ja**	
Serverne hævet fra gulvet				**Ja**	
Brandskab i IT-lokalet				**Nej**	
UPS-anlæg				**Ja**	

Drift af datacentre og netværk (Backup)

- Skriftlige procedurer for sikkerhedskopiering
- Registrering og mærkning af sikkerhedskopiering
- Sikkerhedskopiering omfatter alle relevante systemer og data
- Nok generationer til imødegåelse af læsevanskeligheder i en recovery-situation
- Betryggende opbevaring og håndtering af sikkerhedskopierne,
  - Opbevaring i eksternt sikkerhedsarkiv,
  - Medarbejdere har ikke adgang til alle data og sikkerhedskopier
- Regelmæssige tests af sikkerhedskopiernes fuldstændighed og læsbarhed.

Adgangssikkerhed

- Adgangskontrol
  - Sikkerhed på filniveau
  - Sikkerhed i løbende drift
  - Sikkerhed ved ekstern kommunikation
- Logning/fejlrapport af utilsigtede hændelser
- Rapportering om sikkerhedsnedbrud
- Personadskillelse og begrænsning i brugerrettigheder
- Uautoriseret adgang – hacking
- Særlige bruger-id

Adgangssikkerhed

- Identifikation af brugerne
  - Entydig bruger-ID og personligt hemmeligt kodeord
- Krav, procedurer og kontroller vedr. anvendelsen og udskiftningen af kodeord
- Begrænsninger af den enkelte brugers adgang, som understøtter funktionsadskillelse og begrænser adgangen til et arbejdsmæssige behov.
- Logning af forsøg på sikkerhedsbrud og anvendelse af priviligerede brugerprofiler.
- Funktionsadskillelsen opretholdes via opsætning af systemsoftware
  - Valg af installationsparametre og
  - ændring af eventuelle standardkodeord
- Systemopsætningen sikrer en effektiv begrænsning i adgangen til funktioner og programmer, der kan omgå sikkerhedssystemet
- Netværket og netværksintegrationen er hensigtsmæssigt sikret mod uautoriseret access og afsløring af dataindholdet
- Forholdsregler mod uautoriseret adgang via kommunikationslinier
- Kontrol med anvendelsen af særlige bruger-ID med udvidede beføjelser til brug i nødsituationer.

Konsekvens ved ineffektive Generelle IT kontroller

- Applikationskontroller eller it afhængige manuelle kontroller er ikke til at stole må
- IT baseret revisionsbevis er ikke til at stole på
- Revisionsholdet skal revurdere:
  - Hvad der kan gå galt på revisionsmålsniveau
  - Revisionsmål
  - Risikovurdering (kombinationen mellem Iboende og kontrolrisiko)

Alternative Generelle IT Kontroller

- Gennemgang af logs over brugeradgange
- Logs over programændringer
- Involvering af IT chefen i driften

IT overvejelser ved revisionen

- Intern revision
- Omfattende IT revision
- Revisionsplan
- Generelle IT kontroller
- Applikationskontroller
- Anvendelse af specialister
- Management letter
- IT i revisionsprotokollen

Risikoområder – IT anvendelsen

- Systemændringer
- Brugeradministration
- Oprettelse, ændringer og sletning af salgspriser
- Adgangsrettigheder til varelagerpriser (vareforbrug)
- Debitorstamdata
- Kreditorstamdata
- Cash management data
- Prisændring i forbindelse med fakturering
- Valideringsregler ved input

Planlægning

- Transaktionsmængder
- Kompleksitet
- Afhængighed/ Forretningskritiske
- Effektivitet (Revision)
- Systemsammenhænge
- Bogføringsloven
- Revisionsstrategi
- Besvigelser

Generelle udfordringer for revisoren

- IT driften outsourcet
- Validering af rapporter/anvendes i revisionen
- Hvem udfører IT revisionen
- Kompetence
- Grænseflader mellem revision/specialist (IT revisor)
- Dokumentation for systemrevision
- Anvendelse af systemrevision
- Reduktion af substansrevision

Forslag til revisionshandlinger

- Der er ingen udvikling - kun vedligehold - revisor skal kontrollere, at alle produkter er kvalitetssikret
- Gennemgang af organisationsdiagram. Sikre funktionsadskillelse mellem IT-afdelingen og økonomiafdelingen.
- Afhængighed til enkeltpersoner kan undersøges
- Tilstrækkelig kompetence hos IT-medarbejderne
- Stikprøvevis kontrollere sladrelister for uregelmæssigheder
- Revisor skal kontrollere at opdateringer sker i et nøje planlagt forløb
- Interview med medarbejdere omkring selskabets vedligeholdelse
- Kontrollere batch-kørsler særligt vedrørende lager
- Kontrollere ind- og uddata i kørsler
- Kontrollere rapport for driftsfejl, forstyrrelser, hacking
- Gennemgå systembeskrivelser og sikre, at de overholder lovgivningen samt løbende opdateres.

Revisors gennemgang omfatter

- Revisionen gennemføres ved interview, observationer og efterprøve det indsamlede materiale.
- Funktionsadskillelse og adgangskontroller
- Forretningsgange
- Beskyttelse mod skader og tyveri
- Driftsafvikling og -udvikling
- Kontroller fungerer i hele perioden
- Kontroller tilstrækkelige til at underbygge revision
- Brug af IT-specialister
- Overblik over driftsformer og autorisationssystemer
- Forretningsgange og driftsformer
- Kontrol af logisk adgangskontrol og systemsoftware
- Gennemgå parameteropsætning

Afslutning

Forståelse af virksomheden og dens omgivelser

- Virksomhedens drift:
  - involvering i E-handel, såsom salg og marketing over internettet
- Mål og strategier samt tilknyttede forretningsrisici
  - brug af IT (en potentiel relateret forretningsrisiko kunne for eksempel være, at systemer og processer ikke er kompatible)

Bilag 1: Interne kontrolelementer

- Kontrolmiljø
- Virksomhedens risikovurderingsproces
- Informationssystemet, herunder de tilknyttede forretningsprocesser, der er relevante for regnskabsaflæggelse og kommunikation
- Kontrolaktiviteter
- Overvågning af kontroller

Bilag 2: Forhold og begivenheder, der kan indikere risici for væsentlig fejlinformation

Interne IT-kontroller for mindre virksomheder

Kendetegn

- Omfattet af samme love og standarder som større virksomheder med undtagelse af systembeskrivelse
- Formål at sikre, at registreringer og regnskaber er pålidelige
- Anvender it for nemmere at administrere oplysninger og informationer
- Den typiske danske virksomhed

Væsentlige kontroller

Adgangskontroller

Fortsat drift (Business Continuity)

Udvikling- og vedligeholdelse (Change Management)

Sikkerhed af data (Data Security Protokols)

Kapacitetsstyring

Revisors fokus skal være på ovennævnte

Oversigt over væsentligste elementer

Adgangs-kontroller	Fortsat drift	Udvikling og vedligeholdelse	Sikkerhed af data	Kapacitets-styring
Password Login og adgang Brugerprofiler Adgang fra eksternt net	Ansatte Hardware Back-up	Udviklings-afdeling Kommunikation af ændringer og tilpasninger Udvikling af programmer Intern formåls-beskrivelse for udviklings-afdeling	Ledelse og kontrol Sårbarhed og risici for ledelsen Firewalls Intern netværks-styring	Ressource-planlægning Styring af fremtidigt behov Netværksrapporter kvartalsvis

Revision og svagheder i IT

Case – har det betydning for revision at:

- Server placeret på fladt gulv i en kælder. Brandslukning er sprinkler med vand.

- Consol står altid ”sign on”. Der er direkte adgang til databaser, administrative værktøjer og kommandolinier

- Alle systemændringer leveres af NN. NN er imødekommende og laver alle tilretninger, der måtte ønskes.

- Nødplan er 10 år gammel og baseret på daværende teknologi.

- Der foreligger ingen dokumentation for back-up

Revisionsstrategi

Kontrolbaseret revisionsstrategi

- Forventning om gode kontroller
- Ledelsen fokuserer på kontrol
- Kontrolbaseret revision
- Cost/benefit vurdering
- Proces-kompleksitet
- Basal funktionsadskillelse er et krav
- Godt kontrolmiljø

Substansrevisionsstrategi

- Forventning om utilstrækkelig kontroller
- Ingen ledelsesmæssig fokus
- Overskuelige processer
- Små datamængder eller uhomogene datamængder
- Utilstrækkelig funktionsadskillelse
- Utilstrækkelige generelle kontroller

Gennemgang af brugersystemer

Gennemgang af brugersystemer – 1

Gennemgang af brugersystem

- Systemets funktioner
- Behandling af inddata
- Anvendte registre

– Program- og Data-filer

- Behandling af uddata
- Kontroller
- Transaktions- og kontrolspor

Gennemgang af brugersystemer – 2

Systemets funktioner

- Oversigt over samlede brugersystemer
- Revisionsmæssig betydning vurderes for hvert system
- Udvælgelse af væsentlige systemer
- Detaljeret beskrivelse med ord og flowchart
- Rotationsprincip

Gennemgang af brugersystemer – 3

Systemets funktioner (fortsat)

- Beskrivelsen skal indeholde
  - Alle hovedfunktioner i systemet
  - Rækkefølgen af hovedfunktioner
  - Alle hovedtransaktioner
  - Alle hoveddatafiler
  - Alle væsentlige udskrifter/filer fra systemet
  - Kontrolspor
  - Afstemning af system
  - Tilknyttede funktioner

Gennemgang af brugersystemer – 4

Behandling af inddata

- Data fødes en gang og kun en gang
- Fejl i inddata genererer flere fejl
- Kontroller skal forebygge og opdage fejl, herunder:
  - Kun autoriserede data registreres
  - Alle autoriserede data kommer med
- Inddata kan være automatiske posteringer, der skal dokumenteres

Gennemgang af brugersystemer – 5

Anvendte registre (programfiler)

- Indeholder programkoder og kildekoder
- Krav til sikkerhedskopi af programfiler og ikke kun datafiler
- Krav til kopi af systemopdateringer, så data kan genudskrives og gendannes
- Sikkerhed for ændringer siden sidste revisionsperiode
- Undgå ændringer i styresystem

Gennemgang af brugersystemer – 6

Anvendte registre (datafiler)

- Udskrift over filerne med angivelse af deres funktion
- Post-/feltbeskrivelse
- Datadefinitioner
- Krav til sikkerhedskopiering af stamdatafiler

Gennemgang af brugersystemer – 7

Behandling af uddata

- IT-systemer kan danne mange foruddefineret og brugerdefinerede rapporter
- Hvad kan systemet genererer
- Hvem kan danne udskrift
- Bruger/læseadgang styres

Gennemgang af brugersystemer – 8

Kontroller

- Forebyggende
- Opdagende
- Korrigerende

Kontroltyper

- Inputkontroller
- Proceskontroller
- Outputkontroller

Gennemgang af brugersystemer – 9

Inputkontroller

- Fornuftig formularopbygning
- Fuldstændighedskontrol
- Gyldighedskontrol
- Grænsekontrol
- Kombinationskontrol
- Validitetskontrol
- Filkontrol

TEST AF KONTROLLER

Gennemgang af brugersystemer – 10

Proceskontroller

- Kontroltotaler/cifre
- Fortløbende nummerering/sekvens-kontrol
- Recovery/restart
- Automatisk logning af differencer
- Rimelighedskontrol

TEST AF KONTROLLER

Gennemgang af brugersystemer – 11

Outputkontroller

- Kontroltotaler
- Nummerkontrol
- Afstemning
- Distributionskontrol
- Automatisk generede transaktioner

TEST AF KONTROLLER

Dokumentation og rapportering

Dokumentation

Hvor dokumenteres anvendelse af IT-revision

- Revisionsplan
- Revisionsstrategi
  - Substans- og systembaseret
- Arbejdspapirer
- Management Letter
- Revisionsprotokol
- Afslutningsnotat

Dokumentation

- Planlægningsnotat og arbejdspapirer er det væsentligste område for dokumentation for anvendelse af IT-revision.
- Revisor skal altid kunne dokumentere det udførte arbejde.
- Revisors overvejelser og konklusion skal fremgå klart af arbejdspapirerne
- Konklusion af indledende vurdering af IT-revision skal nævnes i planlægningsnotat.
- Gennemgang af generelle IT-kontroller bør nævnes i management letter og revisionsprotokol.
- Inddrages specialister udarbejdes ofte særskilt rapport til IT-afdelingslederne for en opfølgning på konstaterede forhold.

Omtale i revisionsprotokol

- Revision af IT-systemer
- Overordnet konklusion på IT-revisionen
- Eksempler på bemærkninger i revisionsprotokol
  - Ændringshåndtering
  - Adgange til systemer og data
  - Logisk funktionsadskillelse mellem IT-udvikling og –drift
  - Magtfulde adgangsrettigheder (operativ system og/eller databaser)

  - Identifikation og dokumentation af risici ved IT anvendelsen
  - Sikkerhedskopiering
  - Nødplaner og katastrofeberedskab
  - Styring af projekter
  - Procedurer til løbende overvågning af IT-sikkerheden

Revisionspåtegning

Forbehold

- Uenighed med ledelsen
- Utilstrækkeligt revisionsbevis

Eksempel

- Manglende bogførings-grundlag

Supplerende oplysninger

- Enig med ledelsen i den regnskabsmæssige behandling
- Ledelsen kan ifalde ansvar
- Simpel uagtsomhed –> ingen omtale
- Groft uagtsomhed -> omtale

Eksempel

- Manglende overholdelse af bogføringsloven

IT revision i praksis

IT-revision i praksis – 1

Ikke anvendelse af IT-revision

- IT-anvendelse ikke væsentlig
  - Intet økonomisk tab, regnskab kan revideres og ingen usikkerheder
- Ikke cost-effektiv – reviderer udenom systemet
- Grundlæggende krav ikke opfyldt
- Manglende kontrolmiljø
- Manglende funktionsadskillelse

IT-revision i praksis – 2

Anvendelse af IT-revision

- Komplekse IT-systemer
- Specialudviklede systemer
- Stor IT-afhængighed
- Store datamængder
- Automatiske generede posteringer
- Særskilt IT-afdeling (indikation)
- Branchespecifik (f.eks. finansielle virksomheder)

Kompetencer – Anvendelse af specialist

Anvendelse af udpeget ekspert ISA 620

- R's ansvar anden persons arbejde på andet område end regnskab eller revision. Arbejde anvende til at opnå tilstrækkeligt og egnet revisionsbevis
- Revisor fulde ansvar
  - Afgøre om brug af ekspert
  - Afgøre om arbejdet er hensigtsmæssigt
- Intern eller ekstern ekspert
- Betydeligheden og risici
- Ekspert underlagt kvalitetsstyringen
- Vurdere fornødne kompetence, færdigheder og objektivitet
- Opnå tilstrækkelig forståelse af ekspertens arbejde
- Skriftlig aftale
- Vurdere det udførte arbejde

Anvendelse af Intern Revision (ISA 610)

- Intern revision del af interne kontrol og ledelsesstruktur
- Forståelse af virksomheden og dens omgivelser
- Effektiv kommunikation mellem Intern og Ekstern revision
- Anvende intern revisions arbejde
- Ekstern revisors ansvar
- Intern revisions direkte assistance under ledelse, tilsyn og gennemgang af ekstern revision
- Organisatoriske placering og kompetencer samt kvalitetsstyring
- ER foretage alle betydelige vurderinger
- Kommunikere med øverste ledelse om anvendelse af intern revision
- Trusler mod revisors objektivitet

Revisionsmæssige overvejelse ved serviceleverandør/outsourcing

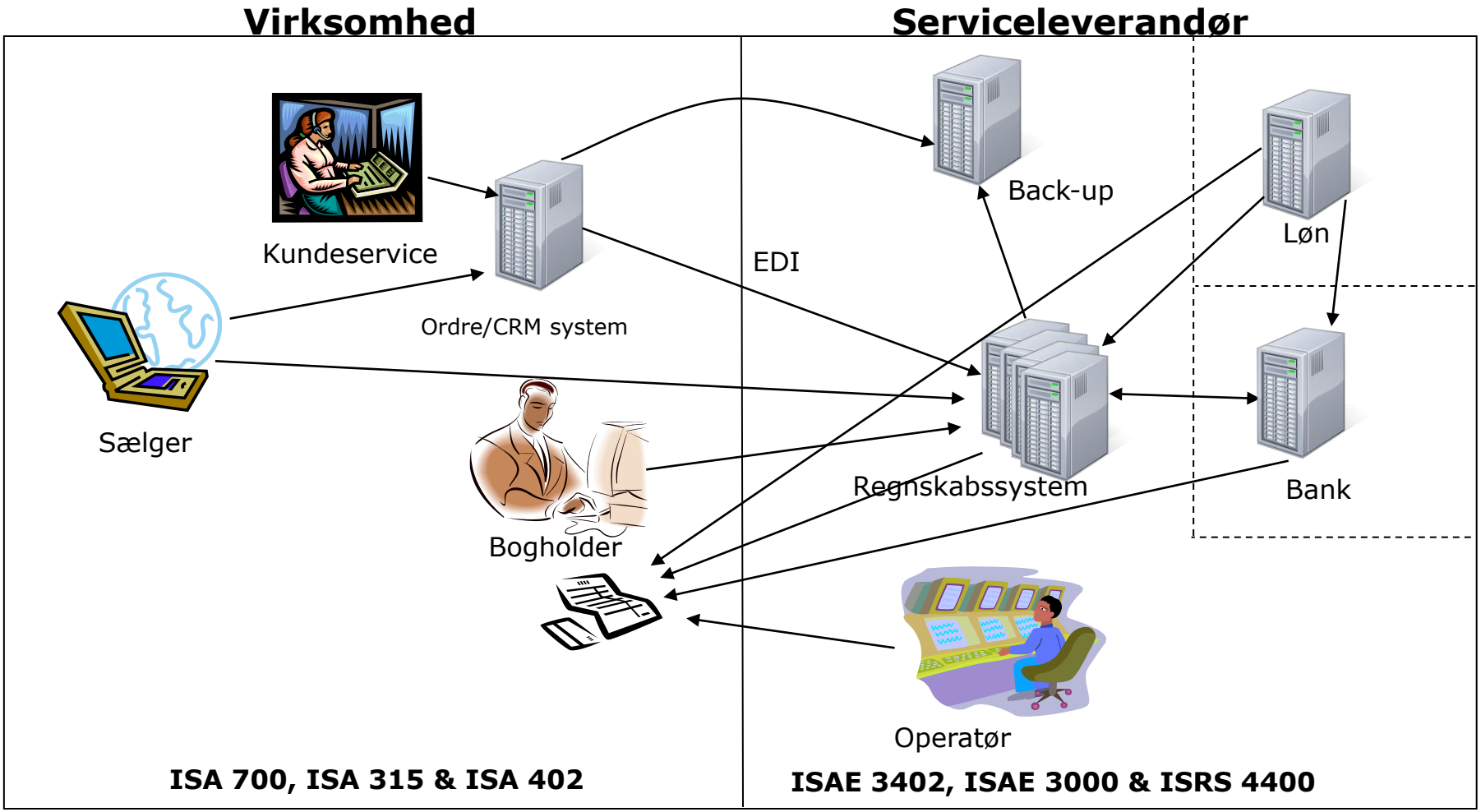
Outsourcing

Virksomheder outsourcer aktiviteter til eksterne leverandører:

- Det kan være ydelser, som spænder fra en specifik opgave efter virksomhedens anvisninger til at erstatte en virksomheds samlede forretningsenheder eller -funktioner.
- Ydelserne er integreret i virksomhedens forretningsmæssige aktiviteter.
- Ikke alle ydelser er relevante for revisionen.

- Ydelserne er relevante for revisionen brugervirksomhedens regnskab, når disse ydelser og kontrollerne er en del af informationssystemet eller forretningsprocesser relevante for regnskabsaflæggelsen.
- Andre kontroller kan også være relevante for revisionen (f.eks. kontroller til sikring af aktiver).

Interaktion brugervirksomhed og serviceleverandør



Outsourcing

- Ydelserne er en del af informationssystem/ regnskabsaflæggelses-processen, når de påvirker nogle af følgende faktorer:
- Transaktioner i driften, der er betydelige for regnskabet
- Procedurerne i it og manuelle systemer, der igangsætter, bogfører, behandler, korrigerer og overfører transaktioner til finansbogholderiet og rapporterer dem i regnskabet
- Regnskabsregistre, der understøtter information og specifikke konti i regnskabet, der anvendes til at igangsætte, bogføre, behandle og rapportere transaktioner, herunder korrektion af fejlbehæftet information, og hvordan informationen overføres til finansbogholderiet
- Måden informationssystemet opfanger begivenheder og forhold, som er betydelige for regnskabet
- Regnskabsaflæggelsesprocessen til udarbejdelse af regnskabet, herunder betydelige regnskabsmæssige skøn og oplysninger
- Kontroller med posteringer også ikke-rutinemæssige posteringer, der benyttes til at registrere ikke-tilbagevendende, usædvanlige transaktioner eller reguleringer

Mål for brugervirksomhedens revisor

- Revisors arbejde afhænger af arten og betydeligheden af ydelserne og deres relevans for revisionen

- Når brugervirksomheden anvender ydelser fra en serviceleverandør, er målene for brugervirksomhedens revisor:
- Opnå en forståelse af arten og betydeligheden af de leverede ydelser
- Ydelsernes indvirkning på interne kontroller med relevans for revisionen
- Tilstrækkelig til at identificere og vurdere risiciene for væsentlig fejlinformation
- Udforme og udføre revisionshandlinger som reaktion på risici
- Interaktion mellem serviceleverandørens og virksomhedens aktiviteter
- Forholdet mellem virksomheden og serviceleverandøren, herunder relevante kontraktvilkår for serviceleverandørens aktiviteter

Ikke tilstrækkelig forståelse

Revisor er ikke i stand til at opnå en tilstrækkelig forståelse ->

Revisor opnå forståelsen ved hjælp af følgende handlinger:

- Indhente en type 1- eller type 2-erklæring
- Kontakte serviceleverandøren gennem virksomheden for at indhente specifik information
- Besøge serviceleverandøren og udføre handlinger, for at indhente information om relevante kontroller hos serviceleverandøren
- Anvende anden revisor til at udføre handlinger, for at indhendte information om relevante kontroller hos serviceleverandøren

Cases

- Bank
- Løn
- IT drift ydelser
- Systemudvikling

Ydelser fra finansielle institutioner

Standarden gælder ikke for ydelser leveret af finansielle institutioner

- Ydelser begrænset til behandling af transaktioner på virksomhedens konto hos den finansielle institution
- Ydelser virksomheden specifikt har godkendt
- For eksempel
  - En banks behandling af bevægelser på en checkkonto
  - En børsmæglers behandling af værdipapirtransaktioner

Nødvendige handlinger

- Tegningsberettigede og fuldmagtsforhold
- Egne regler for kodeord (kompleksitet og interval for ændring)
- Gennemgang af brugerrettigheder
- Placering af ind- og udbetalingsfiler på netværket

Ydelser leveret fra lønbureau eller -system

HR og løn proces anses for væsentlig

- Lønomkostninger og tilhørende balanceposter væsentlige
- Indberetning og afregning til SKAT med videre
- Forpligtelser (feriepenge, skyldige skatter, evt pension)

Typiske outsourcede ydelser

- Lønbehandling og -administration
- Lønsystem der afvikles hos serviceleverandøren
- Lønsystem der afvikles hos brugervirksomheden
- Digitale lønsedler

Handlinger

- Revision af processen
- Serviceleverandørens revisor eller revisor selv

IT driften af finansielle applikationer

IT specifikke risici for en virksomheds interne kontrol

IT generelle kontroller vigtig for revision

- Drift af datacentre og netværk
- Anskaffelse, ændring og vedligeholdelse af systemsoftware
- Anskaffelse, udvikling og vedligeholdelse af applikationssystemer
- Programændring
- Adgangssikkerhed

Typiske outsourcede ydelser

- IT drift og ændringshåndtering
- Systemudvikling og ændringshåndtering
- Brugeradministration
- IT sikkerhed
- Netværk
- Sikkerhedskopiering og beredskab
- Servicedesk og IT service
- Forsyning

IT driften af finansielle applikationer (fortsat)

Nødvendige handlinger

- Overblik over ydelserne og ansvar
- Kontrakt
- Overblik over risici og kontroller
- Lovgivning
- Sikkerhedspolitik (egen og serviceleverandøren)
- Serviceleverandøren eller udføre handlinger selv
- Programændring
- Adgangssikkerhed

Revisionserklæring

- Beskrivelse af ydelserne fra serviceleverandør
- Høj grad af sikkerhed med beskrivelse af kontroller og udførte test
- Specifik eller generel erklæring
- Perioden
- Brugervirksomhedens handlinger

Systemudvikling – standardsystem med få ændringer

Forståelse af ydelsen

- Udvikling sker typisk hos tredjepart (Microsoft, SAP eller lignende)
- Begrænset tilretning, dog parameter opsætning og tilpasning af rapporter
- Systemleverandør/-konsulent står for implementering af ændringer og opsætning
- Brugervirksomheden har ikke selv it udviklere

Nødvendige handlinger

- Overblik over ydelserne og ansvar – herunder omfanget af ændringer
- Gennemgå kontrakt
- Påse at der er er dokumentation for opsætning og parametervalg
- Adgangsforhold til systemadministrator – begrænses til få og ingen i økonomi
- Overvej at medtage i protokol eller regnskabserklæring, at udviklere har adgang til produktionsmiljøet
- Få overblik over udførte ændringer i årets løb – f.eks. få kopi af leverandørens fakturaer
- Overvej indhentelse af en erklæring specifik på udviklingsrutiner og system. Vurder om specifik eller generel erklæring

Gennemgang af revisors erklæring

- Påse at overholdelse af bogføringslovens krav til systemdokumentation er omtalt i erklæring
- Perioden
- Brugervirksomhedens handlinger

Gennemgang af serviceleverandørens revisionserklæring

- Vurdere serviceleverandørens revisors faglige kompetence og uafhængighed af serviceleverandøren
- Vurdere om perioden som omfattet af erklæring
- Vurdere om det er rette type erklæring
  - Type 2 i forbindelse med revision af årsregnskab
  - Type 1 i forbindelse med indgåelse af kontrakt
- Dækker den kontrakten
- Overholdes virksomhedens sikkerhedspolitik
- Specifik eller generel erklæring
- Vurder om komplementerende kontroller hos virksomheden er udformet og implementeret
- Forhold som skal omtales i protokol eller management letter samt revisor skal reagere på
- Er der underleverandører som er betydelige og ikke inkluderet i erklæringen

8 gode råd ved outsourcing

- Involveres tidligt i forløb – kommenter udkast til kontrakt
- Sikre tilstrækkelig information om ydelserne – vurder indvirkning på virksomheden og revision
- Beskrivelse af kontroller og revisors test af kontroller samt resultat heraf
- Begræns egne øvrige handlinger i fornødent omfang
- Overvej omtale i protokol eller management letter om forhold
- Vurder om der er behov for selv at udføre handlinger (altid vurdering af adgangsforhold og funktionsadskillelse på applikationsniveau)
- Fokus på risici og væsentlighed
- Kontakt faglig ekspertise – evt. ekstern

Erklæringer i forbindelse med IT anvendelsen

Erklæringstyper

- ISAE 3402
- ISAE 3000
- ISRS 4400

- Type 1 eller type 2
- Helheds- eller partiel metoden
- Perioden
- Kontrolmål

Spørgsmål

Seniorrådgiver Hans Henrik Aabenhus Berthing
Statsautoriseret revisor | CGEIT | CRISC | CISA | CIA

Tlf 35 36 33 56 | Mobil 22 20 28 21 | CVR-nr. 33 68 40 96
E-mail hhberthing@verifica.dk

Verifica Statsautoriseret Revisionsvirksomhed