Beslutsunderlag

DATUM: 2022-09-15
AVDELNING: STA / RIE
HANDLÄGGARE: Jenny Gawelin
HANTERINGSKLASS Ö P P E N

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

DNR 2022-01038

Policy för operativa risker

Förslag till direktionens beslut

Direktionen beslutar att fastställa Riksbankens Policy för operativa risker och att den träder i kraft samma dag. Genom detta beslut upphävs tidigare Regel för operativa risker från den 9 november 2020.

Ärendet

Policy för operativa risker har uppdaterats i syfte att tydliggöra processen för dessa risker i sin helhet och samtidigt genomgå den årliga översynen av Riksbankens styrande dokument.

Ny policy har tagits fram som omfattar i huvudsak följande förändringar:

- Befintlig regel har uppdaterats till policy i syfte att skapa en logisk struktur för de styrande dokumenten som hanterar operativa risker
- Beskrivning av regeln för beredning av väsentliga verksamhetsförändringar har lagts till
- Avsnitt om kontinuitetshantering har utgått för att regleras genom kommande policy gällande beredskap

Överväganden

För att skapa en logisk struktur för de styrande dokumenten som hanterar operativa risker så har *regeln för operativa risker* uppdaterats till att bli en policy. Bland annat ska regeln för *beredning av väsentliga verksamhetsförändringar* vara underordnad den uppdaterade policyn.

Utöver ovan nämnd justering så har följande uppdateringar gjorts:

Förtydligande avseende rapportering av risker. Mindre justeringar och uppdateringar i avsnitt *3 Metoder för att hantera operativa risker*. Bland annat inkluderar avsnitt 3 nu även en beskrivning av beredningsprocessen för väsentliga verksamhetsförändringar

som är ny från i maj 2022. Kontinuitetshantering har utgått i och med att området kommer regleras genom policy gällande beredskap.

POLICY FÖR OPERATIVA RISKER

BESLUTSDATUM:	2022-12-19
BESLUT AV:	Direktionen
ANSVARIG AVDELNING:	STA/Riskenheten
FÖRVALTNINGSANSVARIG:	Riskanalytiker operativ risk
DIARIENUMMER:	2022-01038
HANTERINGSKLASS:	ÖPPEN

Policy för operativa risker

Innehåll och syfte

Syftet med denna policy är att fastställa de huvudprinciper som ska tillämpas för att effektivt hantera Riksbankens operativa risker. Målet är att ha en god intern styrning och kontroll av de operativa riskerna genom en effektiv och ändamålsenlig riskhantering.

Målgrupp

Policyn omfattar samtliga medarbetare.

Innehållsförteckning

1 Inledning

Policy för operativa risker fastställer hur Riksbanken arbetar med att hantera operativa risker och vilka metoder och processer som etablerats.

1.1 Bakomliggande regelverk

Lagen (1988:1385) om Sveriges riksbank 9 kap. 1 § där det framgår att följande moment ska ingå i riskhanteringen: riskanalys, kontrollåtgärder, uppföljning och dokumentation.

1.2 Definitioner

Operativ risk avser risken för förlust till följd av icke ändamålsenliga eller otillräckliga interna processer eller rutiner, mänskliga fel, felaktiga system eller externa händelser.[1]

Medarbetare avser alla arbetstagare och de uppdragstagare som har tillgång till riksbanksutrustning, det vill säga om uppdragstagaren har en riksbanksdator och Riksbankens system, och som deltar i Riksbankens dagliga verksamhet.

Incident avser en händelse som har eller riskerar att få negativ påverkan på Riksbankens verksamhet, tillgångar eller förtroende.

Väsentlig verksamhetsförändring kan vara exempelvis någon av följande förändringar som beslutas av direktionen eller av en avdelning:

- en ny tjänst (exempelvis RIX) eller produkt (exempelvis kontanter)
- en ny process eller ett IT-system
- en operationell eller organisatorisk förändring.

2 Roller och ansvar

Direktionen är ytterst ansvarig för att verksamheten bedrivs med god intern styrning och kontroll.

Avdelningscheferna ansvarar för att kontinuerligt identifiera, bedöma, analysera och åtgärda de operativa risker som uppstår inom deras verksamhetsområde i enlighet med riskanalysprocessen. Identifierade risker och åtgärdsplaner ska följas upp och löpande rapporteras till riskenheten och direktionen. Avdelningscheferna ska även beakta operativa risker och behov av riskreducerande åtgärder i sin verksamhetsplanering. Avdelningschefen ska säkerställa att processen för beredning

[1] 2.3.1. Eurosystem ESCB SSM Operational Risk Management policy: The risk of negative financial, business and/or reputational impacts resulting from inadequate or failed internal governance and business processes, people, systems, or from external events.

av väsentliga verksamhetsförändringar följs. Avdelningscheferna ansvarar för att incidenter hanteras på sin avdelning.

Varje medarbetare ansvarar för att rapportera samtliga incidenter som denne upptäcker så snart som möjligt.

Riskenheten ska tillhandahålla ändamålsenliga verktyg och metoder för hantering av operativa risker. Riskenheten ska följa upp riskhanteringen och oberoende rapportera Riksbankens samlade risker till direktionen.

3 Metoder för att hantera operativa risker

Det finns operativa risker inom all verksamhet på Riksbanken. De riskerna ska analyseras regelbundet för att kunna hanteras på mest effektiva sätt. De metoder som ska användas beskrivs nedan. För att erhålla jämförbara riskbedömningar avseende operativa risker är det av vikt att metoder, inklusive mått och skalor[2], som beskrivs nedan används.

3.1 Riskanalysprocessen

Riksbanken har en gemensam process för hantering av operativa risker som baseras på ECBS:s ”Framework for Operational Risk Management”. Den metod som används för att identifiera, bedöma, hantera och åtgärda operativa risker inom verksamheten är en självutvärdering av risker och kontroller; även kallad riskanalys avseende operativa risker. Målet med riskanalysen är att identifiera de högsta operativa riskerna för att säkerställa att dessa hanteras enligt Riksbankens riskaptit.

Alla avdelningar på Riksbanken ska utföra riskanalyser. En avdelningschef bör ta ställning till om en riskanalys även ska göras på enhetsnivå. Avdelningschefen ska säkerställa att riskanalysen inkluderar risker relaterade till Riksbankens processer och system, vilket innebär att information från andra avdelningar kan behöva inhämtas.

För att skapa möjlighet till aggregering och analys, ska risker identifieras utifrån orsak, händelse och konsekvens samt kategoriseras enligt de riskkategorier och risktyper som anges i bilaga 2.

För risker som en avdelningschef bedömer vara väsentliga och behöver begränsas, ska det upprättas en åtgärdsplan. Åtgärdsplanen ska följas upp regelbundet, minst tertialvis. Det ska finnas närmare detaljerade bestämmelser som beskriver hur riskanalysen ska utföras.

[2] Se bilaga 1.

3.2 Incidentrapportering

Den samlade bilden av de incidenter som inträffar skapar möjlighet till effektiva åtgärder för riskreducering. Riksbanken ska ha en gemensam incidentrapporteringsprocess för att löpande hantera risker i verksamheten men också för att kunna dra lärdom av incidenter.

Alla medarbetare bör vara uppmärksamma på omständigheter eller händelser i deras dagliga arbete som kan få negativa effekter för Riksbanken. Om en medarbetare upptäcker en incident ska denne rapportera den så snart som möjligt. Det är sedan den berörda avdelningen som ska bedöma incidenten, vidta åtgärder för att hantera problemen samt begränsa risken för att incidenten inträffar igen. Dessa åtgärder, så kallade riskreducerande åtgärder, ska ställas i relation till hur kostnadseffektiva de är. I bilaga 3 finns instruktioner för hur avdelningarna ska gradera olika incidenter.

Riskenheten ansvarar för att det ska finnas detaljerade bestämmelser om vad en incident är samt hur den ska rapporteras.

3.3 Väsentliga verksamhetsförändringar

Vid förändringar i verksamheten kan de operativa riskerna öka. För att hantera dessa risker ska det inom Riksbanken finnas en process för beredning av väsentliga verksamhetsförändringar. Processen ska identifiera och utvärdera de risker som följer av förändringarna. Om en förändring bedöms vara väsentlig ska man tillämpa processen för beredning av väsentliga verksamhetsförändringar. Det innebär att den som ska besluta om förändringen ska utvärdera vilka avdelningar, enheter och funktioner som påverkas av förändringen. Påverkade avdelningar, enheter, funktioner samt de obligatoriska enheterna ska sedan identifiera och bedöma risker förknippade med förändringen. Riskenheten kvalitetsgranskar slutligen riskbedömningen och överlämnar den därefter till den som ska besluta om förändringen.

Riskenheten ansvarar för att det ska finnas detaljerade bestämmelser som beskriver beredningsprocessen för väsentliga verksamhetsförändringar.

4 Rapportering

Avdelningscheferna ska regelbundet, åtminstone årsvis, rapportera till riskenheten och direktionen identifierade väsentliga operativa risker, samt åtgärder och uppföljning av dessa.

Riskenheten ska till direktionen regelbundet rapportera, utifrån bedömd risk och väsentlighet, en oberoende sammanställning av Riksbankens samlade operativa risker. Riskenheten ska även regelbundet rapportera om efterlevnaden av de metoder och processer som beskrivs under punkt 3.1–3.3. Vidare ska riskenheten rapportera de väsentliga incidenter som har inträffat. Om riskenheten bedömer att det finns väsentliga operativa risker som avdelningarna inte har identifierat, kan riskenheten

komplettera riskbilden med dessa. Rapporteringen ska tydligt återspegla vem som äger risken, risknivån samt status på åtgärder. I riskenhetens rapportering av operativa risker ska tydliggöras om avdelningen och riskenheten värderar riskerna på olika sätt.

5 Riskaptit och risklimiter

Operativa risker ska begränsas så långt det är ekonomiskt försvarbart. Om en hög risk ska accepteras måste det stämmas av med riskenheten och risken ska övervakas och följas upp kontinuerligt.

De limiter som operativa risker ska bedömas efter anges i riskmatrisen i bilaga 1 till denna policy.

6 Efterlevnad

Berörda avdelningschefer ansvarar för att denna policy genomförs och efterlevs inom deras respektive avdelning. Riskenheten ansvarar för att följa upp efterlevnaden och att rapportera denna till direktionen

7 Ikraftträdande och övergångsbestämmelser

Regeln träder ikraft 2022-12-19. Denna policy träder i kraft 2022-12-19 och ersätter den *Regel for operativa risker* som beslutades 2020-11-09 (dnr 2020-01140).

7.1 Versionshistorik

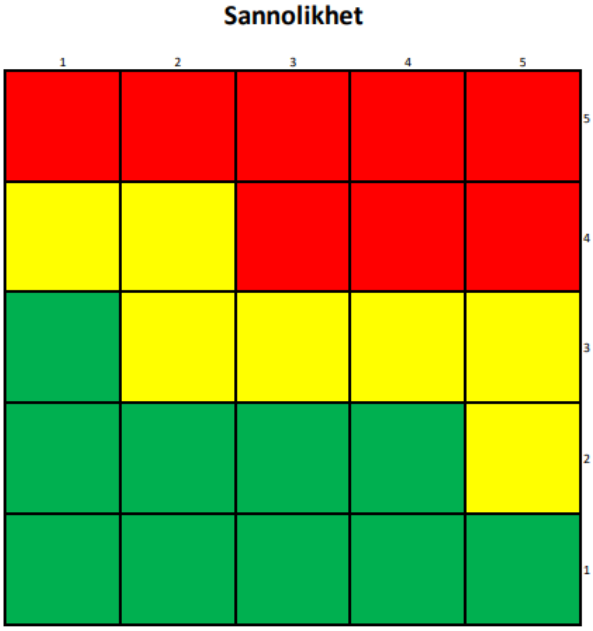
Senast granskad	Version	Kommentar till ändringar
2022-10-31	1.0	Ny policy som ersätter den tidigare regeln med motsvarande innehåll.

Bilaga 1. Riksbankens riskvärderingsmatris

Bilaga - Riksbankens riskvärderingsmatris

Mycket liten	Liten	Medel	Stor	Mycket stor	S
Händelse inträffar knappast (Mer sällan än vart tionde år)	Händelsen inträffar förmodligen inte (En gång under en tioårsperiod)	Händelsen kan inträffa (En gång under en femårsperiod)	Händelsen inträffar förmodligen (En gång vartannat år)	Händelsen kommer med stor sannolikhet att inträffa (Minst en gång per år)	Uppskattning av frekvens

Hög risk: bör som regel få hanteringen begränsa. Vill riskägaren acceptera krävs en avstämning med riskchefen.
Medelhög risk: Riskägaren avgör hantering men bör begränsas i den mån det är ekonomiskt försvarbart
Låg risk: Riskägaren avgör hantering



K	Verksamhet *Förmåga att leverera enligt Riksbankens uppdrag och strategiska mål*	Tillgångar	Förtroende *Negativ uppmärksamhet i media*
Mycket allvarlig	Kraftigt negativ påverkan både internt och på externa parter under en lång tid.	>100mnkr	Långvarig negativ uppmärksamhet nationellt och/eller internationellt
Allvarlig	Påtaglig negativ påverkan på effektivitet eller måluppfyllnad eller på externa parter under en längre tid eller vid ett mycket kritiskt tillfälle	10mnkr-100mnkr	Negativ uppmärksamhet nationellt och/eller internationellt
Märkbar	Påtaglig negativ påverkan på effektivitet eller måluppfyllnad, eller påverkan på andra parter under en kort tid	1mnkr-10mnkr	Negativ uppmärksamhet nationellt
Liten	Kännbar effektivitets-påverkan men endast begränsad negativ påverkan på måluppfyllnad eller på andra	100tkr-1mnkr	Enstaka negativ uppmärksamhet nationellt
Obetydlig	Endast begränsad negativ påverkan på det interna arbetet	< 100tkr	Ingen negativ uppmärksamhetet

Bilaga 2. Riskkategorier och risktyper

Operativa risker	
Riskkategori	**Risktyp**
Personrisker avser alla interna risker som kan relateras till anställda, konsulter eller andra behöriga personer.	**1. Bemanningsrisker** uppstår då det inte finns ett tillräckligt antal personer tillgängliga vid varje givet tillfälle.
	2. Kompetensrisker uppstår då tillgänglig personal inte har ”rätt” kompetens för att genomföra verksamhetens uppdrag med tillräcklig kvalitet eller i rätt tid. **3. Arbetsmiljörisker (psykosocial ohälsa)** uppstår då personal inte har rätt förutsättningar kopplat till arbetsbelastning, återhämtning etc.
	4. Beteenderisker uppstår då medarbetare, konsulter, entreprenörer eller besökare inte beter sig i enlighet med verksamhetens eller allmänhetens förväntningar och regler eller begår brott.
Process- och styrningsrisker avser alla interna risker som kan relateras till brister i styrning och utformning av verksamheten och dess processer.	**5. Styrningsrisker** uppstår vid otydlighet eller motsägelsefullhet i styrning, ledarskap och samordning.
	6. Compliancerisker uppstår då delar av eller hela banken inte lever upp till externa (lagar, förordningar mm) och interna regler samt god sed eller standard. Som t.ex. limiter fastställda av direktionen i en regel. Andra exempel på compliancerisker är penningtvättsrisker och risk för sanktionsbrott. **7. Legala risker** uppstår då delar av eller hela banken inte lever upp till avtal eller vid rättstvist.
	8. Processutformningsrisker uppstår om verksamheten har otydliga eller ineffektiva processer eller det saknas ändamålsenliga styrande dokument eller kontroller.
	9. Förändringsrisker uppstår vid förändringsaktiviteter, både i projekt och i löpande verksamheten eller till följd av bristande förändringsberedskap.
	10. Lokal- och miljörisker uppstår vid brister i fysisk arbetsmiljö, i miljöhänsyn eller vid brister i den interna infrastrukturen för säkerhet, elförsörjning, värme och kyla, vatten och avlopp, etc. **11. Informationssäkerhetsrisker** uppstår vid påverkan av informationens **tillgänglighet** (information eller informationssystem har inte varit tillgängliga), **konfidentialitet** (att information nått obehörig/informationsförlust), eller **riktighet** (att information manipulerats eller ändrats oavsiktligt).
Systemrisker avser alla risker som kan relateras till brister i utformning, funktion eller säkerhet i tekniska stödsystem.	**12. Tillgänglighetsrisker** uppstår när förutsättningarna för tillgång till verksamhetsstödjande IT-system, inklusive kommunikationslösningar, inte uppfylls.
	13. IT-säkerhetsrisker uppstår när bankens IT-säkerhet avseende riktighet och sekretess äventyras. IT-säkerhetsrisker omfattar inte tillgänglighet till system.
	14. Funktionalitetsrisker uppstår då bankens systemstöd inte uppfyller verksamhetens krav, behov och förväntningar.
Externa risker avser risker som uppstår i relationer med externa parter eller till följd av externa händelser.	**15. Leveransrisker** uppstår till följd av brister i externa leveranser som banken är beroende av för sin verksamhet och kan gälla såväl tjänster som produkter och data.
	16. Hot- och angreppsrisker uppstår till följd av att externa angripare med uppsåt kan begå brottsliga handlingar riktade mot Riksbanken.
	17. Omvärldsrisker finns genom att händelser inträffar i omvärlden och påverkar Riksbankens verksamhet (även om de inte är direkt riktade mot Riksbanken).

Bilaga 3. Riksbankens incidentkategorier

Hög	**Verksamhet:** Påtaglig negativ påverkan på effektivitet eller måluppfyllnad eller på externa parter under en längre tid eller vid ett mycket kritiskt tillfälle *eller* **Tillgångar:** >10Mkr *eller* **Förtroende:** Negativ uppmärksamhet nationellt och/eller internationellt
Medel	**Verksamhet:** Kännbar effektivitetspåverkan men endast begränsad negativ påverkan på måluppfyllnad eller på andra parter *eller* **Tillgångar:** 100tkr-10Mkr *eller* **Förtroende:** Enstaka negativ uppmärksamhet nationellt
Låg	**Verksamhet:** Endast begränsad negativ påverkan på det interna arbetet *eller* **Tillgångar:** < 100tkr *eller* **Förtroende:** Ingen negativ uppmärksamhet

Checklista

Syftet med denna checklista är att dokumentera kvalitetsgranskning av en policy eller regel. Checklistan ska fyllas i av förvaltningsansvarig.

Checklistan ska bifogas beslutsunderlaget till beslutsfattare.

Namn på styrande dokument: Policy för operativa risker

Datum för kvalitetsgranskning: 2022-09-05

Namn på förvaltningsansvarig: Jenny Gawelin

Aktivitet	**Genomfört**	**Ej tillämpligt**
Dokumentet är skrivet enligt befintlig mall	X	
Dokumentet är avstämt mot andra styrande dokument	X	
Dokumentet har blivit språkgranskat (av Kommunikationsenhetens klarspråksansvarige om dokumentet beslutas av direktionen)	X	
Dokumentet har genomgått en juridisk granskning	X	
En införandeplan är framtagen		X
En kommunikationsplan är framtagen		X
En utbildningsplan är framtagen		X
Det finns ett beslut om översättning till engelska, när så behövs		X
Dokumentet är granskat av Regelefterlevnadsfunktionen	X	
Checklistan har stämts av med regelefterlevnadsfunktionen	x	