KORTRAPPORT

De finansiella företagens förberedelser inför Dora-regelverket

11 september 2024

Sammanfattning

EU-förordningen om digital operativ motståndskraft för finanssektorn (Dora-förordningen) ska tillämpas från den 17 januari 2025.[1] Den innebär nya krav på i stort sett alla företag inom den finansiella sektorn för hantering av deras IT-risker. För att Finansinspektionen (FI) ska få en bättre förståelse av hur företagen förbereder sig inför kraven, har vi ställt frågor till dem genom en enkät. Flera olika typer av företag under FI:s tillsyn har svarat på enkäten. Det är banker och kreditmarknadsbolag, betalningsinstitut, försäkringsbolag, värdepappersbolag och fondbolag, och företag som ansvarar för clearing, handelsplattformar och central värdepappersförvaltning.

Enkätsvaren visar att majoriteten av företagen bedömer att de i hög utsträckning ligger i fas med sina förberedelser. De arbetar i stort sett alla med en gapanalys som grund för förberedelserna. De flesta företagen anser även att hanteringen av tredjepartsrisker är det mest utmanande regelområdet. Och eftersom regelverket är nytt för både FI och företagen, medför det en viss osäkerhet om hur vissa delar av förordningen ska tolkas. Företagen nämner bland annat att det finns osäkerheter om förordningens definition av kritiska eller viktiga funktioner. Resultatet av enkäten visar också på en viss variation i svaren mellan olika företagstyper. Detta eftersom företagens storlek och tidigare erfarenhet av reglering inom informations-, kommunikations- och teknologiområdet, så kallade IKT-risker, kan skapa olika förutsättningar för dem i det förberedande arbetet.

Bakgrunden till förordningen är finanssektorns allt större beroende av teknik, som i sin tur innebär ett ökat behov av skyddsåtgärder mot cyberangrepp och andra IKT-risker. I takt med att det finansiella systemet alltmer digitaliseras och sammanlänkas blir det, liksom hela samhället, mer sårbart för risker inom IKT-området. För att säkerställa att finanssektorn lever upp till samhällets krav och förväntningar krävs det regler. Dessa krav har nu formulerats i EU:s Dora-förordning och FI har i uppdrag att i sin tillsyn följa upp att reglerna följs.

[1] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/101.

Inledning

Enkäten bestod av 27 frågor där varje företag ombads beskriva sina förberedelser utifrån nuläget. Syftet var att ge Finansinspektionen (FI) en uppfattning om hur företagen ligger till med sina förberedelser, och vilka utmaningar de står inför kopplat till att genomföra regelverket. Slutsatserna i denna rapport baseras på svaren från de 49 företag som deltog i enkäten. Det går således inte att dra generella slutsatser om enskilda företag eller grupper av företag. För detta hade ett större urval krävts.

Företagens allmänna förberedelser

I det inledande avsnittet svarade företagen på om de påbörjat förberedelserna inför tillämpningen av Dora-förordningen. Endast ett företag svarade att det inte hade börjat förbereda sig. Övriga företag fick därefter ange på vilket sätt de förbereder sig med hjälp av flera möjliga svarsalternativ. Som framgår av diagram 1 svarade nästan alla företag (45 av 48) att de initierat en gapanalys och att den ligger till grund för företagets förberedelser. Nästan lika många företag (44 respektive 40) svarade att de arbetar med genomförandeprojekt och resursplanering som en del i förberedelserna. (Se diagram 1.)

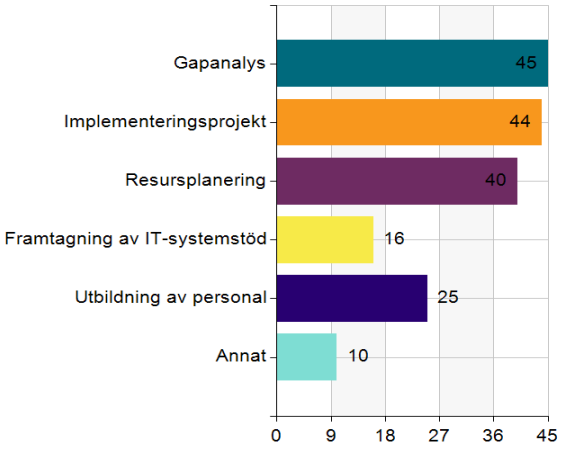

Diagram 1: På vilket sätt har företagen påbörjat sina förberedelser?

Det framgår även av svaren att majoriteten av företagen bedömde att de låg i fas med sina förberedelser: 31 svarade att de i hög grad låg i fas och 4 att de befann sig helt i fas. Andelen företag som bedömde att de låg i fas var störst bland banker. (Se diagrammen 2 och 3.)

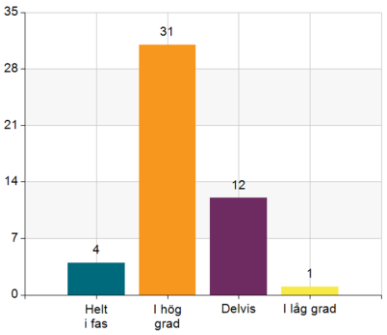

Diagram 2: Ligger företaget i fas?

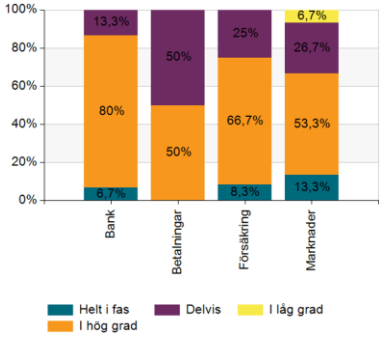

Diagram 3: Fördelat per typ (%).

IKT-riskhantering

Finansiella företag ska enligt Dora-förordningen genomföra en styrnings- och kontrollram som beskriver hur företaget hanterar sina IKT-risker[2], en så kallad IKT-riskhanteringsram. Företaget ska även identifiera alla IKT-stödda funktioner, IKT-tillgångar och informationstillgångar, för att kunna bedöma de risker som påverkar det inklusive de processer som är beroende av tredjepartsleverantörer. För att snabbt kunna återställa verksamheten är företaget därtill skyldigt att införa en heltäckande IKT-kontinuitetspolicy som ska testas årligen.

Företagen fick i enkäten svara på i vilken utsträckning de hade genomfört en IKT-riskhanteringsram enligt artikel 6 i Dora-förordningen. En stor del av dem ansåg att de delvis hade gjort detta (se diagram 4). Att det är ett omfattande arbete att införa en IKT-riskhanteringsram framgår även av kommentarerna till denna fråga. Flera företag nämnde dessutom att ett arbete pågår inom många av verksamhetens olika delar. Därutöver angav flera företag att de har ett återstående arbete med att samordna olika delar inom IKT-området till en sammanhållen IKT-riskhanteringsram. Svaren visar att försäkrings- och marknadsområdet har lägst andel företag som i hög utsträckning anser sig ha genomfört en IKT-riskhanteringsram (se diagram 5).

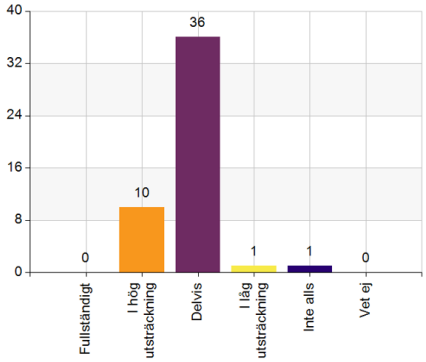

Diagram 4: IKT-riskhanteringsram.

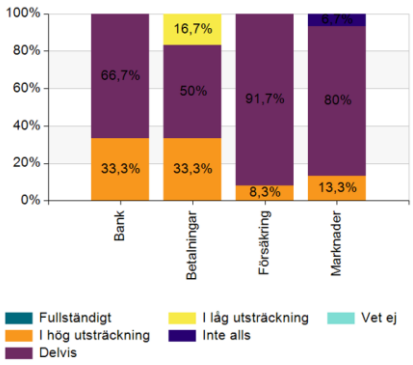

Diagram 5: Fördelat per typ (%).

[2] IKT-risk: varje rimligen identifierbar omständighet i samband med användningen av nätverks- och informationssystem som, om de inträffar, kan äventyra säkerheten i nätverks- och informationssystem, verktyg eller processer som är teknikberoende, funktioner och processer eller tillhandahållandet av tjänster genom att orsaka negativa effekter i den digitala eller fysiska miljön.

IKT-relaterade incidenter

Finansiella företag ska enligt Dora-förordningen inrätta och följa en process, för att hantera sina IKT-relaterade incidenter i verksamheten. Det innefattar att upptäcka, hantera, klassificera och rapportera sådana incidenter. Företagen ska också rapportera allvarliga IKT-relaterade incidenter till FI enligt de mallar som nu tas fram av de europeiska tillsynsmyndigheterna. Enligt Dora-förordningen får företagen också frivilligt rapportera betydande cyberhot till FI. Dessa krav behandlas i förordningens tredje kapitel.

Företagen ombads i enkäten att svara på i vilken utsträckning de har inrättat en process för att rapportera allvarliga IKT-relaterade incidenter till FI enligt artikel 19 i Dora-förordningen. Som framgår av diagram 6 nedan svarade flertalet, 31 företag, att de delvis har en process för rapportering. De formatmallar som ligger till grund för att rapportera in incidenter har under året utvecklats av EU-tillsynsmyndigheterna. Ett antal företag nämner även i sina kommentarer att de behöver anpassa sina respektive verksamheter till de nya tidsramar och tröskelvärden som bestäms för dessa formatmallar. En del företag anger även att de redan har processer och rutiner på plats för rapportering av andra typer av incidentrapportering, exempelvis enligt FI:s föreskrifter FFFS 2018:4 och FFFS 2021:2.[3]

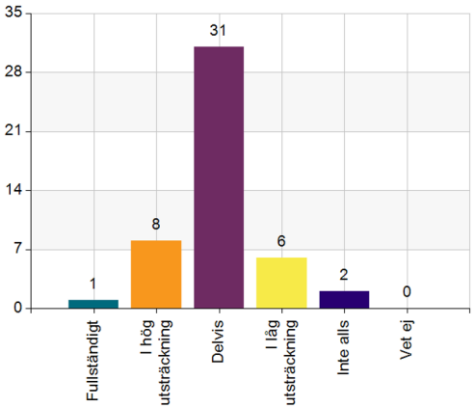

Diagram 6: Process för IKT-incidenter.

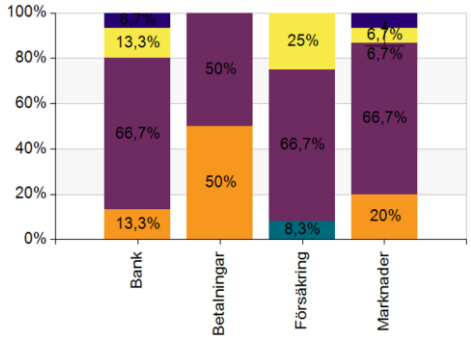

Diagram 7: Fördelat per typ (%).

Test av digital operativ motståndskraft

Enligt Dora-förordningen ska ett finansiellt företag upprätta ett heltäckande program för att testa sin digitala operativa motståndskraft. Testning görs för att upptäcka eventuella brister och sårbarheter. Företaget ska åtminstone årligen testa alla sina IKT-system och IKT-tillämpningar som stödjer kritiska eller viktiga funktioner. Kraven på testning regleras i förordningens fjärde kapitel.

Företagen ombads i enkäten att svara på om de årligen testar alla sina IKT-system och IKT-tillämpningar som stödjer kritiska eller viktiga funktioner i linje med vad som

[3] Se FFFS 2018:4 – Finansinspektionens föreskrifter om verksamhet för betaltjänstleverantörer respektive FFFS 2021:2 – Finansinspektionens allmänna råd om rapportering av händelser av väsentlig betydelse.

framgår av artikel 24 i Dora-förordningen. Här svarade 28 av företagen att de årligen testar de system som stödjer kritiska eller viktiga funktioner, och 15 att de inte genomför sådana tester (se diagram 8). Andelen företag som svarade ja var högst bland banker och marknader (se diagram 9).

I kommentarerna indikerade några företag att de tester som genomförs i dag inte täcker samtliga element, bedömningar eller metoder som krävs enligt förordningen. En del företag beskrev även att tester inte utförs av oberoende parter i samma utsträckning som Dora-förordningen kräver.

Däremot angav några företag att befintliga policyer, procedurer, protokoll och verktyg för testprogram redan finns på plats i verksamheten. Det framgick dock även att dessa testprogram i viss uträckning behöver formaliseras samt säkerställa oberoende för att leva upp till förordningens krav.

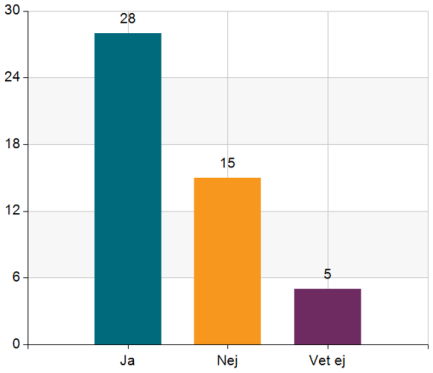

Diagram 8: Görs årliga tester?

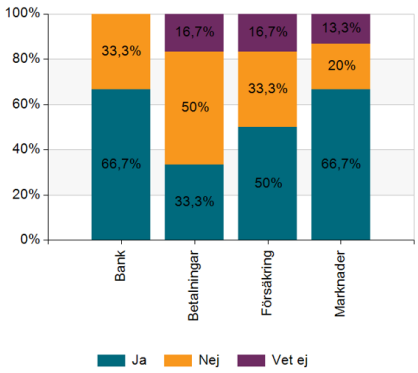

Diagram 9: Fördelat per typ (%).

Hantering av IKT-tredjepartsrisker

Dora-förordningen (kapitel 5) anger hur tredjepartsrisker ska hanteras, med särskilda krav på utkontraktering av IKT-tjänster som stödjer kritiska funktioner. Förordningen fastställer ett antal nyckelprinciper för att vägleda finansiella företag att hantera IKT-tredjepartsrisker på ett heltäckande sätt. Detta innefattar bland annat minimikrav som företagen ska inkludera i avtal för att kunna använda IKT-tjänster, för att stärka motståndskraften.

Företagen ombads att svara på i vilken utsträckning de upprätthåller och uppdaterar ett register med information om alla sina kontraktsmässiga arrangemang om IKT-tjänster enligt kraven i Dora-förordningen. På frågan svarade 15 företag att de i hög utsträckning upprätthåller ett register, 22 svarade delvis och 9 svarade i låg utsträckning (se diagram 10).

Som framgår av diagram 11 tillhör företagen som svarade fullständigt på frågan grupperna bank och försäkring. Inom gruppen betalningar svarade merparten av företagen att de i hög utsträckning upprätthåller och uppdaterar ett sådant register. I gruppen bank och marknad svarade omkring hälften från respektive grupp att de delvis

uppfyller kraven. I gruppen försäkring svarade en tredjedel av företagen i låg utsträckning, en tredjedel svarade delvis och resterande i hög utsträckning eller fullständigt.

Flera företag svarade att de har ett avtalsregister, men att det återstår arbete med att samla in all väsentlig information som krävs enligt Dora-förordningen. Vissa företag framförde även att de i dagsläget har lagt ut verksamhet och har ett IKT-register med detaljerad information enligt EBA:s riktlinjer om utkontraktering, men att dessa behöver anpassas till kraven i Dora-förordningen. Företagens kommentarer visar vidare att registren upprätthålls genom avtalshanteringssystem och automatiserade processer. Vissa företag svarade även att detta i dag hanteras genom manuella processer.

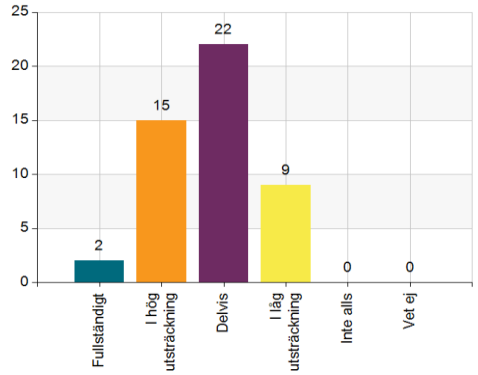

Diagram 10: IKT-tredjepartsrisker.

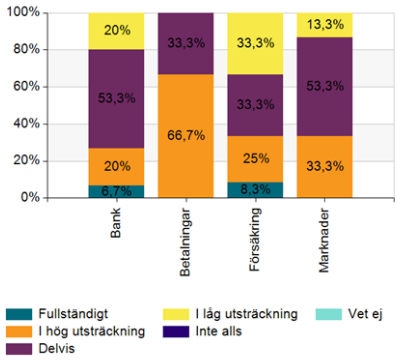

Diagram 11: Fördelat per typ (%).

Utmaningar som företagen ser med regelkraven

Företagen ombads i enkäten även att svara på vilka krav i Dora-förordningen som de bedömer är särskilt utmanande. Flest företag pekade då på hanteringen av tredjepartsrisker (se diagram 12). Flera företag nämnde även att företagets verksamhet och tjänster är starkt beroende av tredjepartsleverantörer inom IKT-området. Några företag svarade att det finns utmaningar med att övervaka leverantörskedjor i flera nivåer. 20 procent menade att IKT-riskhanteringsramverket är det mest utmanande området att införa, medan 19 procent ansåg att testning av digital operativ motståndskraft var det mest utmanande.

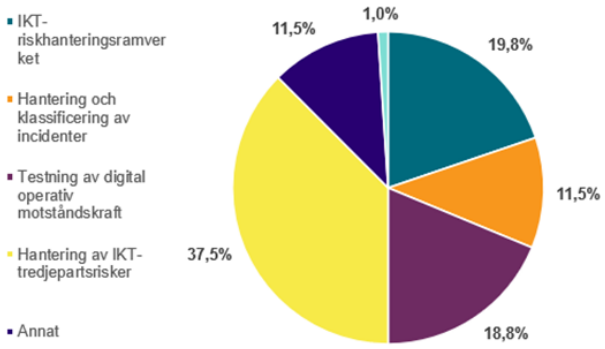

Diagram 12: Utmaningar i införandet av Dora-förordningens krav (%).

Iakttagelser och slutsatser: Nästan alla företag har börjat förbereda sig – men arbete återstår

FI:s enkät visar att ett omfattande förberedelsearbete pågår i finanssektorn inför Dora-förordningens ikraftträdande. I stort sett alla företag som besvarade enkäten arbetar med en gapanalys som grund för förberedelserna. När det gäller allmänna förberedelser visar enkätsvaren att bankerna har kommit längre än övriga företag.

Ytterligare en iakttagelse är att många av företagen upplever att kravet på att hantera tredjepartsrisker är särskilt utmanande. Svaren visar även att det finns ett starkt beroende till tredjepartsleverantörer inom IKT-området för finansiell verksamhet. Några företag indikerar i sina svar även att övervakning av leverantörskedjor i underliggande led är en utmaning.

Dora-förordningen innebär särskilda utmaningar för företag som väljer att lägga ut sina IKT-tjänster till tredjepartsaktörer. Regelverkets krav på en sådan hantering är omfattande. Detta eftersom företag kommer behöva ha en process för att uppdatera sina kontraktsmässiga arrangemang med leverantörer av IKT-tjänster som stödjer kritiska eller viktiga funktioner. Varje företag behöver även uppdatera sin policy för tredjepartsriskhantering i linje med de nya kraven, förbättra sin förmåga att övervaka leverantörer i underliggande led samt säkerställa att kontraktsmässiga arrangemang registreras och rapporteras till FI. För dessa företag innebär förordningen en betydligt högre grad av externt samarbete och det är av stor vikt att företagen säkerställer att de fullt ut kan kontrollera sina IKT-risker.

Utöver tredjepartsriskhantering går det att utläsa av svaren att det finns en osäkerhet när det gäller definitionen av kritiska eller viktiga funktioner enligt förordningen. Detta kan få stor påverkan på ett antal system och applikationer som företagen behöver omfatta i sin IKT-riskhanteringsram. Tolkningen påverkar även omfattningen av företagens arbete med oberoende testning som ska genomföra på regelbunden basis. Företagen måste också anpassa sig till nya tröskelvärden och tidsramar enligt kraven för incidentrapportering. För de ska lyckas med att införa samtliga områden i Dora-förordningen är det mycket viktigt att kompetensutvecklande åtgärder prioriteras i verksamheten.

Merparten av svaren indikerar vidare att företagen upplever att förordningen är ett komplext regelverk att införa.

Resultatet från denna enkät ger en inblick i företagens förberedande arbete inför förordningen samt belyser olika utmaningar med tillämpningen. Det bör dock understrykas att det inte går att dra några generella slutsatser om enskilda företag eller grupper av företag i denna studie, då ett större urval hade varit nödvändigt. Slutsatserna i denna enkät baseras därför enbart på de deltagande företagens svar och bör inte tolkas som representativt för sektorn som helhet. Förutsättningarna kan variera kraftigt

beroende på företagens storlek samt vilka typer av tjänster företaget tillhandahåller. Företagens erfarenheter av att följa regelkrav inom IKT-området varierar också. Detta eftersom tidigare regler och standarder har sett olika ut för olika företagstyper och därmed hanterats på olika sätt.

Sammanfattningsvis kan vi konstatera att nästan alla företag – om än i varierad utsträckning – har kommit i gång med sina förberedelser för att kunna tillämpa Dora-förordningen. Trots detta framgår att nästan samtliga företag har arbete som återstår. Det är inte osannolikt att detsamma gäller många företag som inte har deltagit i FI:s enkät.

FI följer upp företagens arbete i sin tillsyn

FI fortsätter att följa upp företagens arbete med att anpassa sig till kraven enligt förordningen i den löpande tillsynen och genom riktade tillsynsaktiviteter.

Vi kommer under hösten att ordna ytterligare ett FI-forum för berörda företag och intressenter och informera om den andra omgångens tekniska regulatoriska standarder. Utöver detta genomför FI även, tillsammans med de finansiella EU-tillsynsmyndigheterna, en övning med syfte att förbereda företagen inför den obligatoriska rapportering som ska göras av utkontrakterad verksamhet enligt Dora-förordningen. Inom EU deltar vi fortsatt i olika arbetsgrupper och ett intensivt arbete pågår även med att färdigställa samtliga policymandat relaterat till förordningen.

Vi arbetar också internt med att förbereda oss inför den tillsyn som vi ska utöva enligt regelverket när det har trätt i kraft.