Cybersäkerhetsrisker och reglering

Introduktion till DORA (Digital Operational Resilience Act)

Agenda

Dagens agenda

01 Introduktion till DORA
- Lite bakgrundshistoria

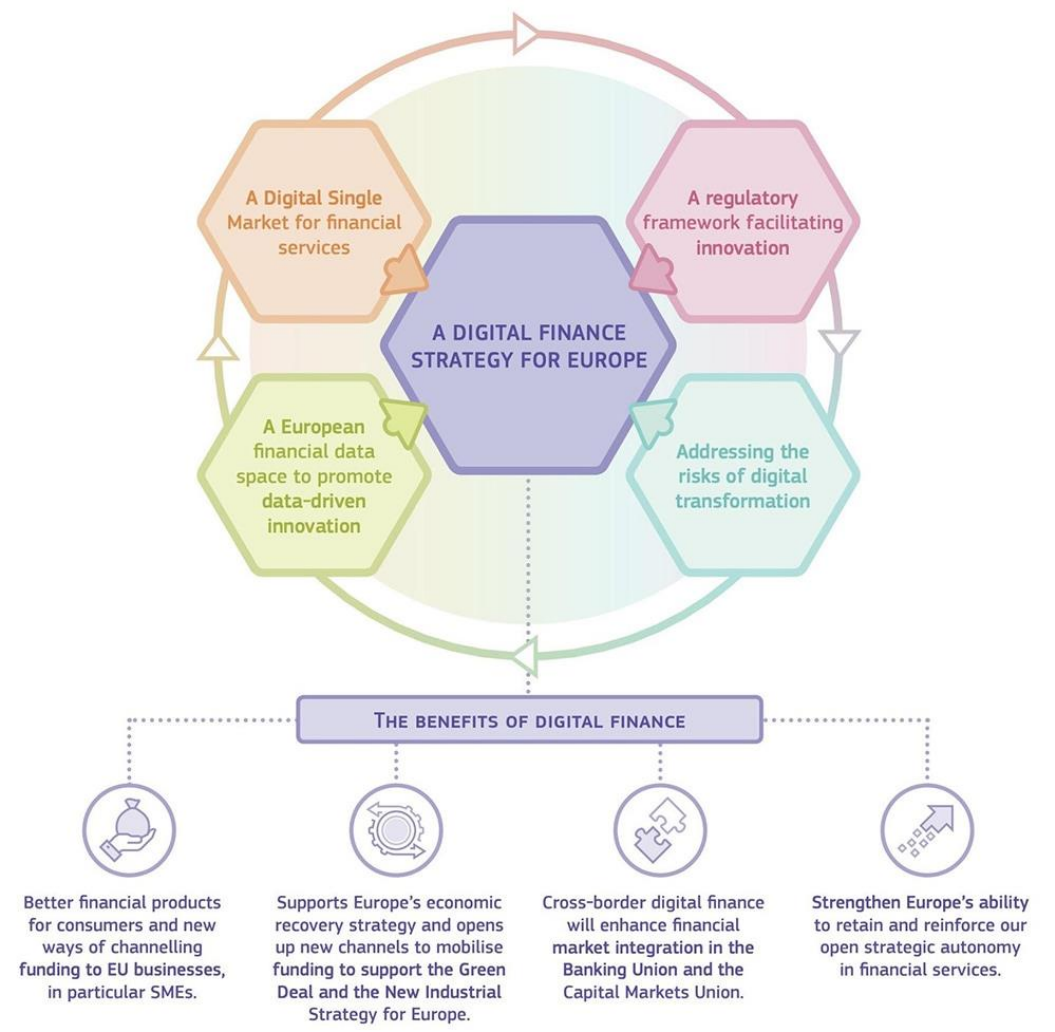
02 DORA regleringen
- Vad omfattar den?

03 Risker man vill adressera
- Motivation

"Digitalisation and operational resilience in the financial sector are two sides of the same coin"

DORA en del av någonting större

En del av EU:s Digital Finance Package



Digital Operational Resilience Act (DORA)

VAD, NÄR, HUR?

Vad är DORA?

- En EU förordning som adresserar de ökade riskerna inom information- och cybersäkerhet samt outsourcing för bolag inom den finansiella sektorn

När kommer DORA?

- EU Kommissionen har accepterat DORA förordningen, och den förväntas publiceras i slutet av 2022. Implementationstiden beräknas vara 24 månader och därmed kommer DORA gälla i slutet av 2024 eller tidigt 2025

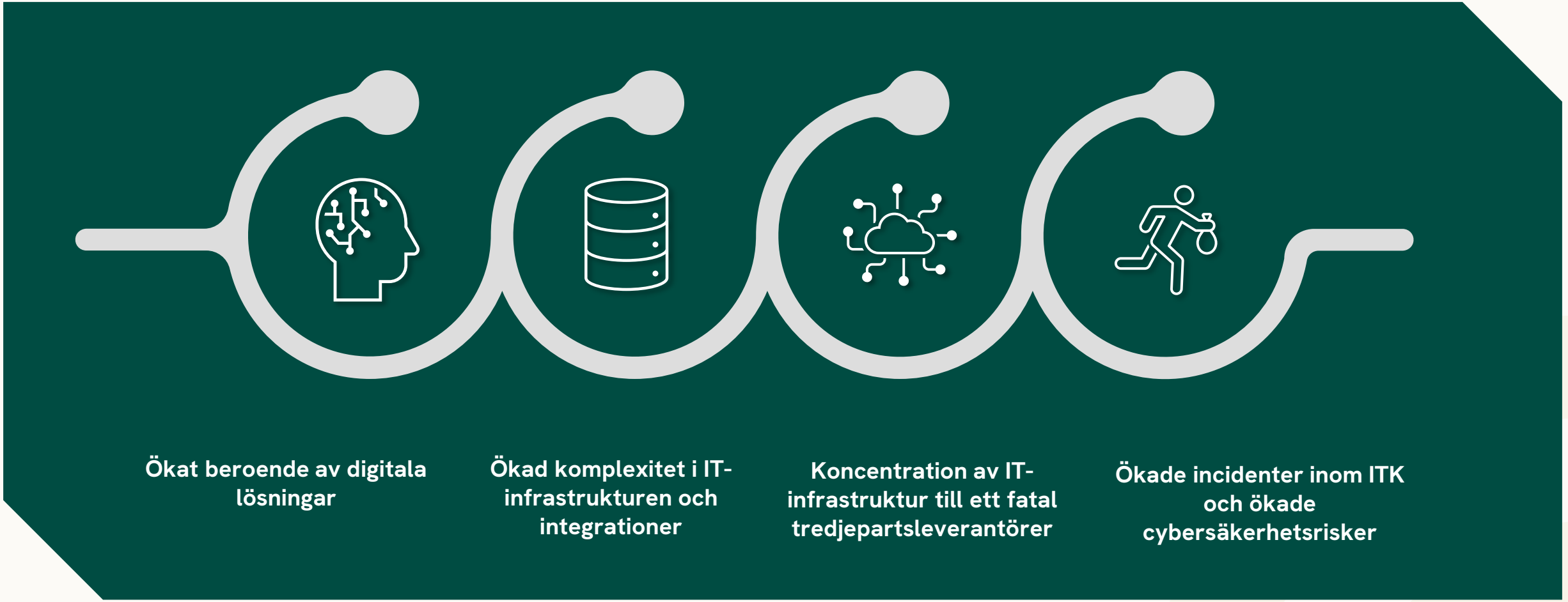
Kommer jag omfattas av DORA?

- JA! Målet med DORA är att skapa gemensamma krav för alla bolag inom bank och finanssektorn och en stor mängd bolag omfattas

Vi har redan infört EIOPAs IKT regelverk, betyder det att vi efterlever DORA?

- Det finns subtila skillnader mellan EIOPAs IKT reglering och DORA, men om både IKT och den molnbaserade regleringen är fullt ut införda i verksamheten så är mycket av jobbet gjort.

Reglering och Finansinspektionens tillsyn

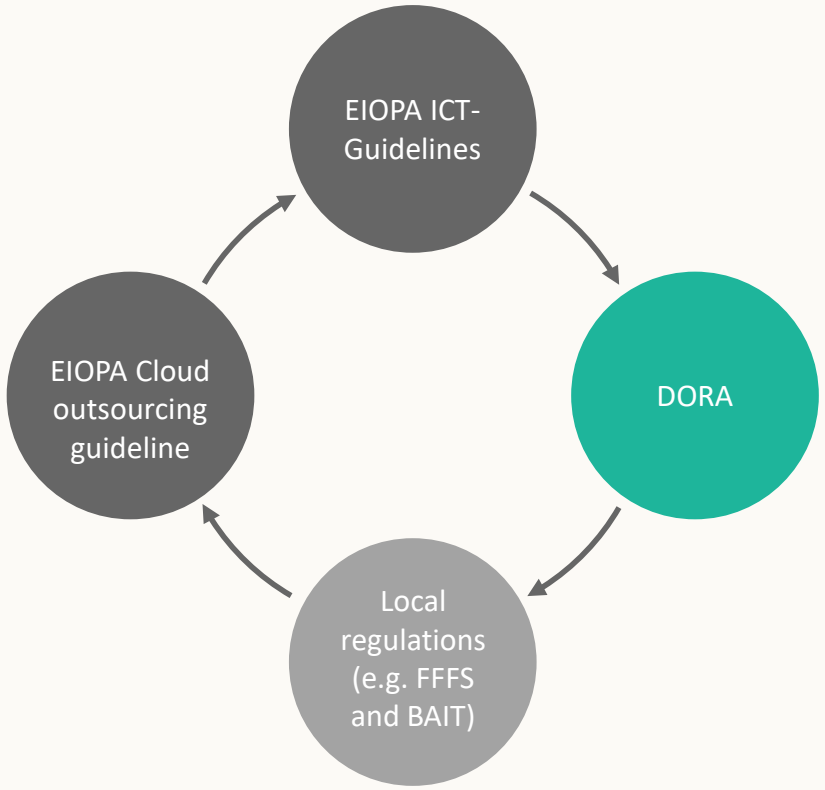


- Försäkringsrörelselagen (FRL) – operativa risker på övergripande nivå
- EIOPAs riktlinjer om informations- och kommunikationsteknologi (IKT)
- EIOPAs riktlinjer om användning av molntjänster

Kommande reglering

- Digital Operational Resilience Act (DORA)

Jämförelse med nuvarande reglering – vad är nytt?



Nuvarande reglering

Fokus ligger på att etablera IKT och säkerhetsriskhantering på försäkringsbolagen, fokus på både riskhantering, IT, informationssäkerhet, kontinuitetshantering, och outsourcing.

DORA

Förutsätter IKT riskhantering (inkl. Ledningssystem för informationssäkerhet) som en grundnivå

Fokus på:

- Testning av IKT (utökade krav)
- IKT baserad incidentrapportering
- FI mandat förändras (i Sverige)
- Informationsutbyte mellan finansiella aktörer (hot och incidenter)
- Minska koncentrations och risker för onödiga beroende inom IKT
- Fastställer och stärker rollen för EU finansiell övervakningsmyndigheter (ESA)

IKT – vad i all världen är det?

En kort tidsresa genom IT

1

ADB

Automatisk behandling av data med hjälp av datorer. Rationaliserade det manuella arbete med komplexa beräkningar. Specialist funktioner.

2

IT

Samarbete mellan datorer (nätverksuppkopplade datorer).
Tog över traditionellt kontorsarbete. Intåget av standardiserat globalt nätverk (Internet).

3

IKT

IT and Kommunikations-teknologi - Utökar IT genom att inkludera tele-kommunikation, UC och nätverk. Begreppet brukar omfatta datorer, mobiler, serverar, infrastruktur och externa leverantörer (exv. Cloud).

Begrepp inom informationssäkerhet

Kärt barn har många namn...

Informations-säkerhet

Definition

Informationssäkerhet är ett samlingsnamn för all form av säkerhet som omfattar information. Det kan omfatta bland annat styrningen av säkerhet, klassning av information, säkerhet inom IT, fysisk säkerhet, cybersäkerhet samt personsäkerhet

IT-säkerhet

Definition

IT-säkerhet ansvarar för att skydda en organisations värdefulla IT-tillgångar som information, maskinvara ("hårdvara") och programvara ("mjukvara"). IT-säkerhet koncentrerar sig på hot och skydd förenade med användning av informationsteknik ("IT").

Cyber-säkerhet

En definition av flera

The Financial Stability Boards Cyber Lexikon definierar Cyber Säkerhet: Skydda konfidentialitet, integritet och tillgänglighet av information och/eller informationssystem genom cyber mediet. Andra skyddsegenskaper som autentisering, oförnekbarhet, och stabilitet kan också omfattas

Vem omfattas av DORA?

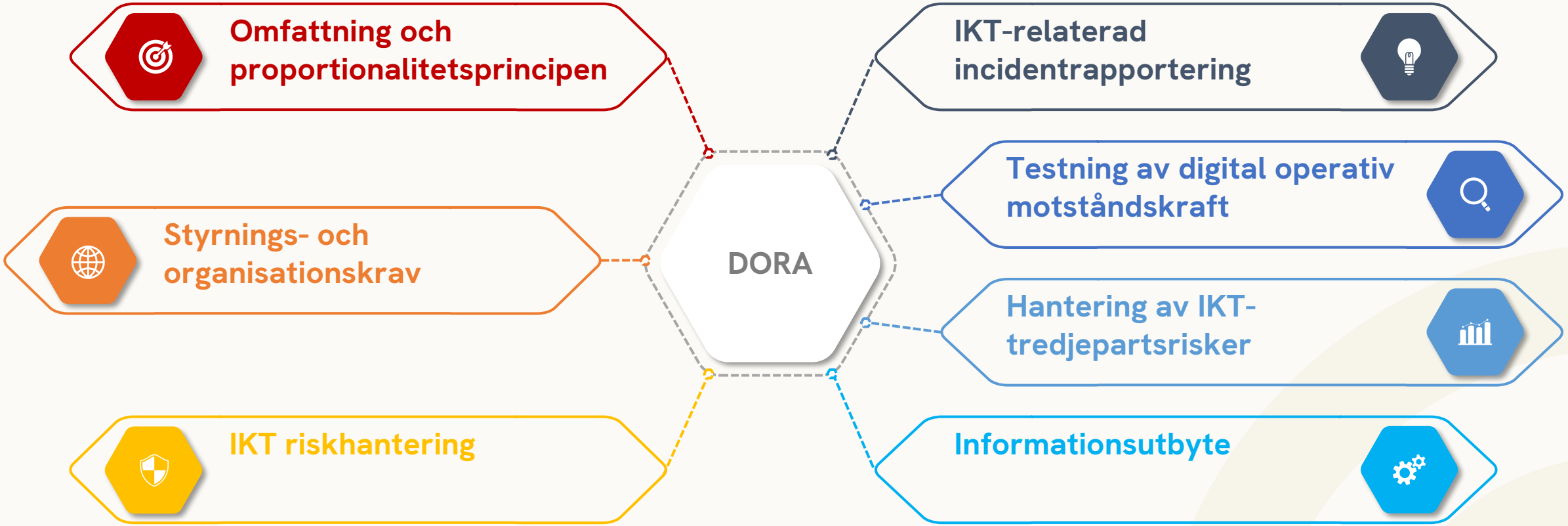
Målsättningen är att skapa gemensamma standarder och krav för hela bank & finansbranschen inom informationssäkerhet

- Kreditinstitut
- Betalningsinstitut
- Institut för elektroniska pengar
- Värdepappersföretag
- Leverantörer av kryptotillgångstjänster, emittenter av kryptotillgångar, emittenter av tillgångsanknutna token och emittenter av betydande tillgångsanknutna token
- Värdepapperscentraler
- Centrala motparter
- Handelsplatser
- Transaktionsregister
- Förvaltare av alternativa investeringsfonder
- Förvaltningsbolag
- Leverantörer av datarapporterings-tjänster
- Försäkrings- och återförsäkringsföretag
- Försäkringsförmedlare, Återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet
- Tjänstepensionsinstitut
- Kreditvärderingsinstitut
- Lagstadgade revisorer och revisionsföretag
- Administratörer av kritiska referensvärden
- Leverantörer av gräsrotsfinansieringstjänster
- Värdepapperiseringsregister
- Tredjepartsleverantörer av IKT-tjänster

Direktivet omfattas av proportionalitets-principen, där hänsyn tas till den finansiella enhetens affärsbehov, storlek och komplexitet

DORA är uppdelad i 7 olika regleringsområden

Detaljnivån är omfattande och uppdelade i 50 Artiklar. Regleringen omfattar allt från finansiella enheter (institut), reglerande EU organ och nationella tillsynsmyndigheter.



Regleringen omfattar till största del informationssäkerhet och outsourcing

IKT riskhantering

IKT-relaterat risk- och kontrollramverk (Artikel 5-6)

- **Styrelsen är ansvariga** för införandet av ett IKT baserat riskramverk (styrnings och kontrollramverk), och behöver:
  - ❑ Definiera roller och ansvar
  - ❑ Fastställa riskaptiten
  - ❑ Säkerställa att det finna tillräckligt med resurser
  - ❑ Övervaka IKT kontinuitetsförmågan / bolagets motståndskraft
  - ❑ Övervaka bolagets incidenthanteringsförmågan
  - ❑ Övervaka bolagets styrning av tredjepartsleverantörer
  - ❑ Säkerställa att det finns ett system för hantering av informationssäkerhet (baserat på erkända internationella standarder och branschledande metoder samt i linje med eventuella tillsynsrekommendationer)
  - ❑ Säkerställa att det finns kommunikationsplaner samt utpekad talesperson (informera kunder, motparter eller allmänheten om incidenter eller större sårbarheter)

- Säkerställa att det finns en roll eller ansvarig för tredjepartshantering (i ledningen)

- Ansvarsuppdelning mellan operativ IKT hantering, kontrollfunktioner och internrevision, baserat på modellen för tre försvarslinjer.

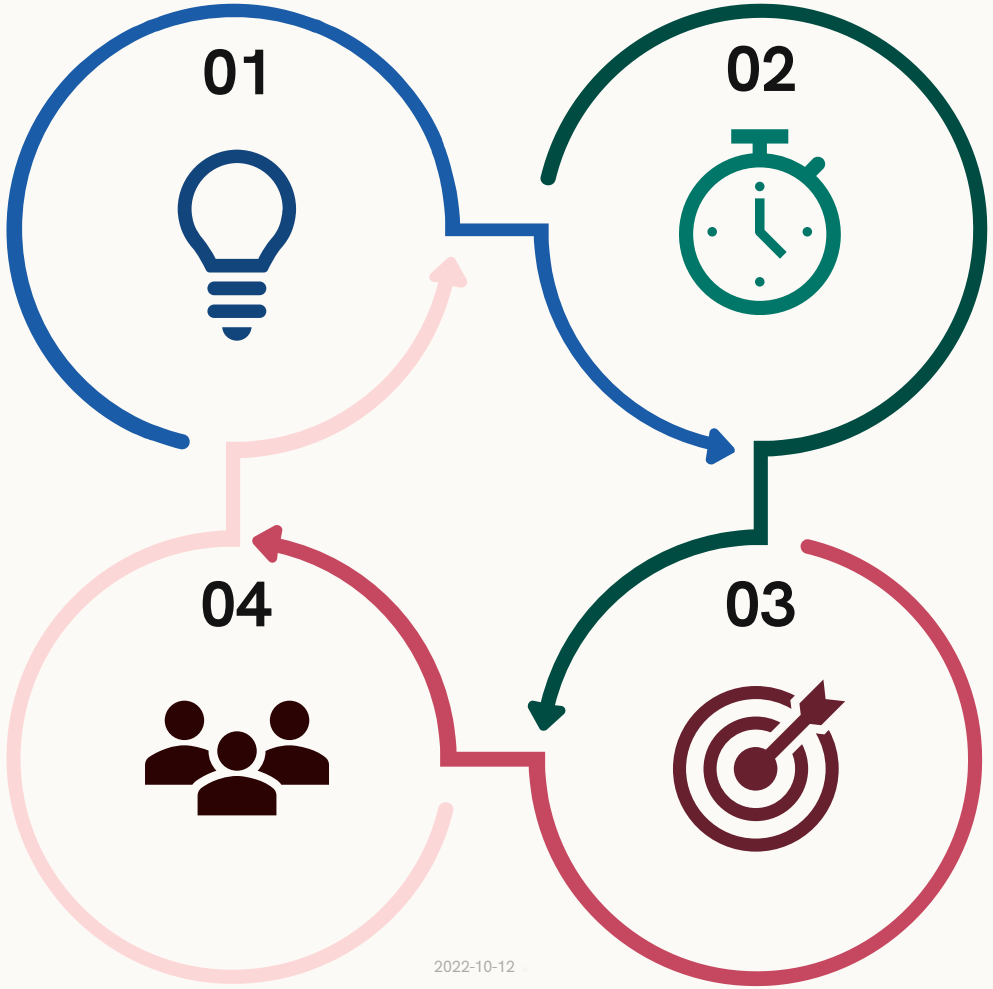
IKT riskhantering

Detaljer avseende cybersäkerhetsramverk (Artikel 7-10)

01. Identifiera

Artikel 7:

- Kartlägga verksamheten (jmf. process-kartläggning)
- Identifiera alla IKT-risker inkl. förändringar och systemförändringar
- Behörighetshantering



02. Skydda & förebygga

Artikel 8:

- Övervaka och kontrollera IKT-miljön
- Säkerställa motståndskraft, genom att använda den senaste IKT-tekniken och processerna
- Utarbeta riktlinjer för informationssäkerhet.

04. Åtgärda & återställa

Artikel 10:

- IKT-kontinuitetsplan samt årlig testning
  - Resultatet av testerna ska rapporteras till FI
- Alla kostnader och förluster för IKT-avbrott och IKT-incidenter ska rapporteras till den nationella tillsynsmyndigheten (dvs. FI).

03. Upptäcka

Artikel 9:

- Snabbt upptäcka onormal verksamhet
- Regelbunden testning av upptäcksförmågan
- Upptäcksförmågan ska bestå av varningströskelvärden

IKT-relaterad incidentrapportering

Hantering, klassificering och rapportering

3. Rapportering av större IKT-relaterade incidenter

Artikel 17

- De finansiella enheterna ska rapportera större IKT-relaterade incidenter till myndighet samt informera kunder
- Rapportering: 1-dag, 1-vecka, 1-månad

4. Harmonisering av rapporeringsinnehåll och mallar

Artikel 18

ESA i samråd med ENISA och ECB kommer utarbeta Tekniska Standarder för tillsyn

2. Klassificering av IKT-relaterade incidenter

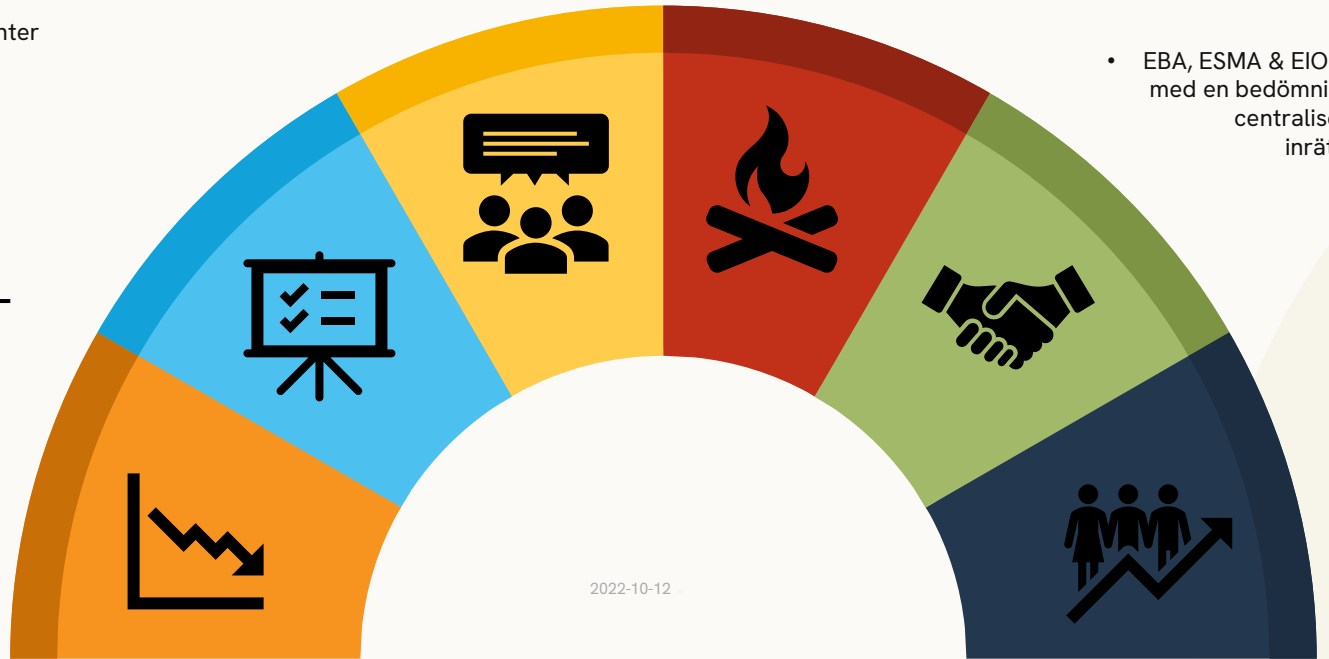
Artikel 16

- Klassificera IKT-relaterade incidenter

5. Centralisering av rapportering av större IKT-relaterade incidenter

Artikel 19

- EBA, ESMA & EIOPA ska utarbeta en gemensam rapport med en bedömning av genomförbarheten av ytterligare centralisering av incidentrapporteringen genom inrättandet av en gemensam EU-knutpunkt



1. Process för hantering av IKT-relaterade incidenter

Artikel 15

- Process för incidenthantering
- Indikatorer för tidig varning så som larm

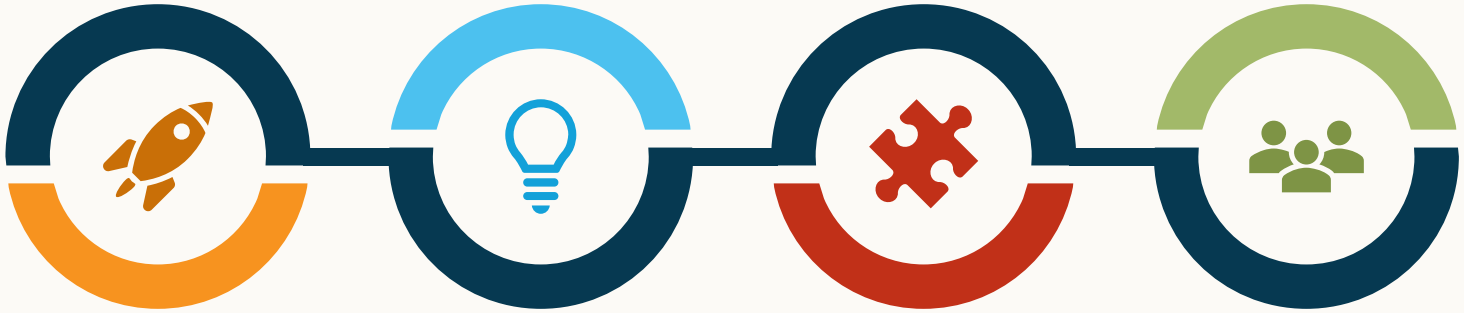
6. Återkoppling från tillsynsmyndigheterna

Artikel 20

- När den behöriga myndigheten har mottagit en rapport enligt Artikel 17 ska den bekräfta mottagandet och så snart som möjligt lämna all nödvändig återkoppling eller vägledning till den finansiella enheten

Testning av digital operativ motståndskraft

Olika former av säkerhetstestning inklusive krav på hotstyrd penetrationstestning



Allmänna krav för testning av digital operativ motståndskraft

Artikel 21

- Ramverk för testning av digital operativ motståndskraft

- Tester ska genomföras av oberoende parter

Testning av IKT-verktyg och IKT-system

Artikel 22

- Testningsprogrammet:
  - sårbarhetsanalyser och skanningar
  - analyser av öppen källkod
  - källkodsgranskningar (när så är möjligt)
  - nätverkssäkerhetsbedömningar
  - gapanalyser
  - fysiska säkerhetsgranskningar
  - frågeformulär
  - scenariobaserade tester
  - kompatibilitetstester
  - prestandastester
  - tester ändpunkt till ändpunkt (end-to-end) och
  - Penetrationstester

Avancerad testning av IKT-verktyg och IKT-processer baserat på hotstyrd penetrationstestning

Artikel 23

- Utökade krav på G-SII och O-SII (var 3:je år)

- Ska minst omfatta kritiska funktioner och tjänster och ska genomföras på produktionssystem i drift

- Tester ska valideras av de behöriga myndigheterna (som sedan utfärdar ett intyg).

Krav för testare

Artikel 24

- Det finns sundhetskrav på de testare (bl.a. certifierats av ett ackrediteringsorgan).

Hantering av IKT-tredjepartsrisker

Ett omfattande kapitel som i utgår från EBA:s Outsourcing guideline och EIOPA:s Guideline on outsourcing to Cloud Service providers

Krav på utläggning av verksamhet

Omfattar huvudprinciper för en sund hantering av IKT-tredjepartsrisker

Granskning och tillsyn av utlagd verksamhet

Tillsysnsramverk för kritiska tredjepartsleverantörer av IKT-tjänster.

Hantering av tredjepartsleverantörer

Innan utläggning

IKT riskhanteringsramverket ska omfatta utkontraktering som en integrerad del av ramverket och omfatta:

- **Register** omfattande alla utkontrakteringsarrangemang vilket minst årligen ska **rapporteras** till FI.
- **Preliminär utvärdering** av utkontrakteringsleverantören innan man får ingå avtal. Utvärderingen ska omfatta:
  - Efterlevnad av höga, relevanta och de senaste standarderna för informationssäkerhet.
  - Utvärdering hur väl leverantören och dess tjänster passar den
  - Utvärdering av koncentrationsrisker
- En riskbaserad plan för **inspektion och revision** av tredjepartsleverantören.
- Tillräckliga **avslutskriterier** och **exit-strategier**
- **Informationssäkerhetskrav** i kontraktet med leverantören

Krav på en ”**multi-vendor strategi**” för outsourcing inkl. **outsourcing policy**.

Under utkontraktering samt ESA mandate

ESA pekar ut vilka leverantörer som anses **kritiska** för den finansiella sektorn.

ESA utpekar en Lead Overseer, för varje kritisk tredjepart, som utarbetar en granskningsplan. Lead Overseer har följande mandat:

- Kan begära in all nödvändig information, dokumentation och rapporter
- Genomföra generella **utredningar och kontroller**
- Stoppa användandet av kedjad outsourcing
- Genomföra **platsbesök** och besöka vilka lokaler eller faciliteter de önskar (även globalt)
- **Försegla lokaler, bokföringsmaterial eller affärsdokumentation** under inspektioner
- **Revidera** alla relevanta IT-system, nätverk, tillgångar, information eller data
- ESA kan tillfälligt begära finansiella enheter att **helt eller delvis avbryter eller avslutar** användningen av en viss IKT-tredjepart tills riskerna åtgärdats

Får besluta om **Vite** (1% av den kritiska tredjepartsleverantörens globala omsättning per dag, i högst 6 månader).

Arrangemang för informationsutbyte

Arrangemang för utbyte av information och underrättelse om cyberhot

Artikel 40

- Finansiella enheter får **utbyta information och underrättelser om cyberhot**, indikatorer på äventyrad säkerhet, taktiker, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg för att förbättra den enheternas digitala operativa motståndskraft, öka medvetenheten om cyberhot, begränsa eller hindra spridning av cyberhot eller begränsningsstrategier, åtgärds- och återställningsplaner.

- Detta måste ske inom en **betrodd grupp** av finansiella enheter och genom arrangemang som skyddar informationsutbytet, affärshemligheter, personuppgifter och följer riktlinjer för konkurrenspolitiken

- Arrangemangen ska innehålla fullständiga villkor för deltagande, och om så är lämpligt om myndigheters deltagande

- Finansiella enheterna ska underrätta behöriga myndigheter om sitt deltagande i arrangemang för informationsutbyte

Riskbilden som reglerare bedömer den idag

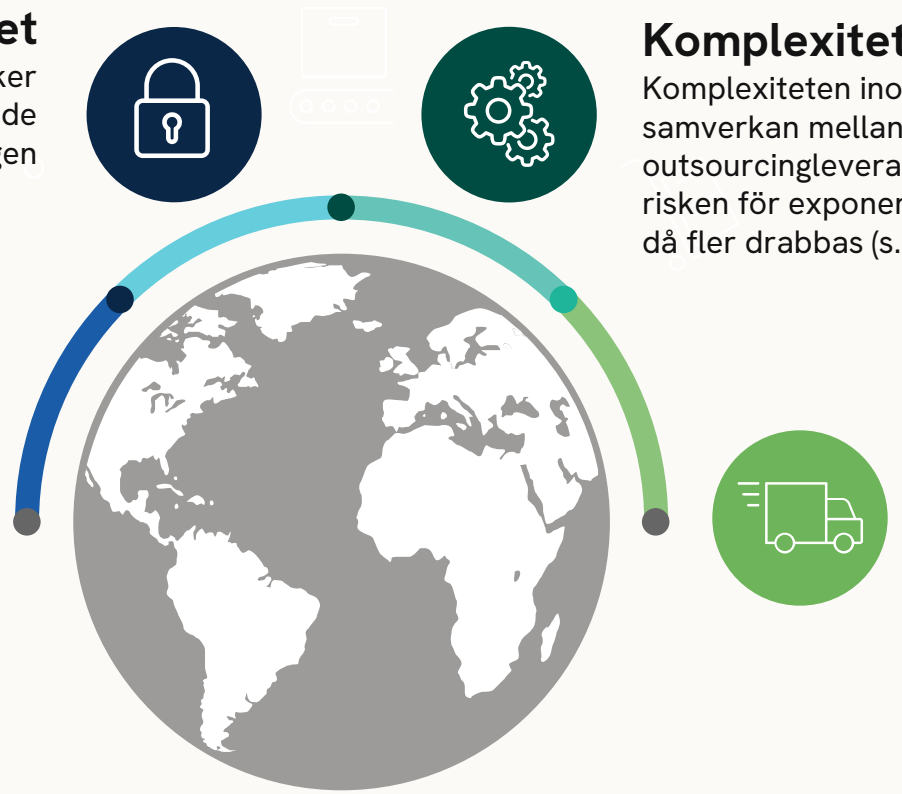
I den senaste riskrapporterna från både EU myndigheter och FI lyfts IT och informationssäkerhetshot fram som en av sektorns största risker.

Cybersäkerhet

Specialiserade och professionella cybersäkerhetsattacker sker löpande inom Europa vilka kräver specifika och anpassade säkerhetsåtgärder inom informationssäkerhetshanteringen

Komplexitet

Komplexiteten inom banker ökar, på grund av ökad samverkan mellan banker och andra institut, beroende av outsourcingleverantörer och FinTech vilka dramatiskt ökar risken för exponering samt ökar konsekvensen av incidenter då fler drabbas (s.k. *systemrisker*)



Ökat antal incidenter inom ICT

Ökande frekvens av incidenter relaterade till IT-och informationssäkerhet

Digitalisering driver risk

IT och informationssäkerhetsrisker ökar inom Europa till en av de största riskkategorierna inom bank-och finanssegmentet. Detta kan minska möjligheten till digitalisering. Vissa leverantörer växer sig snabbt mycket stora med många kunder, vilket kan leda till *koncentrationsrisker*

Då IT, i en form eller annan, är integrerad i nästan alla interna processer så väl som produkter och tjänster, är IT-risker idag ett signifikant hot och kan äventyra ett instituts överlevnad

Frågor?

Tack för ert deltagande

Vem är jag?

Fredrik Ohlsson
Advisory Sweden Operational Risk Partner

fredrik.ohlsson@fcg.se

+46 72 179 49 51

Har ni frågor eller funderingar så får ni gärna höra av er till mig!


FCG