UTKAST BESLUT

DATUM:	2023-11-08
AVDELNING:	Avdelning för intern styrning och verksamhetsstöd
HANDLÄGGARE:	Jenny Gawelin
DIARIENUMMER:	2023-01042
HANTERINGSKLASS:	ÖPPEN

Policy för operativa risker

Riksbankens beslut

Riksbanken fastställer ändringar i Riksbankens policy för operativa risker i enlighet med bilaga 1 med ikraftträdande 1 december 2023.

Skälen för beslutet

Policy för operativa risker har uppdaterats i enlighet med den årliga översynen av styrande dokument, i syfte att tydliggöra principer för hantering av operativa risker, samt renodla och ytterligare synkronisera med andra styrande dokument såsom Policy för intern styrning och kontroll och Regel för beredning av väsentliga verksamhetsförändringar.

Uppdateringar i policyn omfattar i huvudsak följande förändringar:

- Beskrivning av riskhantering, som är grunden till hur operativa risker ska hanteras, har lagts till. Denna omfattar stegen; identifiera, värdera, hantera, åtgärda, följa upp, kommunicera och rapportera operativa risker, på en övergripande nivå.
- Beskrivning av de operativa riskprocesserna riskanalys samt beredning av väsentliga verksamhetsförändringar utgår. Dessa regleras i underliggande styrande dokument.
- Bilagor med riskvärderingsmatris, riskkategorier och incidentkategorier utgår. Dessa inkluderas i underliggande styrande dokument.
- I stycket Definitioner har ”riskaptit” med definition lagts till.

- I stycket ”Riskaptit och risklimiter” har risklimiter utgått, då riskvärderingsmatrisen med risknivåer/limiter kommer inkluderas i underliggande styrande dokument. Riskaptit har en något uppdaterad beskrivning.
- I stycket ”Efterlevnad” har riskenhetens ansvar för att följa upp efterlevnad av riskaptit och verksamhetens riskhantering förtydligats.

Utöver ovan nämna förändringar har följande redaktionella justeringar gjorts:

- Mindre justeringar i stycket Roller och ansvar; avdelningschefens, medarbetares och riskenhetens ansvar är synkroniserat med ny arbetsordning, direktionens ansvar är uppdaterat,
- Stycket Incidentrapportering har kortats ned.
- Stycket Rapportering har kortats ned och beskrivs som ett av stegen i riskhantering istället för under en egen rubrik.
- Versionshistoriken är borttagen från policyn enligt ny mall.

Beslutet har fattats av direktionen (riksbankschefen Erik Thedéen, förste vice riksbankschefen Anna Breman samt vice riksbankscheferna Per Jansson, Martin Flodén och Aino Bunge) efter föredragning av regelefterlevnadsspecialist Alexandra Prochéus. I den slutliga handläggningen har riskchef Lena Arfalk medverkat.

POLICY FÖR OPERATIVA RISKER

BESLUTSDATUM:	2023-11-08
BESLUT AV:	Direktionen
ANSVARIG AVDELNING:	AIS/Riskenheten
FÖRVALTNINGSANSVARIG:	Riskanalytiker operativ risk
DIARIENUMMER:	2023-01042
HANTERINGSKLASS:	ÖPPEN

Policy för operativa risker

Innehåll och syfte

Syftet med policyn är att fastställa de huvudprinciper som ska tillämpas för att hantera Riksbankens operativa risker. Målet är att ha en effektiv och ändamålsenlig riskhantering av de operativa riskerna.

Målgrupp

Policyn gäller för samtliga medarbetare. Begreppet medarbetare avser alla arbetstagare och de uppdragstagare som har tillgång till en riksbanksdator och till Riksbankens system och som deltar i Riksbankens dagliga verksamhet.

Innehållsförteckning

1 Inledning

Denna policy fastställer principer för hantering av operativa risker, den riskaptit som riskhanteringen ska förhålla sig till samt principer för hantering och rapportering av incidenter.

1.1 Bakomliggande regelverk

Lagen (2022:1568) om Sveriges riksbank 7 kap. 8 §.

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.

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.

Riskaptit är ett uttryck för den aggregerade risknivån direktionen är villig att acceptera för att Riksbanken ska nå sina mål.

2 Roller och ansvar

Direktion ansvarar för att fastställa Riksbankens riskaptit, samt att det finns ett ramverk för operativ riskhantering som möjliggör att verksamheten drivs i enlighet med detta.

Avdelningscheferna ansvarar för att hantera och rapportera de operativa risker som uppstår inom deras verksamhetsområde. Detta bör genomföras kontinuerligt samt vid behov. Avdelningscheferna ska även beakta operativa risker och behov av riskreducerande åtgärder i sin verksamhetsplanering. Avdelningscheferna ansvarar för att incidenter hanteras och rapporteras på sin avdelning.

Varje medarbetare ska uppmärksamma chefer och andra berörda på operativa risker som de identifierar i Riksbankens verksamhet och rapportera incidenter.

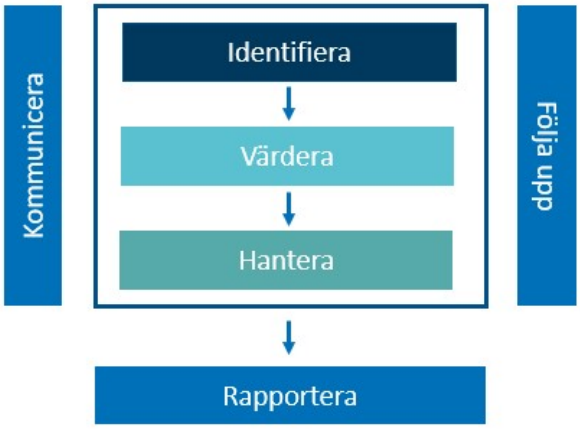
Riskenheten ska tillhandahålla ändamålsenliga metoder, verktyg och riktlinjer för hantering av operativa risker och incidenter. Riskenheten ska följa upp risk- och incidenthanteringen och oberoende rapportera sin bedömning av Riksbankens operativa risker samt incidenter till direktionen.

3 Riskaptit

Riksbanken ska sträva efter att hålla de operativa riskerna på en nivå som står i relation till den verksamhet som bedrivs samt begränsa dessa risker så långt det är ekonomiskt försvarbart. Riksbanken har således en låg riskaptit för operativa risker. Arbetet i Riksbanken ska präglas av god etik och sund riskkultur samt tydliga roller och ansvar. En avvägning ska alltid göras mellan förväntad kostnad av att hantera risken och den konsekvens som risken innebär om den inträffar. Det ska finnas riktlinjer för hantering, uppföljning och rapportering av operativa risker som återspeglar riskaptiten.

4 Riskhantering

Operativa risker ska hanteras regelbundet på alla avdelningar, samt vid behov, såsom vid större verksamhetsförändringar. Verksamhetsöverskridande processer ska omfattas och möjliggöra att operativa risker hanteras effektivt och i enlighet med Riksbankens riskaptit.



Figur 1 Steg inom riskhantering

Identifiera

Syftet med riskidentifiering är att upptäcka och förstå risker som kan förhindra att målen uppfylls eller är ett hot mot bankens verksamhet, tillgångar eller anseende. Ingångsvärden för att identifiera operativa risker ska användas som underlag, såsom incidenter som har inträffat, sårbarheter och indikatorer på framväxande risker.

Värdera

Vid riskvärderingen bedömer verksamheten vilken konsekvens en händelse kan få och hur sannolikt detta är. Syfte och mål med riskvärdering är att ge stöd vid beslutsfattande och val av lämplig strategi för att bemöta risken. Vid värderingen ska Riksbankens riskvärderingsmatris användas.

Hantera

Efter att verksamheten identifierat och värderat risker ska beslut tas om lämplig hantering för respektive risk. När en risk ska begränsas ska åtgärdsplan tas fram som tydligt beskriver vad som ska utföras med ansvarig och datum för slutförande av åtgärden.

Följa upp

Risker och dess åtgärder ska av verksamheten med regelbundenhet följas upp. Risker ska följas upp genom att löpande bevaka de faktorer som bedöms orsaka risken. Åtgärder ska följas upp så att de utförs enligt plan och att dessa ger önskvärd effekt på risken.

Rapportera

Rapportering av relevant information om identifierade risker och åtgärder ska göras regelbundet samt vid behov. Verksamheten ska rapportera risker bland annat i samband med tertialuppföljning av verksamhetsplanering, vid väsentliga förändringsinitiativ och efter genomförd riskanalys.

Kommunicera

Relevant information om risker och åtgärder ska delas mellan berörda avdelningar och verksamheter för att uppnå god riskmedvetenhet och möjliggöra effektiv hantering.

5 Incidentrapportering

Riksbanken ska ha en gemensam incidentrapporteringsprocess och gemensam incidenthistorik för att för att kunna lära sig av inträffade incidenter och därigenom öka förmågan att proaktivt hantera risker i verksamheten. Genom att systematiskt följa upp alla typer av incidenter ökar Riksbankens möjlighet att identifiera och genomföra effektiva förbättringsåtgärder.

Om en medarbetare upptäcker en incident ska incidenten rapporteras så snart som möjligt.

6 Efterlevnad

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

7 Ikraftträdande och övergångsbestämmelser

Denna policy träder i kraft den 1 december 2023 och ersätter Policy för operativa risker som beslutades 8 november 2022, dnr 2022-01038.