TIL NY PERSONDATAFORORDNING HERUNDER DPO

Sikkerhed & Revision 2016 den 2. september 2016

PFA PENSION

AGENDA

- Præsentation
- Hvorfor Persondata
- Hvor er PFA
- Univers af udfordringer
- Ny Persondataforordning
- Hvem skal have en DPO
- Hvad skal DPO
- 3LoD
- Hvem kan være DPO

PRÆSENTATION MORTEN BENDTSEN

- Koncernrevisionschef i PFA Pension (15. maj 2015 -)
- Revisionschef i Finansiel Stabilitet (1. februar 2012 til 30. april 2015)
- Områdechef i Danske Banks interne revision (+10 år)

HVORFOR PERSONDATA (1), BESTYRELSENS KRAV

Intern Revision i PFA varetager også rollen som Intern Auditfunktion i regi af Solvens II.

Intern Revision er ansvarlig for at udføre revision af operationelle forhold, regeloverholdelsen, kapital- og risikostyring samt pålideligheden af intern og ekstern rapportering.

Koncernrevisionschefen påtegner ikke årsregnskabet.

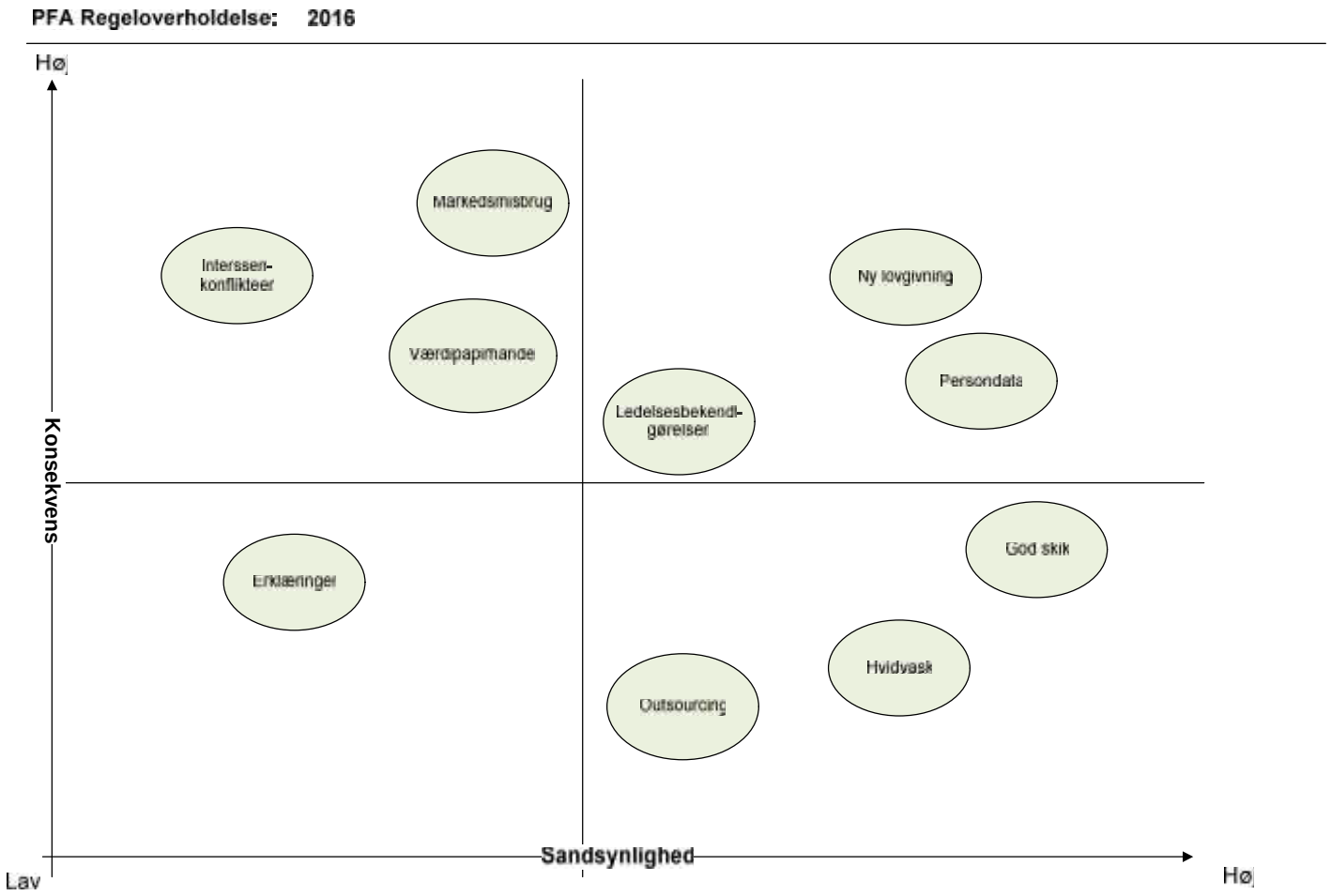
I årsprotokollatet afgiver Intern Revision en konklusion om det interne kontrol kontrolsystem.

Gennem uafhængig og objektiv efterprøvning skal Intern Revision skabe værdi og forbedringer af koncernens processer, risikoforståelsen og den interne kontrol samt understøtte målopfyldelsen og forandringsprocessen i koncernen.

HVORFOR PERSONDATA (2), FINANSTILSYNETS KRAV

Reference		Indhold
§ 21 stk. 1		Den af intern revision udførte revision skal omfatte alle væsentlige og risikofyldte områder i virksomheden jf. bilag 4
§ 27		Den interne revision skal i årsprotokollatet konkludere, hvorvidt virksomhedens risikostyring, compliancefunktion, forretningsgange og interne kontroller på alle væsentlige og risikofyldte områder er tilrettelagt og fungerer på betryggende vis, jf. bilag 4
Bilag 4		Intern Revision skal fx: • Vurdere, hvorvidt virksomheden har identificeret alle væsentlige risici og rapporteret dette til bestyrelsen • Udfordre ledelsens syn på risikostyring i virksomheden • Vurdere pålideligheden af ledelsesrapporteringen, samt overholdelse af love og regler • Bistår bestyrelsen med at beskytte virksomhedens aktiver, omdømme og fortsat drift • Have fokus på de forretningsgange og kontroller, der understøtter virksomhedens beslutningsprocesser • Effektivitetsvurdering (IAS 610) af risikofunktioner Revisionen skal, uanset om intern revision påtegner årsregnskabet delårsregnskaber eller ej, omfatte virksomhedens regnskabsaflæggelsesproces.

HVORFOR PERSONDATA (3), IBOENDE RISIKO

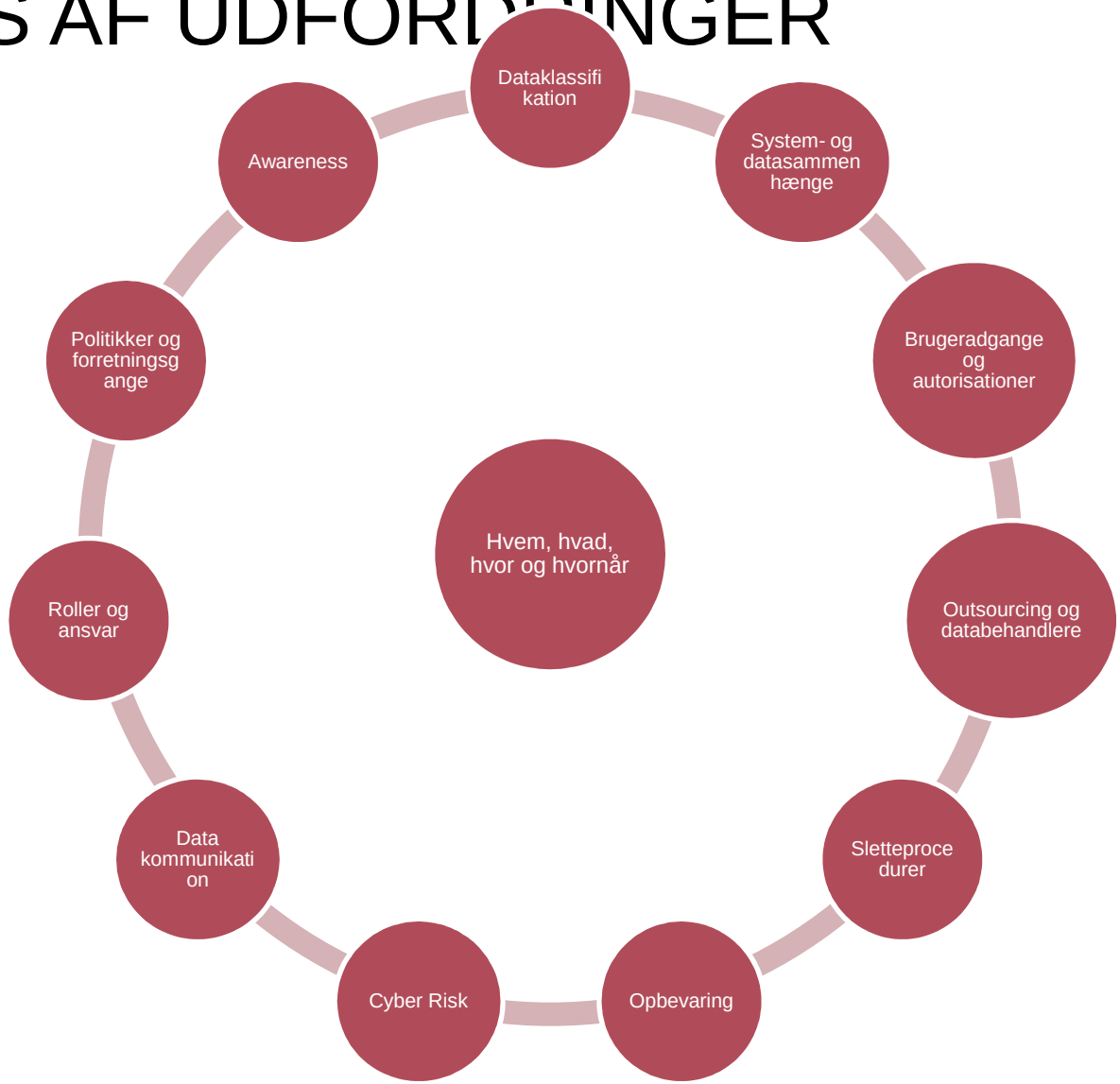


HVOR ER PFA

- Modenhedsvurdring udarbejdet af PWC (base-line og i forhold til kommende krav)
- Risikoanalyse udarbejdet af Compliance funktionen i PFA
- Drøftelser i revisionsudvalg og i koncernledelsen
- Foranalyse (Intern Revision deltager som observatør)

- Datatilsynets hjemmeside om persondatareformen => 21. juni 2016 ”Q&A”

UNIVERS AF UDFORDRINGER



NY PERSONDATAFORORDNING (1)

- Same, same eller ……

- Dokumentationskrav
- Risikostyring, herunder DPO
- Rettigheder
- Samtykke
- Incidents (databrud)
- Proaktivt tilsyn
- Sanktioner

- Man skal udarbejde politikker, forretningsgange, drøfte risikoniveauer, gentænke udviklingsmodel for IT, udarbejde beredskabsplaner for databrud, gentænke databehandleraftaler og assurancekrav

NY PERSONDATAFORORDNING (2)

- Konsekvenserne er stigende

- Omdømme: øget risiko for negativ presseomtale og kundereaktion
- Konkurrenceparametre: øget krav fra kunder herunder fremvisning
- Store bøder: 75 mio. kr. til 1,0 mia. kr. (hvad er omsætning?)

HVEM SKAL HAVE EN DPO

Det skal man, hvis man kan nikke ja til bare ét af disse tre punkter:

- Hvis man er en offentlig myndighed (undtagen domstole)
- Hvis man er en virksomhed, hvis primære ydelse er at behandle persondata, som forudsætter jævnlig og systematisk overvågning af de registrerede personer
- Hvis man er en virksomhed, hvis primære ydelse er at behandle ”særlige kategorier af oplysninger” om registrerede personer, fx politisk tilhørsforhold, helbredsoplysninger, seksuel orientering etc.

- PFA rammer punkt nr. 3

- Alle virksomheder skal overhold persondataforordningens krav DPO’en er ikke virksomhedens interne kontrol men et ekstra sikkerhedslag for den registrerede!

HVAD SKAL DPO (1)

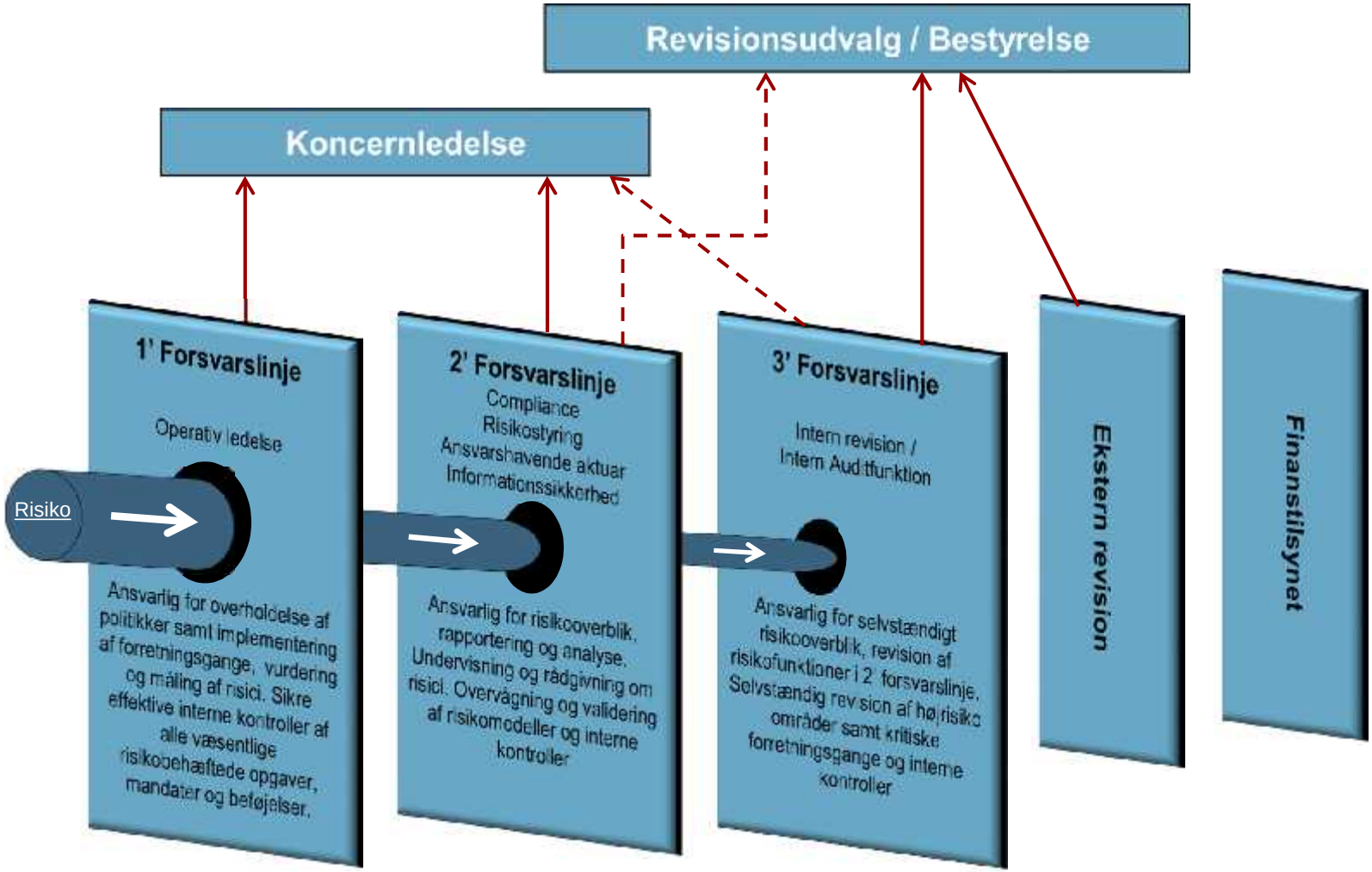
Forudsætninger:

- Rapportering og reference til ”øverste ledelsesniveau”
- Opgaver skal løses ”uafhængigt”
- Skal inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger
- Efteruddannelse
- Ikke underlagt instrukser
- Ikke tildelt instruktionsbeføjelser
- Beskyttet stilling

HVAD SKAL DPO (2)

- Overvåge efterlevelsen af persondataforordningen og virksomhedens politikker
- Rådgivning og oplyse om rettigheder og forpligtelser ift. databehandling
- Holder ledelsen orienteret om dens forpligtelser i forhold persondataloven
- Fungerer som primær kontaktperson for tilsynsmyndigheder (fx Datatilsynet)

3LOD


Revisionsudvalg / Bestyrelse
Koncernledelse
1' Forsvarslinje
Operativ ledelse
Risiko
Ansvarlig for overholdelse af politikker samt implementering af forretningsgange, vurdering og måling af risici. Sikre effektive interne kontroller af alle væsentlige risikobehæftede opgaver, mandater og beføjelser.
2' Forsvarslinje
Compliance
Risikostyring
Ansvarshavende aktuar
Informationssikkerhed
Ansvarlig for risikooverblik, rapportering og analyse. Undervisning og rådgivning om risici. Overvågning og validering af risikomodeller og interne kontroller
3' Forsvarslinje
Intern revision / Intern Auditfunktion
Ansvarlig for selvstændigt risikooverblik, revision af risikofunktioner i 2. forsvarslinje. Selvstændig revision af højrisiko områder samt kritiske forretningsgange og interne kontroller
Ekstern revision
Finanstilsynet

HVEM SKAL VÆRE DPO