

EUs Digital Operational Resilience Act (DORA)

- En introduction

Agenda

Introduktion

Motivation till DORA

Omfattning av DORA

Risker som EU vill adressera

Tankar kring implementation

2024-04-12

10-TUSEN METERSHÖJD

Varför DORA?

***IKT resiliens är idag en av de största
risker mot enskilda institut
och mot finanssektorn i sin helhet***



NÄR BÖRJAR DORA GÄLLA?

Tidslinje för DORA

DORA är en Förordning inte ett Direktiv

EU-förordning som har trätt i kraft är direkt tillämplig och gäller i alla medlemsländer utan att inkorporeras eller transformeras till nationella rättsregler. Den blir en del av den nationella lagstiftningen genom sitt ikraftträdande. Förordningar ska tillämpas direkt av nationella domstolar och andra myndigheter.

2022-12-27

2025-01-17

**DORA träder i
kraft**

**DORA blir
tillämplig**

Regulatoriska Tekniska Standarder (RTS)

Utöver DORA Förordningen så fastställer EU Kommissionen RTSer som omfattar tillkommande krav utöver DORA. Dessa RTSer har samma legala status som DORA själv och består av detaljerade krav¹.

1: Utöver RTSer finns även ITSer (Implementing Technical Standards)



FINANSINSTITUT ÄR IDAG FULLSTÄNDIGT BEROENDE AV IKT & IKT
LEVERANTÖRER

Motivation till EU- förordningen



Mycket starkt
beroende av digitala
lösningar för nästan
alla delar av
verksamheten

Ökad komplexitet i
IT-infrastrukturen
och integrationer
mellan finansinstitut

Koncentration av IT-
infrastruktur till ett
fåtal tredjeparts-
leverantörer



Ökat antal
incidenter och
ökade risker
inom IKT



I flera av de senaste stabilitetsrapporterna från både lokala och internationella myndigheter lyfts IKT risker
upp på första, andra eller tredje plats.

IKT rankas som en fantastisk möjliggörare både affärs-, effektivitets- och marknadsmässigt men samtidigt som
en av de allvarligaste riskerna mot finansiell institut idag.

IKT BREDDAR OMFATTNINGEN UTÖVER IT

Vad betyder IKT?



ADB

Beskrivning av ADB

Automatisk behandling av data med hjälp av specialiserade datorer och mjukvara. Rationaliserade det manuella arbete med komplexa beräkningar.

Specialistfunktioner.



Informations Teknologi

Beskrivning av IT

Samarbete mellan mer generella datorer (nätverksuppkopplade administrativa datorer).

Hårdvara och mjukvara styrs och hanteras inom bolaget och hanterade mycket av det traditionella kontorsarbetet.

Intåget av standardiserat globalt nätverk (Internet).



IT & Kommunikations- teknologi

Beskrivning av IKT

Utökar IT genom att inkludera telekommunikation, UC och nätverk. Begreppet brukar omfatta datorer, mobiler, serverar, infrastruktur och externa leverantörer exv. virtualisering via moln-tjänsteleverantörer och nya arbetsmetoder så som Agila modeller.

Till stor del styrs och hanteras IT-resurserna hos en/flera tredjeparts-leverantörer över internet.

IKT omfattar hela det ekosystem som ett finansiellt institut behöver för att kunna verka på en marknad. Det inkluderar samarbetspartners och tredjepartsleverantörer.



BETYDER OLIKA SAKER FÖR OLIKA PERSONER

Begrepp inom säkerhet



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, hårdvara och programvara. IT-säkerhet koncentrerar sig på hot och skydd förenade med användning av informationsteknik ("IT").



Cybersäkerhet

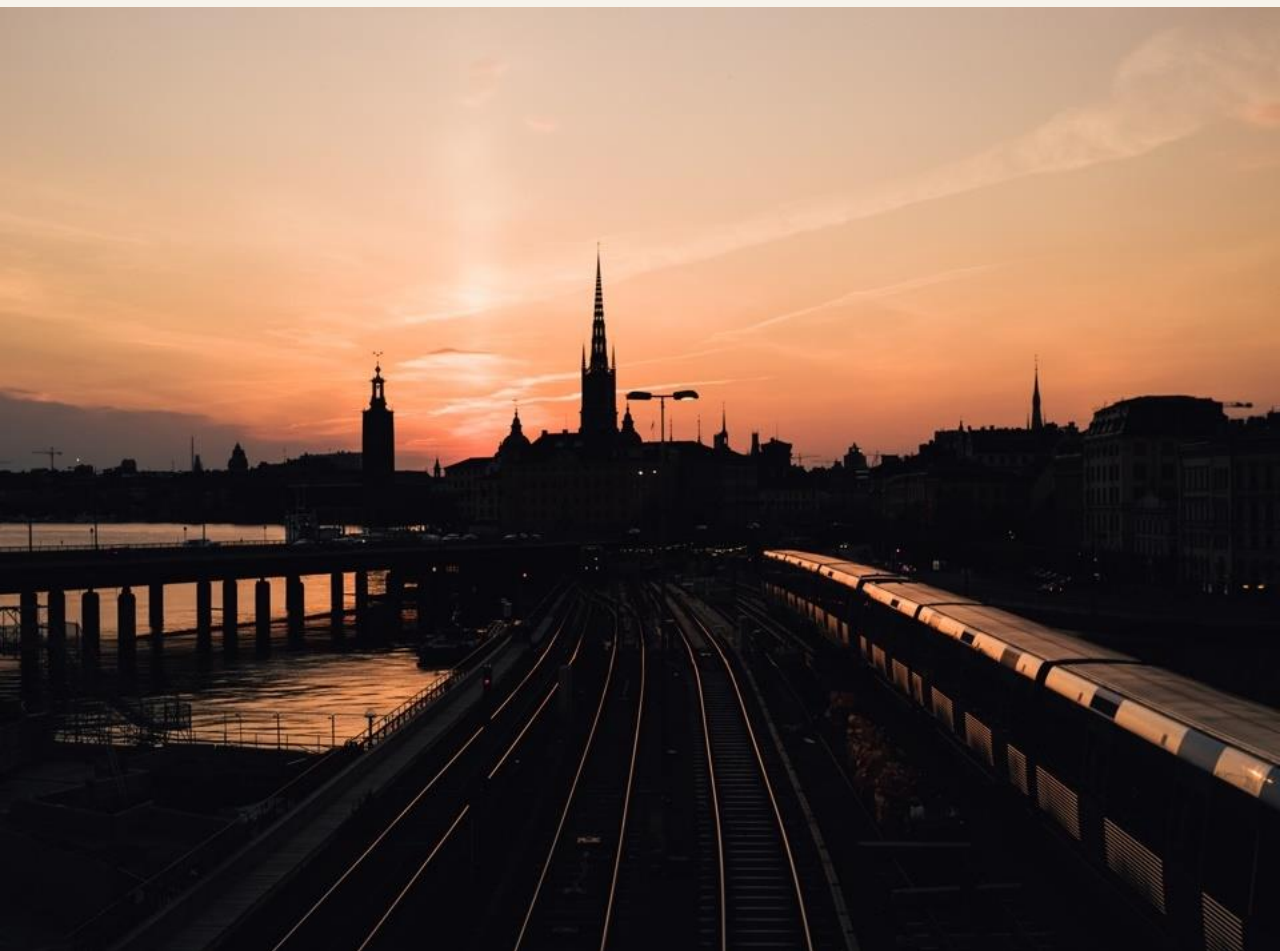
En definition av flera

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



Nomenklaturen skiljer sig mellan professionella definitioner och i dagligt tal





RESILIENS ♥ MOTSTÅNDSKRAFT

Syftet med DORA är att säkerställa ett instituts digitala operativa motståndskraft



Digital Operativ Motståndskraft

Förmågan att bygga upp, säkerställa och se över sin operativa integritet ur ett tekniskt perspektiv genom att, direkt eller indirekt, med användning av tjänster från IKT-tredjepartsleverantörer, säkerställa hela skalan av IKT-relaterad kapacitet som behövs för att hantera säkerheten i de nätverks- och informationssystem som en finansiell enhet använder och som stöder ett fortlöpande tillhandahållande av finansiella tjänster och deras kvalitet.

Eller enklare uttryckt:

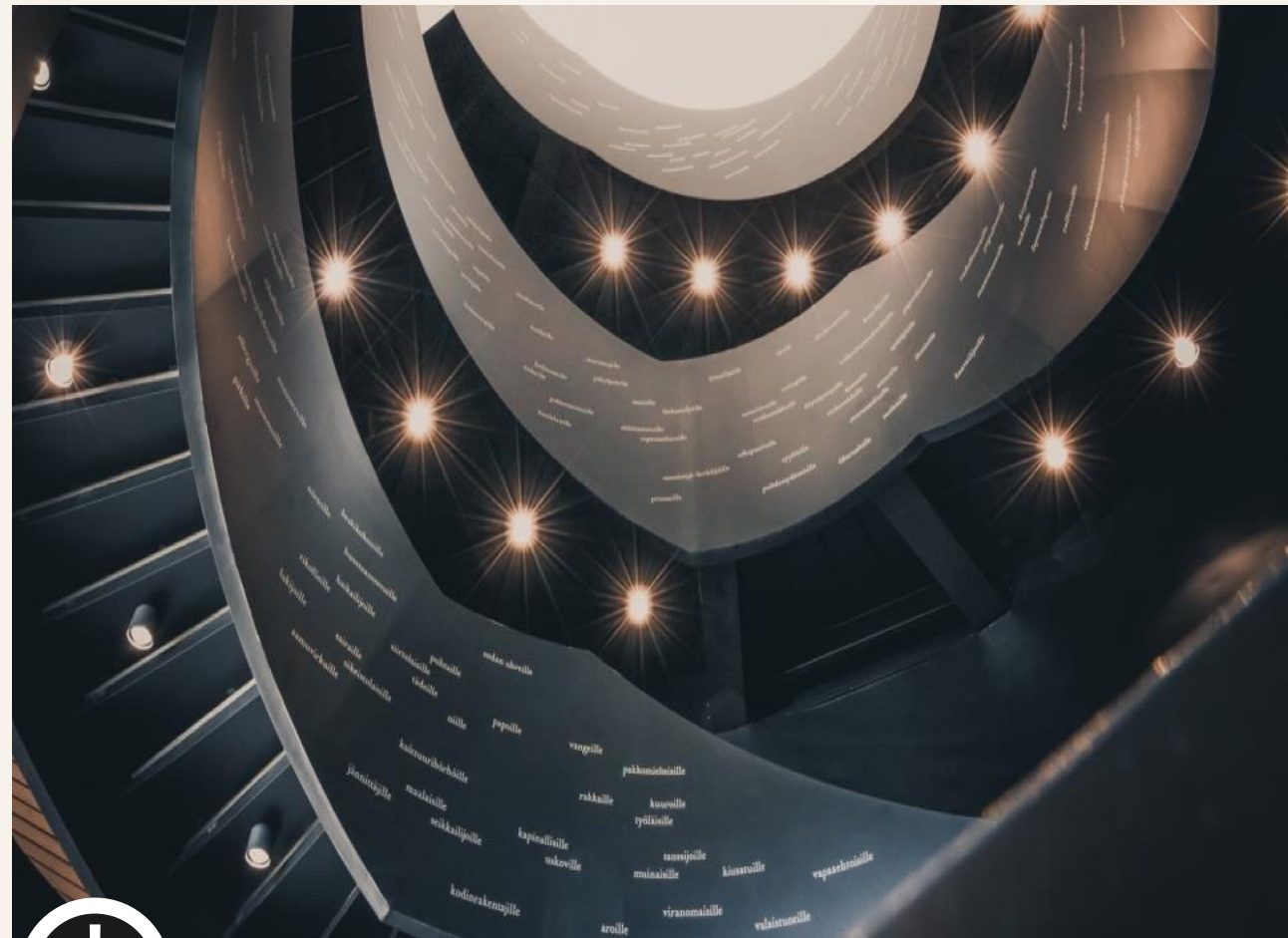
Ett institut och hela finanssektorns förmåga att identifiera och förbereda sig för, reagera och anpassa sig till, återhämta sig och lära sig av störningar eller avbrott i verksamheten.

Resiliens är mycket bredare än kontinuitetshantering

MÅLSÄTTNING ÄR ATT SKAPA GEMENSAMMA STANDARDS OCH KRAV
FÖR *NÄSTAN* HELA FINANSSEKTORN

Vem omfattas av DORA?

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



Direktivet omfattas av proportionalitetsprincipen, där hänsyn tas till den finansiella enhetens affärsbehov, riskprofil, storlek och komplexitet



Proportionalitet

Beakta

Storlek, riskprofil samt naturen, skalan och komplexiteten i hela affärsverksamheten

Hela kap 2 (Risk Management) och relevanta delar av kap 3, 4 och 5.

Storlek

Fasta intervaller på EU-nivå

Mikrobolag – undantagna i stor utsträckning

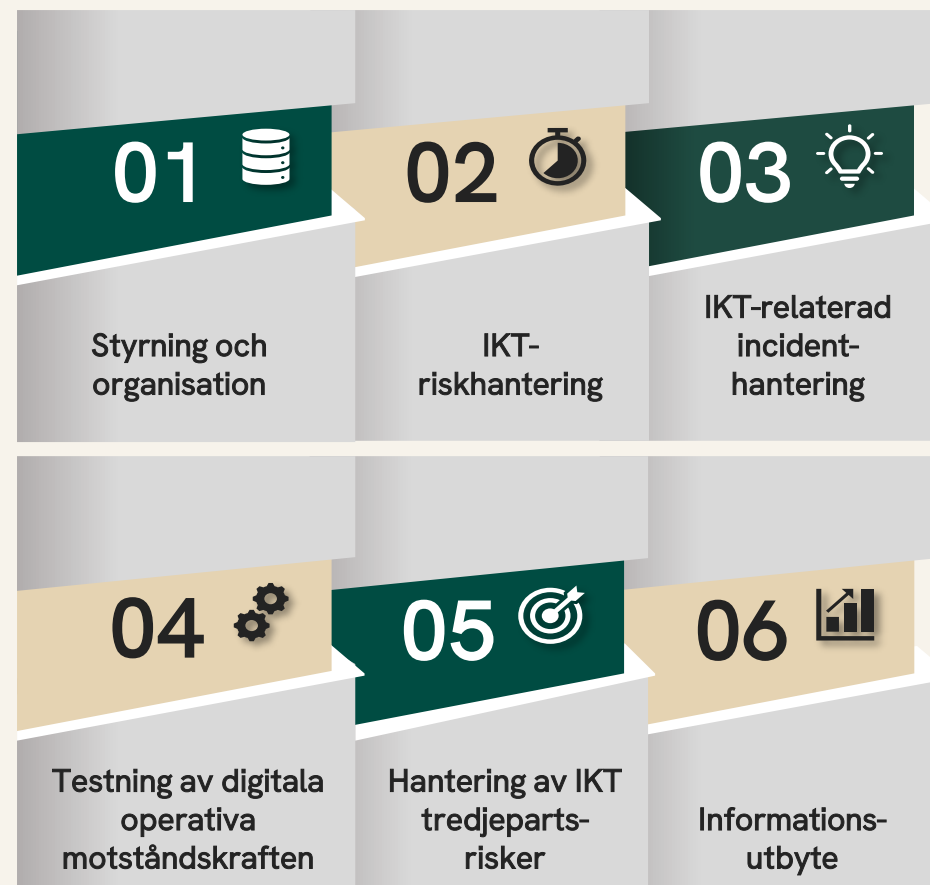
- >10 anställda
- Årlig omsättning och/eller årlig balansomslutning > 2 MEUR.





OMFATTANDE DETALJNIVÅ I DORA OCH RTS:ERNA.

DORA är uppdelad i 6 övergripande regleringsområden



Detaljnivån är omfattande och uppdelade i 64 artiklar. Regleringen omfattar allt från finansiella enheter (institut), reglerande EU organ och nationella tillsynsmyndigheter.

UTÖKADE KRAV PÅ STYRELSEN INOM RISKHANTERING FÖR IKT

Styrning och organisation

Styrelsen är ansvariga för införandet av ett IKT baserat riskramverk (styrnings och kontrollramverk), och behöver:

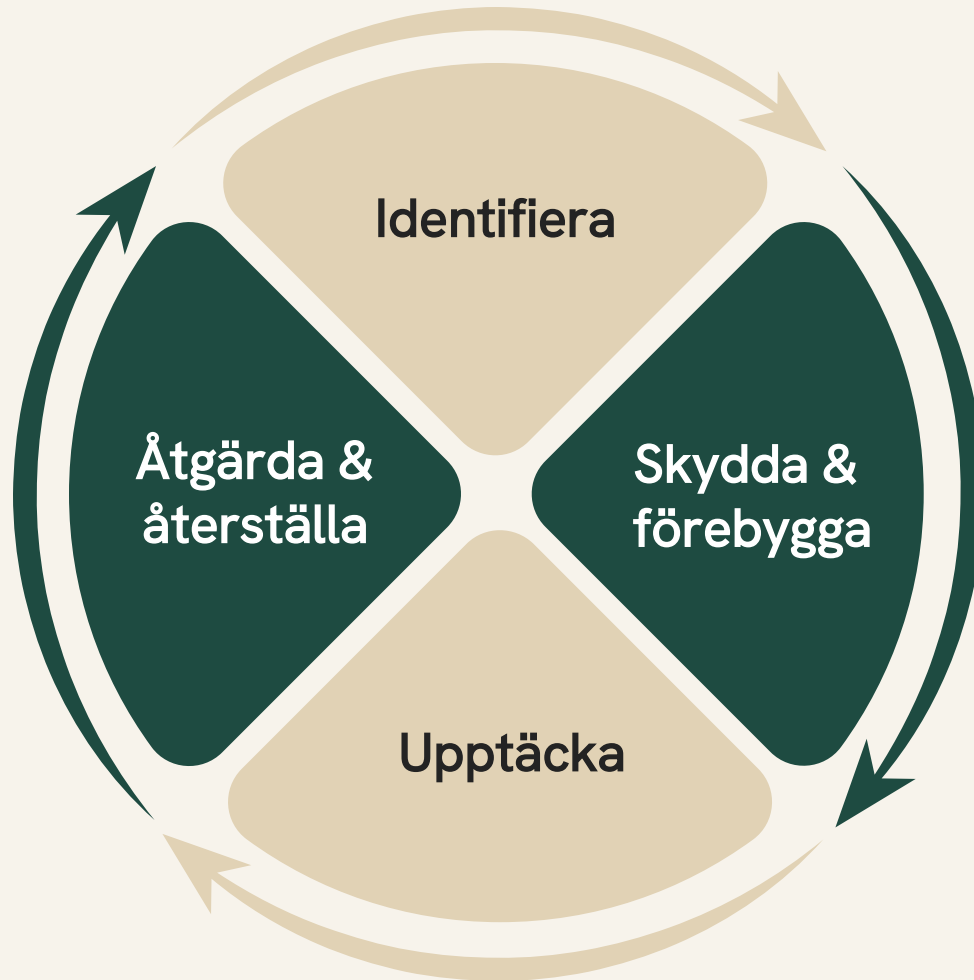
- Definiera tydliga roller och ansvar & säkerställ tillräckliga resurser
- Fastställa lämplig risktoleransnivå
- Anslå och regelbundet se över lämplig budget för att uppfylla behov av digital operativ motståndskraft när det gäller alla typer av resurser
- Övervaka IKT kontinuitetsförmågan / bolagets motståndskraft, inkl. informeras om IKT-relaterade incidenter
- Övervaka bolagets incidenthanteringsförmågan
- Informeras och övervaka bolagets arrangemang med tredjepartsleverantörer inkl. godkänna riktlinjer för IKT arrangemang
- Säkerställa att det finns ett system för hantering av informationssäkerhet (baserat på erkända internationella standarder och branschledande metoder samt i linje med eventuella tillsynsrekommendationer)
- Löpande få särskild utbildning för att säkerställa tillräckliga och aktuella kunskaper inom IKT-risker

Säkerställa att det finns en roll eller ansvarig för hantering av tredjepartsleverantörer (i ledningen)

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



Rapportering till styrelsen är en fundamental princip i DORA



- Riskramverket behöver anpassas för att passa in i en IKT-baserad operativ modell
- RTS som detaljerar området ytterligare

SIGNIFIKANTA FÖRÄNDRINGAR FÖR ATT ANPASSA RISKRAMVERKET

IKT-riskhantering

Alla krav inom DORA utgår från riskhantering. DORA ställer krav på ett riskramverk för IKT med målen att leda till:

- Sund, heltäckande och väldokumenterad IKT-riskhanteringsram,
- Resilienta IKT-system och verktyg,
- Löpande identifiera all källor till IKT risker (inkl. omvärldsbevakning),
- Anpassa både proaktiva- och reaktiva skydd för IKT miljön,
- Identifiera onormala aktiviteter i IKT miljön (teknisk standard kommer),
- Upprätta kontinuitetshantering och återställningsplaner som en del av den operativa resiliensen (här finns en RTS som detaljerar kraven),
- Kommunikationsplaner inkl. talespersoner.

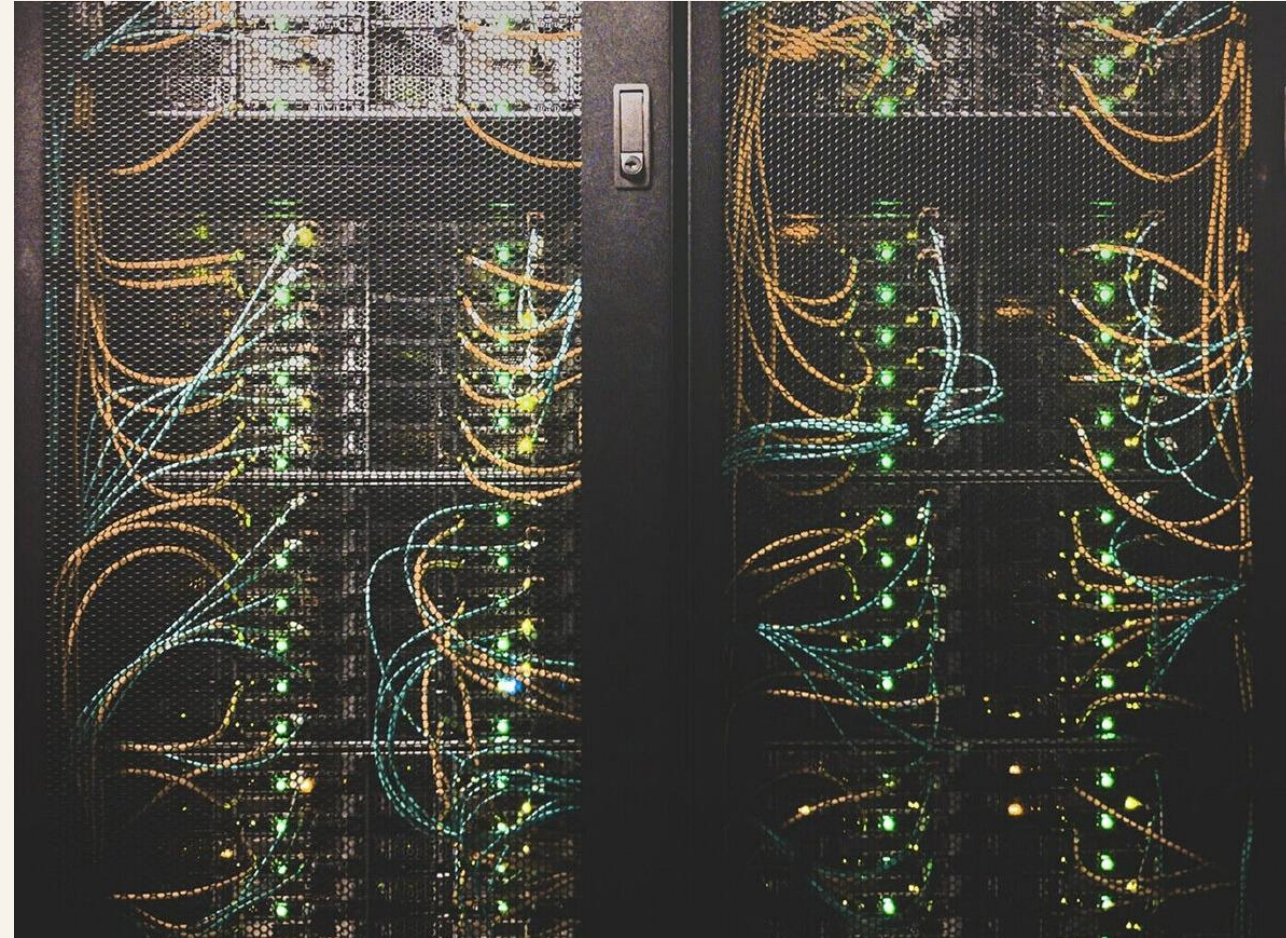
INCIDENTER BEHÖVER FORMELLT RAPPORTERAS

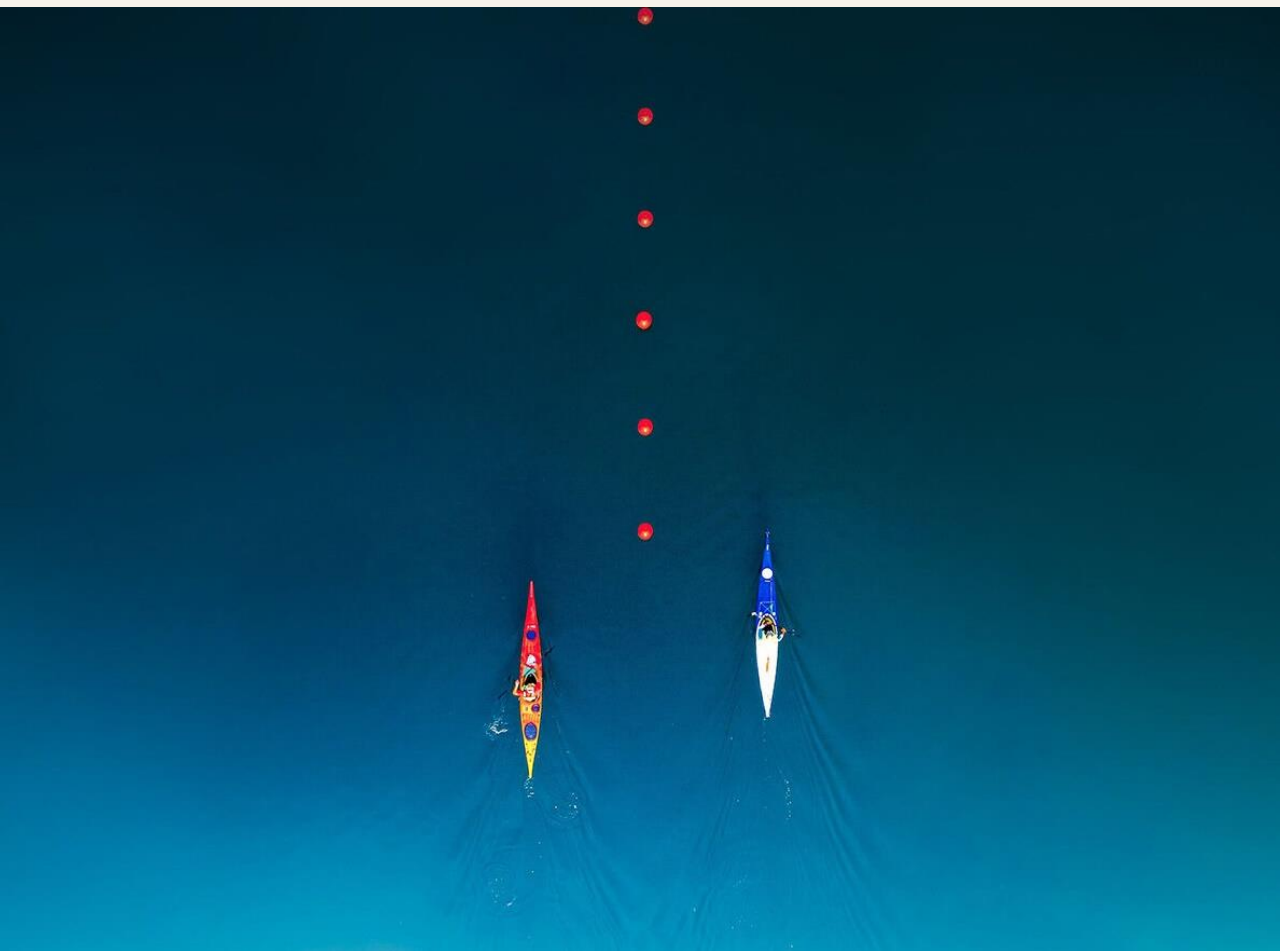
IKT incidenthantering

Institutioner ska etablera och förvalta en styrningsprocess för övervakning och loggning av IKT-incidenter.

- Denna IKT incidenthanteringsprocess ska **klassificera** incidenter (enligt kommande Teknisk Standard)
- Signifikanta incidenter, enligt klassificering, ska **rapporteras till Finansinspektionen**

Finansinspektionen ska stötta institutioner vid incidentrapportering genom **nödvändig återkoppling eller vägledning**





TESTER OMFATTAR AVANCERADE PENETRATIONSTESTER

Digital operativ motståndskraft - testning

Testningens målsättning är att säkerställa institutionernas riskhanteringsramverk ur ett förberedelse och eventuella brist perspektiv. Detta för att löpande uppdatera riskramverket för att säkerställa tillämpligheten

- Alla institutioner ska testa sina IKT system och verktyg, minst var tredje år
- Tillkommande krav på testning finns för de institutioner som av Finansinspektionen utpekas som väsentliga/kritiska

Institutioner bör utarbeta ett **testningsramverk** för att hantera testningen av IKT-system vid nyanskaffningar eller vid förändringar.

Upprätta strategi för digital operativ resiliens

KRAVEN PÅ TESTNING ÄR OMFATTANDE

Testning av digital operativ motståndskraft

1



Allmänna krav för testning av digital operativ motståndskraft

2



Testning av IKT-verktyg och IKT-system

3



Krav för testare

4



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



STRUKTUREN ÄR DET SAMMA SOM TIDIGARE REGLERING

Utkontraktering av IKT-tjänster

Övergripande principer innan utläggning

Omfattar huvudprinciper för sund hantering av IKT-tredjepartsrisker innan utläggning.

Utkontraktering



Granskning och tillsyn av utlagd verksamhet

Tillsynsramverk för kritiska tredjepartsleverantörer av IKT-tjänster.

ÖVERGRIPANDE PRINCIPER INNAN UTLÄGGNING

Hantering av tredjepartsleverantörer

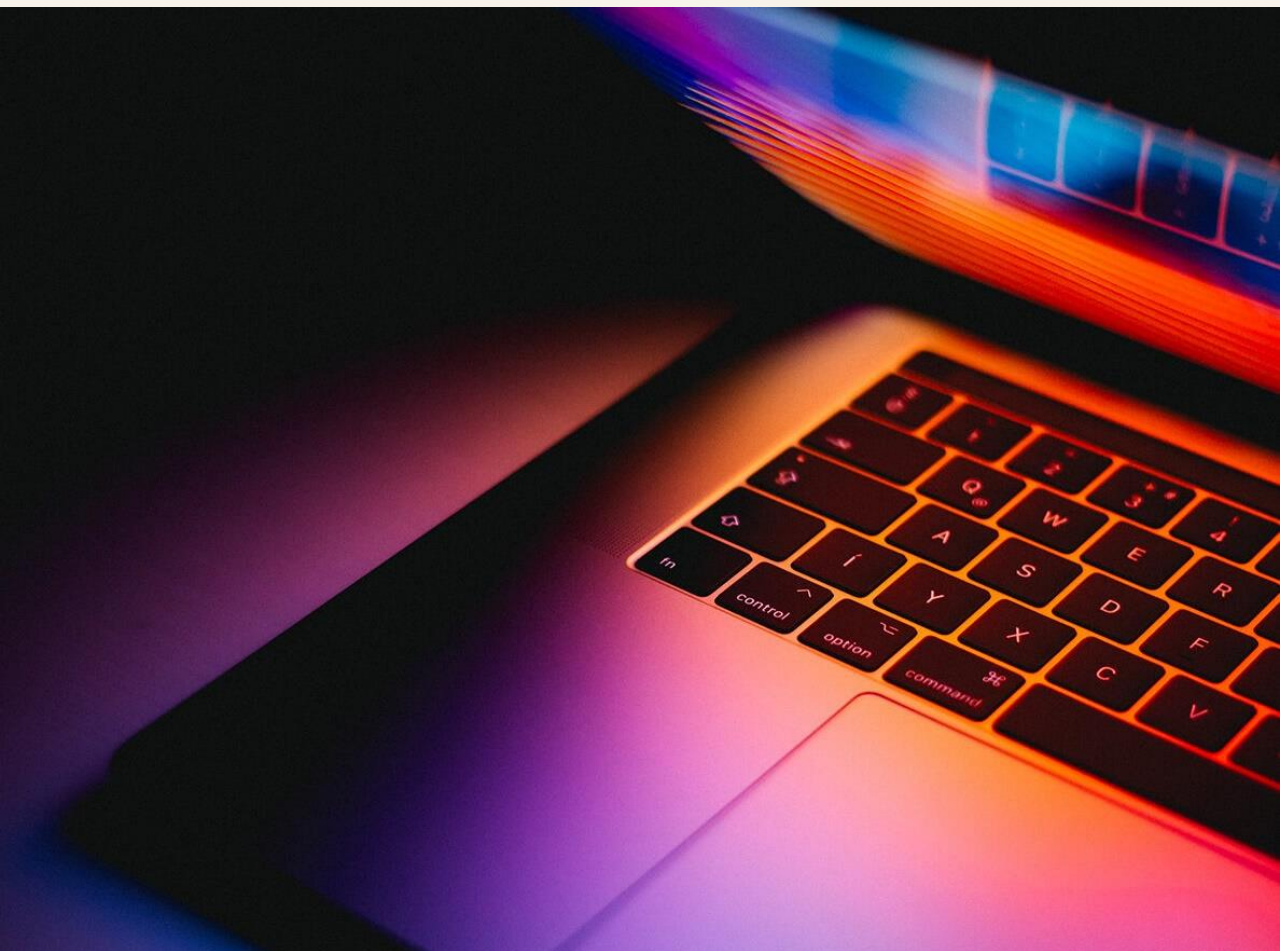
Innan utläggning

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
- DueDiligence av utvalda leverantörer
- En riskbaserad plan för **inspektion och revision** av tredjepartsleverantören. Insynskraven är långtgående.
- Tillräckliga **avslutskriterier** och **exit-strategier**
- **Informationssäkerhetskrav** i kontraktet med leverantören



- Informationssäkerhetskravställningen utökas
- Koncentrationsrisk är nytt analysområde
- Alla IKT leverantörer omfattas



UTÖKAR KRAVEN JÄMFÖRT MED EBA/EIOPA/ESMA (CLOUD)
OUTSOURCING

Hantering av tredjepartsleverantörer

Under utkontraktering

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

Finansinstitutens ansvar avseende INSYN, STYRNING, ÖVERVAKNING, KONTROLL och MÄTNING är omfattande och långtgående

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

FÖRMÅGAN ATT UTBYTA INFORMATION I EN VÄRLD STYRD AV BANKSEKRETESS OCH GDPR

Arrangemang för informationsutbyte

Arrangemang för utbyte av information och underrättelse om cyberhot

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 även myndigheters deltagande

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





REGULATORY TECHNICAL STANDARDS

Tekniska Standarder?

2024-01-17

Första omgången

- Artikel 15. ytterligare harmonisering av verktyg, metoder, processer och policyer för IKT-riskhantering
- Artikel 16. Förenklad IKT-riskhantering
- Artikel 18. Klassificering av IKT-relaterade incidenter och cyberhot
- Artikel 28. Allmänna principer för hantering av IKT-tredjepartsrisker
- Artikel 28 (ITS) - Allmänna principer - punkt 10 - förslag till tekniska standarder för genomförande för att fastställa standardmallar för det register över uppgifter som avses i punkt

2024-07-17

Andra omgången

- Artikel 20. Harmonisering av rapporteringsinnehåll och mallar
- Artikel 20 (ITS) - fastställa standardiserade mallar, formulär och förfaranden för att finansiella enheter ska kunna rapportera en större IKT-relaterad incident och en större drifts- eller säkerhetsrelaterad incident, samt standardiserade mallar för informationsregistret.
- Artikel 26. Avancerad testning av IKT-verktyg, IKT-system och IKT-processer baserad på hotbildsstyrd penetrationstestning
- Artikel 30. Viktiga avtalsbestämmelser för IKT-tredjehands leverantörer
- Artikel 41. Harmonisering av villkor som möjliggör genomförandet för tillsynsverksamheten

2025-01-17

Tillämpningsdatum



IKT ÄR EN SYSTEMRISK

Risker som EU vill adressera

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, beroende till outsourcing-leverantörer och FinTech vilka dramatiskt ökar risken för exponering samt ökar konsekvensen av incidenter då fler drabbas (s.k. **systemrisk**)

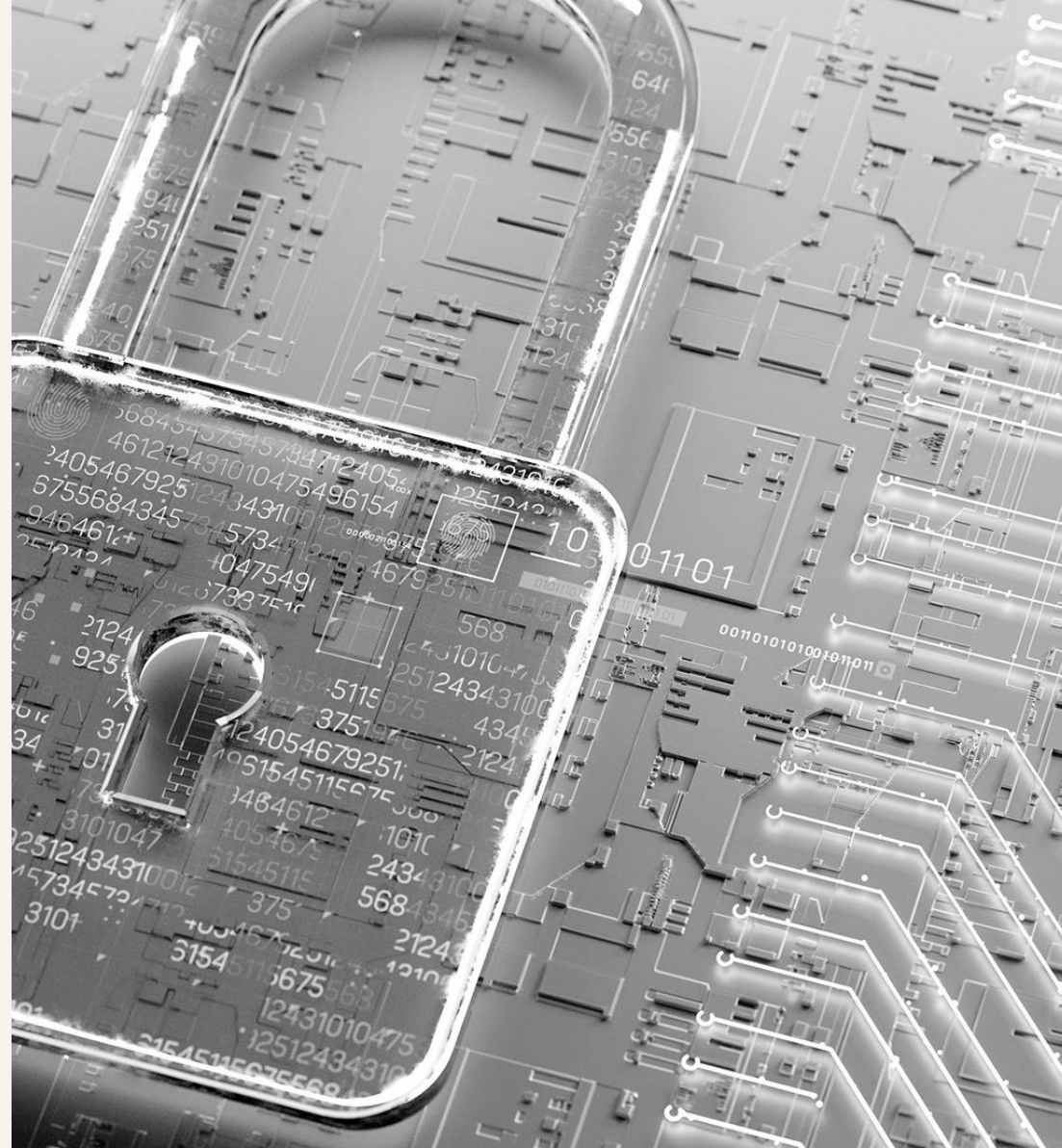


Ökat antal incidenter inom IKT

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. Vissa leverantörer växer sig snabbt mycket stora med många kunder, vilket kan leda till **koncentrationsrisk**

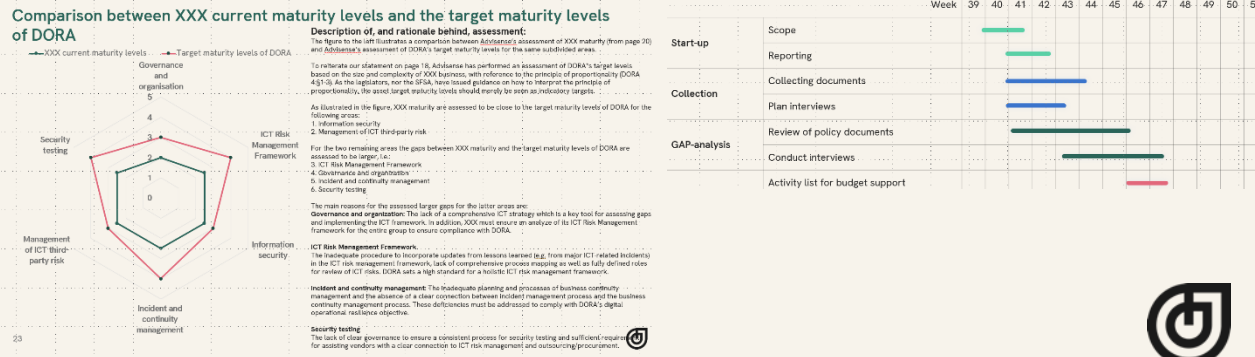




FÖRSTA STEGET I DORA ANALYSEN BESTÅR AV:

GAP-analys och mognadsmätning med handlingsplan

External requirements										DORA's policy									
Chapter no. and title	Article no. and title	Article no. and title	DORA requirement	Other sources	Assessment	Description of deviation	Assessment	Comments	Comments	Comments	Comments	Comments	Comments	Comments	Comments	Comments	Comments	Comments	Comments
3. ICT risk management	1. Governance and organization	1(2024)	No		Completed														
3. ICT risk management	2. Governance and organization	2(2024)	Yes		Major deviation														
3. ICT risk management	3. Governance and organization	3(2024)	No		Completed														
3. ICT risk management	4. Governance and organization	4(2024)	Yes		Major deviation														



IMPLEMENTATION – EFTER GAP & MOGNADSANALYS OCH HANDLINGSPLAN

Hur kan en praktisk implementation se ut?





VILKA ÄR DE STORA FÖRÄNDRINGARNA MED DORA?

Sammanfattning av DORA



DORA är inspirerad av tidigare regleringar inom IKT, outsourcing och intern styrning och kontroll men harmoniserar och utökar kraven och styrningen av IKT.

Målet är att skapa en mer motståndskraftig finanssektor i EU.

ADVISENSE – OM OSS

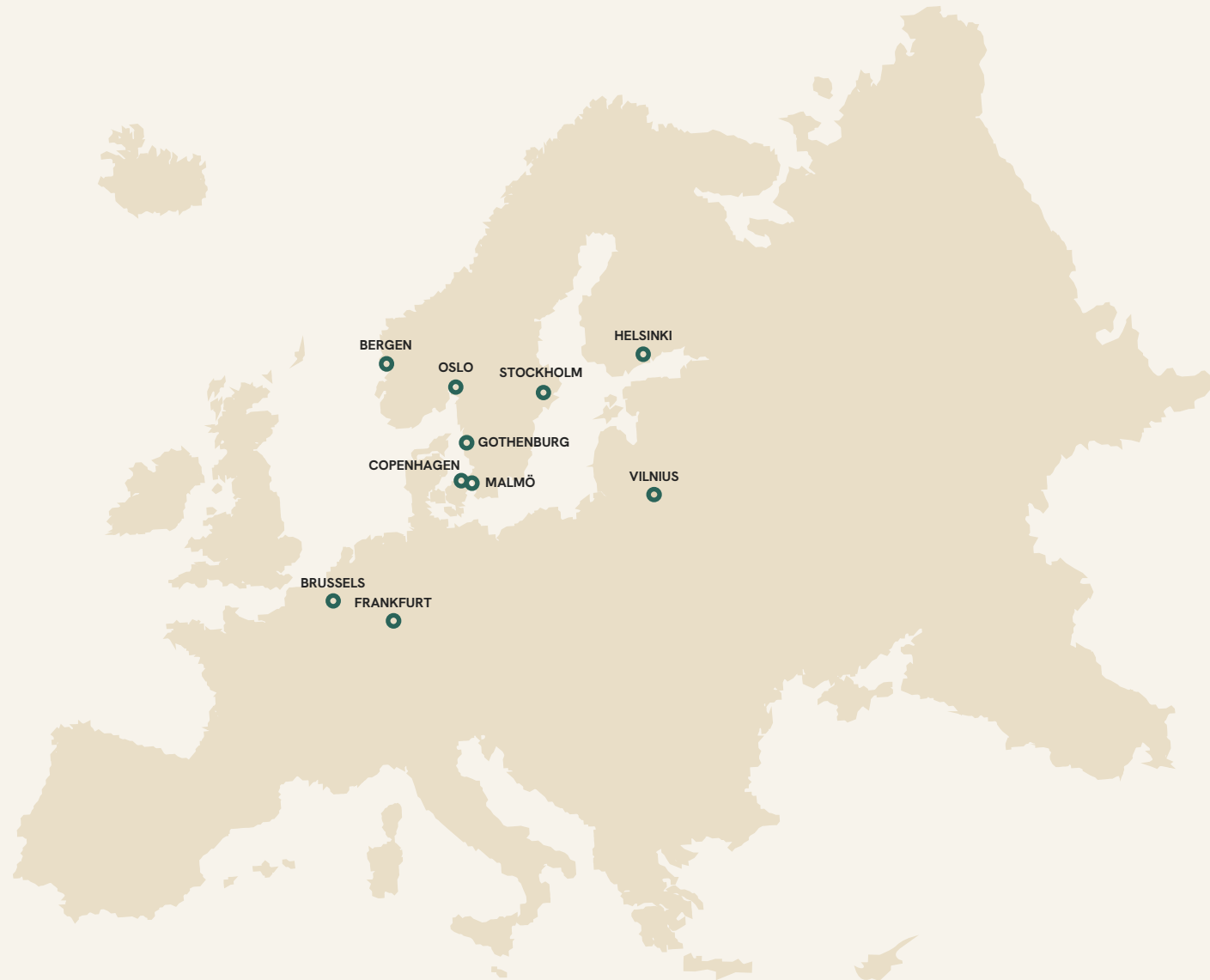
Vi navigerar genom regulatoriska förändringar för att bidra till en mer hållbar finansindustri

Advisense är ett marknadsledande expertföretag i Europa inom governance, risk och compliance med rådgivning och techlösningar i framkant.

Sedan 2008 har vi kombinerat expertis inom regelverk, säkerhet, teknologi och riskhantering för att stötta våra kunder med ledande insikter och praktisk erfarenhet.

Vi hjälper våra kunder navigera i komplexa regelverk och en föränderlig omvärld, och stöttar våra kunder i varje steg i värdekedjan, från analys och rådgivning till implementering och outsourcing.

Advisense har mer än 450 anställda med kontor i Bergen, Bryssel, Köpenhamn, Göteborg, Frankfurt, Helsingfors, Malmö, Oslo, Stockholm och Vilnius.



Kontakt



Fredrik Ohlsson

Managing Director

Fredrik.Ohlsson@Advisense.com

+46 72 179 49 51



Filip Fabri

Senior Associate

Filip.Fabri@Advisense.com

+46 72 161 77 27



Stefan Hederstedt

Director

Stefan.Hederstedt@advisense.com

+46 70 146 38 20

advisense 