

Större tillsynsfokus på bankers IT-risker

I slutet av 2016 publicerade EBA förslag på nya riktlinjer för hur Finansinspektionen ska granska Svenska bankers IT-risker. Förslaget är krävande och förväntas leda till mycket arbete för Svenska banker.

Bakgrund

Nuvarande utformning av översyns- och utvärderingsprocessen (ÖUP eller SREP på engelska) (EBA/GL/2014/13), reglerar hur Finansinspektionen (FI) ska bedriva sin tillsyn av Svenska banker. Det nya förslaget på riktlinjer från EBA tydliggör detaljrikedomen av tillsynsprocessen avseende IT och informationssäkerhet. Kraven inom IT och informations-säkerhet är sedan 2014 fastställda i Sverige genom föreskrifter från FI (FFFS 2014:5). Det nya EBA förslaget ger därför vägledning i hur regelverken ska tolkas.

Föreslagna förändringar

Förslagen på riktlinjer från EBA inom ICT (IT och kommunikationsteknologi), definierar tre övergripande områden:

- Affärsstrategins koppling mot IT och hantering av risker inom IT
- Riskramverk för IT inkl. informations-säkerhetsrisker
- Kontrollramverk för IT inkl. Informationssäkerhet

Vi ser att efterlevnaden av ICT-kraven kommer att kräva förändringar för Svenska banker. Flertalet områden kommer att behöva formaliseras ytterligare, områden såsom IT-strategi samt framtagning av riskramverk för IT- och informations-säkerhetsrisker inklusive kontrollramverk för dessa. Vidare kommer dessa risk- och kontrollramverk behöva införlivas i den övergripande hanteringen av operativ risk.

Vad händer härnäst

Remisstiden stängde den 6:e Januari 2017 och inkomna remisser till EBA behandlas nu. Svenska Bankföreningen har skickat in Svenska kommentarer på remissen och även den Europeiska bankföreningen har lämnat synpunkter. Vi förväntar oss dock inte några större förändringar jämfört med förslaget, och tror att förslagets krav till stora delar kommer ingå i EBA:s slutgiltiga riktlinjer. Därmed kommer kraven att ligga till grund för FI:s bedömning av materiella risker inom IT, inom ramen för kontroll av operativ risk.

Den framtida granskningen av den operativa riskhanteringen inom svenska banker kommer därför sannolikt i större utsträckning omfatta IT.

Länk till guiden [här!](#)

FCG:s tjänster

FCG kan hjälpa ditt företag med att göra nödvändiga förändringar för att redan nu anpassa verksamheten till EBA:s krav rörande IT-risker. FCG har många konsulter med lång erfarenhet av hantering av operativ risk, IT-strategi och IT-styrning samt informationssäkerhet.

Tveka inte att kontakta oss på FCG för ett möte där vi går igenom hur vi kan hjälpa just ditt företag.

Kontakt

Fredrik Ohlsson, Teamchef Operativ risk och IT
+46 72 179 49 51
Fredrik.ohlsson@fcg.se

