advisense

DORA

Introduktion till Digital Operational Resilience Act (DORA)

2023-10-20

Agenda

1. Introduktion DORA
2. Vad Omfattar DORA?
3. Risker som adresseras

Ställ gärna frågor under passet!

VAD, NÄR & HUR?

Vad ?

- **EU förordning** – adresserar ökade risker inom information- och cybersäkerhet samt outsourcing för bolag inom den finansiella sektorn

När ?

- Började gälla 16 jan 2023. Kraven verkställbara från och med **17 jan 2025.**

Omfattas DU?

- JA, sannolikt! En stor mängd bolag omfattas.

Vi har redan infört EIOPA/EBA:s IKT regelverk, betyder det att vi efterlever DORA?

- NJA!

Övergripande om IKT-risker

Inledning

Ökad **digitalisering** och **sammankoppling** leder till IKT-risker, vilket leder till sårbarhet för cyberhot eller IKT-störningar

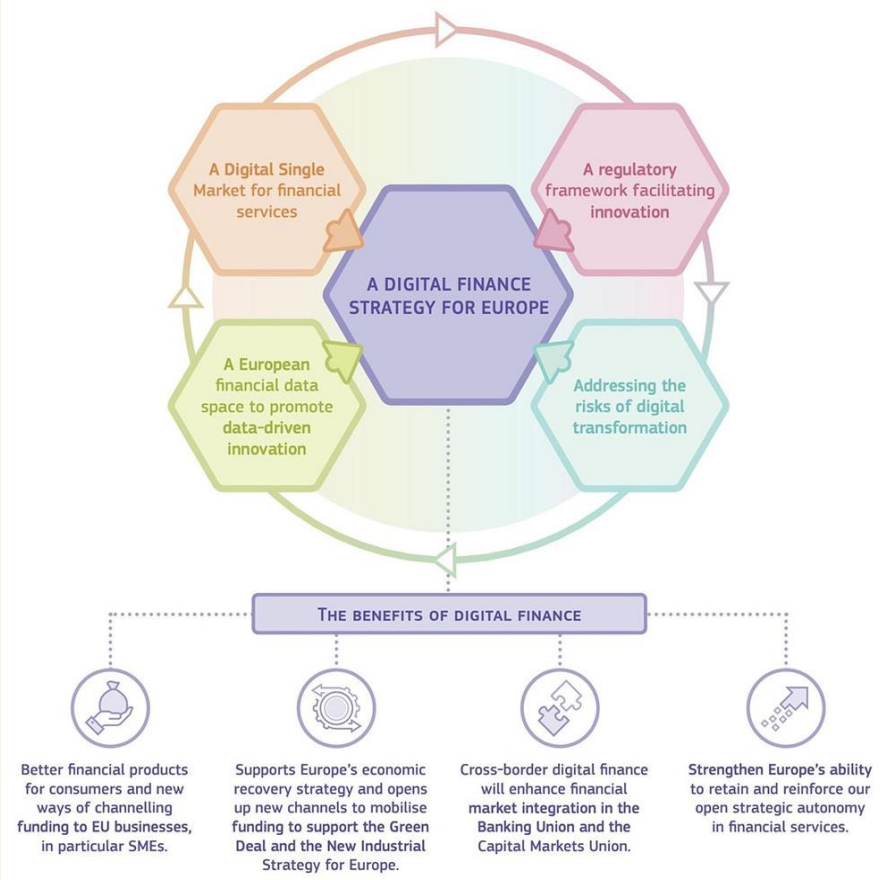
Den **digitala motståndskraft** har ännu inte fullt ut behandlats och integrerats i de operationella ramverken

Europeiska systemrisknämnden (ESRB*) – IKT-risker kan utgöra en **systemisk sårbarhet**

Lokala allvarliga IKT-överträdelser kan leda till nationella och EU risker för stabiliteten i de finansiella systemen

En del av EU:s Digital Finance Package

DORA en del av någonting större



Motivation till DORA

Ökat beroende av digitala lösningar

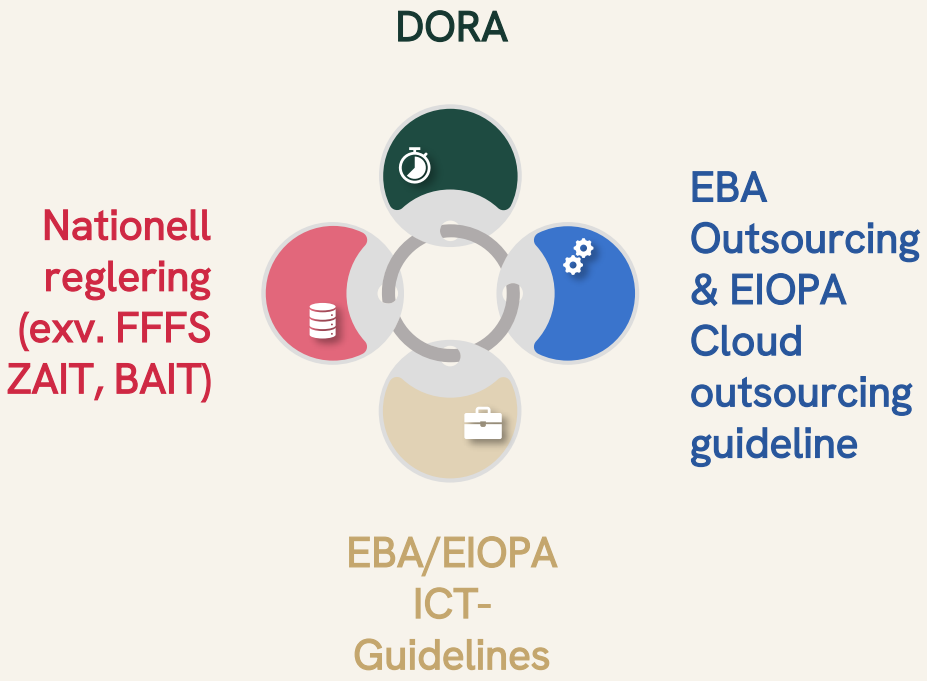
Ökad komplexitet i IT-infrastrukturen och integrationer

Koncentration av IT-infrastruktur till ett fåtal tredjepartsleverantörer

Ökade incidenter och ökade risker inom IKT

DORA bygger vidare på tidigare reglering, så som FFFS 2014:5 och EBA/EIOPA IKT

Jämförelse med nuvarande reglering – vad är nytt?



Nuvarande reglering (EBA/EIOPA IKT och säkerhetsriskhantering & Outsourcing)

Etablera IKT och säkerhetsriskhantering

FOKUS:

- Styrning av IKT
- Riskhantering
- IT

DORA

Förutsätter IKT riskhantering på en grundläggande nivå

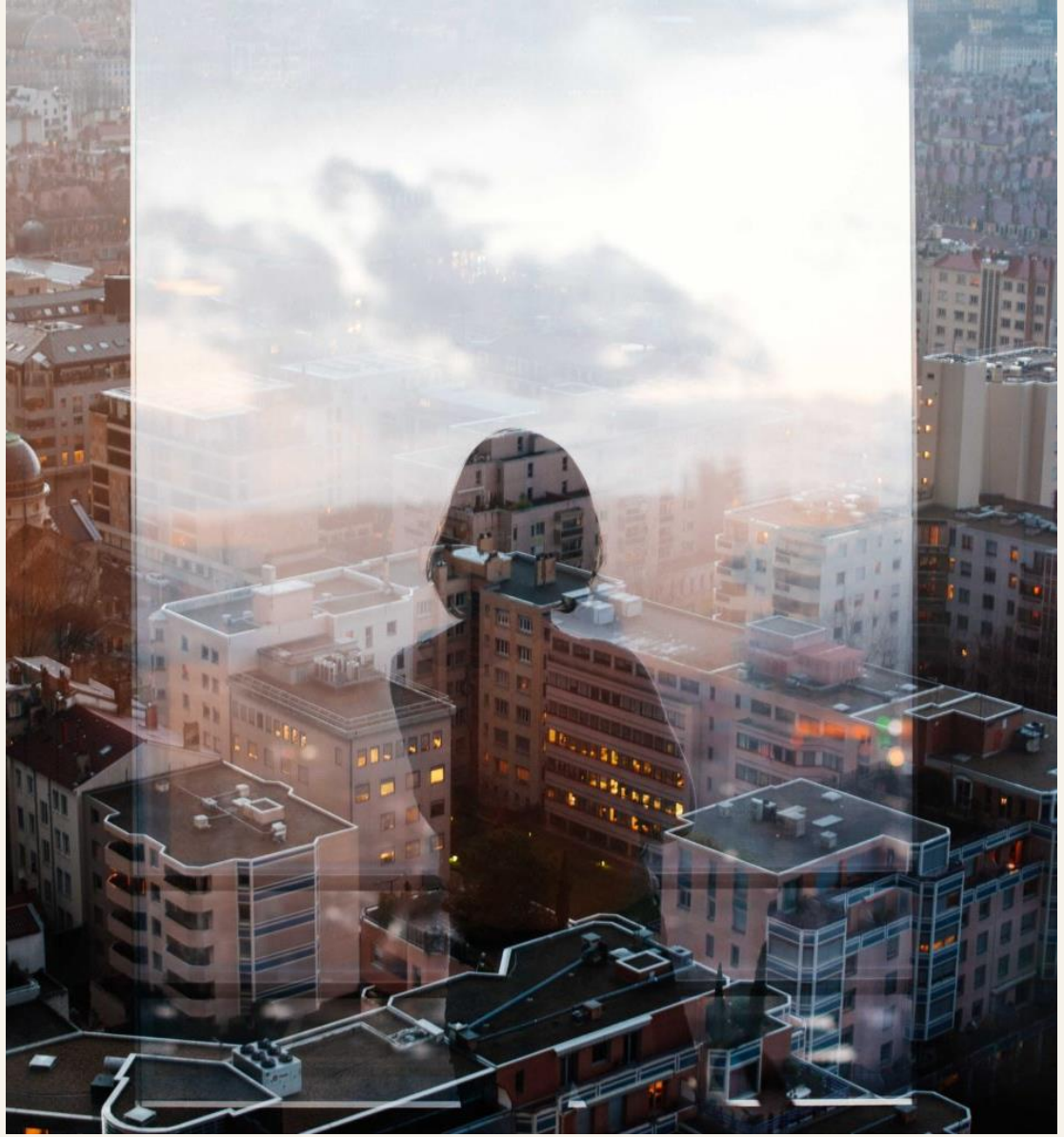
FOKUS:

- Testning av IKT (utökade krav),
- IKT baserad incidentrapportering,
- Utkontraktering till IKT-tredjeparter.

Konsekvenser?

DORA

- FI mandat förändras (i Sverige)
- Minska koncentration och risker för onödiga beroende inom IKT
- Informationsutbyte mellan finansiella aktörer (hot och incidenter)
- Fastställer och stärker rollen för EUs finansiella övervakningsmyndigheter (ESA)



IKT – vad betyder det?

ADB

Beskrivning av ADB

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

Specialist funktioner.

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 och Kommunikationsteknologi

Beskrivning av IKT

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

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

Begreppet informationssäkerhet

Informationssäkerhet

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").

Cybersäkerhet

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.

Syftet med DORA

Digital Operativ Motståndskraft

Beskrivning

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.

Affärsfördelar?

Ökat skydd inom IKT

Ökat IKT-skydd för enskilda institut, partners, marknaden, kunder och även för IKT-tredjepartsleverantörer

Kund & konsumentskydd

Bättre kund- och konsumentskydd kan uppnås

Tillit & rykte

Transparent kommunikation vid cybersäkerhetsrisker, incidenter eller vid kriser ökar tillit och rykte.

Styrning och processkontroll

Ökad styrning och kontroll över institutens interna processer och IKT-stöd

Bryta silos

Ger långtgående fördelar för institut i form av skydd och beslutsstöd

Kontroll över tredjepartsleverantörer

Bättre insyn, styrning, uppföljning och mätning av risker från tredje part

Bättre information

Öppet informationsutbyte kommer att skapa större medvetenhet om hot och risker

Vem omfattas?

- Kreditinstitut
- Betalningsinstitut
- Institut för elektroniska pengar
- Värdepappersföretag
- Leverantörer av kryptotillgångstjänster, m.fl.
- Värdepapperscentraler
- Centrala motparter
- Handelsplatser
- Transaktionsregister
- Förvaltare av alternativa investeringsfonder
- Förvaltningsbolag
- Leverantörer av datarapporterings-tjänster
- **Försäkrings- och återförsäkringsföretag**
- **Försäkringsförmedlare, m.fl.**
- Tjänstepensionsinstitut
- Kreditvärderingsinstitut
- Lagstadgade revisorer och revisionsföretag
- Administratörer av kritiska referensvärden
- Leverantörer av gräsrotsfinansieringstjänster
- Värdepapperiseringsregister
- **Tredjepartsleverantörer av IKT-tjänster**

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

6 övergripande regleringsområden

Regleringen omfattar till största del risk, informationssäkerhet och outsourcing

Styrning och organisation

Intern styrning och kontroll

- Finansiella enheter måste ha interna styrnings- och kontrollramar för effektiv hantering av IKT-risker.

Styrelsens ansvar

- Styrelsen har det slutliga ansvaret och en aktiv roll i styrningen av IKT-riskhanteringsramverket.

Mål och anpassning

- Målet är att säkerställa att affärsstrategin är i linje med riskramverket för ICT.

Implementering av riskramverk

- Styrelsen ansvarar för införandet av ett IKT-baserat riskramverk och måste definiera roller, fastställa risktolerans, säkerställa resurser och övervaka kontinuitetsförmåga.

Övervakning och utbildning

- Styrelsen övervakar IKT-kontinuitet, incidenthantering, tredjepartsarrangemang och säkerställer utbildning för aktuella IKT-kunskaper.

IKT–riskhantering

DORA och IKT-riskhantering

- DORA ställer krav på ett robust IKT-riskramverk för att säkerställa snabb, effektiv, och heltäckande hantering av IKT-risker, samt hög digital operativ motståndskraft.

Resilienta IKT-system och verktyg

- Målet inkluderar resilienta IKT-system och verktyg, kontinuerlig identifiering av källor till IKT-risker, och anpassade proaktiva- och reaktiva skydd för IKT-miljön.

Kommunikation och standarder

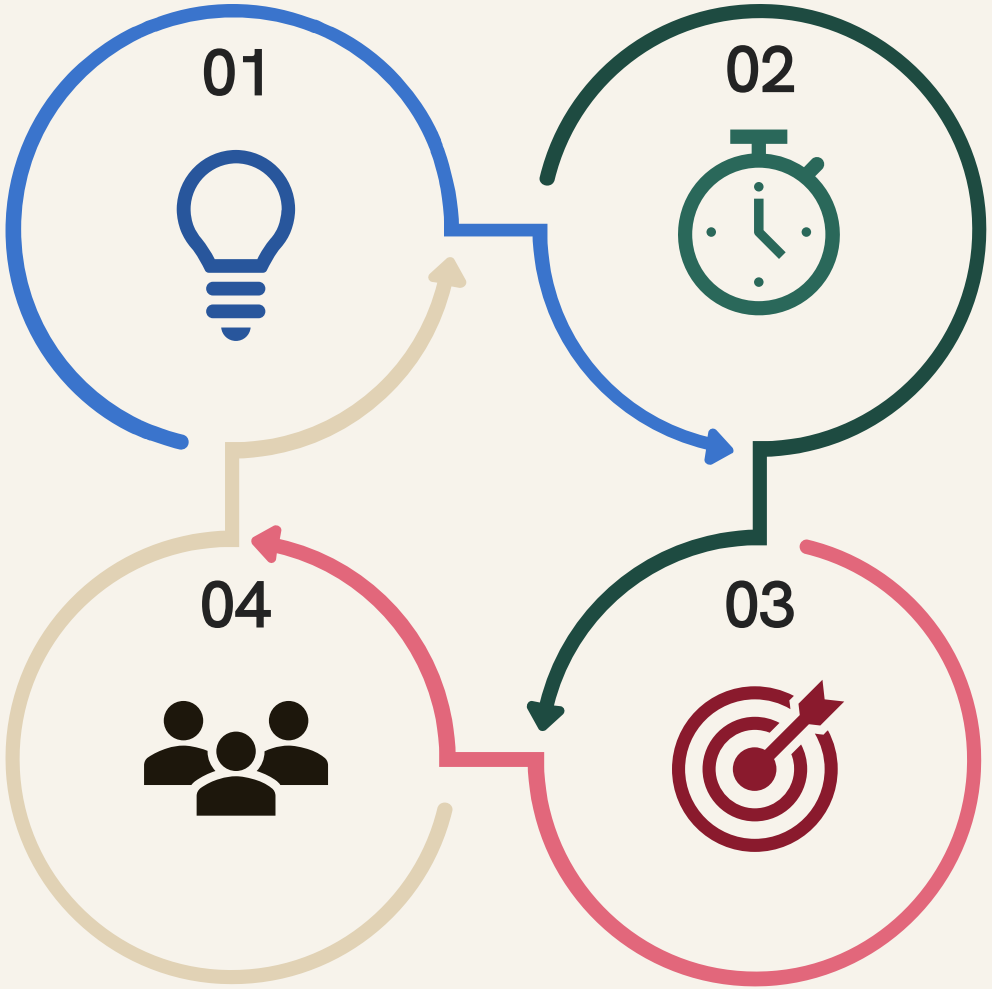
- DORA följer europeiska och internationella standarder inom finansbranschen, inkluderar principer för identifiering, skydda & förebygga, upptäcka, åtgärda & återställa. Kommunikationsplaner inkluderar att informera kunder och allmänheten om IKT-relaterade incidenter.

IKT–riskhantering

01. Identifiera

Artikel 8:

- Kartlägga och klassificera verksamheten
- Identifiera alla IKT-risker
- Löpande identifiera cyberhot och sårbarheter
- Behörighetshantering.



02. Skydda & förebygga

Artikel 9:

- Utarbeta riktlinjer för informationssäkerhet
- Övervaka och kontrollera IKT-miljön och upprätta en säkerhetsstrategi
- Säkerställa motståndskraft, genom att använda de senaste IKT-tekniken och processerna
- Upprätthålla höga standarder för säkerhet, konfidentialitet och integritet hos data

04. Åtgärda & återställa

Artikel 11:

- IKT-kontinuitetsplan
- Kostnader och förluster för IKT-avbrott och IKT-incidenter ska rapporteras till FI
- Säkerhetskopiering och återställning

03. Upptäcka

Artikel 10:

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

IKT - incidenthantering

1. 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**

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

IKT-relaterad incidentrapportering

1. Process för hantering av IKT-relaterade incidenter

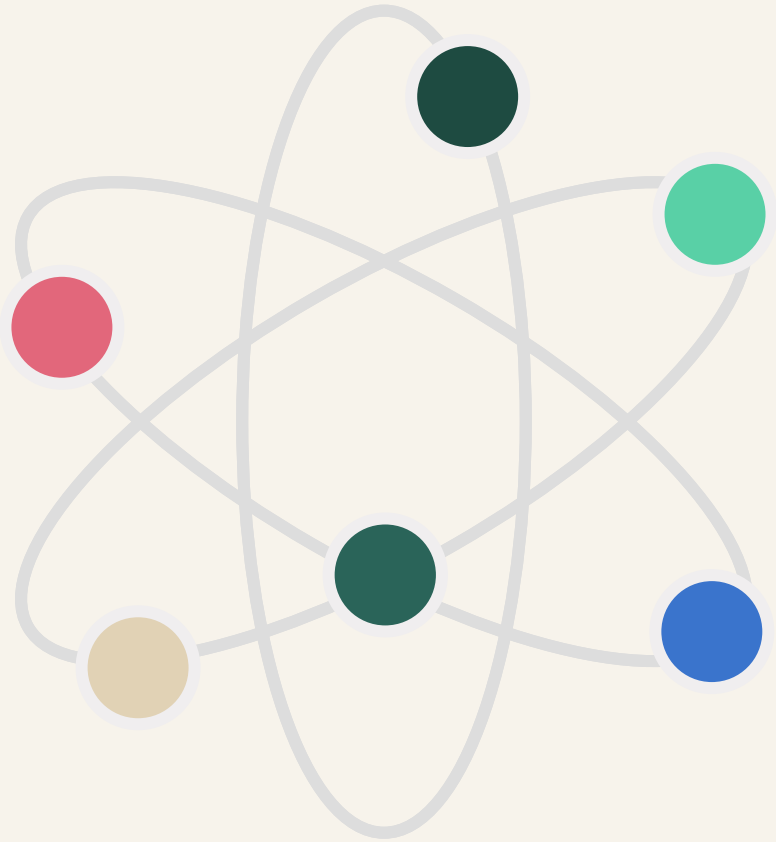
Artikel 17

2. Klassificering av IKT-relaterade incidenter

Artikel 18

3. Rapportering av större IKT-relaterade incidenter

Artikel 19



4. Harmonisering av rapporeringsinnehåll och mallar

Artikel 20

5. Centralisering av rapportering av större IKT-relaterade incidenter

Artikel 21

6. Återkoppling från tillsynsmyndigheterna

Artikel 22
All nödvändig vägledning och återkoppling

Digital operativ motståndskraft – testning

1. 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, mist årligen
   - Tillkommande krav på testning finns för de institutioner som av Finansinspektionen utpekas som väsentliga/kritiska

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

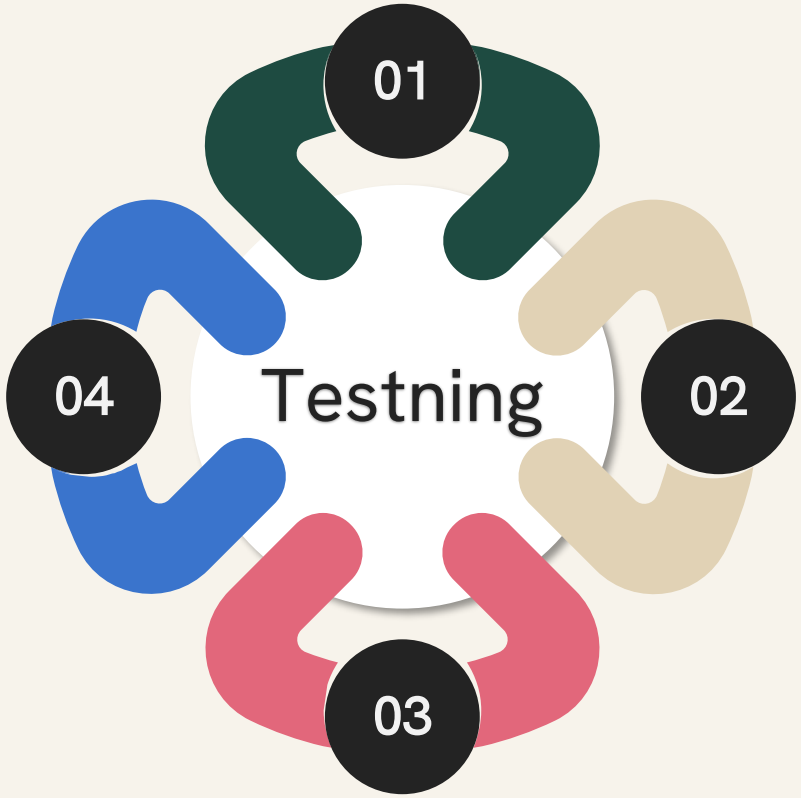
Testning av digital operativ motståndskraft

Krav för testare

Artikel 27

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

Artikel 26



Allmänna krav för testning av digital operativ motståndskraft

Artikel 24

Testning av IKT-verktyg och IKT-system

Artikel 25

Utkontraktering av IKT-tjänster

Tredjepartsriskhantering:

- DORA integrerar tredjepartsrisker i IKT-riskramverket för sund övervakning, inklusive molntjänster.

Outsourcingstrategi och efterlevnad:

- Finansiella bolag måste utveckla outsourcingstrategi och policy, och säkerställa att leverantörer följer lagar och regler.

Krav och övervakning:

- DORA fastställer minimikrav för övervakning av tredjepartsrisker, inklusive outsourcingregister och höga standarder för informationssäkerhet. Övervakning av kritiska IKT-leverantörer ingår i ett EU-ramverk, med potentiella konsekvenser för bolag och möjlighet till exit-klausuler.

Hantering av IKT-tredjepartsrisker

Krav innan utläggning av verksamhet

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

Granskning och tillsyn av utlagd verksamhet

Tillsysnsramverk för kritiska tredjepartsleverantörer av IKT-tjänster.

Hantering av tredjepartsleverantörer – Innan outsourcing

Digital Operational Resilience Act (DORA)

Utkontraktering i IKT-riskhantering

Innan utläggning, integreras utkontraktering i IKT-riskhanteringsramverket med årligt register rapporterat till FI.

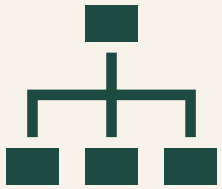
Preliminär utvärdering av leverantör

Före avtal krävs utvärdering av leverantören med fokus på säkerhetsstandarder, tjänster, strategi och koncentrationsrisker.

Riskbaserad inspektion och revision

Inkluderar kontraktsmässiga krav, riskbaserad inspektion, insynskrav och klara avslutskriterier och exitplan.

Hantering av tredjepartsleverantörer – Under outsourcing



Informationssäkerhetskrav och strategi

Krav för informationssäkerhet och "multi-vendor strategi" för outsourcing, inklusive en policy, ingår i kontrakten.

Kritiska tredjepartsleverantörer

ESA identifierar kritiska leverantörer inom den finansiella sektorn under utkontraktering.

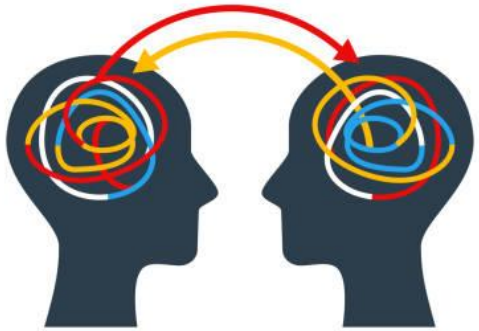
Lead Overseer och sanktioner

ESA utser en Lead Overseer.

ESA kan besluta om vite (1% av leverantörens globala omsättning per dag, upp till 6 månader).

- 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

Arrangemang för informationsutbyte



Arrangemang för utbyte av information och underrättelse om cyberhot

Cyberhot och information

- Finansiella enheter kan dela hotinformation för att stärka sin digitala motståndskraft och öka medvetenheten om cyberhot.

Säkra arrangemang

- Informationsutbytet sker inom en pålitlig grupp och skyddas för affärshemligheter och personuppgifter enligt konkurrenspolitiska riktlinjer.

Tydliga deltagarvillkor

- Arrangemangen måste inkludera klara villkor för deltagande, inklusive eventuellt myndighetsengagemang.

Meddelande till myndigheter

- Finansiella enheter informerar myndigheter om sitt deltagande i informationsutbytearrangemang.

EU myndigheter och FI lyfter IT och informationssäkerhetshot som en av sektorns största risker

Riskbild enligt EU

Cybersäkerhet

Komplexitet

Ökat antal incidenter inom ICT

Digitalisering driver risk

Då IT är integrerat i många interna processer är IT-risker signifikant hot och kan äventyra ett instituts överlevnad

Tack för ert deltagande

Har ni frågor eller funderingar så är ni välkomna att höra av er!

Fredrik Ohlsson
Advisory Sweden
Operational Risk
Partner

Fredrik.Ohlsson@ Advisense.com

+46 72 179 49 51

Filip Fabri
Legal & Compliance
Senior Associate

Filip.Fabri@Advisense.com

+46 72 161 77 27

Advisense

2023-10-20