FINANSTILSYNET

DORA-forordningen i forsikrings- og pensionsselskaber

Rapport

September 2026

Indholdsfortegnelse

Forsikrings- og pensionsselskabers implementering af DORA-forordningen 3
Hovedbudskaber 3
Reglerne på området 4
Krav til virksomhedernes styring af IT-risiko 4
Temaundersøgelsens resultater 5
Behov for bedre styring af IT-risiko 5
Opsummering og opfølgning 6
Om undersøgelsen 7

Forsikrings- og pensionsselskabers implementering af DORA-forordningen

Den stigende digitalisering og adgang til nye teknologier giver forsikrings- og pensionssektoren mulighed for at effektivisere arbejdsgange og udvikle innovative løsninger til gavn for både borgere og samfund. Samtidig medfører digitaliseringen risici, idet virksomhederne bliver mere sårbare overfor cyberangreb og IT-driftsforstyrrelser og mere afhængige af eksterne IT-leverandører. I de seneste år er truslen fra cyberangreb vokset markant, både i omfang og kompleksitet. Det har øget presset på virksomhedernes evne til at beskytte sig mod digitale trusler. Den høje grad af digitalisering og indbyrdes forbundethed i den finansielle sektor udgør dermed en potentiel risiko for både de enkelte virksomheder og den overordnede finansielle stabilitet. For at imødegå disse udfordringer vedtog Europa-Parlamentet og Rådet i december 2022 forordningen om digital operationel modstandsdygtighed (DORA) med virkning fra 2025.

På den baggrund gennemførte Finanstilsynet i perioden fra oktober 2025 til marts 2026 en undersøgelse af udvalgte forsikrings- og pensionsselskabers implementering af DORA-forordningen med særligt fokus på de centrale bestemmelser om IT-risikostyring. Formålet var at få et overblik over branchens modenhed på området og at identificere eventuelle punkter, som kræver ekstra opmærksomhed i virksomhedernes arbejde med den digitale operationelle modstandsdygtighed.

Denne rapport sammenfatter Finanstilsynets observationer og vurderinger fra undersøgelsen og er tænkt som inspiration for alle virksomheder, der arbejder med området. De konkrete virksomheder, der indgik i undersøgelsen, har desuden fået individuel tilbagemelding fra Finanstilsynet.

Finanstilsynet følger løbende op på undersøgelsen og fremdriften i virksomhedernes handleplaner på IT-inspektioner, statusmøder og gennem en række andre tilsynsaktiviteter.

Hovedbudskaber

Undersøgelsen viste, at virksomhederne er godt i gang med at implementere DORA. Den viste dog også, at der er behov for at styrke indsatsen på en række områder, som overordnet omfatter:

1. Ledelsesmæssigt tilsyn med IT-risikostyringen og en tydelig rolle- og ansvarsfordeling
2. Dokumenterede og sammenhængende rammer for virksomhedernes IT-risikostyring
3. Løbende vedligeholdelse og udvikling af de rette kompetencer
4. Styrkelse og test af de operationelle beredskaber
5. Løbende forbedringer af IT-risikostyringen på baggrund af erfaringer fra hændelser og test.

Reglerne på området

DORA etablerer en fælles retlig ramme, der moderniserer og harmoniserer kravene til IT- og cybersikkerhed i den finansielle sektor på tværs af virksomhedstyper i hele EU. Forordningen blev vedtaget i 2022 og har været gældende siden den 17. januar 2025.

Formålet med DORA er at styrke sektorens digitale operationelle modstandsdygtighed, bl.a. overfor cyberangreb. Forordningen stiller krav til, hvordan finansielle virksomheder håndterer risici forbundet med brugen af informations- og kommunikationsteknologi (IT) med fokus på fem områder:

- IT-risikostyring
- Styring, klassificering og indberetning af IT-relaterede hændelser
- Test af digital operationel modstandsdygtighed
- Styring af IT-tredjepartsrisici
- Ordninger for informationsudveksling.

Krav til virksomhedernes styring af IT-risiko

Kravene til virksomhedernes styring af IT-risiko følger af DORA artikel 5-15 og medfører følgende:

Den enkelte virksomhed skal have en intern forvaltnings- og kontrolramme, der sikrer, at den kan håndtere IT-risici effektivt og forsvarligt. Det øverste ledelsesorgan (typisk bestyrelsen) har ansvaret for at fastlægge, godkende og føre tilsyn med rammen for IT-risikostyring og tilhørende politikker for IT-sikkerhed, så virksomheden opretholder høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Rammen for IT-risikostyring skal være robust, omfattende og veldokumenteret. Den skal være en integreret del af virksomhedens samlede risikostyringssystem og sikre et højt niveau af digital operationel modstandsdygtighed. Rammen skal omfatte strategier, politikker, passende niveauer for tolerance af IT-risiko, procedurer og IT-værktøjer, der beskytter alle informations- og IT-aktiver mod risici som f.eks. skade og uautoriseret adgang. Virksomheden skal dokumentere og gennemgå rammen mindst én gang årligt og løbende forbedre den på baggrund af erfaringer, test og revisioner.

Ledelsen skal sikre en klar rolle- og ansvarsfordeling mellem alle, der arbejder med IT, samt gode betingelser for samarbejde og kommunikation. Den skal afsætte de nødvendige ressourcer og et tilstrækkeligt budget til at opretholde et højt niveau af digital modstandsdygtighed. Det omfatter løbende uddannelse af medarbejdere. Virksomheden skal have styr på brugen af tredjepartsleverandører, og ledelsen skal løbende informeres om væsentlige ændringer og risici. Endeligt skal ledelsen holde sig opdateret om IT-risici gennem relevant efteruddannelse.

Når virksomheden etablerer sin ramme for IT-risikostyring, skal den tage stilling til alle relevante IT-aktiver, forretningsfunktioner, risici og afhængigheder, herunder fra tredjepartsudbydere. Rammen skal også sikre passende beskyttelse af IT-systemer gennem f.eks. adgangskontrol, stærk autentificering, ændringsstyring og opdateringer. Virksomheden skal have mekanismer til hurtigt at opdage anormale aktiviteter og IT-relaterede hændelser.

Virksomheden skal udarbejde politikker og planer for IT-driftsstabilitet og genopretning, som løbende testes og opdateres på baggrund af forretningskonsekvensanalyser og IT-risikovurderinger. Sikkerhedskopierings- og gendannelsesprocedurer skal være veldokumenterede og testede, og de skal sikre, at gendannelse sker via systemer, der er fysisk og logisk adskilt fra kildesystemet.

Rammen skal desuden sikre, at virksomheden løbende lærer af hændelser og test, og at disse erfaringer indarbejdes i risikovurderinger og rapporteres til ledelsen med anbefalinger til handlinger. Derudover skal rammen sikre, at virksomheden har klare retningslinjer for kommunikation, der sikrer relevant information til både interne og eksterne interessenter ved større hændelser.

Temaundersøgelsens resultater

Dette afsnit beskriver de centrale observationer og identificerede forbedringspunkter fra undersøgelsen.

Undersøgelsen viser, at virksomhederne generelt har etableret rammer for IT-risikostyring baseret på modellen med tre forsvarslinjer, og at rammerne er integreret i deres samlede risikostyringssystemer. Virksomhederne har udarbejdet overordnede styringsdokumenter på alle de undersøgte områder, f.eks. strategier for digital operationel modstandsdygtighed med angivelse af risikotoleranceniveauer og politikker for IT-sikkerhed, drift og brug af tredjepartsudbydere.

Virksomhederne havde også på undersøgelsestidspunktet enten gennemført eller planlagt at gennemføre interne revisioner eller tilsvarende uafhængige kontroller af rammerne. Generelt har virksomhederne arbejdet med at identificere og kortlægge deres kritiske IT-aktiver, herunder informationsaktiver og de processer, der er afhængige af tredjepartsudbydere af IT-tjenester. Det var dog ikke alle virksomhederne, der havde et fuldstændigt overblik på tidspunktet for undersøgelsen.

Behov for bedre styring af IT-risiko

Finanstilsynet konstaterede ved gennemgangen af virksomhedernes besvarelser, at der fortsat er behov for at forbedre styringen af IT-risiko, bl.a. i forbindelse med forvaltning og organisation af området. En velfungerende ramme for risikostyring og klare politikker er afgørende for, at virksomhederne kan opnå og fastholde et tilstrækkeligt niveau af digital operationel modstandsdygtighed. Det er derfor vigtigt, at virksomhederne løbende gennemgår og justerer deres rammer og centrale styringsdokumenter.

På baggrund af undersøgelsen har Finanstilsynet identificeret følgende forbedringspunkter for virksomhedernes videre arbejde med at indføre og udvikle rammen for styring af IT-risici og styrke deres digitale operationelle modstandsdygtighed i overensstemmelse med DORA:

1. Ledelse og styring af IT-risici

- Bestyrelserne skal have tilstrækkelig information til at godkende, føre tilsyn med og regelmæssigt gennemgå rammen for IT-risikostyring. Ledelserne skal informeres om forhold vedrørende tredjepartsudbydere, væsentlige ændringer og deres indvirkning på kritiske eller

vigtige funktioner, så virksomhederne løbende kan tilpasse niveauet for digital operationel modstandsdygtighed ud fra erfaringer og udviklingen indenfor IT-risici.

- Virksomhederne skal have tydelige rolle- og ansvarsfordelinger mellem de uafhængige kontrolfunktioner, så de udførende og kontrollerende funktioner er tilstrækkeligt adskilt.

- Virksomhederne skal kortlægge og vurdere alle relevante IT-aktiver, -tjenester og -data, herunder også i forhold til single point of failure og tredjepartsleverandører af kritiske eller vigtige funktioner. Virksomhederne skal sikre, at strategier, risici og relevante trusselsscenarier er sammenhængende.

2. Sammenhængende rammer

- Virksomhederne skal styrke og formalisere styringsdokumenter yderligere, så strategier, politikker, procedurer og IT-værktøjer er sammenhængende.

3. Kompetenceudvikling

- Virksomhederne skal løbende udvikle og vedligeholde de rette kompetencer på alle niveauer, og virksomhederne skal have tilstrækkelige ressourcer.

- Virksomhedernes programmer for bevidstgørelse om IT-sikkerhed skal være målrettede og tilpasset uddannelsesbehovet hos ledelserne og de enkelte medarbejdergrupper. Programmerne skal også i relevant omfang omfatte eksterne konsulenter og tredjepartsudbydere.

4. Operationelt beredskab

- Virksomhederne skal teste IT-driftsstabilitets- og genopretningsplaner (BCP'er og DRP'er) systematisk, og virksomhederne skal udarbejde effektive kommunikationsstrategier til brug i IT-kriser samt sikre tydelige rolle- og ansvarsfordelinger.

5. Læring af hændelser

- Virksomhederne skal analysere indvirkningen af egne IT-hændelser, lære fra hændelser i lignende virksomheder og overvåge den teknologiske udvikling, så de løbende kan vurdere og forbedre deres IT-risikostyring.

Opsummering og opfølgning

Temaundersøgelsen viste, at virksomhederne har arbejdet med at implementere kravene fra DORA-forordningen for at øge deres digitale operationelle modstandsdygtighed. Undersøgelsen viste dog samtidig, at virksomhederne på de områder, som denne rapport berører, fortsat skal løfte sikkerhedsniveauet.

Som opfølgning har Finanstilsynet bedt de virksomheder, hvori der er konstateret mangler, om at udarbejde og indsende en handleplan, der beskriver, hvordan de vil rette op på manglerne. Finanstilsynet følger op på fremdriften i handleplanerne gennem forskellige løbende tilsynsaktiviteter, bl.a. statusmøder med virksomhederne. Finanstilsynet vil i den forbindelse vurdere, om manglerne eller en eventuel manglende fremdrift på handleplanerne giver anledning til tilsynsreaktioner.

Derudover iværksætter Finanstilsynet i de kommende år målrettede og risikobaserede IT-inspektioner. Inspektionerne vil omfatte alle fem områder i DORA. Den risikobaserede tilgang betyder, at Finanstilsynet vil fokusere på de delområder, hvor risikoen for væsentlige konsekvenser for den finansielle stabilitet eller tilliden til det finansielle system vurderes at være størst.

Finanstilsynet vil dermed fortsat følge forsikrings- og pensionsselskabernes arbejde tæt for at understøtte, at sikkerhedsniveauet løftes, og at den digitale operationelle modstandsdygtighed i den samlede sektor styrkes.

Om undersøgelsen

Temaundersøgelsen fandt sted i perioden fra oktober 2025 til marts 2026. Den blev gennemført som en struktureret spørgeskemaundersøgelse blandt 14 udvalgte forsikrings- og pensionsselskaber. Spørgeskemaet omfattede spørgsmål om virksomhedernes arbejde med implementering af DORA-forordningens krav, bl.a. IT-risikostyring, håndtering af IT-hændelser og samarbejde med eksterne IT-leverandører.