



**YTSKYDDS
MYNDIGHETEN**

STYRDOKUMENT 2026:4

Riskhanteringspolicy

Identifiering, bedömning och hantering av risker

Riskhanteringspolicy. Identifiering, bedömning och hantering av risker

Styrdokument 2026:4

Diarienummer: YSM 2026/1303

Utgivare: Ytskyddsmyndigheten, Box 112, 842 21 Sveg

registrator@ytskyddsmyndigheten.se, ytskyddsmyndigheten.se

Beslutad av generaldirektören 2026-10-21

Ansvarig avdelning: Avdelningen för regler och tillsyn

Publikationen kan laddas ner från ytskyddsmyndigheten.se. Tryckta exemplar kan beställas från registrator i mån av tillgång.
Citera gärna, men ange källan.

1 Inledning

Riskhanteringspolicyn anger hur Ytskyddsmyndigheten identifierar, bedömer, hanterar och följer upp risker som kan hindra myndigheten från att nå sina mål eller att fullgöra sitt uppdrag. Policyn är en del av myndighetens interna styrning och kontroll.

1.1 Syfte

Myndigheten ska kunna fatta välgrundade beslut om vilka risker som kan accepteras och vilka som ska åtgärdas. Riskhanteringen ska göra det möjligt att prioritera resurser, att upptäcka hot mot verksamheten tidigt och att redovisa till regeringen hur riskerna hanteras.

1.2 Omfattning

Policyn gäller för all verksamhet vid myndigheten och för de processer som stöds av andra aktörer genom avtal. Den omfattar verksamhetsrisker, ekonomiska risker, risker för informationssäkerhet och dataskydd, personalrisker, rättsliga risker och risker kopplade till myndighetens anseende och förtroende.

1.3 Lagstöd

Arbetet följer Ekonomistyrningsverkets föreskrifter och allmänna råd om intern styrning och kontroll, i den mån de gäller för myndigheten. Policyn kompletterar myndighetens övriga styrdokument och ersätter inte de rutiner som gäller för enskilda processer.

2 Begrepp

- **Risk:** en händelse eller ett förhållande som kan påverka myndighetens möjlighet att nå sina mål negativt.
- **Riskbedömning:** bedömning av sannolikheten att en risk inträffar och av konsekvensen om den gör det.
- **Riskregister:** förteckning över identifierade risker med bedömning, ansvarig och åtgärder.
- **Riskaptit:** hur stor risk myndigheten är beredd att acceptera inom ett visst område.
- **Restrisk:** risk som kvarstår efter att åtgärder har genomförts.

3 Riskprocessen

Riskhanteringen genomförs i fyra steg. Varje steg dokumenteras i riskregistret.

1. **Identifiering:** risker som kan hindra målen i verksamhetsplanen identifieras av avdelningarna och av ledningen, och genom genomgång av avvikelser och incidenter.
2. **Bedömning:** varje risk bedöms efter sannolikhet och konsekvens på en skala med nivåerna låg, medel och hög, enligt tabell 1.
3. **Hantering:** för varje risk väljs om den ska minskas, överföras, accepteras eller undvikas. Åtgärden får en ansvarig person och en tidsfrist.

4. **Uppföljning:** åtgärderna följs upp och restrisken bedöms på nytt.

Tabell 1. Riskmatris

Sannolikhet och konsekvens	Konsekvens låg	Konsekvens medel	Konsekvens hög
Sannolikhet låg	Låg	Låg	Medel
Sannolikhet medel	Låg	Medel	Hög
Sannolikhet hög	Medel	Hög	Hög

Källa: egen bedömning. Bedömningen görs före och efter att åtgärder har genomförts.

En risk som bedöms som hög ska alltid få en åtgärd och en ansvarig. En risk som bedöms som medel ska åtgärdas om kostnaden för åtgärden står i rimlig proportion till nyttan. En risk som bedöms som låg kan accepteras, men den ska ändå finnas kvar i riskregistret.

4 Riskregistret

Avdelningen för regler och tillsyn förvaltar myndighetens riskregister. Varje avdelningschef ansvarar för att riskerna inom avdelningen är identifierade och registrerade. Riskregistret uppdateras minst en gång per år och vid väsentliga förändringar i verksamheten, till exempel vid en ny författning, ny teknik eller ett nytt uppdrag.

Riskerna i registret ska vara beskrivna så att det går att förstå vad som kan hända, vad som kan orsaka det och vilken effekt det kan få. Varje risk ska ha en ansvarig chef. En enskild handläggare får inte vara ensam ansvarig för en risk på myndighetsnivå.

5 Riskaptit

Generaldirektören fastställer myndighetens riskaptit i samband med verksamhetsplanen. Riskaptiten anger hur stora risker myndigheten kan acceptera inom områdena verksamhet, ekonomi, informationssäkerhet och anseende.

Myndigheten har låg riskaptit när det gäller rättssäkerhet, sakliga beslut och skyddet av de uppgifter som myndigheten hanterar. Myndigheten kan ha högre riskaptit när det gäller att pröva nya arbetsmetoder, inklusive digitala verktyg, under förutsättning att de riskreducerande åtgärderna är genomförda. Riskaptiten ska beaktas i besluten, men den ersätter inte krav som följer av lag eller förordning.

6 Rapportering

Avdelningscheferna rapporterar riskläget inom sin avdelning till generaldirektören varje kvartal, i samband med den övriga kvartalsrapporteringen. Rapporten ska innehålla nya risker, risker vars bedömning har förändrats och åtgärder som är försenade.

Ledningsgruppen behandlar riskläget vid ett av sina sammanträden per halvår. Om en risk bedöms som hög och inte kan åtgärdas utan dröjsmål ska generaldirektören informeras omedelbart.

Den samlade riskbedömningen ingår i årsredovisningen, där väsentliga risker och hur de har hanterats redovisas.

7 Roller och ansvar

- Generaldirektören fastställer policyn och riskaptiten och beslutar om större åtgärder.
- Överdirektören är ställföreträdare för generaldirektören i frågor som rör riskhanteringen.
- Avdelningen för regler och tillsyn ansvarar för policyn, för riskregistret och för samordningen av riskhanteringen.
- Avdelningscheferna ansvarar för riskerna inom sin avdelning och för att åtgärderna genomförs.
- Avdelningen för verksamhetsstöd ansvarar för riskerna inom ekonomi, it, personal samt registratur och arkiv, och för att riskbedömningarna är kopplade till den interna kontrollen.
- Medarbetarna ska identifiera och rapportera risker i sitt arbete.

8 Uppföljning och revidering

Riskhanteringen följs upp genom den årliga uppföljningen av den interna kontrollen och genom granskning av ett urval av åtgärder. Resultatet redovisas till generaldirektören.

Policyn revideras minst vart tredje år och när väsentliga förändringar sker i myndighetens uppdrag eller i regelverket.

Referenser

Ekonomistyrningsverkets föreskrifter och allmänna råd om intern styrning och kontroll.

Ytskyddsmyndigheten. Intern kontrollplan 2027. Styrdokument 2026:5, dnr YSM 2026/1304.

Ytskyddsmyndigheten. Informationssäkerhetspolicy. Styrdokument, dnr YSM 2024/0119.

Ytskyddsmyndigheten. Verksamhetsplan 2026. Styrdokument, dnr YSM 2025/0902.