Sikring af kædeansvar i NIS2-reguleringen

Revisorerklæringer som et effektivt værktøj

Oktober 2024

Kort om os

Alireza Samini
Partner, Risk Assurance, PwC

T: 2163 0684
E: alireza.samini@pwc.com

Thomas Greimer
Director, Risk Assurance, PwC

T: 2113 4690
E: thomas.greimer@pwc.com

Agenda

1. Kort introduktion til NIS2-reguleringen
2. Forståelse af kædeansvar i praksis
3. Revisorerklæringer som værktøj til at sikre NIS2-compliance
4. Arbejdet med revisorerklæringen
5. NIS2-kontrolmål og kontrolaktiviteter i revisorerklæringen
6. Opsummering
7. Spørgsmål

1

Kort introduktion til NIS2-reguleringen

Kort introduktion til NIS2-reguleringen

NIS2 (Network and Information Security)

Udvidelse af scope

NIS2-direktivet udvider scopet betydeligt. Direktivet skelner mellem ”særligt kritiske" og "kritiske" enheder.

Særligt kritiske/essentielle er de klassiske tilskrevne kritiske infrastruktursektorer såsom energi, transport, bankvæsen, finansmarkedsinfrastrukturer, sundhed, drikkevand, spildevand, digital infrastruktur, IKT-tjenester (B2B), offentlig administration og rumfart.

Kritiske/vigtige omfatter sektorer som post- og kurertjenester, affaldshåndtering, fremstilling, produktion og distribution af kemikalier, produktion, forarbejdning og distribution af fødevarer, fremstilling, digitale udbydere og forskning.

Udvidet fokus på ledelse og governance
Øverste ledelse er forpligtet til at forstå, godkende og stille krav til de foranstaltninger, der mitigerer cybersikkerhedsrisici, som jeres organisation har identificeret. Til det skal organisationer sikre uddannelse og træning i cybersikkerhed for ledelseslagene.

Artikel 20

Foranstaltninger til håndtering af cybersikkerhedsrisici
Der skal udføres risikostyring og implementeres formildende foranstaltninger, herunder politikker for risikoanalyse og forebyggende kapaciteter såsom hændelseshåndtering, **forsyningskædesikkerhed,** kryptografi, HR-sikkerhed osv.

Artikel 21

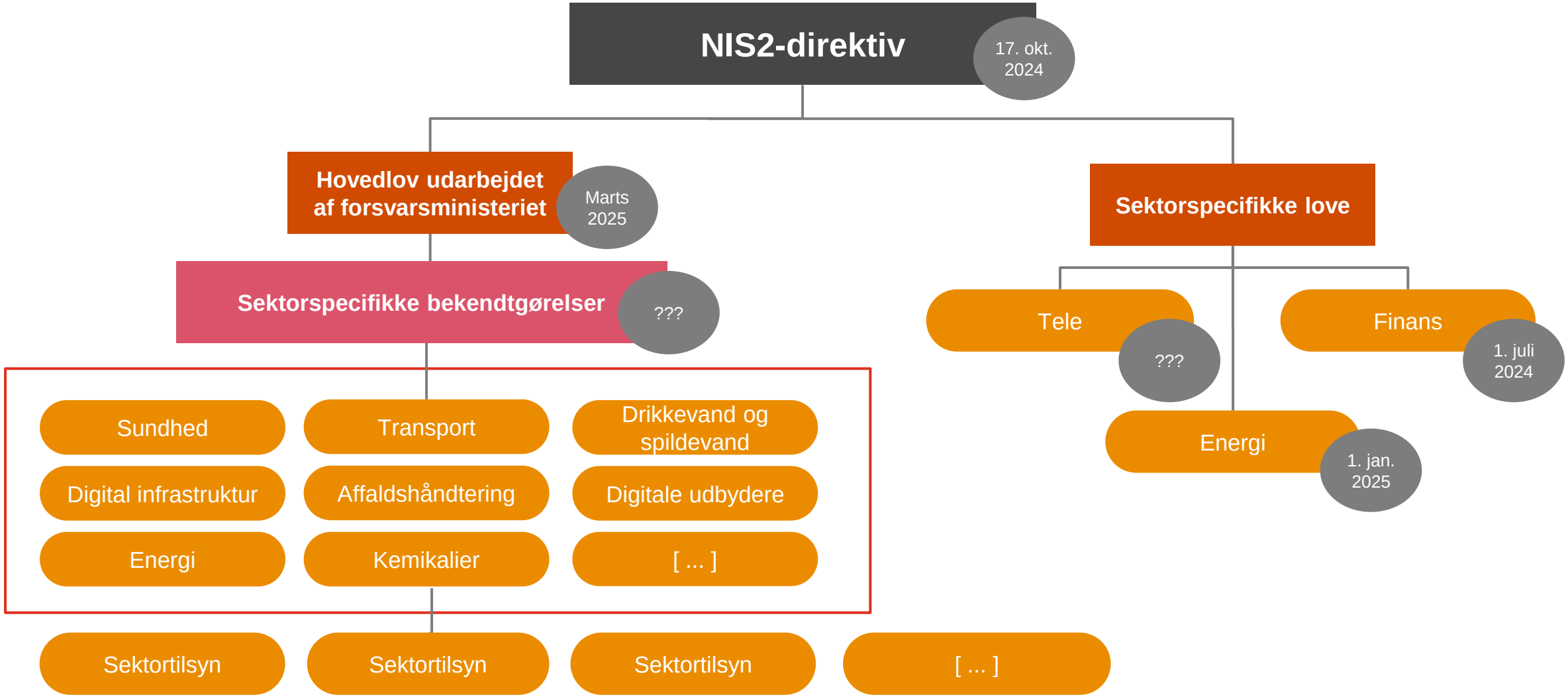
Beredskab og kontinuitet
Hvis der opstår hændelser, skal organisationer sikre kontinuitet i driften. Forretningskontinuitet kan opnås med backup, disaster recovery og krisehåndtering.

Artikel 21

Rapporteringsforpligtelser
Hvis der opstår cybersikkerhedshændelser, er enheden forpligtet til at underrette de kompetente myndigheder (CFCS) inden for 24 timer efter at have fået kendskab til den væsentlige hændelse, efterfulgt af en dybdegående hændelsesunderretning inden for 72 timer og 1 måned.

Artikel 23

Status på implementering i Danmark



2

Forståelse af kæde-ansvar i praksis

Forståelse af kædeansvar i praksis

Leverandørforhold

NIS2-omfattet enhed

Enhedens kunder

Leverandør af net- og informationssystemer

Underleverandør af cloud- og datacentertjenester

Forståelse af kædeansvar i praksis

Betydningen af kædeansvar

- **Ansvarsfordeling og kontrol:** Virksomheder skal sikre, at leverandører opretholder samme cybersikkerhedsniveau. Manglende kontrol over leverandørers sikkerhedspraksis gør det vanskeligt at sikre overholdelse af kravene.
- **Ressourcemæssige udfordringer:** Især for SMV'er kan det være dyrt og administrativt krævende at kontrollere leverandørernes cybersikkerhed. Manglende overvågning kan føre til brud og sanktioner.
- **Sanktioner og juridiske konsekvenser:** Hvis leverandører fejler, kan hovedvirksomheden holdes ansvarlig og risikere store bøder, tab af troværdighed og juridiske tvister.

Forståelse af kædeansvar i praksis

Hvordan kan virksomheder sikre compliance hos underleverandører og partnere?

Til overvågning af compliance hos underleverandører og partnere kan virksomheder implementere forskellige tiltag, eksempelvis:

- Risikovurdering af underleverandører og partnere
- Integrering af cybersikkerhedskrav i kontrakter
- Løbende auditering og compliance-kontrol
- Incident response-krav
- Service level agreements (SLA'er) for cybersikkerhed
- Træning og bevidstgørelse
- Tredjepartserklæringer, certificeringer mv.

3

Revisorerklæringer som værktøj til at sikre compliance

Revisorerklæringer som værktøj til at sikre compliance

Forskel mellem erklæringer, D-mærket og certificeringer

Revisorerklæringer	D-mærket	ISO-certificeringer
• Jf. revisorlovens §16 er revisor offentlighedens tillidsrepræsentant. Revisor skal udføre opgaverne i overensstemmelse med god revisorskik, herunder udvise den nøjagtighed og hurtighed, som opgavernes beskaffenhed tillader. • Uafhængig revisors erklæring om, hvorvidt virksomhedens informationssikkerhedsforanstaltninger overholder visse krav eller standarder, fx ISO 27001 eller andre standarder. • Erklæringer afgives enten pr. en given dato eller dækker en periode (bagudrettet). • Krav om revisors uafhængighed, jf. revisorlovens §24. • Revisionsvirksomheden skal etablere kvalitetssystem for at sikre høj kvalitet i henhold til revisionsstandarder. • Større dybde i test af kontroller.	• Dansk mærkningsordning med fokus på at sikre, at virksomheder lever op til gode standarder inden for digital sikkerhed. • Virksomheden foretager en selvevaluering, som kombineres med audit.	• Certificeringer handler om virksomhedens processer og systemer til styring af informationssikkerhed. Certificeringen er et bevis på, at virksomheden har etableret et effektivt ISMS (Information Security Management System) i overensstemmelse med en international standard. • Er med til at højne modenheden på informationssikkerhed og sikre formalisering af procedurer. Dog ingen sikkerhed for, at kontroller bliver udført.

Revisorerklæringer som værktøj til at sikre compliance

Trepartsforhold

Enhedens revisor

NIS2-omfattet enhed

Enhedens kunder

Leverandørens revisor

Leverandør af net- og informationssystemer

Underleveran-dørens revisor

Underleverandør af cloud- og datacentertjenester

Revisorerklæringer som værktøj til at sikre compliance

Erklæringsskabelon i NIS2 kontekst

06. juni 2024

AI OG DIGITALISERING ——— CYBERSIKKERHED

FSR - danske revisorer lancerer en ny NIS2 (net- og informationssystemer) erklæringstemplate i relation til leverandører eller tjenesteudbydere

FSR - danske revisorer har udarbejdet en ny revisorerklæring, som dækker kravene i NIS2-direktivet og de forpligtelser, som leverandører har i forhold til NIS2-reguleringen.

Erklæringen har fået navnet "Uafhængig revisors ISAE 3000-erklæring med begrænset sikkerhed om foranstaltninger til styring af risici i relation til net- og informationssystemer og rapporteringsforpligtelser i henhold til aftale med [Kunde]".

Erklæringen er ikke et udtryk for minimumskrav og indeholder en række eksempler på kontrolaktiviteter og revisionshandlinger. Disse er alene til inspiration og bør altid tilpasses til den konkrete risikovurdering, de foranstaltninger, der i øvrigt måtte være aftalt parterne imellem, og under hensyn til revisors professionelle vurdering.

Kilde: FSR

Revisorerklæringer som værktøj til at sikre compliance

Hvorfor og hvordan kan en revisorerklæring bruges i forhold til NIS2?

1. **Tredjepartsvalidering:** Revisorerklæringer giver en objektiv vurdering af leverandørers cybersikkerhed og fungerer som bevis for virksomheders due diligence.
2. **Risikoafdækning og tillid:** En revisorerklæring skaber tillid ved at dokumentere leverandørers sikkerhedsforanstaltninger og reducerer risikoen for oversete mangler.
3. **Standardiseret dokumentation:** Revisorerklæringer sikrer ensartet dokumentation og gør det lettere at evaluere leverandører og overvåge deres cybersikkerhedsudvikling over tid.
4. **Reducerede kontrolomkostninger:** Revisorerklæringer gør det muligt at outsource dele af leverandørkontrollen, hvilket minimerer hovedvirksomhedens ressourcer og omkostninger til egen audit.
5. **Forbedret samarbejde i forsyningskæden:** Krav om revisorerklæringer styrker cybersikkerhedskulturen blandt leverandører, da de vil være mere tilbøjelige til at opgradere deres sikkerhedsstandarder. Dette øger den samlede sikkerhed og reducerer risici i forsyningskæden.

Revisorerklæringer som værktøj til at sikre compliance

Indhold af en erklæring

1. **Ledelsens udtalelse**
2. **Uafhængig revisors erklæring**
3. **Beskrivelse af tjenester**
   - Kontrolmiljø
   - Risikostyring
   - Information og kommunikation
   - Overvågning
   - Beskrivelse af kontrolaktiviteter
   - Komplementære kontroller hos kunderne
   - Komplementære kontroller hos serviceunderleverandørerne
4. **Kontrolmål – kontrolaktiviteter – test – testresultat**

4

Arbejdet med revisorerklæringen

Arbejdet med revisorerklæringen

Den overordnede proces

5

NIS2-kontrolmål og kontrolaktiviteter i revisorerklæringen

Kontrolmål

Mapper direkte til artikel 21 pkt. 2 a) til j)

- **Kontrolmål 1: Politikker for risikoanalyse og informationssikkerhed**
  Der foreligger formaliserede politikker og procedurer for at sikre, at der er fastlagt tilstrækkelig vejledning, roller og ansvar for at understøtte en struktureret og formaliseret proces til at identificere risici og forankre informationssikkerhed i organisationen **(16)**.
- **Kontrolmål 2: Håndtering af hændelser (forebyggelse, opdagelse og opfølgning på hændelser)**
  Der foreligger formaliserede procedurer og kontroller for at sikre rettidig og behørig håndtering, herunder opdagelse, løsning af og rapportering af hændelser til kunder **(7)**.
- **Kontrolmål 3: Driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe og krisestyring**
  Der foreligger formaliserede procedurer og kontroller for at sikre fortsat drift og tilgængelighed af tjenester i tilfælde af en katastrofe **(12)**.
- **Kontrolmål 4: Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forbindelserne mellem virksomheden og dens direkte leverandører eller tjenesteudbydere**
  Der foreligger formaliserede procedurer og kontroller for at sikre, at relevante og direkte tjenesteudbydere (herunder underleverandører) igennem hele leverandørkæden identificeres og overvåges for at sikre overholdelse af virksomhedens sikkerhedskrav og serviceleveranceaftaler **(10)**.
- **Kontrolmål 5: Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder**
  Der foreligger formaliserede procedurer og kontroller for at sikre, at kritiske aktiver på behørig vis udvikles, vedligeholdes og beskyttes mod sårbarheder over for interne og eksterne trusler **(16)**.

Kontrolmål

Mapper direkte til artikel 21 pkt. 2 a) til j)

- **Kontrolmål 6: Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici**
  Der foreligger formaliserede procedurer og kontroller for at sikre, at cyberrelaterede risici og trusler identificeres, overvåges og udbedret rettidigt **(6)**.
- **Kontrolmål 7: Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse**
  Der foreligger formaliserede procedurer og kontroller for at sikre, at cyberhygiejnepraksisser er implementeret i virksomheden og at medarbejderne gennemfører løbende træning/uddannelse i cybersikkerhed **(4)**.
- **Kontrolmål 8: Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering**
  Der foreligger formaliserede procedurer og kontroller til at sikre, at kritiske aktiver beskyttes gennem kryptering **(9)**.
- **Kontrolmål 9: Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver**
  Der foreligger formaliserede procedurer og kontroller for at sikre, at personalesikkerhed, adgangskontrol og forvaltning af aktiver struktureres, formaliseres og vedligeholdes for at sikre et passende sikkerhedsniveau **(18)**.
- **Kontrolmål 10: … multifaktorautentifikation … sikker kommunikation … nødkommunikationsenheder internt …**
  Der er indført formaliserede procedurer og kontroller for at sikre en stærk autentificeringsproces for administration af adgang til kritiske aktiver samt sikret nødkommunikation **(5)**.

Kontrolmål og kontrolaktiviteter

Eksempler fra erklæringen

Kontrolmål 5 – Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

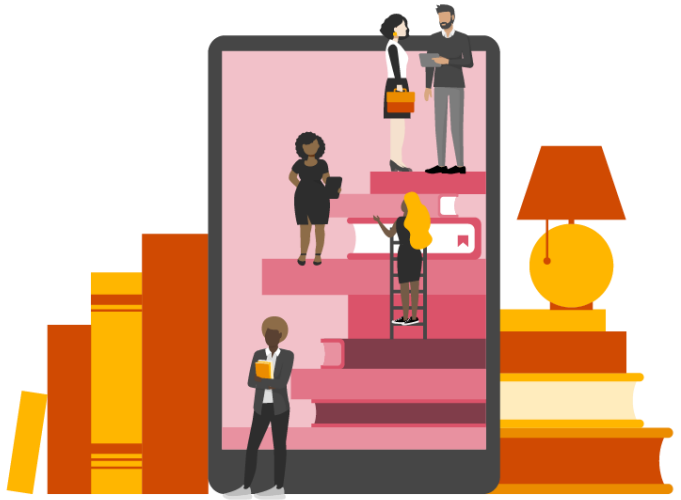
Der foreligger formaliserede procedurer og kontroller for at sikre, at kritiske aktiver på behørig vis udvikles, vedligeholdes og beskyttes mod sårbarheder over for interne og eksterne trusler.

Nr.	NIS2-serviceleverandørens kontrolaktivitet	Revisors udførte vurdering	Resultat af revisors vurdering
5.1	Netværksinfrastruktur og tilhørende dokumentation vedligeholdes og er opdateret, herunder netværksdiagrammer og konfigureringsfiler til enheder (fx routere og switches).	Inspiceret, at der foreligger formaliseret dokumentation i form af netværksdiagram samt overblik over andre relevante netværksudstyr som routere og switches. Inspiceret, at dokumentationen i relation til netværksdiagram og konfigurering er opdateret.	
5.2	Der er etableret kontroller for at sikre fortroligheden og integriteten af data, der sendes gennem offentlige netværk, tredjepartsnetværk eller trådløse netværk, og for at beskytte de forbundne systemer og applikationer.	Forespurgt om tekniske foranstaltninger, der sikrer fortrolighed og integritet af data, der overføres via offentlige netværk, tredjepartsnetværk eller trådløse netværk. Inspiceret en stikprøve på XX netværkskomponenter (firewalls, switches, routere) for at evaluere, at sikkerhedsreglerne er konfigureret i overensstemmelse med godkendte sikkerhedskrav. Inspiceret, at netværkskonfigurationen kun tillader sikre protokoller og porte, der bliver anvendt i relation til krypterede forbindelser. Inspiceret ved en stikprøve på XX, at kryptering anvendes på systemer og hardware, der indeholder eller overfører NIS2-relevante data.	

6
Opsummering

Opsummering

- NIS2 kræver, at virksomheder sikrer, at deres relevante leverandører opretholder samme cybersikkerhedsniveau, hvilket kan føre til kædeansvar for sikkerhedsbrud længere nede i forsyningskæden.
- Ressourcemangel, især hos SMV'er, gør det udfordrende at overvåge leverandørers cybersikkerhed, hvilket kan resultere i brud på kædeansvaret.
- Virksomheder risikerer økonomiske sanktioner og juridiske konsekvenser, hvis leverandører ikke overholder cybersikkerhedskrav.
- Revisorerklæringer fungerer som tredjepartsvalidering og dokumentation for leverandørers overholdelse af relevante NIS2-krav, hvilket skaber tillid og reducerer risiko.
- Revisorerklæringer sikrer standardiseret dokumentation af leverandørers sikkerhedspraksis, hvilket gør det nemmere at evaluere og følge op på over tid.
- Revisorerklæringer er med til at skabe en effektiv overvågning af forsyningskæden via en ensartet og sammenlignelig rammeværk



7
Spørgsmål

Tak for i dag

www.pwc.dk

Succes skaber vi sammen …

Denne publikation er udarbejdet alene som en generel orientering om forhold, som måtte være af interesse, og gør det ikke ud for professionel rådgivning. Du bør ikke disponere på baggrund af de oplysninger, der er indeholdt i denne publikation, uden at indhente specifik professionel rådgivning. Vi afgiver ingen erklæringer eller garantier (udtrykkeligt eller underforstået) hvad angår nøjagtigheden og fuldstændigheden af de oplysninger, der findes i publikationen, og, i det omfang loven tillader, accepterer eller påtager PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, dets aktionærer, medarbejdere og repræsentanter sig ikke nogen forpligtelse, ansvar eller agtpågivenhedspligt for eventuelle konsekvenser, som følger af, at du eller andre handler eller undlader at handle i tillid til de oplysninger, der findes i publikationen, eller for eventuelle beslutninger truffet på baggrund af publikationen.

© 2024 PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab. Alle rettigheder forbeholdes. I dette dokument refererer "PwC" til PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, som er et medlemsfirma af PricewaterhouseCoopers International Limited, hvor hver enkelt virksomhed er en særskilt juridisk enhed.