Riksbanken

Tydliggjord compliance

Stockholm 16 juni 2011

Ernst & Young

Sammanfattning

Ernst & Young har utformat ett förslag på vilka compliance-relaterade aktiviteter som bör utföras på Riksbanken, vilka riskområden man bör fokusera på samt hur ansvaret för aktiviteterna bör vara utformat. Ett antal förbättringsområden har identifierats för att säkerställa ett väl fungerande compliance-arbete inom Riksbanken.

För att compliance-arbetet skall kunna utföras på ett adekvat och ändamålsenligt sätt rekommenderar Ernst & Young att en Compliance-funktion med 1-2 heltidsanställda inrättas. Funktionen bör utföra aktiviteter av rådgivande och uppföljande karaktär.

Ernst & Youngs uppfattning är att Riskenheten har möjlighet att utföra sitt uppdrag självständigt och oberoende från verksamheten givet sin placering i stabsavdelningen. Mot bakgrund av detta rekommenderar Ernst & Young att Compliance-funktionen organisatoriskt placeras inom Riskenheten av tre huvudsakliga anledningar:

1) Riskenheten och Compliance-funktionen ansvarar för två olika riskuniversum men deras rekommendationer till verksamheten kommer i viss utsträckning att sammanfalla. Placeras Compliance-funktionen i Riskenheten kan de på ett naturligt sätt arbeta med samma definitioner, processer, cykler, rapportering etc. Till exempel kan riskanalysen för operativa risker och compliance-risker samordnas.
2) 1-2 heltidstjänster motiverar inte skapandet av en separat funktion med den dubblering och ineffektivitet som medföljer.
3) Ytterligare en omorganisation av Riskenheten för att separera ut compliance-risker medför onödig turbulens och oro.

För att säkerställa ett väl fungerande compliance-arbete inom Riksbanken bör nedanstående framgångsfaktorer beaktas:

- Tydligt definierat mandat för Compliance Officer som är väl förankrat hos Direktionen och avdelningscheferna
- Tillsätt en Compliance Officer med rätt kompetens för rollen
- Compliance Officer skall ha en direkt rapporteringsväg till Direktionen
- Följ upp Compliance Officer utifrån en årlig compliance-plan

Innehållsförteckning

1 Introduktion

1.1 Bakgrund

I mars 2008 tog Direktionen ett principbeslut om att det skall finnas en Regeluppföljningsfunktion inom Riksbanken samt att ge stabschefen till uppgift att inrätta en sådan funktion inom stabsavdelningen. Beslutet var en respons på påpekanden från Internrevision, fullmäktiges revisorer samt Riksrevisionen avseende bristen på regelstödsfunktion hos Riksbanken. När Regeluppföljningsfunktionen hade bildats blev den dock nedprioriterad till förmån för frågor kring intern styrning och kontroll (”ISK”) och som resultat blev inte funktionens ansvarsområden ytterligare detaljerade och tydliggjorda.

I januari 2010 genomförde Riksbanken en omorganisation för att samla de olika funktioner som arbetade med riskfrågor i en och samma enhet. Under 2010 har enheten arbetat med att få nya arbetssätt och rutiner på plats och ett behov av att skapa en förstärkt kontrollstruktur har identifierats. Ett led i detta är att säkerställa att Riksbanken har en Compliance-funktion som överensstämmer med vad som kan förväntas av en centralbank.

1.2 Syfte

Rapporten syftar till att tydliggöra Compliance-funktionens roll och ansvar inom Riksbankens organisation, inklusive vilka risker som ligger inom compliance-området, vilka compliance-relaterade aktiviteter som bör utföras på Riksbanken samt hur arbetet skall organiseras. Ernst & Young har tagit utgångspunkt i hur compliance-arbetet bedrivs inom affärsbanker, centralbanker och utvalda statliga myndigheter för att tydliggöra behovet av compliance hos Riksbanken.

1.3 Avgränsning

Ernst & Young har avgränsat arbetet med att beskriva compliance-arbete som bedrivs inom andra centralbanker till att sammanfatta de rapporter som mottagits från Riksbanken.

1.4 Tillvägagångssätt

Ernst & Young har kartlagt compliance-funktionalitet hos ett antal affärsbanker och statliga myndigheter med finansiell verksamhet. Vidare har Ernst & Young tagit del av dokumentation avseende compliance inom centralbanker.

Drygt 15 av Riksbankens medarbetare har intervjuats, dels medarbetare inom Riskenheten och dels avdelningschefer och andra medarbetare i organisationen. De som intervjuats listas i Appendix. Ernst & Young har även tagit del av skriftliga styrdokument och annan dokumentation från Riksbanken.

2 Compliance hos affärsbanker, centralbanker och myndigheter

Compliance (”regelefterlevnad”) syftar till att upprätthålla en verksamhets anseende och trovärdighet genom att följa externa och interna regelverk. Finansinspektionen definierar regelefterlevnad, enligt nedan:

”Med regelefterlevnad menas i dessa allmänna råd efterlevnad av lagar, förordningar och interna regler samt god sed eller god standard avseende den tillståndspliktiga verksamheten”[1]

2.1 Compliance-risker och konsekvenser

Verksamheter i den finansiella sektorn, liksom myndigheter, har en rad styrande dokument, såväl externa lagar och regler som interna policyer och riktlinjer som de är skyldiga att följa. En Compliance-funktion har inte ansvar för kontroll av efterlevnad av alla dessa regelverk. Nedan exemplifieras de riskområden som vanligen ingår i Compliance-funktionens uppdrag hos affärsbanker samt i viss utsträckning i centralbanker och statliga myndigheter. Inom affärsbanker är skydd av kundens intressen ett resurskrävande riskområde för compliance-funktionen, vilket inte är fallet för flertalet centralbanker och statliga myndigheter. Penningtvätt och finansiering av terrorism är ett prioriterat och resurskrävande riskområde för såväl affärsbanker som centralbanker inom euro-området.

Riskområde	Exempel på styrande dokument
Krav från myndigheter m.fl.	• Tillämpliga lagar, industristandarder, regler och tillstånd • Checklista för affärsförändringar, nya produkter, processer, etc.
Organisatorisk struktur	• Arbetsordning och instruktioner • Organisation, roller/funktioner • Rapporteringslinjer, eskaleringsprocess, delegering av rättigheter, etc. • Rollbeskrivning för chefer och medarbetare
Outsourcing	• Krav på outsourcingleverantör • Kontrakt • Organisation kring avtal/samarbete • Registerföring av outsourcingavtal

Skydd av kundens intressen	• Regler för:
	  • Marknadsföring
	  • Investeringsrådgivning
	  • Klassificering av kunder
	  • Kundinformation
	  • Konsumentkreditlagen
	  • Betaltjänstdirektivet

Hantering av känsligt material	• Banksekretess • Regler för skydd av personliga uppgifter

[1] Finansinspektionens Författningssamling 2005:1

Marknadsmissbruk och insiderhandel	• Regler för:
	  • Egenhandel
	  • Marknadsmissbruk
	  • ”Flaggning”
	  • Portföljförvaltning
	  • Transaktionsrapportering

Process för handel av värdepapper	• Processbeskrivning Utförande • Processbeskrivning Handläggning • Processbeskrivning Aggregering och allokering
Affärsverksamhet och etik	• Etiska regler / ”uppföranderegler” • Intressekonflikter • Övriga regelverk (bedrägeri, mutor, arbete utanför tjänst, anställdas innehav, egenintresse, etc.)
Kunders uppförande	• Lag om penningtvätt och terroristfinansiering • Lag om kunders transaktioner med sanktionerade länder

Utöver ovanstående områden har ett flertal centralbanker även angivit fysisk säkerhet samt arbetsmiljö som riskområden. Några exempel på riskområden som normalt inte ligger inom ramen för en Compliance-funktions uppdrag är:

- Försäkring
- Anställda
- Redovisning
- Skatt
- Bolagsrätt
- Kreditrisk
- Marknadsrisk

Stöd och uppföljning av regelefterlevnad avseende dessa risker brukar vanligtvis hanteras av andra funktioner, till exempel HR, Ekonomi, Riskkontroll, Skatt och Juridik.

Svenska affärsbanker, svenska statliga myndigheter och centralbanker i euro-området styrs i olika grad av externa regelverk och kraven på internt regelverk varierar också. Affärsbankerna, som bedriver tillståndspliktig verksamhet och följaktligen står under tillsyn av Finansinspektionen, styrs av ett omfattande externt regelverk. Därutöver har de även krav på ett omfattande internt regelverk. De svenska myndigheterna styrs i begränsad utsträckning av externa regelverk och detsamma gäller kraven på de interna reglerna. Centralbankerna i euro-området har ett omfattande externt regelverk från ECB, kraven på interna regelverk beslutas lokalt och ingår inte i analysen. Nedan exemplifieras omfattningen på externa regelverk som olika aktörer styrs av samt krav på interna regelverk[2].

[2] Notera att tabellen ej är en komplett sammanställning av styrande regelverk.

	Svenska affärsbanker	Svenska statliga myndigheter	Centralbanker i euro-området
Exempel på externa regelverk som olika aktörer styrs av	• De viktigaste svenska lagarna och förordningarna för bank och kreditmarknaden är ca 25 stycken • Finansinspektionen har ca 50 gällande författningar för banker	• Av Riksdag beslutade tillämpliga lagar och förordningar, t.ex. myndighetsförordning • Regleringsbrev för respektive myndighet • ESV:s föreskrifter och allmänna råd	• ECB regler • Penningtvätts- och terroristfinansierings-direktivet • FATF 40 rekommendationer + 9 specialrekommendationer • Wolfsberg Statement on AML Screening, Monitoring and Searching 2009 • EU:s upphandlingsdirektiv
Exempel på krav på interna regelverk	Finansinspektionens författningar specificerar en rad krav på interna regler, exempelvis: • Riktlinjer och instruktioner för riskhantering och riskkontroll av marknadsrisker • Interna regler för redovisning och värdering • Ansvar, arbetsuppgifter och rutiner för rapportering för den oberoende granskningsfunktionen • Interna regler om åtgärder mot penningtvätt och finansiering av särskilt allvarlig brottslighet	Ekonomistyrningsverket specificerar vissa krav på interna regler t.ex.: • Utarbeta riktlinjer och rutiner för att säkerställa att medarbetarna agerar för verksamhetens mål • Ärendeförteckning	Beslutas lokalt för respektive bank.

De konsekvenser som bristande regelefterlevnad kan medföra är:

- Juridiska sanktioner, t.ex. disciplinåtgärder mot verksamheten, dess ledning eller anställda
- Tillsynsaktioner, t.ex. indragen licens (endast affärsbanker)
- Finansiella förluster, t.ex. straffavgifter
- Ryktesförluster som kan leda till negativ publicitet, minskat förtroende samt förlorad inkomst

2.2 Affärsbanker

Finansinspektionens allmänna råd om styrning och kontroll av finansiella företag, FFFS 2005:1, stipulerar att det bör finnas en funktion som utgör stöd för att verksamheten bedrivs enligt gällande regler. Funktionen skall även följa upp regelefterlevnad. I författningen avser regelefterlevnad efterlevnad av lagar, förordningar och interna regler samt god sed eller god standard. De stora affärsbankerna i Sverige har utformat en sådan funktion vilken de benämner Compliance-funktion.

Compliance-funktionens ansvar innefattar dels en rådgivande och stödjande roll och dels en uppföljande och kontrollerande roll. De svenska affärsbankerna har historiskt fokuserat på

den rådgivande rollen. Under de senaste åren har affärsbankerna stärkt den kontrollerande och uppföljande rollen.

En Compliance-funktions ansvarsområden kan vara omfattande och inkludera flertalet aktiviteter. Emellertid finns ett antal generella aktiviteter som normalt associeras med compliance inom affärsbanker. Dessa aktiviteter beskrivs nedan.

2.2.1 Aktiviteter

Policyer och instruktioner
Compliance-funktionen skall assistera verksamheten i att utveckla policyer, instruktioner och rutiner i syfte till att säkerställa regelefterlevnad. Funktionen skall bistå med rådgivning när policyer och instruktioner uppdateras eller ändras till följd av regelförändringar. Förändringar skall kommuniceras till berörda parter i verksamheten. Vidare skall funktionen ha det primära ansvaret för att utveckla policyer, instruktioner och rutiner för Compliance-funktionen.

Rådgivning
Funktionen rådger verksamheten i compliance-relaterade frågor såsom applicerbara lagar och förordningar, regler och standarder. Funktionen skall löpande och proaktivt besvara frågor för att säkerställa verksamhetens kännedom om förändringar i externa regelverk samt i interna policyer. För att underlätta arbetet är det vanligt att Compliance-funktionen ansvarar för att hålla kontinuerlig kontakt med tillsynsmyndigheter. Vidare kan Compliance-funktionen rådge i arbetet med att utveckla nya produkter och tjänster samt bistå i utvecklingen av effektiva bevakningsmetoder.

Utbildning
Compliance-funktionen säkerställer att utbildningsprogram och träning tillhandahålls till medarbetarna i syfte att tillse att de har god kännedom om interna policyer, instruktioner och om förändringar i externa regler. Arbetet inkluderar ofta regelbundna utbildningar såväl som ad hoc-utbildningar till följd av regelförändringar eller implementering av nya policyer och/eller instruktioner. Utbildning av nyanställda utgör en viktig del av arbetet. Funktionens roll som rådgivare och samordnare av utbildning skall vara väl förankrad och kommunicerad i verksamheten.

Självständig riskanalys
Compliance-funktionen skall självständigt identifiera, dokumentera och värdera compliance-risker som kan uppstå i den dagliga verksamheten eller vid utvecklingen av nya produkter, affärsområden, processer eller nya kundrelationer. Funktionen skall även reflektera över hur man värderar compliance-risker och bedöma verksamhetens effektivitet vad gäller rutiner och instruktioner för att säkerställa compliance. Då brister upptäcks bör funktionen följa upp bristerna och om möjligt formulera förändringsförslag.

Bevakning
Compliance-funktionen bevakar löpande verksamheten. Dels genom granskning av aktiviteter och dels genom att bevaka transaktioner i syfte att identifiera potentiella problem inom områden så som hantering av kundkonton, insiderhandel av anställda och handel för bankens räkning. Bevakning möjliggör verksamheten att i ett tidigt stadium identifiera aktiviteter där externa och interna regler inte efterlevs. En bank betonar vikten av att bevaka och att följa upp rutiner för att säkerställa att bankens produkter och tjänster följer gällande regler. Vidare skall banken bevaka att åtgärder vidtas och rapporteras om överträdelser av tillämpliga regler skett.

Rapportering
Funktionen skall löpande rapportera compliance-relaterade frågor till styrelsen, ledningen och den verkställande direktören. Rapporteringen bör innehålla information om förändringar i riskprofilen samt sammanställningar av den självständiga riskanalys som utförs. Bland de

svenska affärsbankerna rapporterar Compliance-funktionen vanligen till den verkställande direktören samt informerar styrelsen. Funktionen skall ha möjlighet att eskalera identifierade risker och problem till styrelsen, ledningen och den verkställande direktören. Compliance-cheferna på en bank rapporterar samtliga olagliga händelser (oberoende av den finansiella förlust det medfört), väsentliga överträdelser av bankens värderingar och regler samt andra incidenter som kan orsaka anseendeskada.

Utöver de nämnda huvudaktiviteterna är det vanligt att Compliance-funktioner inom affärsbanker är delaktiga i arbetet med att förhindra penningtvätt och finansiering av terrorism. Compliance-funktionen kan exempelvis vara delaktig i screening av nya kunder och att bevaka transaktioner mellan kunder. Vidare kan Compliance-funktionen administrera licenser.

2.2.2 Organisation och rapportering

Finansinspektionen anser att funktionen bör vara underställd styrelsen eller den verkställande direktören och att den i högsta möjliga mån skall nå självständighet från den affärsdrivande verksamheten. Funktionen kan även vara placerad under en annan ledande befattningshavare som har goda kunskaper om verksamheten och de risker som kan uppstå. Denne skall vara direkt underställd den verkställande direktören.

Många affärsbanker har valt att placera Compliance-funktionen separat från andra funktioner såsom riskkontrollenheten eller den juridiska funktionen. Funktionens uppdrag brukar beskrivas i ett compliance-program där man exempelvis detaljerar vilka aktiviteter och utbildningar man avser att genomföra under året.

För att utföra de aktiviteter som åligger funktionen krävs det att medarbetarna inom funktionen har en god kunskap om verksamhetens risker, processer samt applicerbara regler. Det skall falla sig naturligt för medarbetare att vända sig till Compliance-funktionen för frågor kring lagar, regler etc. Kommunikation mellan riskfunktioner och verksamheten är en förutsättning för att riskhanteringen skall bedrivas effektivt. En affärsbank nämner att medarbetarna måste ge Compliance Officer tillgång till all data som denne efterfrågar. Vidare skall medarbetarna vara mycket samarbetsvilliga. Om Compliance Officer inte har möjlighet att utföra sitt uppdrag måste detta eskaleras till chefen för Compliance-funktionen.

2.3 Statliga myndigheter

Ernst & Young har undersökt hur en handfull statliga myndigheter med kapitalförvaltande eller annan finansiell verksamhet utför compliance-arbete. Flertalet av de statliga myndigheter som undersökts har valt att inrätta en Compliance-funktion trots att man inte har någon skyldighet till detta enligt lag. Anledningen till valet kan exempelvis vara att verksamheten strävar efter att vara lika bra eller bättre än motsvarande kommersiella aktörer i termer av intern styrning och kontroll. En annan anledning kan vara att man agerar på marknader där många aktörer lyder under Finansinspektionens tillsyn och att man av den anledningen väljer att vara tillgodose Finansinspektionens krav.

2.3.1 Aktiviteter

De statliga myndigheterna utför många av de uppgifter som beskrivits för affärsbankerna.

Policyer och instruktioner

En myndighet beskriver att Compliance-funktionen skall identifiera behov av att utveckla och förvalta de operationella, finansiella och etiska policyerna och riktlinjerna. Vidare skall funktionen stödja och utveckla metoder för hantering av policyer och riktlinjer.

Rådgivning och utbildning
Compliance-funktionen skall löpande arbeta med att utbilda medarbetare, utveckla den rådgivning som tillhandahålls och informera verksamheten i externa och interna regelverk. Funktionen skall bevaka förändringar i externa regelverk och praxis. Vidare skall funktionen löpande informera om risker som kan uppkomma till följd av bristande regelefterlevnad. En myndighet inkluderar granskning av avtal, rådgivning vid sekretessprövningar och hantering av incidentrapportering som del av den rådgivande rollen. Då de statliga myndigheterna inte är tillståndspliktiga har inte compliance-funktionen till uppgift att kontinuerligt föra en dialog med tillsynsmyndigheter.

Bevakning
Compliance-funktionen skall följa upp att verksamheten följer externa och interna regelverk. Som del i detta arbete utför funktionen kontinuerligt specifika granskningar såväl som självutvärderingar. Specifika granskningar kan innebära att man testar regelefterlevnad i enskilda affärer. Vidare kan funktionen bevaka att riktlinjer faktiskt fastställs och genomförs.

Självständig riskanalys
Compliance-funktionen hjälper till med att identifiera och bedöma risker. En verksamhet har inrättat ett compliance-forum där medarbetare som är intresserade av regler och lagar får möjlighet att diskutera sina frågeställningar. Forumet har inga formella krav eller mandat, utan syftar till att fånga upp aktuella frågor vilket Compliance Officer därefter kan nyttja i sin riskidentifiering.

Rapportering
Många av de statliga myndigheterna rapporterar sina iakttagelser och riskrapporter löpande till den verkställande direktören och informerar styrelsen på årsbasis eller vid behov. I en myndighet rapporterar Compliance-funktionen årligen till styrelsen och kvartalsvis till en ledningsgrupp för compliance-frågor.

2.3.2 Organisation

Till skillnad från affärsbankerna påvisas många olika strukturer bland de statliga myndigheterna. En statlig myndighet har valt att inrätta en Compliance-funktion där ansvaret fördelas mellan Riskenheten och Juridikenheten. En annan har valt att organisera funktionen som en separat enmansenhet under Chefsjuristen och en tredje har valt att en och samma person skall ansvara för både riskkontrollfunktionen och Compliance-funktionen. Den verksamhet som organisatoriskt ligger under Chefsjuristen framför att det skulle finnas många fördelar med att organisatoriskt tillhöra riskkontrollfunktionen då det finns många likheter mellan de två funktionernas arbetssätt och terminologi. Vidare ställs funktionerna inför likartade frågeställningar. En statlig myndighet har valt att endast inrätta en Compliance-funktion inom kapitalförvaltningen.

Verksamheter med mindre Compliance-funktioner betonar vikten av att samordna uppföljningsaktiviteter med andra kontrollfunktioner för att nyttja resurserna så effektivt som möjligt. För att säkerställa funktionens inflytande har exempelvis en myndighet valt att compliance-chefen skall ingå i ledningsgrupper och olika kommittéer.

2.4 Centralbanker

Nedan följer en sammanställning av observationer från ”The Emergence of a Formal Compliance Function Within European National Central Banks” och ”Stocktaking on the Organisation of the Compliance Function”. Den förstnämnda studien bygger på ett antal frågor som Luxemburgs centralbank ställde till samtliga medlemmar av ESBC i november 2007. Den senare bygger på antal frågor som Organisational Analysis Working Group (OWG), på uppdrag av ECB, ställde till samtliga centralbanker inom euro-området, 3 centralbanker utanför euro-området och 2 institutioner i april 2010.

- Förståelsen för vad compliance är och vad det innefattar skiljer sig mellan centralbankerna. Vidare råder det delade meningar om hur compliance-frågor skall hanteras och organiseras i praktiken.
- Flertalet centralbanker adresserar inte compliance i en specifik policy. Compliance-relaterade frågor integreras istället i en mängd policyer och instruktioner. Endast centralbankerna i Nederländerna, Belgien, Portugal och Grekland har stipulerat en specifik compliance-policy
- Majoriteten av centralbankerna anser att compliance inom centralbanker framförallt handlar om regelefterlevnad av etiska riktlinjer. En centralbank har gett Compliance-funktionen i uppgift att dagligen bevaka regelefterlevnad av interna regler, sekretesspolicyn och marknadsmissbruk. En annan centralbank har valt att fokusera på marknadsmissbruk, representation och bisysslor. Många av centralbankerna anser även att penningtvätt och finansiering av terrorism bör vara del av compliance.
- Många centralbanker har decentraliserat compliance-funktionaliteten i organisation, dvs. att aktiviteterna utförs av många funktioner. Ett antal centralbanker anser att compliance-risker kan hanteras i den övergripande riskkontrollen. Andra centralbanker väljer att inrätta en eller flera Compliance Officers som utför hela eller specifika delar av uppdraget.
- Rapportering av compliance-frågor och iakttagelser sker framförallt i samband med Riskfunktionens rapportering.

3 Kartläggning av nuläge inom riksbanken

Compliance-relaterade aktiviteter utförs i stor utsträckning inom Riksbanken redan idag och en funktion för regeluppföljning har etablerats inom Riskenheten. Compliance-aktiviteter utförs dock av ett flertal funktioner och roller och ansvarsfördelningen är inte helt känd i verksamheten.

3.1 Funktionen för regeluppföljning

I den uppdragsbeskrivning för funktionen för regeluppföljning som stabschefen beslutat framgår att funktionen skall ge stöd till verksamheten i dess styrning och kontroll av risken för bristande regelefterlevnad. Vidare skall funktionen följa upp att verksamheten bedriver styrning och kontroll av regelefterlevnadsrisker på ett ändamålsenligt och betryggande sätt. Uppdragsbeskrivningen stipulerar att risken med bristande regelefterlevnad skall analyseras dels avseende de externa regler verksamheten har att följa i genomförandet av verksamhetsmålen och dels i interna bankövergripande regelverk såsom etiska riktlinjer, kommunikationspolicyn, regler om offentlighet och sekretess, miljöpolicyn etc. De aktiviteter som omnämns i uppdragsbeskrivningen beskrivs i tabellen nedan.

Aktivitet	Beskrivning
Stöd	Erbjuda stöd till verksamheten i form av information och utbildning om gällande och kommande regler. Funktionen tar stöd från andra delar av verksamheten eller externt vid behov.
	Rådge verksamheten kring processen för hantering av risken för bristande regelefterlevnad (analys, kontroll, uppföljning och dokumentation) om det efterfrågas.
Riskanalys och regler	Erbjuda stöd till verksamheten avseende regelefterlevnad utifrån avdelningarnas riskanalyser.
Uppföljning och granskning	Verka för uppföljning av verksamhetens arbete med att begränsa risken för bristande regelefterlevnad. Granskningar kan utföras om det bedöms nödvändigt.
Rapportering	Kvartalsvis rapportering till stabschef för vidarebefordran till ledningsgruppen. Rapporteringen i januari och juni skall regelmässigt delges Riksbankschefen genom stabschefen. Rapporteringen skall innehålla en bedömning av rådande status vad gäller risken för bristande regelefterlevnad och bedömning av avdelningarnas rapporter. Januarirapporten skall även inkludera ett förslag till skrivning inför intygandet om intern styrning och kontroll avseende risker med bristande regelefterlevnad i samband med årsredovisningen.

Avseende stöd vid regeltolkning eller annat materiellt stöd hänvisar uppdragsbeskrivningen till interna jurister[3]. Dessa har exempelvis till uppgift att bistå med avtalsdokumentation, rättsutredningar, sekretessprövningar etc. Vid rådgivning kring processen för riskhantering framgår det i uppdragsbeskrivningen att respektive avdelning skall upprätta en förteckning över de externa lagar och förordningar man tillämpar och att regeluppföljningsfunktionen har i uppgift att erbjuda rådgivning även i utförandet av den uppgiften.

De uppgifter som huvudsakligen utförs av funktionen för regeluppföljning i nuläget är juridiskt stöd, förvaltning av det interna regelverket och säkerställande av att förteckningen över de externa regler som avdelningarna lyder under och tillämpar uppdateras kontinuerligt. Uppföljning och granskning av avdelningarnas regelefterlevnad, stöd i riskhanteringsprocessen, självständig riskanalys samt rapportering utförs av Riskenheten, detta sker dock inte i någon större utsträckning.

3.2 Compliance-aktiviteter i Riksbanken

De compliance-relaterade aktiviteter som identifierats i verksamheten, oberoende av utförare, beskrivs i tabellen nedan.

Aktivitet	Nuläge i Riksbanken
Säkerställa att det interna regelverket uppfyller gällande regelverk	Respektive utgivare av interna regler ansvarar för att uppdatera och säkerställa efterlevnad. Ingen oberoende kontroll utförs idag. Funktionen för regeluppföljning förvaltar strukturen och utveckling av det interna regelverket.
Bistå med rådgivning i compliance-relaterade frågor	Jurister ger råd i compliance-relaterade frågor, exempelvis sekretessfrågor och säkerställande att Direktionens och fullmäktiges beslut görs i enlighet med gällande regelverk. Avdelningsjuristerna, inklusive Chefsjuristen, möts regelbundet för informella samtal om legala frågor och risker.
Vid behov tillhandahålla utbildning i compliance-frågor och regel-efterlevnad	Jurister utbildar i interna och i relevanta externa regelverk, t.ex. etiska regler, informationssäkerhet och penningtvätt. Nyanställda utbildas vid anställningstillfället men mer kontinuerlig utbildning efterfrågas.
Självständig analys	Compliance-risker ingår i den ordinarie riskhanteringsprocessen där ansvaret ligger på avdelningscheferna. Riskenheten bidrar med att på en aggregerad nivå värdera compliance-risk.
Följa upp regel-efterlevnad och rapportera överträdelser	Avdelningschefer ansvarar för att verksamheten bedrivs enligt gällande lagar och regler. I sitt arbete har de stöd från avdelningsjurister. Stabsjurist initierar och säkerställer uppdatering av listor som stipulerar relevanta regelverk. Ingen oberoende kontroll utförs idag.
Rapportering av compliance-risker.	Rapportering av compliance-risker ingår i Riskenhetens rapportering.

De ovan nämnda aktiviteterna är framförallt stödjande, kontrollerande aktiviteter relaterade till regelefterlevnad utförs i begränsad omfattning i verksamheten idag.

[3] I den ursprungliga uppdragsbeskrivningen hänvisas till rättsenheten men efter en omorganisation finns ej denna enhet kvar utan juristerna är hemmahörande i avdelningarna.

3.3 Compliance-risker i Riksbanken

Ledande befattningshavare verkar för att bygga en sund riskkultur. Medarbetare anser kulturen vara präglad av eftertänksamhet, integritet och lojalitet, vilket är bra för att eftersträva regelefterlevnad. Chefer och medarbetare är överens om att regelefterlevnad är viktig för Riksbankens verksamhet och anseende medan risken för monetära förluster är begränsad. Nedan följer några exempel på bristande regelefterlevnad som kan leda till försämrat anseende för Riksbanken:

- Oetiska/olagliga bisysslor
- Bristfällig hantering av konfidentiellt material
- Bristande diarieföring
- Bestickning
- Insiderhandel genom nyttjande av information relaterat till policy-arbetet
- Bristfällig hantering av finansiella processer inom KAP
- Brott mot lagen om offentlig upphandling
- Bristfällig hantering vid ansökningsförfaranden
- Egen handel i bankaktier
- Bristfällig hantering av outsourcing-förfaranden

Ovanstående exempel kan indelas i ett antal riskområden för vilka regelefterlevnad är viktigt. Dessa områden åskådliggörs i tabellen nedan. Generellt ansvarar respektive avdelningschef för riskerna i sin verksamhet och att relevanta lagar, regler, policyer etc. efterlevs.

Riskområde	Nuläge i Riksbanken
Externa regler	Ansvaret i termer av att säkerställa regelefterlevnad och identifiera gällande regelverk samt förändringar i dessa ligger på avdelningscheferna. Respektive avdelning har egna jurister som utför arbetet och stödjer avdelningscheferna. Uppföljning av gällande externa regler och lagar görs årligen av avdelningarna, eller ad hoc om en förändring skulle ske. Stabsjurist påminner och följer upp genomförandet. Ingen formaliserad process eller struktur för att säkerställa genomförandet existerar.
	Vid affärsförändringar hos KAP genomförs ett ansökningsförfarande där avdelningsjuristerna ser till att regelverk efterlevs. Större affärsförändringar kräver beslut av Direktionen eller fullmäktige och stabsjuristerna ansvarar för att dessa beslut efterlever gällande lagar och regler.
Affärsverksamhet och etik	Ansvaret för att ta fram det etiska regelverket ligger på STA, bisysslor rapporteras till Chefsjuristen och vid tveksamhet om bisysslan är förenlig med anställningen på Riksbanken tillåts den ej.
Organisatorisk struktur	Stabsjuristerna ansvarar för uppdatering av instruktion och arbetsordning (som beslutas av Direktionen respektive FUM). En bristande kännedom om instruktionen hos enhetschefer har identifierats och det finns ett behov av mer löpande utbildning. Uppföljning av att det interna regelverket efterlevs utförs inte i någon större utsträckning.
Outsourcing	Upphandlingsjurister hos ADM bistår med rådgivning vid upphandlingar. Ingen generell process/ kriterier existerar för vad man bör se över vid uppföljning av outsourcing parter.
Hantering av känsligt material	Varje handläggare ansvarar för att sekretessprövning görs vid behov, avdelningsjurist samt Chefsjurist/stabsjurist rådger i sekretess- och offentlighetsfrågor. Riskenheten ansvarar för ramverket för informationshantering. Ramverket är idag komplext vilket ökar risken för att medarbetare inte efterlever det som stipulerats. Stabsjuristen påminner även om, och för förteckning över, var personuppgifter finns registrerade.

Diarieföring	Det finns ingen formaliserad process för att följa upp att diarieföringen utförs på ett ändamålsenligt sätt.
Marknads-missbruk och insiderhandel	Löpande rapportering av anställdas egenhandel sker till Chefsjuristen (påminnelse går ut årsvis). Avdelningschefer anger vilka medarbetare som ska rapportera innehav. Inga stickprovskontroller utförs för närvarande.
Processen för handel av värdepapper	KAP ansvarar för att processerna utförande och handläggning följer gällande regelverk. Nya rutiner och regeländringar går via ansökningsförfarandet.

4 Relevanta compliance-områden för Riksbanken

Riksbankens styrning skiljer sig från svenska affärsbanker och statliga myndigheter samt andra centralbanker i euro-området i det att antalet externa regelverk som är tvingande för banken är begränsat och kraven på det interna regelverket är få. Riksbankens verksamhet är inte tillståndspliktig och den styrs huvudsakligen av Riksbankslagen och Förvaltningslagen. Riksbanken följer också de delar av ECB:s regelverk som är applicerbara på europeiska centralbanker utanför euro-området.

De konsekvenser som bristande compliance kan leda till för Riksbanken är ryktesförluster som kan resultera i minskat förtroende. Eftersom Riksbanken är helt beroende av sitt anseende för att kunna bedriva policyverksamhet är god compliance av stor vikt för banken. Några av de riskområden som är viktiga för affärsbanker och andra centralbanker är inte relevanta för Riksbanken på grund av hur verksamheten är beskaffad. Exempelvis har Riksbanken endast banker som kunder, så konsumentskydd saknar betydelse och det gör även lagarna om penningtvätt och terroristfinansiering samt kunders transaktioner med sanktionerade länder.

De compliance-områden som är relevanta för Riksbankens verksamhet är:

Riskområde	Exempel på styrande dokument
Externa regler	• Tillämpliga lagar, industristandarder, regler och tillstånd • Checklista för affärsförändringar, nya produkter, processer, etc.
Organisatorisk struktur	• Arbetsordning och instruktion • Organisation, roller/funktioner • Rapporteringslinjer, eskaleringsprocess, delegering av beslutsrätt
Outsourcing	• Krav på outsourcingleverantör • Organisation kring avtal/samarbete
Hantering av känsligt material	• Offentlighets- och sekretesslagen • Regler för skydd av personliga uppgifter

Marknadsmissbruk och insiderhandel	• Regler för:
	  • Egenhandel
	  • Marknadsmissbruk

Process för handel av värdepapper	• Processbeskrivning Utförande • Processbeskrivning Handläggning
Affärsverksamhet och etik	• Etiska regler (”uppföranderegler”) • Övriga regelverk (bedrägeri, mutor, arbete utanför tjänst, anställdas innehav, egenintresse och intressekonflikter, etc.)
Diarieföring	• Offentlighets- och sekretesslagen

4.1 Avgränsning i Compliance-funktionens ansvarsområden

Compliance uppdrag är att tillse att riskerna för bristande efterlevnad av ovanstående styrande dokument hanteras på lämpligt sätt. Det ingår inte i uppdraget att tillse att dokumenten existerar eller att författa dem. Däremot skall Compliance-funktionen påpeka om viktiga styrande dokument saknas. Exempelvis avseende organisatorisk struktur övervakar Compliance-funktionen att verksamheten hanterar risken för att beslut fattas av individer som ej har mandat att fatta dem enligt gällande delegeringsordning och kan kommentera om delegeringsordningen är otillräcklig eller otydlig, däremot är det upp till verksamheten att författa delegeringsordning i linje med arbetsordning och instruktion.

Ett annat exempel är outsourcing, när verksamhet outsourcas är det väsentligt att leverantören efterlever samma uppsättning regler som Riksbankens egna anställda eftersom bristande regelefterlevnad hos outsourcing-leverantören drabbar Riksbanken. Compliance-funktionen, tillsammans med Riskenheten, deltar i outsourcingprocessen och godkänner de kontroller som beslutas samt att tillräcklig kompetens finns kvar hos Riksbanken för att korrekt kunna bedöma de upphandlade tjänsterna. Därefter övervakar Compliance-funktionen efterlevnaden under avtalens löptid. Däremot kan ansvaret för att tillse att Riksbanken efterlever Lagen om offentlig upphandlig ligga kvar hos de upphandlingsjurister som finns inom Administrativa avdelningen.

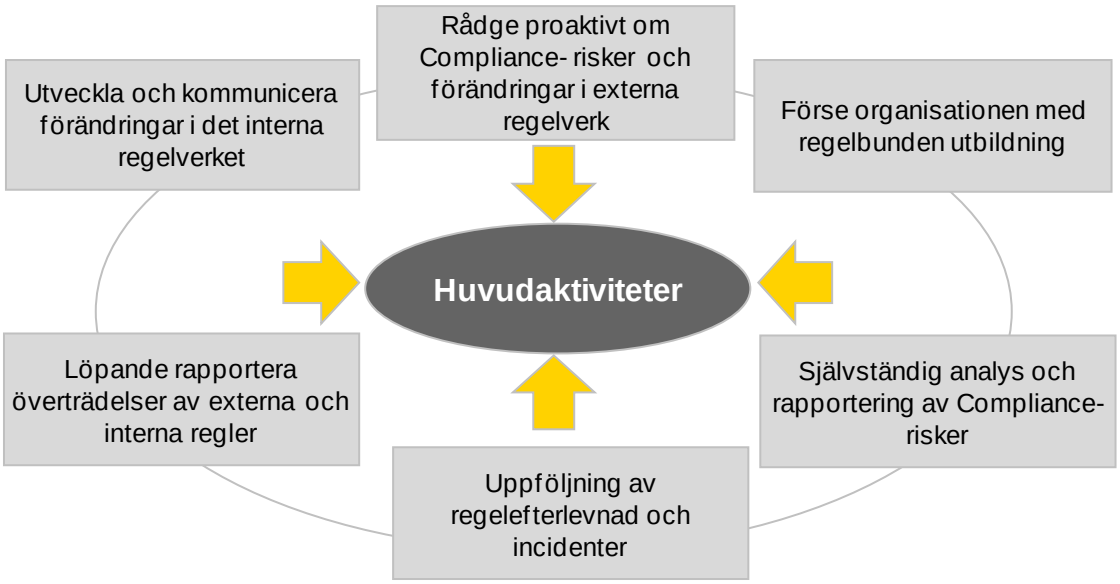
Utöver de riskområden som beskrivs i tabellen ovan finns det en rad ytterligare riskområden inom Riksbanken, som ej ingår inom ramen för uppdraget för en Compliance-funktion. Exempel på riskområden utanför compliance-området är:

- Försäkring
- Personal
- Redovisning
- Skatter
- Kreditrisk
- Marknadsrisk

Som konsekvens ligger även de externa regelverken som styr ovanstående risker, t.ex. LAS, Redovisningsregler etc. utanför Compliance-funktionens ansvarsområde. Legala risker i de kontrakt som Riksbanken skriver med externa parter ingår inte heller i Compliance-funktionens uppdrag.

5 Relevanta compliance-aktiviteter för Riksbanken

Compliance inom Riksbanken bör agera både rådgivande och uppföljande, de sex huvudaktiviteterna åskådliggörs i bilden nedan.



För respektive aktivitet finns ett antal relevanta underaktiviteter som compliance bör utföra för de compliance-riskområden som är tillämpliga för Riksbanken:

Utveckla och kommunicera förändringar i det interna regelverket:

- Assistera verksamheten i att utveckla policyer och regler
- Utveckla regler och rutinbeskrivningar för Compliance-funktionen
- Initiera och säkerställa att process existerar för hantering av beslut avseende vilka externa regelverk och delar därav som Riksbanken bör följa
- Förvalta och utveckla strukturen för det interna regelverket, inklusive mallar för policyer, regler och rutinbeskrivningar

Rådge proaktivt om compliance-risker och förändringar i externa regelverk:

- Rådge verksamheten i frågor kring applicerbara regler, förordningar, policyer, standarder etc.
- Löpande informera om risker som kan uppstå till följd av bristande regelefterlevnad
- Rådge kring design av åtgärder för att hantera compliance-risker
- Säkerställ att en fungerande process finns för att tillse att avdelningschefer har kännedom om ändringar och kommande ändringar i externa och interna regelverk och rådge verksamheten

Förse organisationen med regelbunden utbildning

- Säkerställa att introduktionsutbildning tillhandahålls för nyanställda
- Säkerställa att utbildningsprogram och träning tillhandahålls på löpande basis
- Säkerställa att utbildning sker ad hoc för att säkerställa vetskap kring förändringar i externa och interna regler

Självständig analys och rapportering av compliance-risker

- Ta fram en plan för hantering av materiella compliance-risker som uppdateras årsvis och följs upp regelbundet
- Oberoende identifiera, värdera och dokumentera compliance-risker associerade till den dagliga verksamheten
- Oberoende identifiera, värdera och dokumentera compliance-risker associerade med utveckling av produkter, processer, affärsområden, nya kundrelationer eller förändring i existerande relationer

Uppföljning av regelefterlevnad och incidenter

- Löpande bevaka att verksamheten efterlever interna och externa regler genom granskning av aktiviteter och transaktioner
- Bedöma verksamhetens effektivitet vad gäller rutiner och instruktioner för att säkerställa compliance
- Följa upp brister relaterat till effektivitet och om möjligt formulera förändringsförslag
- Följa upp compliance-incidenter

Löpande rapportera överträdelser av externa och interna regler

- Löpande rapportera compliance-relaterade frågor (förändringar i riskprofilen, incidenter sammanställning av självständig riskanalys etc.) till närmaste chef
- Tertialvis rapportera compliance-relaterade frågor (förändringar i riskprofilen, incidenter, sammanställning av självständig riskanalys etc.) till Direktionen

5.1 Utförare av compliance-aktiviteter

Ovan nämnda aktiviteter bör utföras hos Riksbanken, dock behöver inte en Compliance-funktion kunna utföra alla aktiviteter själv utan även andra funktioner inom Riksbanken bör bidra i compliance-arbetet. Exempelvis i att utbilda kring externa och interna regelverk samt att bistå Compliance-funktionen med expertkompetens vid behov.

6 Gapanalys och förbättringsområden

Nedan beskrivs gap mot de compliance-aktiviteter som Ernst & Young rekommenderar Compliance inom Riksbanken att utföra för de riskområden som ligger inom Compliance ansvarsområde.

Aktivitet	REG[4]	Utförare[5]	Gap	Aktiviteter för att stänga gap
Utveckla och kommunicera förändringar i det interna regelverket				
Assistera verksamheten i att utveckla policyer och regler	JA	REG	• Regeluppföljnings-funktionen involveras ej i tillräcklig utsträckning och saknar förankring i verksamheten • Saknas samsyn kring vilka externa regelverk som Riksbanken skall följa • Rutinbeskrivningar i Riksbanken är ej homogena avseende innehåll	• Ta fram och förankra uppdragsbeskrivning för Compliance inklusive, ansvars-områden och aktiviteter • Definiera och implementera en process för att besluta vilka externa regelverk som Riksbanken bör följa och för att införliva dem i den interna regelverksstrukturen • Förankra och genomdriv krav på hur innehåll i policyer och regler skall utformas
Utveckla policyer och rutinbeskrivningar för Compliance-funktionen	JA	STA		
Initiera och säkerställa att process existerar för hantering av beslut avseende vilka externa regelverk och delar därav som Riksbanken bör följa	NEJ	UTFÖRS EJ		
Förvalta och utveckla strukturen för det interna regelverket, inklusive mallar för policyer, regler och rutinbeskrivningar	NEJ	REG		
Rådge proaktivt om compliance-risker och förändringar i externa regelverk				
Rådge verksamheten i frågor kring applicerbara regler, förordningar, policyer, standarder etc.	JA	REG/ JUR	• Otydlighet kring vem som rådger för vilka lagar, regler etc. • Riskenheten kan rådge i vissa compliance-relaterade frågor, men detta har inte nyttjats av verksamheten • Saknas process för att säkerställa att avdelningarna har kännedom om förändringar	• Tydliggör ansvar för rådgivning i Compliance-funktionens uppdragsbeskrivning • Förankra Compliance rådgivande roll och tillse att man har tillgång till kompetens inom sina ansvarsområden • Definiera och implementera en process för Compliance rådgivande roll
Löpande informera om risker som kan uppstå till följd av bristande regelefterlevnad	NEJ	UTFÖRS EJ		
Rådge kring design av åtgärder för att hantera compliance-risker	JA	UTFÖRS EJ		
Säkerställ att en fungerande process finns för att tillse att avdelningschefer har kännedom om ändringar och kommande ändringar i externa och interna regelverk och rådge verksamheten	NEJ	A-JUR		

[4] Beskrivs i uppdragsbeskrivningen för regeluppföljningsfunktionen

[5] REG=Funktionen för regeluppföljning, RIE=Riskenheten, STA=Stabsavdelningen, S-JUR=Stabsjurister, A-JUR=Avdelningsjurister

Aktivitet	REG	Utförare	Gap	Aktiviteter för att stänga gap
Förse organisationen med regelbunden utbildning				
Säkerställa att introduktionsutbildning tillhandahålls för nyanställda	NEJ	RIE/ STA	• Det finns områden där utbildning inte sker, exempelvis representation och tjänsteresor • Behov av mer löpande utbildning • Saknas en samordnande roll för utbildning inom riskområden för Compliance	• Tydliggör Compliance ansvar avseende samordning av utbildning i uppdrags-beskrivningen • Fastställ för vilka av riskområden utbildningsbehov finns • Ta fram en utbildningsplan • Utse utbildare för respektive riskområde
Säkerställa att utbildningsprogram och träning tillhandahålls på löpande basis	NEJ	RIE/ JUR		
Säkerställa att utbildning sker ad hoc för att säkerställa vetskap kring förändringar i externa och interna regler	JA	RIE/ S-JUR		
Självständig analys och rapportering av compliance-risker				
Ta fram en plan för hantering av materiella compliance-risker som uppdateras årsvis och följs upp regelbundet	NEJ	UTFÖRS EJ	• Compliance-plan saknas • Idag utförs knappt någon självständig analys av compliance-risker	• Ta med Compliance i den operativa riskhanterings-processen
Oberoende identifiera, värdera och dokumentera compliance-risker associerade till den dagliga verksamheten	NEJ	RIE		
Oberoende identifiera, värdera och dokumentera compliance-risker associerade med utveckling av produkter, processer, affärsområden, nya kundrelationer eller förändring i existerande relationer	NEJ	UTFÖRS EJ		
Uppföljning av regelefterlevnad och incidenter				
Löpande bevaka att verksamheten efterlever interna och externa regler genom granskning av aktiviteter och transaktioner	JA	UTFÖRS EJ	• Endast incidenter inom regelefter-levnad följs upp	• Definiera behov av uppföljning och vilka kontroller som skall genomföras
Bedöma verksamhetens effektivitet vad gäller rutiner och instruktioner för att säkerställa compliance	JA	UTFÖRS EJ		
Följa upp brister relaterat till effektivitet och om möjligt formulera förändringsförslag	JA	UTFÖRS EJ		
Följa upp compliance-incidenter	NEJ	RIE		

Aktivitet	REG	Utförare	Gap	Aktiviteter för att stänga gap
Löpande rapportera överträdelser av externa och interna regler				
Löpande rapportera compliance-relaterade frågor (förändringar i riskprofilen, incidenter sammanställning av självständig riskanalys etc.) till närmaste chef	JA	RIE	• Compliance-risker rapporteras ej i någon större utsträckning.	• Inkludera compliance-risker i den operativa rapporteringen
Tertialvis rapportera compliance-relaterade frågor (förändringar i riskprofilen, incidenter, sammanställning av självständig riskanalys etc.) till Direktionen	JA	RIE		

7 Organisation för Compliance-funktionen i Riksbanken

Riksbanken lyder inte under FFFS 2005:1 vilket innebär att man har större spelrum för hur man väljer att organisera Compliance-funktionen än vad affärsbanker har. Affärsbankerna har dock under lång tid arbetat med utformningen av sina Compliance-funktioner vilket Riksbanken kan dra lärdom från. Compliance-funktionen inom Riksbanken bör organiseras så att det möjliggör effektivt och rationellt compliance-arbete.

Alternativen som beskrivs nedan är tre vanligt förekommande strukturer bland affärsbanker och statliga myndigheter (omsatta till Riksbankens verksamhet). Den person eller personer som oberoende och självständigt utför compliance-aktiviteter såsom en Compliance Officer benämns nedan Compliance-funktion.

De tre alternativen är snarlika i termer av att Compliance-funktionen placerats i stabsavdelningen, vars avdelningschef är direktunderställd Direktionen och agerar självständigt från den operativa verksamheten. Ernst & Young uppfattar att Riskenheten har möjlighet att utföra sitt uppdrag självständigt och oberoende från verksamheten givet sin placering i stabsavdelningen och detsamma skulle gälla för en Compliance-funktion.

För att Compliance-funktionen skall kunna utföra de uppgifter som detaljerats ovan är nuvarande resurser inte tillräckliga[6]. Ernst & Young rekommenderar att Compliance-funktionen skall bestå av 1-2 heltidstjänster för att kunna fullgöra sitt uppdrag. Den Compliance Officer som tillsätts skall ha möjlighet att eskalera frågor direkt till Direktionen samt formellt rapportera till Direktionen. Förslagsvis skall Compliance-funktionens iakttagelser rapporteras i den tertialvisa riskrapporteringen.

Ernst & Young rekommenderar att Compliance-funktionen integreras med Riskenheten[7] (alternativ 1 i nedanstående bild) av tre huvudsakliga anledningar:

1) Riskenheten och Compliance-funktionen ansvarar för två olika riskuniversum men deras rekommendationer till verksamheten kommer i viss utsträckning att sammanfalla. Placeras Compliance-funktionen i Riskenheten kan de på ett naturligt sätt arbeta med samma definitioner, processer, cykler, rapportering etc. Till exempel kan riskanalysen för operativa risker och compliance-risker samordnas.
2) 1-2 heltidstjänster motiverar inte skapandet av en separat funktion med den dubblering och ineffektivitet som medföljer.
3) Ytterligare en omorganisation av Riskenheten för att separera ut compliance-risker medför onödig turbulens och oro.

De andra alternativ som utretts är att inrätta en separat Compliance-funktion alternativt att placera en Compliance-funktion rapporterandes till Chefsjuristen.

En separat Compliance-funktion (alternativ 2 i nedanstående bild) blir synlig i organisationen men innebär att man försämrar möjligheten att samordna Riskenhetens och Compliance-funktionens arbete. Möjligheten till koordinering med Riskenheten försämras även om man organiserar Compliance-funktionen under Chefsjuristen (alternativ 3 i nedanstående bild).

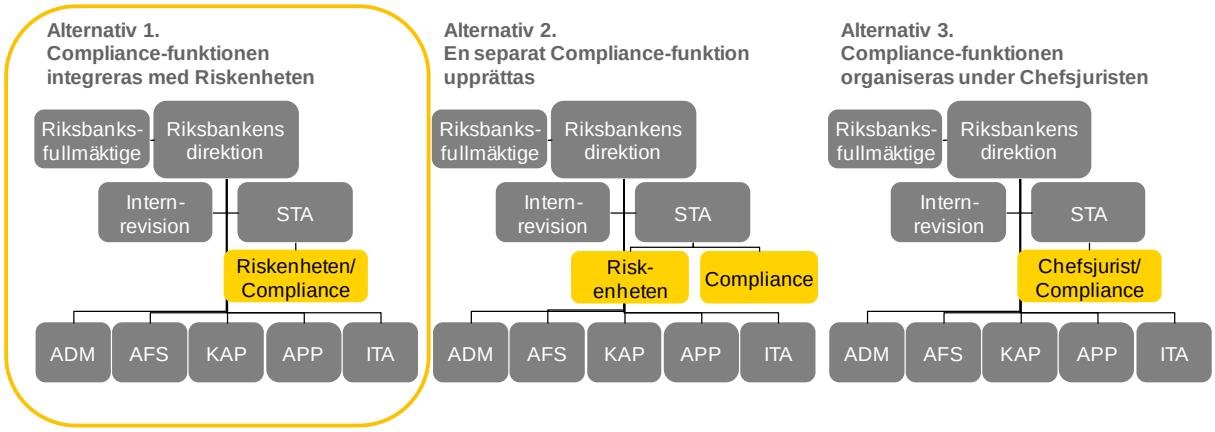
---

[6] På papperet utgörs regeluppföljningsfunktionen av en heltidstjänst, men de två individer som innehar de halvtidstjänster som tillsammans skall utgöra en heltid har ej haft möjlighet att lägga den tiden.

[7] Även för tillståndspliktig verksamhet godkänner Finansinspektionen att funktionen för riskkontroll och funktionen för regelefterlevnad utförs gemensamt i mindre företag om det är alltför kostsamt att separera funktionerna men ställer då särskilda krav på att riskerna för intressekonflikter hanteras. Källa: Finansinspektionens Tillsynsrapport 2011.

Vidare innebär alternativ 3 att Compliance-funktionen organiseras under en enmansfunktion som ej är resurssatt för att ha fler rapporterande områden.

Oberoende av organisation är det av yttersta vikt att Riksbanken verkar för att kontrollfunktionerna skall ges det mandat och inflytande som krävs för att funktionerna skall kunna utföra sitt arbete på ett ändamålsenligt sätt. Detta innebär att avdelningarna måste acceptera den kontrollerande roll som Riskenheten och Compliance-funktionen bör ha.



Alternativ 1. Compliance-funktionen integreras med Riskenheten

Fördelar

- Möjliggör effektivt resursutnyttjande genom att koordinera arbetet
- Ingen organisatorisk förändring
- Möjliggör för de två funktionerna att dra lärdom av varandra och göra en gemensam riskanalys

Nackdelar

- Lång rapporteringsväg till Direktionen kan hämma oberoende
- Compliance-funktionen blir mindre tydlig i organisationen
- Risk för att Compliance-funktionen kontrollerar sig själv

Alternativ 2. En separat Compliance-funktion upprättas

Fördelar

- Förstärker och tydliggör oberoendet. Compliance-funktionen synliggörs i organisationen
- Marknadspraxis bland banker, det finns även statliga myndigheter som valt att inrätta en separat Compliance-funktion
- ”Compliance-kunskap” koncentreras till en specialistfunktion

Nackdelar

- Risk för mindre effektivt resursutnyttjande till följd av sämre möjlighet att koordinera arbetet
- Organisatorisk förändring som kräver ytterligare resurser och kommer ta tid att förankra i verksamheten
- Motstånd i organisationen till att inrätta ytterligare en ”kontrollfunktion”

- Risk att avdelningarna upplever att den separata Compliance-funktionen säkerställer att alla inom Riksbanken följer externa lagar och interna policyer och regler

Alternativ 3. Compliance-funktionen organiseras under Chefsjuristen

Fördelar

- Juridisk kompetens är viktig i ett flertal compliance-frågor
- Juristerna utför många rådgivande compliance-aktiviteter idag

Nackdelar

- Juristerna är decentraliserade så det finns ingen naturlig hemvist för en Compliance-funktion hos Chefsjuristen
- Compliance-funktionen blir mindre tydlig i organisationen
- Risk för minskat samarbete med Riskenheten

8 Rekommendation

Ernst & Young rekommenderar Riksbanken att sätta upp en Compliance-funktion med organisation, ansvarsområden och aktiviteter enligt förslag i avsnitt 4-7 i rapporten. Regelefterlevnad i en organisation uppnås bäst där ledningen verkar för en stark kultur av individuellt ansvarstagande och där medarbetare förstår nyttan av regelefterlevnad.

En stark Compliance-funktion kan bidraga till att verka för en sådan kultur. Funktionen för regeluppföljning som sattes upp i Riksbanken 2008 är ej etablerad i organisationen och har ett otydligt uppdrag. Fördelar med att etablera en Compliance-funktion i Riksbanken med föreslagna ansvarsområden är:

- Tydlig ansvarsfördelning kring regelefterlevnad
- En oberoende funktion som följer upp delegerat ansvar i Riksbanken
- En stödjande och uppföljande funktion som ger mervärde till verksamheten

De viktigaste framgångsfaktorerna för att etablera effektiv och stark regelefterlevnad i Riksbanken beskrivs nedan.

8.1 Framgångsfaktorer

Tydligt definierat mandat för Compliance Officer som är väl förankrat hos Direktionen och avdelningscheferna

De compliance-relaterade aktiviteter som i dagsläget utförs är mestadels av rådgivande karaktär och Riskenheten beskriver att de har mötts av ett motstånd till uppföljning och kontroll i organisationen. I intervjuer har Ernst & Young noterat att verksamheten tycks oroa sig för att kontroller ska vara resurskrävande och man har upplevt att flertalet granskare har efterfrågat likartade uppgifter (Internrevision, Riksrevision, fullmäktiges revisorer och Riskenheten). Nyttan av compliance-kontroller har inte heller kommunicerats och det finns få historiska incidenter som motiverar kontroll.

Ernst & Young vill betona vikten av att utföra de uppföljande och kontrollerande aktiviteterna som beskrivits för att säkerställa en effektiv och adekvat hantering av compliance-risker. Det är av stor vikt att Compliance Officer inom Riksbanken får ett tydligt mandat att utföra kontroller och att detta är väl förankrat hos både Direktionen och avdelningscheferna. Vår erfarenhet är att även kontrollerande aktiviteter med tiden kommer att betraktas som positiva och stödjande för verksamheten.

Exempel på kontroller som Compliance Officer kan genomföra är att tillse att avdelningarna på ett tillfredsställande sätt säkerställer efterlevnad av instruktion och delegeringsordning och att identifiera gap mellan styrande dokument och verksamhetens beteende. Compliance Officer kan även tillse att avdelningarna säkerställer efterlevnad av regler för anställdas egenhandel samt de eventuella externa regelverk man beslutat att efterleva i det dagliga arbetet. Compliance Officer kan verifiera att tillräckliga kontroller implementerats i processerna och att de är dokumenterade i processbeskrivningar. Compliance Officer har även en naturlig roll i exempelvis ansökningsprocessen.

En Compliance Officer med det mandat och ansvarsområde som Ernst & Young rekommenderar kommer ej utföra kontroller av avvecklingslimiter i Dimension.

Tillsätt en Compliance Officer med rätt kompetens för rollen

Den person som tillsätts som Compliance Officer måste ha nödvändiga kvalifikationer, erfarenhet och ”personlighet” för rollen. Han eller hon behöver ha en övergripande förståelse för Riksbanken och dess verksamhet samt förstå relevanta lagar och regler.

Rätt person på rätt plats kan göra Compliance-funktionen till en stödfunktion som avdelningschefer och medarbetare naturligt går till vid behov, vars kontrollerande och uppföljande roll betraktas som ett led i avdelningschefernas arbete med att förbättra sin verksamhet.

Compliance Officer skall ha en direkt rapporteringsväg till Direktionen

För att säkerställa Compliance Officers oberoende skall denne ha en direkt rapporteringsväg till Direktionen.

- Det är viktigt att Compliance Officer har en formell rapporteringsväg direkt till Riksbankschefen för att minska beroendet av Compliance Officers bedömning av huruvida en risk eller incident skall eskaleras. En välfungerande tertialrapportering i kombination med rätten att eskalera frågor direkt till Riksbankschef eller Direktion kan fylla detta syfte. Riksbanken bör dock regelbundet utvärdera att Compliance Officers rapportering till Direktionen och Riksbankschefen fungerar tillfredsställande.
- Utöver rapportering till Riksbankschef bör Compliance Officer ha en regelbunden kommunikation med avdelningarna, detta förbättrar informationsflödet och kan även stärka compliance roll gentemot verksamheten.

Följ upp Compliance Officer utifrån en årlig compliance-plan

Compliance Officers första uppdrag bör vara att ta fram en compliance-plan för vad som ska genomföras under året. Direktionen skall besluta planen och ledningsgruppen informeras. Exempel på innehåll i planen är:

- De viktigaste compliance-riskerna för Riksbanken
- Hur första, andra och tredje ansvarslinjen hanterar riskerna
- Kontroller och uppföljning som compliance skall genomföra
- De utbildningar som man avser att genomföra

Compliance Officer bör sedan följas upp gentemot den lagda planen för att verifiera att uppdraget utförs som planerat och att tillräckliga resurser läggs.

9 Implementeringsplan

Implementeringen av en Compliance-funktion föreslås ske i tre steg:

Bered mandat och uppdragsbeskrivning för Compliance officer

- Definiera ansvarsområden och aktiviteter utifrån förslag i rapport
- Förankra hos ledningsgrupp
- Förankra hos Direktion

Uppdragsbeskrivning och mandat beslutas av Direktionen

Tillsätt Compliance Officer

Ta fram rollprofil, Compliance Officer ska bland annat:

- Definiera och implementera en process för att besluta vilka externa regelverk som Riksbanken bör följa och för att införliva dem i den interna regelverksstrukturen
- Förankra och genomdriva krav på hur innehåll i policyer och regler skall utformas
- Förankra Compliance rådgivande roll och tillse att man har tillgång till kompetens inom sina ansvarsområden
- Inkludera compliance-risker i den operativa riskhanteringsprocessen
- Ta fram compliance-plan

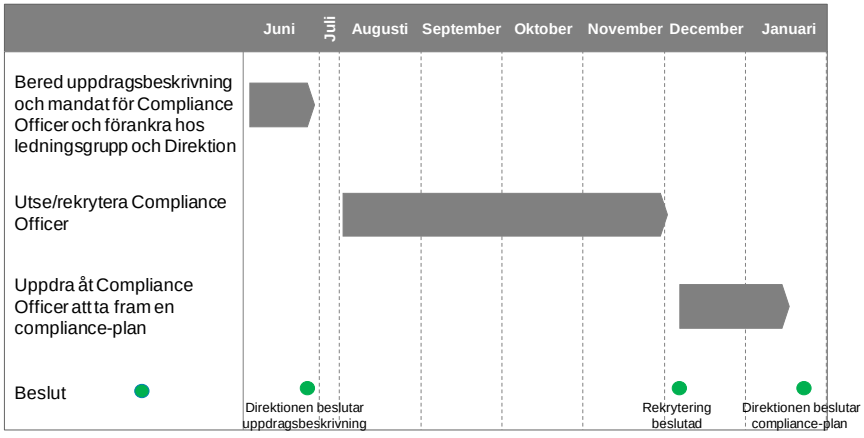
Rekrytera Compliance Officer internt eller externt baserat på rollprofil

Uppdra åt Compliance Officer att ta fram en compliance-plan

Exempel på innehåll i compliance-plan:

- De viktigaste compliance-riskerna för Riksbanken
- Hur första, andra och tredje - ansvarslinjen hanterar riskerna
- Kontroller och uppföljning som compliance skall genomföra
- De utbildningar som man avser att genomföra

Compliance-plan beslutas av Direktionen



Förankra mandat och uppdragsbeskrivning i samband med beslut av Direktionen. Efter sommaren kan rekrytering påbörjas i augusti. När Compliance Officer har rekryterats bör denne omedelbart få uppdraget att ta fram en compliance-plan.

Appendix – Intervjulista

Agneta Rönström
Eric Frieberg
Eva Julin
Hans Ohlson
Heidi Elmér
Jeanette Eklöf
Kai Barvell
Lars Andersson
Magnus Vesterlund
Maria Johansson
Mattias Persson
Olof Fredriksson
Patrick Bailey
Per Mattsson
Pether Burvall
Sophie Degenne
Svante Öberg
Åsa Sydén

Appendix – Instruktion för Compliance Officer

Compliance Officer är ansvarig för samtliga compliance-aktiviteter som utförs på Riksbanken och skall på en löpande basis rådge verksamheten i compliance-frågor.

Compliance Officer skall rapportera till chefen för Riskenheten men med möjlighet att eskalera direkt till Direktionen.

Compliance Officer skall i den tertialvisa rapporteringen förse Direktionen med en sammanställning av väsenliga händelser, iakttagelser, uppföljning av utestående frågor etc.

Compliance Officer skall årligen presentera för Direktionen ett compliance-program som stipulerar vilka aktiviteter och utbildningar funktionen avser att genomför under året. Compliance-programmet skall godkännas av Direktionen.

Compliance Officer skall verka självständigt och oberoende från verksamheten. Vidare skall han eller hon ha ges fullständig åtkomst till de system och andra uppgifter som krävs för att utföra sitt uppdrag. Bristfällig samarbetsvillighet skall rapporteras till Direktionen.

Compliance Officer är ansvarig för nedan angivna områden:

Riskområde	Exempel på styrande dokument
Externa regler	• Tillämpliga lagar, industristandarder, regler och tillstånd • Checklista för affärsförändringar, nya produkter, processer, etc.
Organisatorisk struktur	• Arbetsordning och instruktioner • Organisation, roller/funktioner • Rapporteringslinjer, eskaleringsprocess, delegering av beslutsrätt
Outsourcing	• Krav på outsourcingleverantör • Organisation kring avtal/samarbete
Hantering av känsligt material	• Offentlighets- och sekretesslagen • Regler för skydd av personliga uppgifter

Marknadsmissbruk och insiderhandel	• Regler för:
	  • Egenhandel
	  • Marknadsmissbruk

Process för handel av värdepapper	• Processbeskrivning Utförande • Processbeskrivning Handläggning
Affärsverksamhet och etik	• Etiska regler (”uppföranderegler”) • Övriga regelverk (bedrägeri, mutor, arbete utanför tjänst, anställdas innehav, egenintresse och intressekonflikter, etc.)
Diarieföring	• Offentlighets- och sekretesslagen

Compliance Officer är ansvarig för nedan angivna arbetsuppgifter:

Utveckla och kommunicera förändringar i det interna regelverket:

- Assistera verksamheten i att utveckla policyer och regler
- Utveckla regler och rutinbeskrivningar för Compliance-funktionen
- Initiera och säkerställa att process existerar för hantering av beslut avseende vilka externa regelverk och delar därav som Riksbanken bör följa
- Förvalta och utveckla strukturen för det interna regelverket, inklusive mallar för policyer, regler och rutinbeskrivningar

Rådge proaktivt om compliance-risker och förändringar i externa regelverk:

- Rådge verksamheten i frågor kring applicerbara regler, förordningar, policyer, standarder etc.
- Löpande informera om risker som kan uppstå till följd av bristande regelefterlevnad
- Rådge kring design av åtgärder för att hantera compliance-risker
- Säkerställ att en fungerande process finns för att tillse att avdelningschefer har kännedom om ändringar och kommande ändringar i externa och interna regelverk och rådge verksamheten

Förse organisationen med regelbunden utbildning

- Säkerställa att introduktionsutbildning tillhandahålls för nyanställda
- Säkerställa att utbildningsprogram och träning tillhandahålls på löpande basis
- Säkerställa att utbildning sker ad hoc för att säkerställa vetskap kring förändringar i externa och interna regler

Självständig analys och rapportering av compliance-risker

- Ta fram en plan för hantering av materiella compliance-risker som uppdateras årsvis och följs upp regelbundet
- Oberoende identifiera, värdera och dokumentera compliance-risker associerade till den dagliga verksamheten
- Oberoende identifiera, värdera och dokumentera compliance-risker associerade med utveckling av produkter, processer, affärsområden, nya kundrelationer eller förändring i existerande relationer

Uppföljning av regelefterlevnad och incidenter

- Löpande bevaka att verksamheten efterlever interna och externa regler genom granskning av aktiviteter och transaktioner
- Bedöma verksamhetens effektivitet vad gäller rutiner och instruktioner för att säkerställa compliance
- Följa upp brister relaterat till effektivitet och om möjligt formulera förändringsförslag
- Följa upp compliance-incidenter

Löpande rapportera överträdelser av externa och interna regler

- Löpande rapportera compliance-relaterade frågor (förändringar i riskprofilen, incidenter sammanställning av självständig riskanalys etc.) till närmaste chef
- Tertialvis rapportera compliance-relaterade frågor (förändringar i riskprofilen, incidenter, sammanställning av självständig riskanalys etc.) till Direktionen