FI-forum: Dora-regelverket

14 maj 2024

Agenda

09.00–09.10	**Inledning**
09.10–09.30	**Dora-förordningen**
09.30–10.00	**Tekniska standarder**
10.00–10.10	**Inskickade frågor**
10.10–10.15	**Nästa steg**
10.15–10.30	**Frågestund**

Dora-förordningen

Digital operativ motståndskraft –

Introduktion och pågående utveckling

14 maj 2024

Vad innebär Dora?

Digital operativ motståndskraft

Beskrivning och syfte med Dora

- Nytt EU-regelverk med syfte att harmonisera tidigare regler
- Unikt genom att vara övergripande och ställa krav på samtliga aktörer på finansmarknaden
- Fokus på digital operativ motståndskraft, resiliens
- Tillämpbar från 17 januari 2025

Vilka omfattas av förordningen?

- Kreditinstitut
- Betalningsinstitut
- Leverantörer av kontoinformationstjänster
- Institut för elektroniska pengar
- Värdepappersföretag
- Leverantörer av kryptotillgångstjänster
- Värdepapperscentraler
- Centrala motparter
- Handelsplatser
- Transaktionsregister
- Förvaltare av alternativa investeringsfonder
- Förvaltningsbolag
- Leverantörer av datarapporteringstjänster
- Försäkrings- och återförsäkringsföretag.
- Försäkringsförmedlare
- Tjänstepensionsinstitut
- Kreditvärderingsinstitut
- Administratörer av kritiska referensvärden
- Leverantörer av gräsrotsfinansieringstjänster
- Värdepapperiseringsregister
- Tredjepartsleverantörer av IKT-tjänster

Finansinspektionens förberedelser

- Föreskriftsprojekt
- Lagförslag, digital operativ motståndskraft
- Del av pågående utveckling för tekniska standarder, EBA/Esma/Eiopa
- Systemstöd för inrapportering
- Informationsinsatser
- Dora-övning om inrapportering

Vad innehåller Dora?

DORA - innehåll

Fem områden är centrala:

1. **IKT-riskhantering**
   - IKT-riskhanteringsramverk
2. **IKT-relaterad incidentrapportering**
   - Hantering, klassificering och rapportering
3. **Testning av digital operativ motståndskraft**
   - Program för testning av digital motståndskraft
4. **Hantering av IKT-tredjepartsrisker**
   - Riskhantering av tredjepartsrisk
5. **Informationsutbyte**
   - Cyberhot

IKT-riskhantering

- IKT-riskhanteringsram
- IKT-system, IKT-protokoll och verktyg
- Identifiering
- Skydd och förebyggande
- Upptäckt
- Åtgärder och återställande
- Strategier för säkerhetskopiering och metoder för återskapande och återställande
- Lärande och utveckling
- Kommunikation
- Ytterligare harmonisering av verktyg, metoder, processer och strategier för IKT-riskhantering
- Förenklad IKT-riskhanteringsram

IKT-relaterad incidentrapportering

- Process för hantering av IKT-relaterade incidenter
- Klassificering av IKT-relaterade incidenter och cyberhot
- Rapportering av allvarliga IKT-relaterade incidenter och frivillig anmälan av betydande cyberhot
- Harmonisering av rapporteringsinnehåll
- Centralisering av rapportering av allvarliga IKT-relaterade incidenter

Testning av digital operativ motståndskraft

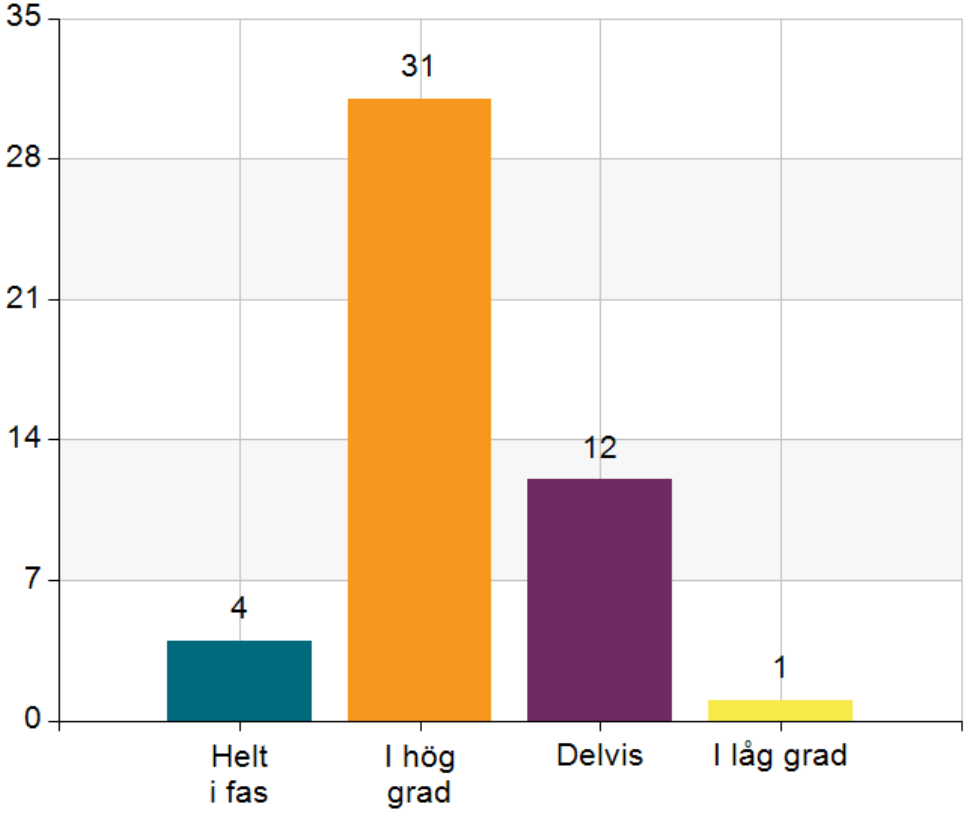
- Allmänna krav för testning av digital operativ motståndskraft
- Testning av IKT-verktyg och IKT-system
- Avancerad testning av IKT-verktyg, IKT-system och IKT-processer baserad på hotbildsstyrd penetrationstestning

Hantering av IKT-tredjepartsrisker

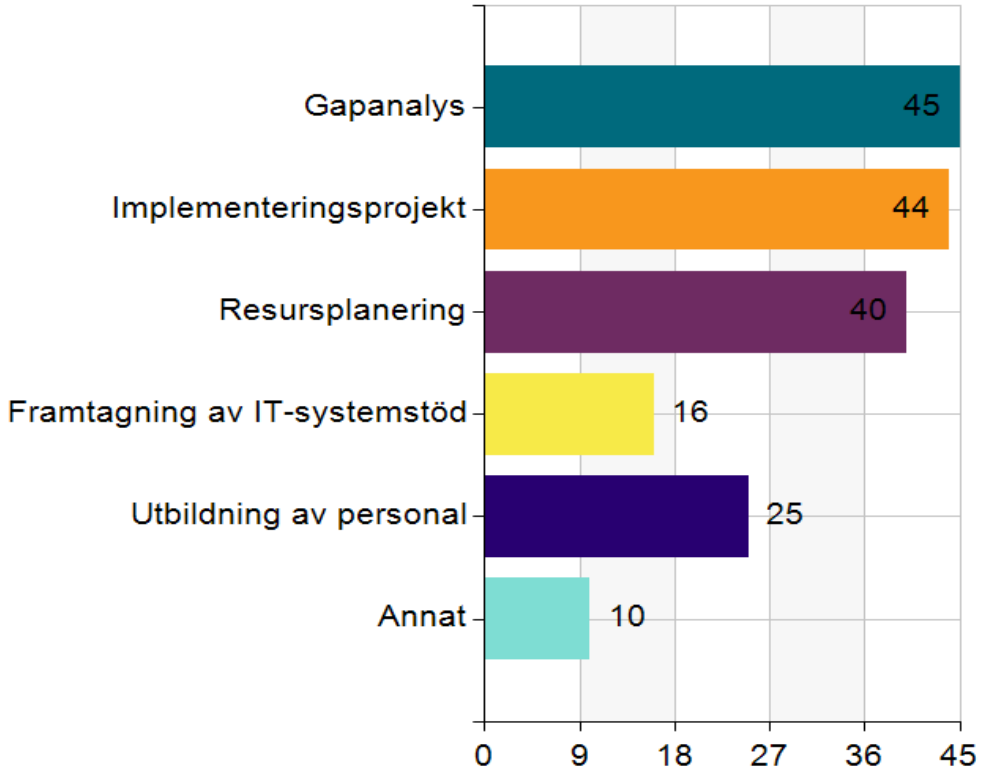
- Allmänna principer
- Ansvar vid utkontraktering
- Viktiga avtalsbestämmelser
- Tillsynsram för kritiska tredjepartsleverantörer av IKT-tjänster

Enkät om företagens förberedelser

Ligger företaget i fas med sina planerade förberedelser inför Dora-förordningen?

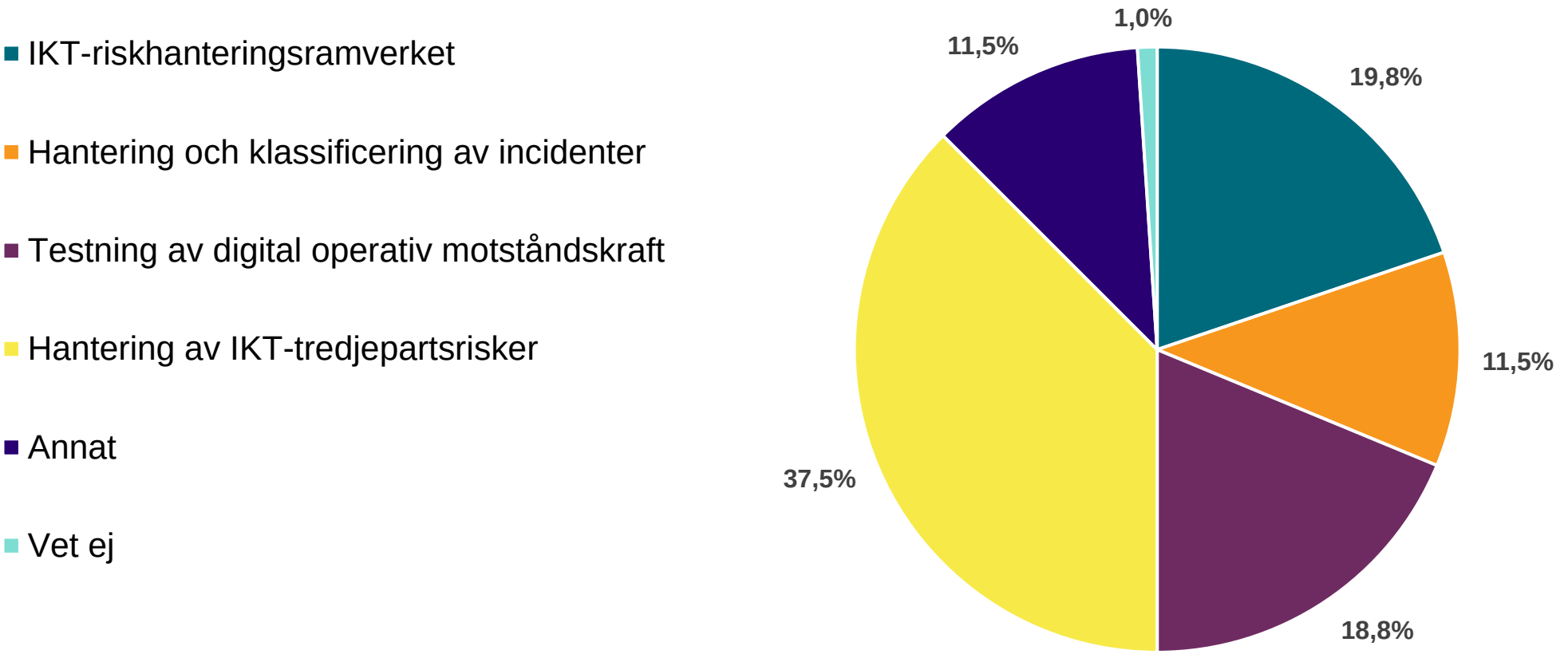


På vilket/vilka sätt har företaget påbörjat sina förberedelser inför Dora-förordningen?



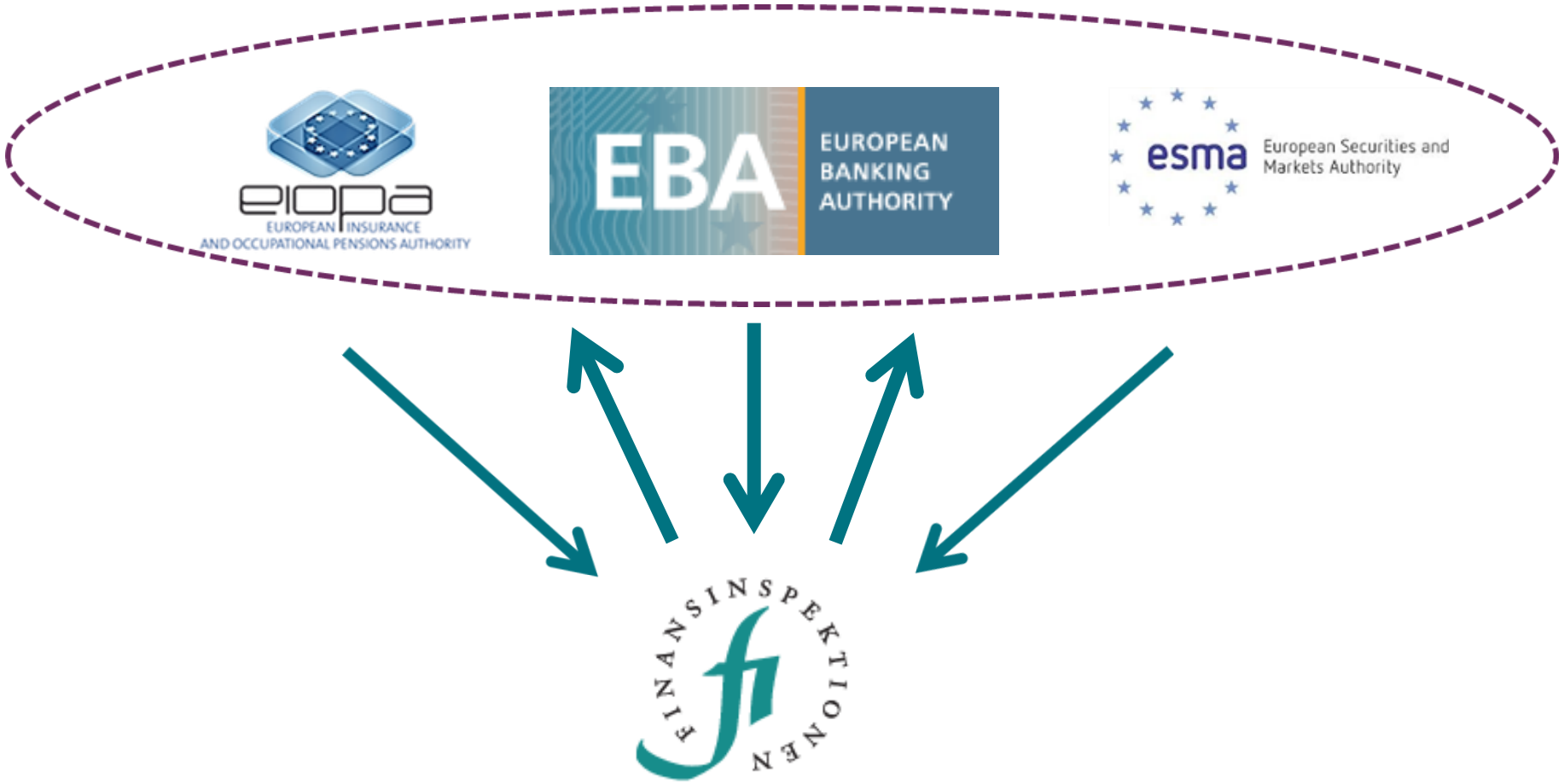
Utmaningar i Dora-regelverket

Vilka delar av Dora-regelverkets krav upplevs som särskilt utmanande att införa?



Arbetet inom EU och tekniska standarder

EU:s tillsynsmyndigheter



Tekniska standarder publicerade 17 januari 2024

- RTS on ICT risk management framework and on simplified ICT risk management framework
- RTS on criteria for the classification of ICT-related incidents
- RTS to specify the policy on ICT services supporting critical or important functions provided by ICT third-party providers
- ITS to establish the templates for the register of information

RTS on ICT risk management framework and on simplified ICT risk management framework

RTS as mandated under Articles 15 and 16(3) of DORA

Title II Article 15

15(a)	15(b)	15(c)	15(d,e,f)	15(g)
Chapter I: ICT security policies, procedures, protocols, and tools	**Chapter II**: Human Resources Policy and Access control	**Chapter III**: ICT-related Incident Detection and Response	**Chapter IV**: ICT Business continuity management	**Chapter V**: Report on the ICT risk management framework review

Title III Article 16 (3)

Chapter I: Simplified ICT Risk management framework

RTS on ICT risk management framework and on simplified ICT risk management framework

1. Ytterligare harmonisering av verktyg, metoder, processer och strategier för IKT-riskhantering

Exempel:

- Hantering av IKT-förändringar
- Åtkomsthantering
- IKT-kontinuitetshantering

2. Förenklad IKT-riskhanteringsram

RTS on criteria for the classification of ICT-related incidents

RTS on criteria for the classification of ICT-related incidents

- Klassificeringskriterier
- Allvarliga IKT-relaterade incidenter
- Betydande cyberhot
- Allvarliga IKT-relaterade incidenters relevans för behöriga myndigheter i andra medlemsstater

RTS to specify the policy on ICT services supporting critical or important functions provided by ICT third-party providers

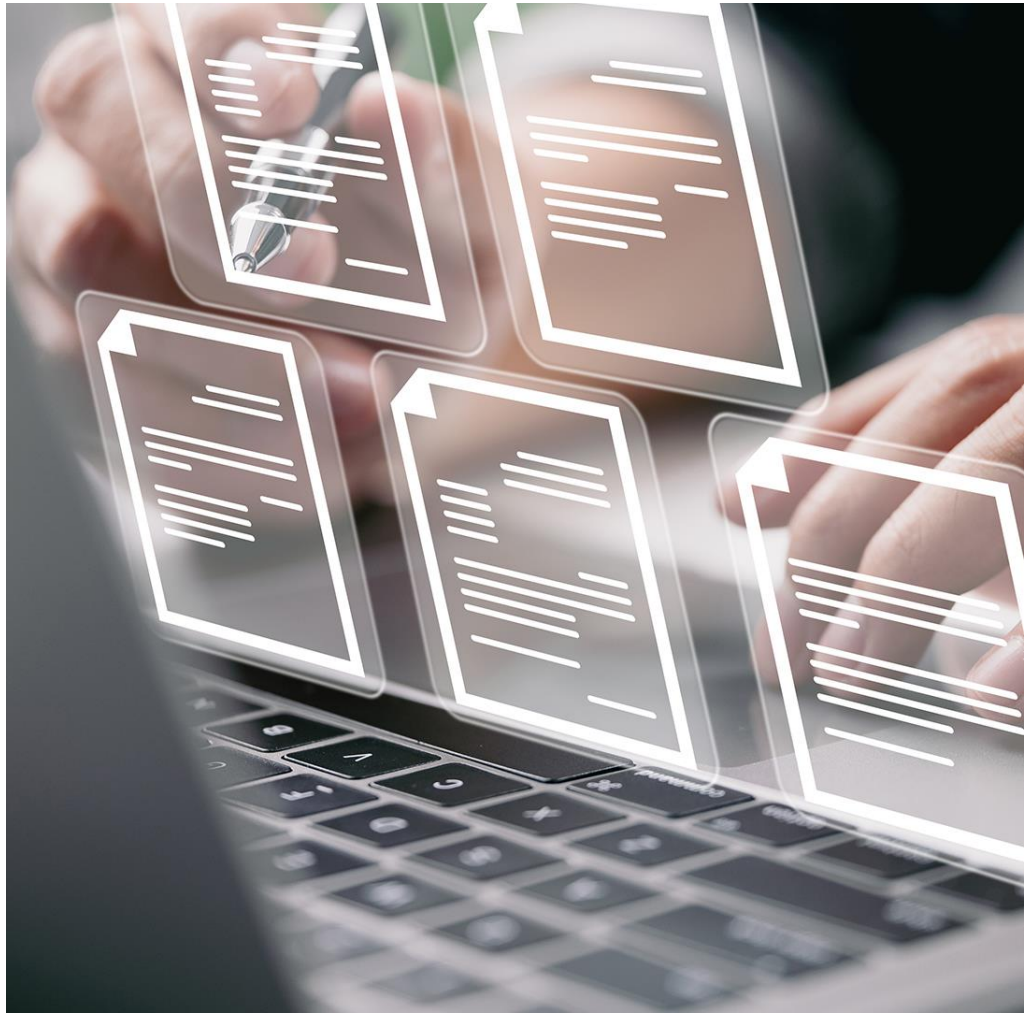
RTS to specify the policy on ICT services supporting critical or important functions provided by ICT third-party providers

- Styrning
- Livscykel för kontraktsmässiga arrangemang
- Due diligence-granskning
- Avtalsklausuler
- Övervakning av kontraktsmässiga arrangemang
- Exitplaner och uppsägning av kontraktsmässiga arrangemang

ITS to establish the templates for the register of information

ITS to establish the templates for the register of information

- Krav för att upprätthålla och uppdatera informationsregister
- Dataformat
- Innehåll
- Omfattning
- Mallar



Inskickade frågor

Nästa steg


Fler frågor?

Här hittar du Finansinspektionen

Kontakt

finansinspektionen@fi.se

08-408 980 00

Följ oss på

Twitter.com/finansinsp

Youtube.com/finansinspektionen

Linkedin.com/company/finansinspektionen

Facebook.com/finansinsp

Instagram.com/finansinsp/

FI-FORUM