Nya regler om styrning och riskhantering

FI-forum

20 maj 2014

Agenda och inledning

Christer Furustedt

Avdelningschef Banktillsyn

Agenda

- Inledning
- Rättsliga aspekter
- Styrning, riskhantering och kontroll
- Kaffepaus: 14.30-15.00
- Hantering av operativa risker
- Informationssäkerhet, it-verksamhet och insättningssystem

Företagen och det finansiella systemet

- Reducera komplexiteten
- Öka motståndskraften
- Stärka ledningen

Rättsliga aspekter

Sara Björkman

Enhetschef Bankrätt kreditinstitut

Markus Ribbing

Jurist Bankrätt stora banker

Rättsliga frågor

- Ebas GL 44
- Tillämpningsområde
- Proportionalitet
- CRD 4, kommande krav

Styrning, riskhantering och kontroll

Christer Furustedt

Avdelningschef Banktillsyn

Elisabeth Siltberg

Enhetschef Kreditrisker

Agnieszka Arshamian

Analytiker Styrning och operativa risker

Maris Ritums

Institutsansvarig Tillsyn stora banker

Organisatoriska krav

- Tydlig organisationsstruktur
- Befattningsbeskrivningar
- Riskstrategi och riskaptit
- Insamling av riskdata

Krav på styrelse och vd

- Styrelse och vd
- Ansvar för riskaptit, riskstrategi, interna regler etc.
- Uppföljnings- och utvärderingsansvar

Intressekonflikter

- Fokus på identifiering
- Dokumentationskrav
- Ska hanteras

Riskhantering och riskkontroll

- 6 kap. 2§ LBF
- FFFS 2005:1
- GL 44
- Tillsyn

Riskhantering och riskkontroll

- Helhetssyn
- Medvetenhet och ansvar
- Ökad finansiell stabilitet och bättre konsumentskydd.

Riskhantering

- Ramverk
- Riskkultur
- Varför är rapporteringen så viktig?

Riskkontroll

- Kontroll – analys – rapportering
- Identifiera och analysera potentiella risker
- Inrättandet av riskchef i ledningen stärker riskperspektivet

Regelefterlevnad

- Risker för bristande regelefterlevnad
- Funktion för regelefterlevnad
  - identifiera risker
  - övervaka och kontrollera
  - Informera och utbilda
  - delta i processen för godkännande

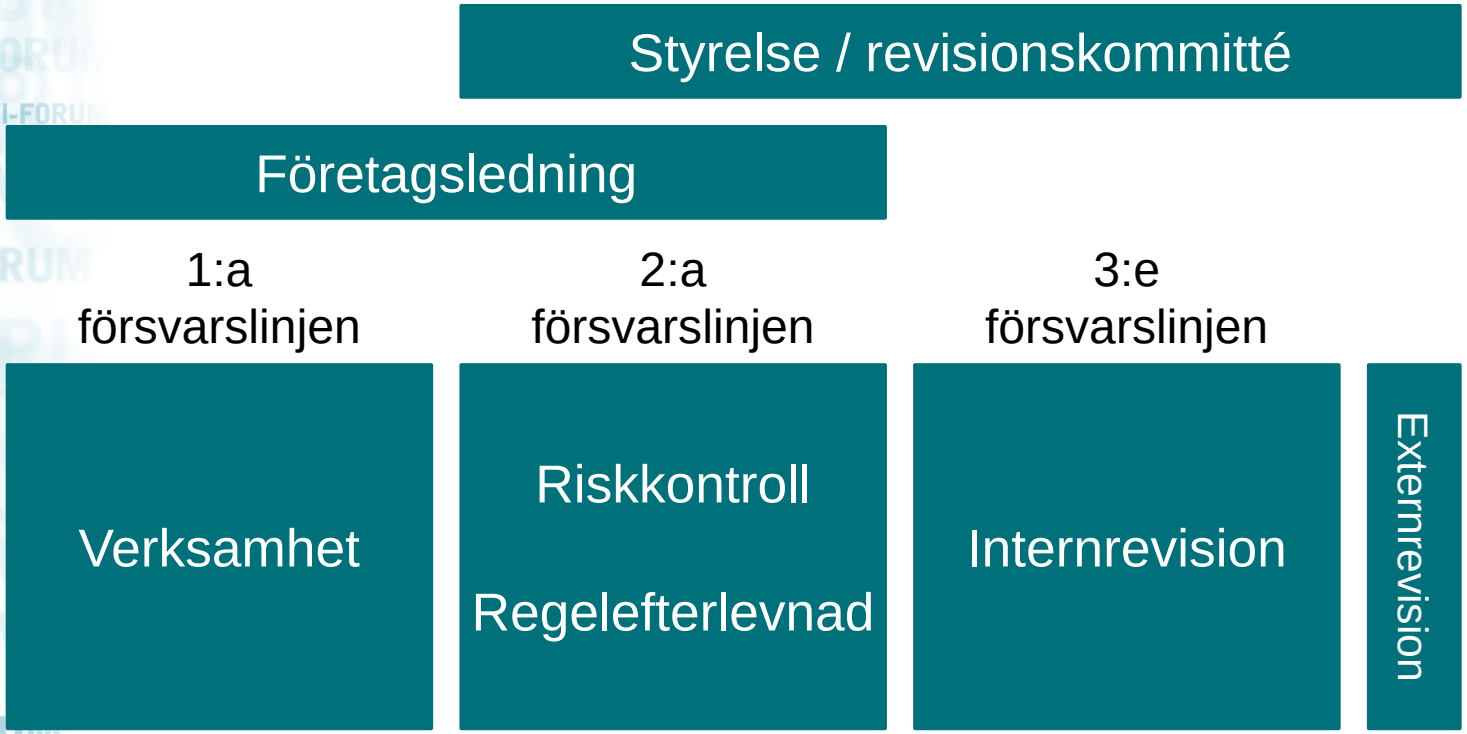
Internrevision
Vad är nytt eller förtydligat?

- Mer specifik än 2005:1; tydliggör ansvarsområden.
- Arbetet ska vara riskbaserat.
- Utvärdera riskhantering utifrån beslutad riskstrategi och riskaptit.
- Få löpande info och utbildning om nya produkter och tjänster.
- Kunskap om redovisning och värdering av tillgångar.
- Granska och utvärdera tillförlitligheten i företagets finansiella rapportering, inklusive åtaganden utanför BR.

Internrevision - viktiga aspekter

- Övergripande förväntan är att fånga risker och brister i tid.
- Riskbaserat arbetssätt i en föränderlig omvärld, dvs. bör kunna prioritera när så behövs.
- Måste ha kompetens att kunna utmana affärsverksamheten, riskorganisationen och compliance.
- Ska ha resurser samt tillgång till den info som krävs.
- Bör ha styrelsens och VLs gehör.
- Dokumentera uppföljningen av rekommenderade åtgärder.
- I god tid eskalera brister som inte är åtgärdade.

Nivåer avseende riskhantering och kontroll



Uppdragsavtal

- Ersätter FFFS 2005:1 för kreditinstitut
- Interna regler
- Kontroll över den utlagda verksamheten
- Uppdragstagaren följer relevanta regler
- Specifika krav på uppdragstagaren och uppdragsgivaren

Frågor?

Kaffepaus 14.30-15.00

Hantering av operativa risker

Agnieszka Arshamian

Analytiker Styrning och operativa risker

Anders Hedberg

Institutsansvarig Tillsyn stora banker

Henrik Lindstrand

Analytiker Styrning och operativa risker

Föreskrifter och allmänna råd om hantering av operativa risker

Styrning och ansvar
Identifiering och mätning
Rapportering

Hantering av operativa risker i verksamheten:
- Processer
- Personal
- Legala risker
- Säkerhetsarbete
- It-system
- Process för godkännande
- Kontinuitetshantering

Särskilda krav på hantering av operativa risker inom värdepappersrörelse och valutahandel

Föreskrifter och allmänna råd om Informationssäkerhet, it-verksamhet och insättningssystem

Informations-säkerhet

It-verksamhet

Insättnings-system

Styrning och ansvar

- Riskaptit
- Risklimiter
- Interna regler
  - typ av operativa risker
  - metoder och processer
  - övervakning av riskaptit och limiter

Identifiering och mätning

- Identifiera operativa risker i
  - produkter
  - tjänster
  - funktioner
  - processer
  - it-system
- Riskindikatorer
- Incidenthantering

Rapportering

- Riskindikatorer
- Överträdelser av riskaptit och risklimiter
- Allvarliga incidenter
- Test av planer

Hantering av risker i verksamheten

- Processer
- Personal
- Legala risker
- Säkerhetsarbete
- It-system
- Process för godkännande
- Kontinuitetshantering

Vp-rörelse och valutahandel

- Åtskillnad av arbetsuppgifter
- Personal
- Transaktionshantering
- Hantering av säkerheter
- Övervakning och kontroll

Processer

- Väsentlig betydelse
- Ansvar
- Dokumentation
- Kontroller

Personal

- Kontroll vid nyanställning
- Bemanningsplanering
- Ersättare för nyckelpersoner
- Kompetenshantering
- Befattningsbeskrivningar, mandat, limiter
- Tystnadsplikt
- Byte av arbetsuppgifter

Legala risker

- Interna regler
  - lagar, förordningar och andra regler
  - korrekta avtal
  - arkivering
  - rättsliga processer
- Ansvar

Säkerhetsarbete

- Interna regler
  - tillgångar
  - skyddsåtgärder
- Proaktivt arbete
- Informationssäkerhet, se FFFS 2014:5

Process för godkännande

- Omfattning: produkter, tjänster, marknader, processer, it-system, verksamhet, organisation
- Interna regler
- Riskkontrollens roll
- Ansvar för riskhantering efter införande

Process för godkännande

- Moment i processen
  - kontroll av regelefterlevnad
  - analys av risknivåer
  - kontroll: personal, kompetens, interna regler, verktyg, stöd- och kontrollfunktioner
  - dokumentation av beslut

Kontinuitetshantering – interna regler

- Fastställs av vd
- Metoder och rutiner
- Beredskapsplaner, kontinuitetsplaner och återställningsplaner
- Roller och ansvar
- Principer för agerande
- Principer och frekvens för test (processer som anses vara av väsentlig betydelse ska testas minst årligen)

Kontinuitetshantering - konsekvensanalys

- Regelbundenhet
- Omfatta samtliga affärsenheter och samtliga stödfunktioner
- Beakta beroenden
- Konsekvensanalysen innefattar utlagd verksamhet
- Prioriteringar och mål
- Dokumenterade beredskapsplaner, kontinuitetsplaner och återställningsplaner

Kontinuitetshantering – kommunikation och rapportering

- Kommunikation och utbildning
  - rutiner för intern och extern kommunikation
  - utbildning för de anställda
- Rapportering
  - minst årlig rapportering till styrelse
  - resultat från tester av beredskapsplaner, kontinuitetsplaner och återställningsplaner

Frågor?

Informationssäkerhet, it-verksamhet och insättningssystem

Anders Lindgren

Analytiker Styrning och operativa risker

Mattias Dandoy

Analytiker Styrning och operativa risker

Informationssäkerhet

- Ledningssystem för informationssäkerhet
- Mål och inriktning
- Ansvar och samordning
- Klassificera informationen
- Analysera riskerna
- Interna regler

Informationssäkerhet

- Ledningssystem för informationssäkerhet
- Mål och inriktning
- Ansvar och samordning
- Klassificera informationen
- Analysera riskerna
- Interna regler

Informationssäkerhet

- Ledningssystem för informationssäkerhet
- Mål och inriktning
- Ansvar och samordning
- Klassificera informationen
- Analysera riskerna
- Interna regler

Informationssäkerhet

- Ledningssystem för informationssäkerhet
- Mål och inriktning
- Ansvar och samordning
- Klassificera informationen
- Analysera riskerna
- Interna regler

Informationssäkerhet

- Ledningssystem för informationssäkerhet
- Mål och inriktning
- Ansvar och samordning
- Klassificera informationen
- Analysera riskerna
- Interna regler

Informationssäkerhet

- Ledningssystem för informationssäkerhet
- Mål och inriktning
- Ansvar och samordning
- Klassificera informationen
- Analysera riskerna
- Interna regler

Informationssäkerhet

- Ledningssystem för informationssäkerhet
- Mål och inriktning
- Ansvar och samordning
- Klassificera informationen
- Analysera riskerna
- Interna regler

It-verksamhet

- Säkerhet
- Mål och strategi
- Ansvariga
- Processer
- Dokumentation över it-system
- Uppdragsavtal

It-verksamhet

- Säkerhet
- Mål och strategi
- Ansvariga
- Processer
- Dokumentation över it-system
- Uppdragsavtal

It-verksamhet

- Säkerhet
- Mål och strategi
- Ansvariga
- Processer
- Dokumentation över it-system
- Uppdragsavtal

It-verksamhet

- Säkerhet
- Mål och strategi
- Ansvariga
- Processer
- Dokumentation över it-system
- Uppdragsavtal

It-verksamhet

- Säkerhet
- Mål och strategi
- Ansvariga
- Processer
- Dokumentation över it-system
- Uppdragsavtal

It-verksamhet

- Säkerhet
- Mål och strategi
- Ansvariga
- Processer
- Dokumentation över it-system
- Uppdragsavtal

It-system, dokumentation

- beskrivning av hur systemet används och beroenden,
- tekniska parametrar
- hur systemet fungerar och ska underhållas
- vad som krävs för den dagliga driften av systemet.

It-verksamhet

- Säkerhet
- Mål och strategi
- Ansvariga
- Processer
- Dokumentation över it-system
- Uppdragsavtal

Insättningssystem

- Tillämpningsområde
- Insättningssystem
- Riskanalys
- Funktioner och rutiner
- Dokumentation
- Granskning och rapportering

Frågor?


FINANSINSPEKTIONEN