

I **september 2020** publicerade kommissionen ett utkast till lagstiftningen. I **juni 2022** nåddes en överenskommelse vilket handlar om ett omfattande regelverk som ska öka motståndskraft och säkerhet i finansiell sektor samt kunna hantera väsentliga störningar. I **januari 2023** godkände rådet lagstiftningen. Nu har finansiella bolag cirka 2 år på sig att justera processer och rutiner för att efterleva det nya regelverket. Allt ska vara klart **17 januari 2025**.



## Ny lag påverkar er

"Digital Operational Resilience Act" eller Förordningen om digital operativ motståndskraft (DORA) är EU:s nya regelverk kring hanteringen av digitala risker och cyberhot i finansbranschen. Syftet med lagstiftningen är att förstärka konkurrenskraften och innovationskraften genom att öka motståndskraften i den finansiella sektorn. Lagstiftningen utökar redan existerande krav beträffande riskhantering av digitala risker.

## Nyckelområden

### Intern styrning och kontroll

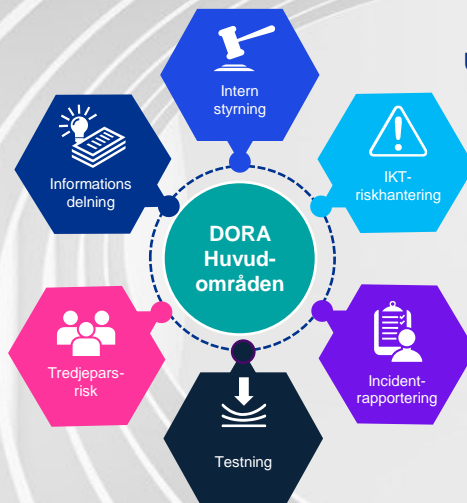
Utveckla roller, ansvar och mandat samt styrelsens uppföljning av digitala risker.

### Informationsdelning

Utveckla processer för att dela information och underrättelser om cyberhot och digitala risker för att stärka försvarsförmågan.

### Tredjepartsrisk

Utveckla processer för att hantera och övervaka tredjepartsrisker kopplade till informations- och kommunikationsteknologier.



### Riskhantering

Utveckla ramverket för riskhantering av digitala risker inklusive riskstrategi, kontroll och rapportering.

### Incidentrapportering

Harmonisering och rationalisering av relaterad incidentrapportering kopplade till informations- och kommunikationsteknologier.

### Testning av digital operativ motståndskraft

System, processer och funktioner för riskhanteringen av digitala risker ska testas regelbundet för att säkerställa beredskap och kontinuitet.

## Hur kan KPMG hjälpa er?

- Gap-analys för att identifiera nuvarande och framtida krav.
- Tillhandahålla specialistkompetens inom varje nyckelområde.
- Stöd för att uppfylla nya krav för er organisation (strategier, handlingsplaner, kapacitet).
- Kvalitetssäkring av redan utförda arbeten eller befintliga handlingsplaner.

## Kontakt



**Olof Arwinge**

olof.arwinge@kpmg.se  
076-876 96 16  
GRC & Enterprise Risk Management



**Emelie Taleporos**

emelie.taleporos@kpmg.se  
070-914 27 63  
Financial & Operational Risk



**Prashant Joshi**

prashant.joshi@kpmg.se  
070-836 51 46  
Cyber Security