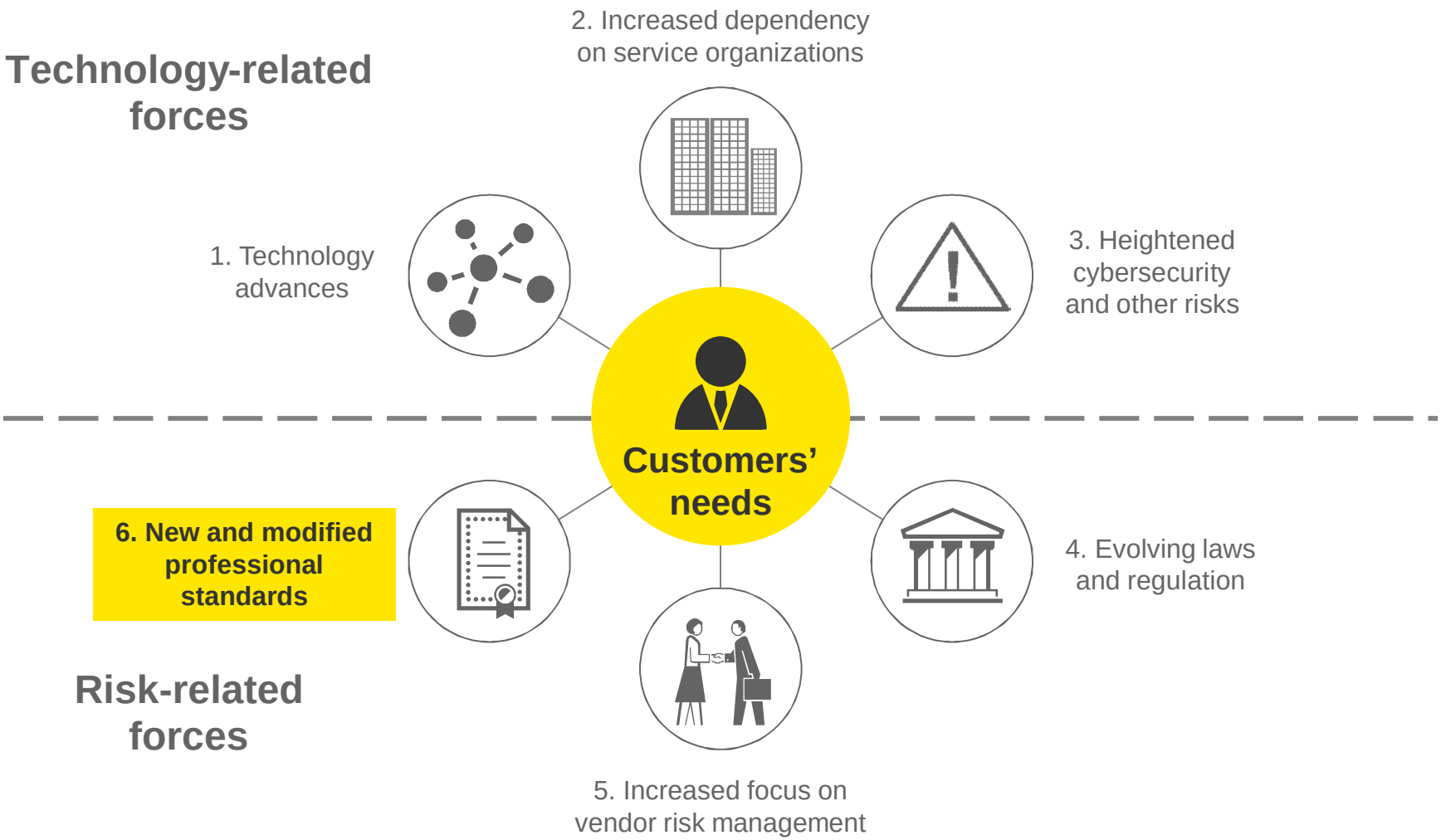
Sikkerhed & Revision 2016

Ændringer i ISAE 3000 og ISAE 3402

Claus Thaudahl Hansen

Building a better working world

Changes in standards within the market



Ændringer i standarderne
Indledning

- Ingen nye standarder, så fortsat til brug ved trepartsforhold
  - ISAE 3000 – andre erklæringsopgaver med sikkerhed
  - ISAE 3402 – til brug i outsourcing forhold, hvor processer og kontroller understøtter finansiel rapportering
- Og ved topartsforhold:
  - ISRS 4400 – Aftalte arbejdshandlinger baseret på instruktion

- Ny ISAE 3000 standard omskrevet, så den følger strukturen kendt fra ISAE 3402

- Ajourføring af ISAE 3402 som følge af den nye ISAE 3000

- Virkning for erklæringer, der blev afgivet 15. december 2015 eller senere

Ændringer i standarder
De væsentligste forskelle – ISAE 3000

- Ny ISAE 3000 standard
- Omfanget af standarden udvidet
- Mere præcise beskrivelser af kravene til det udførte arbejde, men kravene er grundlæggende de samme
- Fortsat muligt at udarbejde direkte og indirekte erklæringer med høj eller begrænset grad af sikkerhed
  - Men benævnes nu attestationserklæring henholdsvis direkte erklæring

Ændringer i standarder
De væsentligste forskelle – ISAE 3000

- Krav til beskrivelse af målekriterierne i erklæringen, svarende til, når man i årsregnskabet henviser til retvisende billede i h.t. årsregnskabsloven

- Modtager af erklæringen skal selv kunne finde frem til målekriterier
  - F.eks. Krav i Dankorthåndbogen
  - F.eks. ISO 27001

- Nye krav til beskrivelse af kvalitetssikring hos revisor

Ændringer i standarder
Kvalitetsstyring

Den opgaveansvarlige partners karakteristika

31. Den opgaveansvarlige partner skal:

(a) Være beskæftiget i et firma, der anvender ISQC 1 eller andre faglige krav, eller krav i lov eller øvrig regulering, der er mindst lige så krævende som ISQC 1 (jf. afsnit A60-A66),

(b) have færdigheder og teknikker vedrørende erklæringsopgaver med sikkerhed, der er udviklet gennem omfattende oplæring og praktisk anvendelse, og (jf. afsnit A60),

(c) have tilstrækkelige kompetencer i relation til erklæringsemnet og målingen eller vurderingen heraf til at påtage sig ansvaret for konklusionen i erklæringen med sikkerhed (jf. afsnit A67-A68).

Ændringer i standarder
Kvalitetsstyring – ISAE 3000 og 3402

Teamets bemanding

32. Den opgaveansvarlige partner skal (jf. afsnit A69):

(a) Være sikker på, at de personer, der skal udføre opgaven, tilsammen har de kompetencer og færdigheder, der kræves for at (jf. afsnit A70-A71):

(i) Udføre opgaven i overensstemmelse med relevante standarder og gældende krav i lov og øvrig regulering

(ii) osv

Ændringer i standarder
Kvalitetsstyring – ISAE 3000 og 3402

De nye afsnit i erklæringen om kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i såvel IESBA's Etiske regler som FSR – danske revisorers retningslinjer for revisors etiske adfærd (etiske regler for revisorer), som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Ernst & Young Godkendt Revisionspartnerselskab er underlagt international standard om kvalitetsstyring, ISQC 1 og anvender således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende krav i lov og øvrig regulering.

Ændringer i standarder
De væsentligste forskelle – ISAE 3402

- Ingen store ændringer, men visse tilpasninger
- Service leverandørens revisor skal overholde den nye ISAE 3000 standard – ikke den gamle
- En række definitioner i ISAE 3402 m.v. ændret / tilpasset, bl.a.:
- Serviceleverandørens revisor – en ~~praktiserende~~ revisor, der er antaget til at xxxx
- ~~Udsagn fra ledelsen –~~ Udtalelse fra ledelsen
- ~~Fastslå om de kriterier, der skal anvendes er egnede~~, vurderer kriteriernes egnethed

Ændringer i standarder
De væsentligste forskelle – ISAE 3402

Definition af Intern revisionsfunktion

– ~~en vurderingsfunktion, der er etableret eller stillet til rådighed som en service for serviceleverandøren. Dens opgaver omfatter blandt andet undersøgelse, vurdering og overvågning af intern kontrols hensigtsmæssighed og effektivitet.~~ en funktion i en virksomhed, der udfører aktiviteter vedrørende erklæringsopgaver med sikkerhed og rådgivning, som er udformet for at vurdere og forbedre effektiviteten i virksomhedens ledelse, risikostyring og interne kontrolprocesser.

Kommende ændringer i standarderne

- Ved brug af Carve-out metoden:
  - Komplementende kontroller hos underleverandøren medtages og testes
- Ved brug af både Carve-out og helhedsmetoden:
  - Monitoringskontroller over for underlevandøren
- Yderligere fokus på IPE – Information Produced by the Entity
  - F.eks. fuldstændighed af rapporter, der genereres af service leverandøren og som brugervirksomheden anvender ved regnskabsaflæggelsen.

Et andet hot topic set fra dansk perspektiv

- En række ISAE 3402 erklæringer udarbejdes efter carve-out metoden
- Særligt inden for den finansielle sektor og fælles datacentraler imidlertid krav om brug af helhedsmetoden
- Helhedsmetoden flere steder baseret ISRS 4400 rapportering fra underleverandører til data centralerne
- Sådan vil det næppe fortsætte
- Helhedsmetode baseret på brug af ISAE 3402 fra underleverandører
- Konsolidering på alle sektioner i erklæringen dvs.
  - Udtalelse fra ledelsen
  - Revisors erklæring
  - Beskrivelse af ydelsen
  - Test af kontroller
- Ikke gentagelse af information, men fuld transparens for brugervirksomheden i erklæringen til underleverandører

SOC 2 rapporterne

- Vi ser stigende interesse i det europæiske marked for SOC 2 erklæringer, der adresserer fortrolighed, integritet og tilgængelighed m.v. Båret af udviklingen i USA og de serviceleverandører, der har amerikanske kunder.

- Særligt fra kunder hos IT driftsleverandører – ikke så udbredt fra kunder hos f.eks. løn og asset management leverandører.

- Problemet med SOC 1 fra en IT driftsleverandør kan være, at ".. alt egentlig OK…" , men brugervirksomheden ved ikke, om kontroller og processer vedr. fortrolighed, integritet og tilgængelig er tilstrækkelige

- Men SOC 2 løser ikke alle problemer
  - Hvad nu med koblingen til kontroller over finansiel rapportering?

SOC 2 rapporterne

- I USA er ændringer på vej i bagvedliggende standarder, så amerikanske standarder, styrer SOC2, kommer tættere på ISAE 3000
- EYs holdning til brug af SOC 2 ved finansiel rapportering
- Et særligt fokus på Privacy (som jo ikke har noget at gøre med finansiel rapportering)

Privacy
… commitments and system requirements

*"The entity has established … to enable it to meet its **commitments and system requirements** as they relate to security, availability, processing integrity, confidentiality, or privacy, or any combination thereof."*

Commitments

- EU/Switzerland-US Safe Harbor
- Binding Corporate Rules (BCR)
- Business associate agreements (BAAs)
- Public-facing privacy notice

System requirements

- EU General Data Protection Regulation (GDPR)
- Health Information Portability and Accountability Act (HIPAA) privacy, security, and breach notification rules
- State and other federal privacy and data protection regulations

Privacy
European Union (EU) General Data Protection Regulation (GDPR)

Update on the status of the EU GDPR

- Effective date early part of 2018
- Key provisions
- Penalty for noncompliance
  - Fines up to 4% of global annual turnover

SOC reporting considerations

- Does the scope of the SOC report include the processing of EU citizen personal data?
- What is the service organization doing in preparation for EU GDPR compliance?
- Can you leverage plans to perform a privacy SOC pre-assessment to identify EU GDPR compliance gaps?
- Do the GDPR remediation plan dates align with goals for SOC reporting dates?

SOC 2 - Privacy
New criteria

Notice and communications of commitments ► Notice to data subject and communication to user entities	Typically both of these criteria are applicable
Choice and consent ► Choices available to the individual	These criteria may be applicable if the service organization interacts with the data subjects
Collection ► Process for collecting information based on valid consent	These criteria may be applicable if the service organization collects personal information
Use, retention and disposal ► Limiting the use of personal information ► Retaining only as long as necessary ► Properly disposing of personal information	Applicability of these criteria varies depending on level of access to data and contractual obligations

Privacy
New criteria

Disclosure and notification ► Consent to disclose ► Record/accounting of disclosure ► Third party responsibilities ► Breach notification	Typically these criteria are applicable
Security for privacy	Now uses the common criteria approach
Quality ► Accuracy, completeness and relevance	These criteria may not be applicable depending on the service you provide
Monitoring and enforcement ► Privacy related complaints and disputes ► Compliance and ongoing monitoring	Typically all of these criteria are applicable

Kaffepause

Kontakt oplysninger

Claus Thaudahl Hansen
Mobil 25 29 36 39
Claus.t.hansen@dk.ey.com