# Finansinspektionens författningssamling

Utgivare: Finansinspektionen, Sverige, www.fi.se
ISSN 1102-7460

**FFFS 2014:5**
Utkom från trycket
den 17 april 2014

## Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem;

beslutade den 11 april 2014.

Finansinspektionen föreskriver[1] följande med stöd av 5 kap. 2 § 4 förordningen (2004:329) om bank- och finansieringsrörelse samt 6 kap. 1 § 9–12 och 29 förordningen (2007:572) om värdepappersmarknaden, och lämnar allmänna råd.

### 1 kap. Tillämpningsområde

**1 §** Dessa föreskrifter innehåller bestämmelser om hur ett företag ska hantera informationssäkerhet, it-verksamhet och insättningssystem.

**2 §** Föreskrifterna gäller för följande företag:

1. bankaktiebolag,
2. sparbanker,
3. medlemsbanker,
4. kreditmarknadsbolag,
5. kreditmarknadsföreningar, och
6. värdepappersbolag.

#### Definitioner

**3 §** I dessa föreskrifter och allmänna råd används samma definitioner som i 1 kap. 3 § Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut och Finansinspektionens föreskrifter (FFFS 2014:4) om hantering av operativa risker, om inget annat anges i föreskrifterna.

Därutöver betyder

1. *informationssäkerhet:* skydd av konfidentialitet, riktighet och tillgänglighet hos information,

2. *it-verksamhet:* ett företags organisation, processer och personal för att hantera it-system.

3. *konfidentialitet:* förhållandet att information inte görs tillgänglig eller avslöjas för obehöriga,

[1] Jfr Europaparlamentets och rådets direktiv 2009/14/EG av den 11 mars 2009 om ändring av direktiv 94/19/EG om system för garanti av insättningar, vad gäller täckningsnivån och utbetalningsfristen (EUT L 68, 13.3.2009, s. 3, Celex 32009L0014).

4. *riktighet:* egenskap hos information som innebär att informationen inte förändras obehörigen, av misstag eller på grund av funktionsstörning,

5. *spårbarhet:* en möjlighet att entydigt kunna härleda utförda aktiviteter och vilken person eller systemfunktion som har utfört dessa, och

6. *tillgänglighet:* en möjlighet att kunna använda information i förväntad utsträckning och inom önskad tid.

## 2 kap. Informationssäkerhet

### Ledningssystem för informationssäkerhet

**1 §** Ett företag ska arbeta strukturerat och metodiskt med informationssäkerhet genom att använda sig av ett ledningssystem enligt 2–9 §§.

### Mål och inriktning

**2 §** Ett företag ska dokumentera mål och inriktning för sin informationssäkerhet. Styrelsen eller den verkställande direktören ska besluta om målen och inriktningen.

### Ansvar för informationssäkerhet och samordning

**3 §** Ett företag ska säkerställa att det är tydligt hur ansvaret för informationssäkerheten inom verksamheten är fördelad.

**4 §** Ett företag ska utse en person som ansvarar för att leda och samordna arbetet med informationssäkerhet.

### Informationsklassificering

**5 §** Ett företag ska klassificera sin information för att den ska få rätt skyddsnivå. Klassificeringen ska utgå från de krav som ställs på informationens konfidentialitet, riktighet och tillgänglighet i verksamheten.

Företaget ska dokumentera klassificeringen enligt första stycket och utse personer eller funktioner som ansvarar för den information som hanteras inom verksamheten.

### Riskanalys

**6 §** Ett företag ska årligen och vid förändringar som har betydelse för informationssäkerheten, analysera de risker som är hänförliga till företagets informationssäkerhet. Företaget ska utifrån dessa analyser och inträffade incidenter besluta om hur det ska hantera identifierade risker.

Företaget ska dokumentera riskanalyserna och sina beslut om åtgärder.

### Interna regler

**7 §** Ett företag ska fastställa interna regler för sitt arbete med informationssäkerhet.

Företaget ska beakta arten, omfattningen och komplexiteten i sin verksamhet när det utformar de interna reglerna för informationssäkerhet.

*Allmänna råd*

De interna reglerna bör ange krav på

1. fysisk säkerhet,
2. skydd av datakommunikation och drift,
3. spårbarhet i it-system,
4. att produktionsmiljön för it-system är separerad från test- och utvecklingsmiljöer,
5. styrning av åtkomst till information,
6. säkerhetskrav på it-system vid inköp, utveckling, underhåll och avveckling,
7. rapportering och hantering av incidenter relaterade till informationssäkerhet, och
8. regelbunden kontroll av företagets it-system mot den fastställda skyddsnivån för information enligt 5 §.

**8 §** Ett företag ska i de interna reglerna enligt 7 § särskilt ange hur företaget ska tilldela, ändra och ta bort åtkomstbehörigheter till it-system. Företaget ska regelbundet, dock minst årligen, kontrollera att befintliga åtkomstbehörigheter är begränsade till behov utifrån tilldelade arbetsuppgifter.

**9 §** Ett företag ska se till att de interna reglerna enligt 7 § regelbundet utvärderas och uppdatera dessa om det behövs.

## 3 kap. It-verksamhet

### Säkerhet

**1 §** Ett företag ska se till att dess it-system är tillräckligt säkra i förhållande till arten hos den information som det hanterar i systemen.

*Allmänna råd*

Företaget bör när det bedömer om it-systemen är tillräckligt säkra utgå från den klassificering av information som ska göras enligt 2 kap. 5 §.

### Mål och strategi

**2 §** Ett företag ska ha dokumenterade övergripande mål och strategier för sin it-verksamhet.

Den verkställande direktören ska besluta om företagets övergripande mål och strategier enligt första stycket och regelbundet utvärdera och uppdatera dessa om det behövs.

### Ansvariga

**3 §** Ett företag ska säkerställa att det är tydligt vem som ansvarar för de olika delarna av företagets it-verksamhet. För varje it-system ska företaget utse en person eller funktion som ansvarar för företagets krav på systemet.

### Processer

**4 §** Ett företag ska ha ändamålsenliga processer för hur det hanterar sina it-system. Företaget ska dokumentera processerna och beskriva de förhållanden som är av betydelse för att det ska kunna hantera it-systemen på ett kontrollerat sätt.

Företaget ska beakta verksamhetens art, omfattning och komplexitet när det tillämpar första stycket.

*Allmänna råd*

De processer som företaget ska dokumentera bör omfatta

1. inköp, utveckling, underhåll och avveckling,
2. drift, inklusive säkerhetskopiering, samt återställning av system och data,
3. incidenthantering,
4. ändringshantering, och
5. test.

### Dokumentation över it-system

**5 §** Ett företag ska ha en dokumentation över varje enskilt it-system som är av betydelse för verksamheten. Vilka systemen är ska framgå av en förteckning som regelbundet ska ses över och uppdateras om det behövs.

### Uppdragsavtal

**6 §** Bestämmelser om uppdragsavtal finns i 10 kap. Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut och 9 kap. Finansinspektionens föreskrifter (FFFS 2007:16) om värdepappersrörelse.

## 4 kap. Insättningssystem

### Tillämpningsområde

**1 §** Bestämmelserna i detta kapitel gäller för företag som tar emot eller avser att ta emot insättningar som omfattas av insättningsgaranti enligt lagen (1995:1571) om insättningsgaranti.

### Insättningssystem

**2 §** Ett företag ska när det hanterar sin information om insättare och deras insättningar använda it-system som gör det möjligt för företaget att automatiskt

sammanställa data om insättare och deras insättningar i enlighet med Riksgäldskontorets föreskrifter (RGKFS 2011:2) om instituts skyldighet att lämna uppgifter om insättare och deras insättningar.

### Riskanalys

**3 §** Ett företag ska årligen analysera de risker som är hänförliga till de it-system som företaget använder för att hantera sin information om insättare och deras insättningar. Analysen ska innefatta skyddet för informationens riktighet och systemintegriteten hos it-systemet. Analysen ska även omfatta informationens konfidentialitet och tillgänglighet.

Med *systemintegritet* avses i detta kapitel att ett it-system kan upprätthålla sin avsedda funktion och därigenom skyddas mot oönskad påverkan, ändring eller insyn.

### Funktioner och rutiner

**4 §** Ett företag ska se till att it-systemen enligt 2 § har tekniska funktioner och att det finns administrativa rutiner för att säkerställa

1. åtkomstkontroll,
2. att aktiviteter i it-system och ändringar av it-system är spårbara,
3. systemintegritet,
4. informationens riktighet,
5. att systemets drift kan återställas efter avbrott, och
6. att information är tillgänglig i enlighet med Riksgäldskontorets föreskrifter (RGKFS 2011:2) om instituts skyldighet att lämna uppgifter om insättare och deras insättningar.

Företaget ska dessutom besluta om de tekniska funktioner och administrativa rutiner som är nödvändiga utifrån de riskanalyser det ska utföra enligt 3 §.

### Dokumentation

**5 §** Ett företag ska utöver de krav som anges i 3 kap. 5 § dokumentera de tekniska funktioner och administrativa rutiner som företaget ska ha enligt 4 §.

Dokumentationen ska regelbundet ses över och uppdateras om det behövs.

### Granskning och rapportering

**6 §** Företagets funktion för internrevision ska årligen granska företagets insättningssystem samt de tekniska funktioner och administrativa rutiner som är av betydelse för säkerheten i systemet. Om företaget saknar en funktion för internrevision ska det uppdra den årliga granskningen till någon som har särskild kompetens inom säkerhetsområdet.

Granskningen ska dokumenteras och rapporteras till företagets styrelse.

*Allmänna råd*

Företaget bör i granskningen utgå från etablerade principer för säkerhet.

---

Dessa föreskrifter och allmänna råd träder i kraft den 1 juni 2014.

MARTIN ANDERSSON

Anders Lindgren