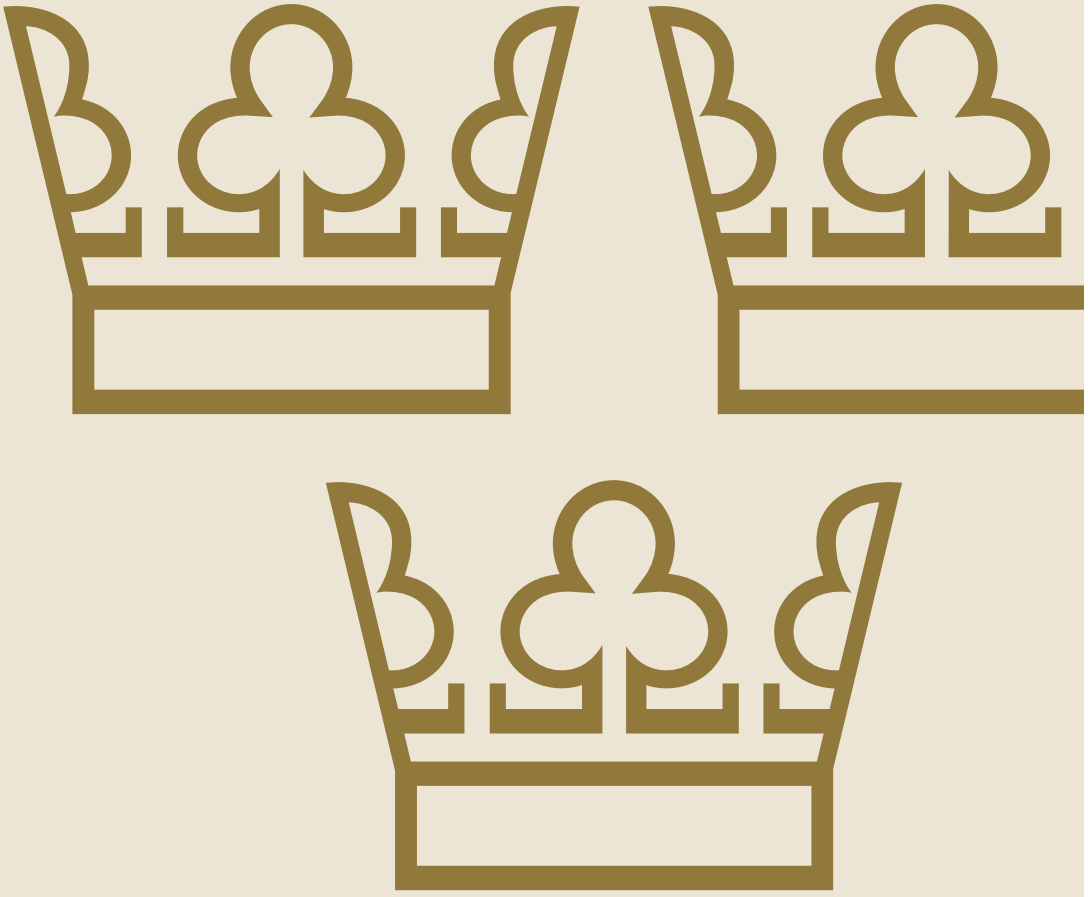
RIKSGÄLDEN
SWEDISH NATIONAL DEBT OFFICE

2022-12-14

Policy för intern styrning och kontroll

2023



Fastställd:	2022-12-14
Fastställd av:	Styrelsen
Informationsägare:	Riskchef

Policy för intern styrning och kontroll

Med intern styrning och kontroll (ISK) avses den process som ska säkerställa att myndigheten med rimlig säkerhet fullgör sina uppgifter, uppnår verksamhetens mål och uppfyller de krav (verksamhetskraven) som framgår av 3 § myndighetsförordningen (2007:515). Styrelsen ska se till att kraven uppfylls genom att verksamheten bedrivs effektivt och enligt gällande rätt och de förpliktelser som följer av Sveriges medlemskap i Europeiska unionen, att den redovisas på ett tillförlitligt och rättvisande sätt samt att myndigheten hushållar väl med statens medel.

Styrelsen ska säkerställa att det inom myndigheten finns en god intern miljö som skapar förutsättningar för en väl fungerande process för intern styrning och kontroll. Processen ska även förebygga att verksamheten utsätts för korruption, otillbörlig påverkan, bedrägeri och andra oegentligheter.

Arbetet med intern styrning och kontroll utgår från förordningen (2007:603) om intern styrning och kontroll. Enligt förordningen ska processen för intern styrning och kontroll omfatta genomförande och dokumentation av riskanalys, åtgärder och uppföljning. Processen ska också vara integrerad med övrig styrning av verksamheten. Även internrevisionsförordningen (2006:1228) och förordningen (2000:605) om årsredovisning och budgetunderlag ingår i det samlade regelverket för intern styrning och kontroll.

Riskhantering

Riksgälden ska identifiera och hantera väsentliga risker i verksamheten, det vill säga risker för att myndigheten inte kan fullgöra sina uppgifter, uppnå verksamhetens mål och uppfylla verksamhetskraven.

På Riksgälden hanteras genomförande och dokumentation av riskanalys, åtgärder och uppföljning i riskhanteringsprocessen.

Riksgäldens riskhantering omfattar finansiella och operativa risker, som definieras närmare i Riksgäldens Finans- och riskpolicy, där de finansiella riskerna även regleras.

Riksgälden definierar operativ risk som risken för förluster till följd av ej ändamålsenliga eller fallerade processer, människor, system eller yttre händelser. Legala risker är en del av operativa risker.

Säkerhetsrelaterade risker och incidenter ingår i operativa risker och hanteras i samråd med säkerhetsfunktionen. Säkerhetsområdet definieras i Riksgäldens Säkerhetspolicy.

Operativa risknivåer

Riksgäldens risknivåer för operativa risker anger att Riksgälden kan acceptera låga och medelhöga risker medan höga och mycket höga risker ska begränsas - om det är möjligt. Det finns fyra risknivåer inom Riksgälden och den accepterade risknivån reglerar hur risker ska hanteras inom respektive nivå.

1. **Låga risker** - är inom accepterad risknivå och kan accepteras men bör bevakas.

2. **Medelhöga risker** - är inom accepterad risknivå men bör begränsas och, eller bevakas.

3. **Höga risker** - är över accepterad risknivå och ska begränsas med åtgärdsplaner.

4. **Mycket höga risker** - är över accepterad risknivå och ska prioriteras och omedelbart begränsas med hjälp av åtgärdsplaner.

I samtliga fall ska en avvägning göras mellan kostnaden för att begränsa risken mot nyttan av att begränsa den.

Riskhanteringsprocessen

Riskanalys

Riksgälden ska genomföra ändamålsenliga riskanalyser minst årligen, där väsentliga risker identifieras och hanteras inom ramen för Riksgäldens verksamhet. En sammanställning av myndighetens väsentliga risker ska tas fram och andra riskanalyser ska beaktas i arbetet.

Riskhantering är centralt för Riksgälden eftersom kostnaderna för förvaltningen av statsskulden, stöd till banker i kris, hanteringen av statens betalningsmodell, prissättningen av garantier och krediter samt eventuella obalanser i finansieringssystemet för kärnavfall bland annat beror på förmågan att bedöma och hantera risker.

Åtgärder

Riksgälden ska med ledning av riskanalyserna vidta nödvändiga åtgärder för att hantera identifierade risker.

Riksgälden ska i samband med riskanalyser bedöma de befintliga kontrollerna i verksamheten och vidta åtgärder om kontrollerna behöver stärkas.

Uppföljning

Riksgälden ska regelbundet följa upp och uppdatera riskanalyserna samt bedöma om vidtagna åtgärder har haft avsedd effekt.

Dokumentation

Riksgäldens riskanalyser och de åtgärder som vidtas med anledning av analyserna ska dokumenteras.

Underlag för bedömning av ISK

Riksgälden ska ha styrande dokument, rutiner, metoder och modeller som ska vara dokumenterade, ha hög kvalitet och säkerhet, samt vara kända av personalen. Styrande dokument ska gås igenom regelbundet i syfte att förbättra och revidera dem utifrån förändringar i verksamheten och omvärlden.

Riksgälden ska regelbundet följa upp att processen för intern styrning och kontroll är ändamålsenlig och tillämpas på ett betryggande sätt.

Riksgälden ska tillämpa en systematisk och regelbunden uppföljning för att kunna bedöma den interna styrningen och kontrollen. Uppföljning av verksamhetens aktiviteter, ekonomi, risker och åtgärder ska ske regelbundet. Ett sammanfattande dokument för arbetet med intern styrning och kontroll ska upprättas som underlag för styrelsens årliga bedömning av denna process.

Ansvar

Styrelsen är ytterst ansvarig för att verksamheten bedrivs med god intern styrning och kontroll. Styrelsen ska regelbundet få information om det pågående arbetet för att med rimlig säkerhet kunna bedöma om Riksgäldens nivå på intern styrning och kontroll är betryggande. I det ingår att styrelsen ska

informeras om aktuell riskstatus. Styrelsen ska också informeras om incidenter som har haft stor påverkan på verksamheten, tillsammans med vidtagna åtgärder.

Riksgäldsdirektören leder den löpande verksamheten, verkställer styrelsens beslut och ansvarar för intern styrning och kontroll inför styrelsen.

Riksgäldens chefer ansvarar för att skapa förutsättningar för informationsflöde och kompetensutveckling som behövs för att uppnå god intern styrning och kontroll i arbetet. De ansvarar även för riskhantering inom den egna verksamheten, samt för att konkretisera hur avdelningen, eller enheten ska uppnå sina mål.

Medarbetare har ett ansvar att känna till riktlinjer och instruktioner samt att följa dessa. Om en medarbetare uppmärksammar en incident ska hen rapportera händelsen. Orsak till händelsen ska följas upp och relevanta åtgärder ska vidtas.

Riskkontrollfunktionen ansvarar för den oberoende och övergripande riskkontrollen samt den samlade riskrapportering som lämnas till riksgäldsdirektören.

Compliancefunktionen ansvarar för Riksgäldens process för regelefterlevnad.

Dataskyddsombudet ansvarar för att oberoende övervaka Riksgäldens efterlevnad av dataskyddsförordningen.

Internrevisionen är direkt underställd styrelsen och ansvarar för att granska verksamheten, samt ge råd och stöd, utifrån de av styrelsen beslutade riktlinjerna för internrevision.