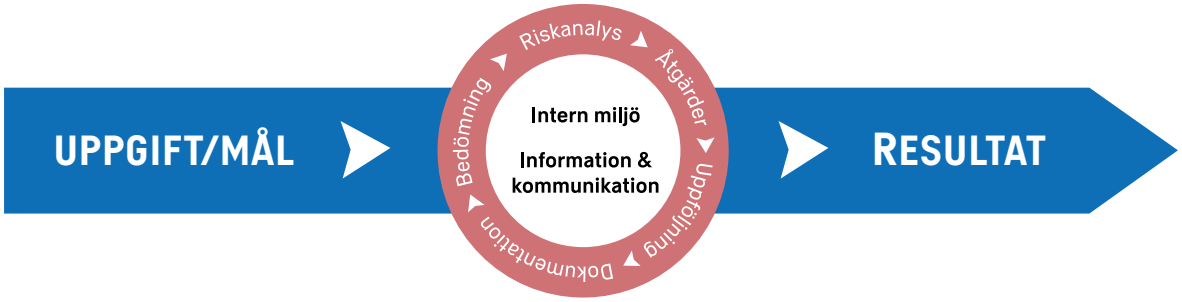
FÖRSVARSMAKTEN



Handbok
Intern styrning och kontroll

2019

Handbok
Intern styrning och kontroll

H ISK 2019

Bilder på omslaget: FSV GP med tillstånd från ESV
Grafisk bearbetning: EKDIR PUBLIKATIONER
Produktionsid: 190221001
Produktionsformat: Word
Publikationsområde: LEDS PLANEK
Tryck: Behovstryckning

VIDAR handling: **FM2019-2643**

Beslut om fastställande av Handbok Intern styrning och kontroll

Handbok Intern styrning och kontroll 2019 (H ISK 2019) fastställs att gälla från och med 2019-03-01.
Publikationen har inget registrerat M-nr.

Följande upphävs 2019-03-01:
Handbok intern styrning och kontroll FM2016-1692:3, gällande från 2016-12-01.

Publikationen tillgängliggörs genom publicering på intranätet emilia samt på www.forsvarsmakten.se.

Detta beslut är fattat av ekonomidirektör Helena Holmstedt. I den slutliga handläggningen har som föredragande deltagit överstelöjtnant Hampe Klein.

Helena Holmstedt
Ekonomidirektör

Hampe Klein

ÄNDRINGAR

Nr	Mom	Omfattning	Datum föredragning Beslut av	VIDAR handling nr
0		Ursprunglig fastställelse	2019-02-27 Ekonomidirektören	FM2019-2643

Sida avser sidnummer i den rättade versionen.
Ändringar i texten framgår av ändringsmarkör.

Kom ihåg!

Om du läser denna publikation i pappersform – kontrollera att du har den senaste utgåvan. Fastställd och gällande utgåva finns alltid publicerad på Försvarsmaktens intranät.

Förord

Den här handboken innehåller anvisningar med förklaringar och beskrivningar av intern styrning och kontroll i Försvarsmakten.

Risker har under lång tid hanterats inom specifika områden i Försvarsmakten. Den systematiska riskhanteringen som har utvecklats ska även fortsättningsvis genomföras enligt de metoder som utvecklats inom dessa områden. Det finns dock ingen av de tidigare metoderna som är tillämplig för att hantera intern styrning och kontroll utifrån förordningen (2007:603) om intern styrning och kontroll. Därför har metoden i denna handbok utvecklats för detta ändamål.

Intern styrning och kontroll är en integrerad del av Försvarsmaktens verksamhet och syftar till att ge en rimlig försäkran om att givna uppgifter löses samt att uppsatta mål uppfylls. Handboken beskriver vad som ska göras för att få en systematisk riskhantering i Försvarsmakten.

Det handlar om ordning och reda i verksamheten. God intern styrning och kontroll kännetecknas av:

- Säkerställande av att målen med verksamheten uppfylls.
- Hantering av uppkomna risker i verksamheten.
- Prioritering och fokusering på de i sammanhanget viktigaste riskerna.
- Åtgärder och kontroller genomförs för att hantera risker.
- Ett aktivt stöd och engagemang för intern styrning och kontroll hos chefer på alla nivåer.

Handboken tar upp hur riskhanteringen genomförs på alla ledningsnivåer för att ge underlag till myndighetsledningens bedömning och säkerställande av intern styrning och kontroll. Metoden som beskrivs i handboken är en praktisk tillämpning av förordning (2007:603) om intern styrning och kontroll.

Sedan förra utgåvan av handboken har styrande förordningar[1] ändrats, varvid de nya lydelserna har inarbetats. Vidare har handboken uppdaterats utifrån utvecklingen av Försvarsmaktens arbete med intern styrning och kontroll. Begreppen intern miljö samt information och kommunikation har beskrivits. Ett nytt kapitel om myndighetens arbete med att förebygga och upptäcka oegentligheter har tillkommit.

Inget i handboken omfattas av sekretess.

[1] Förordning (2007:603) om intern styrning och kontroll, internrevisionsförordning (2006:1228) samt förordning (2000:605) om årsredovisning och budgetunderlag.

Innehåll

1. Inledning

Allt arbete med intern styrning och kontroll inom myndigheten syftar till att Försvarsmakten ska kunna lösa uppgifter och nå de mål som riksdagen och regeringen satt upp. Den främsta uppgiften för Försvarsmakten är att upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp.

Intern styrning och kontroll är en integrerad del av Försvarsmaktens verksamhet som syftar till att ge en rimlig försäkran om att målen uppfylls inom följande kategorier:

- Effektivitet och produktivitet i verksamheten
- Tillförlitlig och rättvisande rapportering
- Efterlevnad av tillämpliga lagar och förordningar samt regler
- God hushållning med statens medel

En systematiserad riskhantering medför att Försvarsmakten kan arbeta på ett mer strukturerat och genomtänkt sätt med intern styrning och kontroll (ISK). Riskerna dokumenteras och kan på ett tydligare sätt värderas mot varandra. Vid riskhantering används fem moment. Dessa är:

- Riskanalys
- Åtgärder
- Uppföljning
- Dokumentation
- Bedömning

Riskhanteringen ger ökat fokus på ansvar för att åtgärder identifieras i organisationen och att vidtagna åtgärder följs upp. Ansvaret vilar på chefer såväl som på medarbetare att analysera risker kopplade till uppdrag och uppgifter samt att följa upp att riskerna hanteras på lämpligt sätt. Riskhanteringen syftar till en ökad systematik som förväntas ge följande fördelar:

- Ökade möjligheter för ledningen att få överblick samt att jämföra och prioritera risker och åtgärder.
- Tydligare samband mellan risker och åtgärder. Genom hänvisning till riskanalysarbetet kan ledningen i förekommande fall härleda prioriteringar i verksamhetsplaneringen.
- Ökade möjligheter att orientera uppdragsgivaren om risker och problem kopplade till givna uppdrag och uppgifter.
- Ökad medvetenhet och förståelse för risker i myndigheten.
- Ökat förtroende för Försvarsmakten.

Observera!
Arbetet med riskhantering kan endast ge en rimlig försäkran det vill säga ingen absolut säkerhet, avseende intern styrning och kontroll för organisationens ledning. Syftet är att identifiera risker kopplade till verksamhetens mål och utforma åtgärder på ett medvetet och tydligt sätt.

Bild 1.1 Integration av intern styrning och kontroll i verksamheten/Ekonomistyrningsverket.

2. Intern miljö samt information och kommunikation

2.1. Intern miljö

Den interna miljön formas av Försvarsmaktens organisation och kultur. Myndighetsledningen säkerställer att det finns en god intern miljö som ger förutsättningar för Försvarsmakten att fullgöra uppgifterna, uppnå målen och uppfylla verksamhetskraven.

I Försvarsmaktens arbetsordning (FMArbO) framkommer bland annat hur ÖB har valt att strukturera verksamheten och fördela arbetsuppgifter och ansvar. Myndighetens kultur består bland annat av ledarskapet, det vill säga hur myndighetsledningen väljer att styra och leda verksamheten samt medarbetarskapet, det vill säga hur medarbetarna i organisationen tar till sig och omsätter styrning och ledning. Den interna miljön har formats av myndighetens styrning och etiska riktlinjer som beskrivs i värdegrunden, men också i interaktionen mellan ledning och medarbetare i en organisation.

Försvarsmaktens värdegrund är en aspekt av den interna miljön som har växt fram genom interna normer och förhållningssätt i organisationen. Hur värdegrunden påverkar Försvarsmakten beror också på med vilken moral organisationen och de enskilda individerna omsätter den i verksamhet.

Den interna miljön påverkas också av den verksamhet som ska bedrivas. Myndighetsledningen säkerställer att det finns en god intern miljö genom bland annat medarbetarundersökningar, avgångsintervjuer och internrevisionens granskningar. Genom bland annat arbetet med FM 2025 strävar myndighetsledningen efter att Försvarsmakten utvecklar och förändrar den interna miljön. Den interna miljön ska vara så gynnsam som möjligt för att myndigheten ska fullgöra sina uppgifter och nå verksamhetens mål.

På samma sätt som ledningen tar stöd av medarbetare för att genomföra verksamheten, behöver den ta stöd av medarbetare för att följa upp och utveckla den interna miljön. För det behöver ledningen ha en uppfattning om hur den interna miljön är utformad, samt hur den behöver förändras och utvecklas för att på bästa sätt stödja verksamheten.

2.2. Information och kommunikation

Kännedom om risker och hur de hanteras behöver vara kända inom Försvarsmakten.

Det uppnås genom att informera och kommunicera. Genom styrdokument och andra informationskanaler kommunicerar högre chef identifierade väsentliga risker, det vill säga omständigheter som utgör en väsentlig risk att uppgifter inte kan fullgöras. Uppgiftsmottagare genomför en riskanalys kopplad till givna uppdrag och kommunicerar väsentliga risker samt hur de hanteras till uppdragsgivaren.

3. Styrning och kontroll

Grundläggande för statliga myndigheter är att styra verksamheten på ett sådant sätt att regeringens mål uppfylls i enlighet med författningar, instruktioner, regleringsbrev och annan styrning. Inom myndigheter omsätts regeringens styrning i interna styr- och måldokument. Kontroll genomförs genom uppföljning av verksamheten och sammanställning och analys av resultaten. Resultatet analyseras för att göra bedömningen om Försvarsmakten har haft en betryggande intern styrning och kontroll och redovisas till regeringen i årsredovisningen.

3.1. Myndighetsledningen

Överbefälhavaren är chef för Försvarsmakten och leder myndigheten med utgångspunkt i de uppgifter riksdag och regering ställer. Inom ramen för regeringens beslut och inriktningar har ÖB att avväga hur myndigheten ska fördela sina resurser för att lösa uppgifterna.

Generaldirektören ska stödja överbefälhavaren med uppföljning och analys av de uppdrag eller andra uppgifter överbefälhavaren har ställt till underställda chefer. Generaldirektören ska leda utvecklingen av myndighetens interna styrning och kontroll.

3.2. Direkt underställda chefer till ÖB

Chefen för ledningsstaben ska leda, samordna och följa upp verksamheten i Högkvarteret i syfte att stödja överbefälhavarens interna styrning och kontroll samt strategiska ledning av Försvarsmakten. ÖB direkt underställda chefer (DUC) utvecklar de uppdrag och uppgifter som tilldelats i FMArbO och Försvarsmaktens verksamhetsplan (FMVP) samt i egna dokument, till exempel verksamhetsuppdrag. Detta för att säkerställa att tilldelade uppgifter omhändertas. Produktionschefen ställer uppdrag och uppgifter till försvarsgrensstaber och underställda organisationsenheter förutom Högkvarteret och Särskilda operationsgruppen.

3.3. Försvarsgrenschef

Försvarsgrenschefer leder, samordnar och följer upp verksamheten vid de organisationsenheter som underställts dem inom ramen för tilldelat mandat.

3.4. Chef för organisationsenhet

Chef för organisationsenhet (C OrgE), förutom Högkvarteret och Särskilda operationsgruppen, ska planera, genomföra och följa upp verksamhet på uppdrag av produktionschefen alternativt försvarsgrensstab samt på order från insatschefen eller taktisk chef.

4. Riskanalys

4.1. Inledning

Riskanalys innebär samordnade aktiviteter för att identifiera och värdera risker, för att därefter ta ställning till om och hur uppdagade risker ska hanteras. Omständigheter utgör en risk när de påverkar Försvarsmaktens möjligheter att fullgöra uppgifterna, nå målen eller genomföra uppdragen för verksamheten. Om myndigheten bedömer att verksamheten kan komma att utsättas för otillbörlig påverkan, bedrägeri eller annan oegentlighet, ska åtgärder vidtas för att hantera sådana omständigheter.

Riskanalys ska genomföras av den som tilldelats uppgifter och uppdrag från högre chef. Vid behov ska genomförd riskanalys uppdateras för att säkerställa att den omfattar aktuella risker. Dokumentation ska upprättas i den utsträckning som är nödvändig för de identifierade riskerna som ska hanteras. Målet med en riskanalys är att ge kontinuerlig kontroll över riskerna samt att skapa en organisationskultur som ger ett väl avvägt risktagande och hantering av risker. Åtgärder för att reducera risker ska ske till den nivå som anses rimlig.

Riskanalys omfattar all verksamhet i Försvarsmakten. Riskhantering i specifika områden där etablerade metoder finns hanteras på särskilt sätt vad gäller såväl riskidentifiering som åtgärder och uppföljning. Exempel på detta är systematiskt arbetsmiljöarbete, organisatoriska risker enligt föreskrifterna om organisatorisk och social arbetsmiljö (AFS 2015:4), riskanalys inför och vid insatser och övningar. Det är dock viktigt att alla riskområden, oavsett grund, beaktas gemensamt då de i de flesta fall berör varandra.

Alla riskbedömningar, utredningar och åtgärdsplaner ska integreras som en naturlig del i ordinarie lednings- och beslutsprocesser då de utgör ett underlag för chefens beslutsfattande.

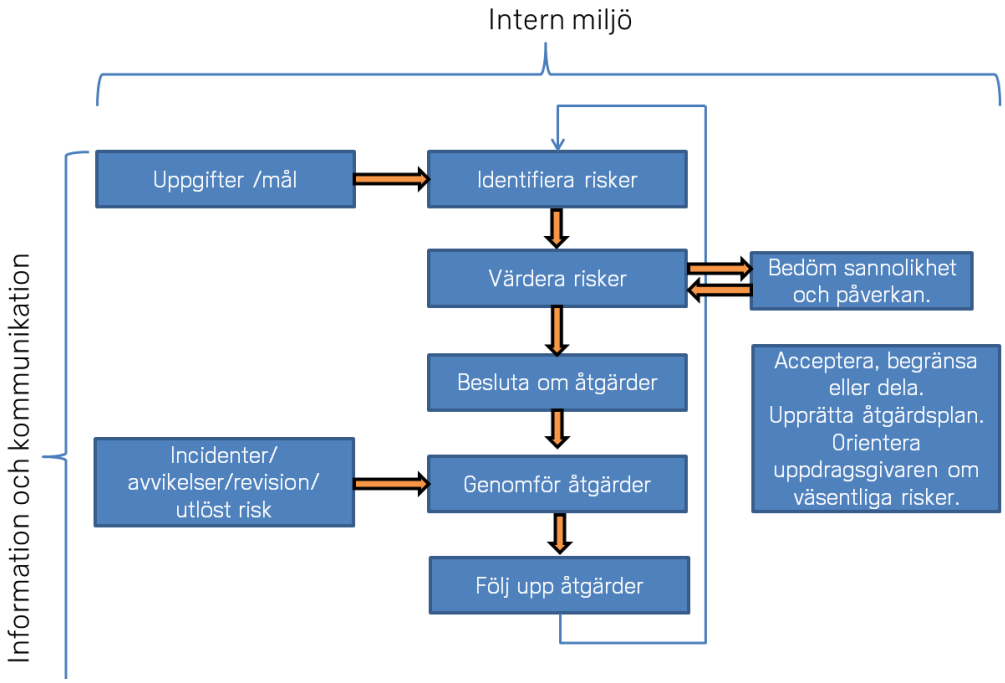


Bild 4.1. Illustration över de delar som ingår i arbetet med risker/Ekonomistyrningsverket.

4.2. Riskanalys av uppdrag och uppgifter

Regeringen styr Försvarsmaktens verksamhet huvudsakligen genom regleringsbrev, förordning (2007:1266) med instruktion för Försvarsmakten samt särskilda regeringsbeslut. Vid ÖB:s årliga avvägning genomförs en riskanalys som kompletteras utifrån styrningarna i regleringsbrevet. De väsentligaste riskerna på myndighetsnivån som finns kopplade till uppdragen och uppgifterna dokumenteras med åtgärdsplaner som kontinuerligt följs upp. Allteftersom uppgifter delegeras inom Försvarsmakten till C OrgE, genomförs riskanalyser med åtgärdsplaner som följs upp och dokumenteras. Väsentliga risker med åtgärdsplaner återrapporteras till uppdragsgivaren. ÖB DUC med uppdrag och uppgifter återrapporterar väsentliga risker i månadsrapporteringen.

4.2.1. Identifiera risker

Med risk menas i detta sammanhang en omständighet som påverkar Försvarsmaktens möjlighet att fullgöra en uppgift eller nå ett uppsatt eller ålagt mål.

Riskidentifiering i förhållande till uppgifter och mål ska därför vara utgångspunkten för riskhantering och utgör det *första steget* i att ta fram riskanalys. Inledningsvis granskas de omständigheter som kan påverka möjligheten att nå uppsatta mål. Riskidentifiering innebär att chefer och medarbetare beskriver de omständigheter som är kända. Omständigheterna behöver inte ha inträffat som händelser inom verksamheten för att de ska fångas upp i identifieringen. Riskidentifieringen kan exempelvis göras i form av en utvärderande workshop eller som en mer strukturerad SWOT[2]-analys.

Riskidentifieringen genomförs övergripande av de uppgifter som tilldelats. Detta för att ge en helhetsbild av nuläget inom aktuell enhet eller motsvarande, och att exponera de riskområden som därefter bör undersökas mer i detalj. Varje relevant risk bör beskrivas koncist och på ett sätt som gör det möjligt för andra i organisationen att kunna förstå riskens orsak och påverkan samt effekt på verksamhetens mål. Risk uttrycks ofta som en kombination av påverkan och sannolikhet. Riskbeskrivningar ska vara begripliga, entydiga, ge underlag för prioritering och kunna följas upp.

Exempel

- *Det är en risk att .....<osäkerhet mot mål>.....orsakad av < existerade omständigheter>....vilket resulterar i <effekter på mål>*
- *Som ett resultat av…<existerade omständigheter>, uppstår…<osäkerheter>, vilket leder till…< effekter på mål>*

I riskbeskrivningen i samband med riskidentifiering ska *orsak* till risken och riskens *konsekvens* samt *effekten* på verksamhetsmålen dokumenteras. Det ger underlag för att bedöma förebyggande och skadebegränsande åtgärder.

[2] Strengths, weaknesses, opportunities and threats.

Då riskerna har identifierats ska de värderas. De identifierade riskerna ska dokumenteras av de som genomför riskanalysen. Nedan finns de fyra riskområden som Försvarsmakten använder samt exempel på riskfaktorer kopplade till dessa.

Påverkan att genomföra verksamheten effektivt

- Tillgång till nyckelpersonal.
- Tillgång och tillgänglighet till materiel.
- Personalomsättning.
- Rekrytering.
- Verksamhetssäkerhet
- IT-tjänster och IT-säkerhet.
- Säkerhetstjänst
- Infrastruktur.
- Systematiskt arbetsmiljöarbete.
- Kriskommunikation.

Påverkan att följa lagar, förordningar, avtal[3] och interna regler och styrningar

- Avtalsinnehåll.
- Okunskap om interna regler och rutiner.
- Fel eller bristande information om lagar och förordningar.
- Svårigheter att hålla sig uppdaterad på förändringar i lagar, förordningar och avtal som styr verksamheten.
- Målkonflikter – exempelvis att utbetalning i rätt tid prioriteras före att utbetalningen blir rätt.
- Otydlig uppgiftsställning.
- Oegentligheter.

Påverkan att rapportera och följa upp verksamhet på ett rättvisande sätt

- Felaktig eller bristfällig bokföring.
- Administrativt stöd saknas eller är bristfälligt.
- Bristande kompetens i organisationen.
- Brister i rutiner för löpande uppföljning.
- Ledningens intresse för uppföljning, information och kommunikation.
- De tekniska system som finns är inte ändamålsenliga.
- Bristande förändringsvilja i organisationen.

Påverkan att genomföra verksamhet med god hushållning av statens medel

- Sena eller uteblivna betalningar.
- Risk för oegentligheter vid till exempel utbetalningar.
- Risk för att andra behov än verksamhetens styr hur pengarna används.
- Myndighetens utgifter kan inte motiveras, exempelvis ogynnsamma avtal.
- Kostnads-/nyttokalkyler saknas.

[3] Exempel på avtal är; ramavtal, kollektivavtal, bilaterala och multilaterala avtal.

4.2.2. Värdera risker

Vid en systematisk identifiering av risker är det inte ovanligt att antalet identifierade risker blir stort. Det är därför nödvändigt att prioritera vilka av riskerna som ska hanteras vidare utifrån hur allvarliga konsekvenser respektive risk bedöms ha. Det är en fördel om uppgiftställarens egen riskanalys är tillgänglig i det fortsatta arbetet. Det sker lämpligen genom att de identifierade mest väsentliga riskerna dokumenteras till exempel i FMVP och Produktionsledningens verksamhetsuppdrag (PROD VU).

Den vanligaste metoden för att värdera riskerna är att använda riskmatrisen där sannolikhet och påverkan värderas. Ibland räcker det dock med en konsekvensanalys om sannolikheten inte behöver värderas. Det gäller exempelvis vid mål som innebär nollvision. Som vägledning i riskvärderingen finns en beskrivning av indikatorer som tjänar som stöd för värdering av riskernas sannolikhet och påverkan.

Sannolikhet (indikatorerna tjänar som hjälp vid bedömningen av sannolikhet)
Mycket hög
Händelse som kommer att ske och som kan inträffa när som helst.
Hög
Händelser som är kända för att kunna inträffa och som kan förväntas inträffa.
Medel
Händelser som kan inträffa och som kanske kan förväntas inträffa.
Låg
Händelsen kan inträffa vid något enstaka tillfälle. Det finns kända fall av händelsen.
Mycket låg
Händelsen har inte inträffat förut och bedöms inte hända inom en överskådlig framtid.

Påverkan (indikatorerna tjänar som hjälp vid bedömningen av påverkan)
Mycket stor
Har mycket stor påverkan på möjligheten att lösa uppgiften och konsekvensen är mycket allvarlig. Stor skada på förtroende och varumärke, stor negativ medieuppmärksamhet. Stora ekonomiska konsekvenser och stor påverkan på budget. Mycket allvarliga brister i styr- och kontrollmiljön.
Stor
Har stor påverkan på möjligheten att lösa uppgiften och konsekvensen är allvarlig. Stora skada på förtroende och varumärke, betydande negativ medieuppmärksamhet. Stora ekonomiska konsekvenser och betydande påverkan på budget. Allvarliga brister i styr- och kontrollmiljön.
Betydlig
Har betydlig påverkan på möjligheten att lösa uppgiften och konsekvensen är kännbar. Viss skada på förtroende och varumärke, viss negativ medieuppmärksamhet. Betydande ekonomiska konsekvenser och kännbar påverkan på budget. Kännbara brister i styr- och kontrollmiljön.
Ringa
Har ringa påverkan på möjligheten att lösa uppgiften och konsekvensen är måttligt kännbar. Viss skada på förtroende och varumärke, viss medieuppmärksamhet. Små ekonomiska konsekvenser och liten påverkan på budget. Kännbara brister i styr- och kontrollmiljön.
Försumbar
Har försumbar påverkan på möjligheten att lösa uppgiften och konsekvensen är obetydlig. Ingen skada på förtroende och varumärke, ingen negativ medieuppmärksamhet. Försumbara ekonomiska konsekvenser och försumbar påverkan på budget. Försumbara brister i styr- och kontrollmiljön.

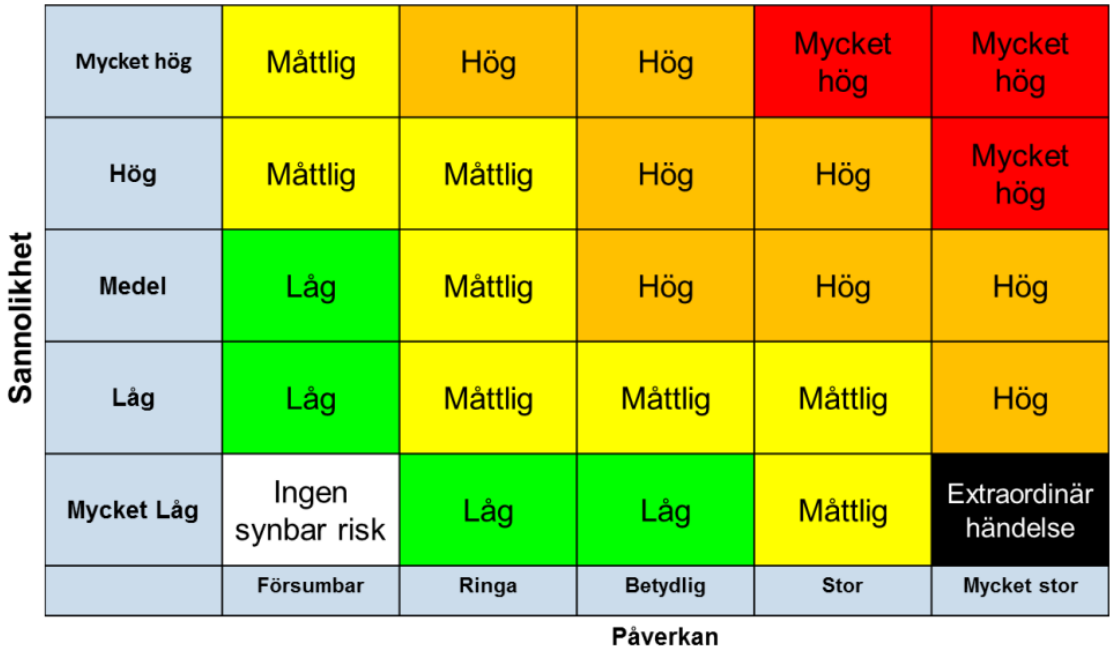


Bild 4.2. Riskvärdering/Försvarsmakten.

4.2.3. *Hantering av risker.*

Det tredje steget i riskhanteringen är att ta ställning till hur riskerna ska hanteras. De identifierade riskerna som bedöms som väsentliga ska rapporteras till uppgiftslämnaren tillsammans med föreslagna åtgärder.

Acceptera risk (1). Risken kvarstår utan att någon åtgärd vidtas. Valet av detta alternativ beror på att risken bedöms vara värd att ta och att alternativa hanteringar inte är kostnadseffektiva eller genomförbara. De tre ”ettorna” i figuren nedan visar att dessa risker kan förekomma i större delen av spannet av riskexponeringar.

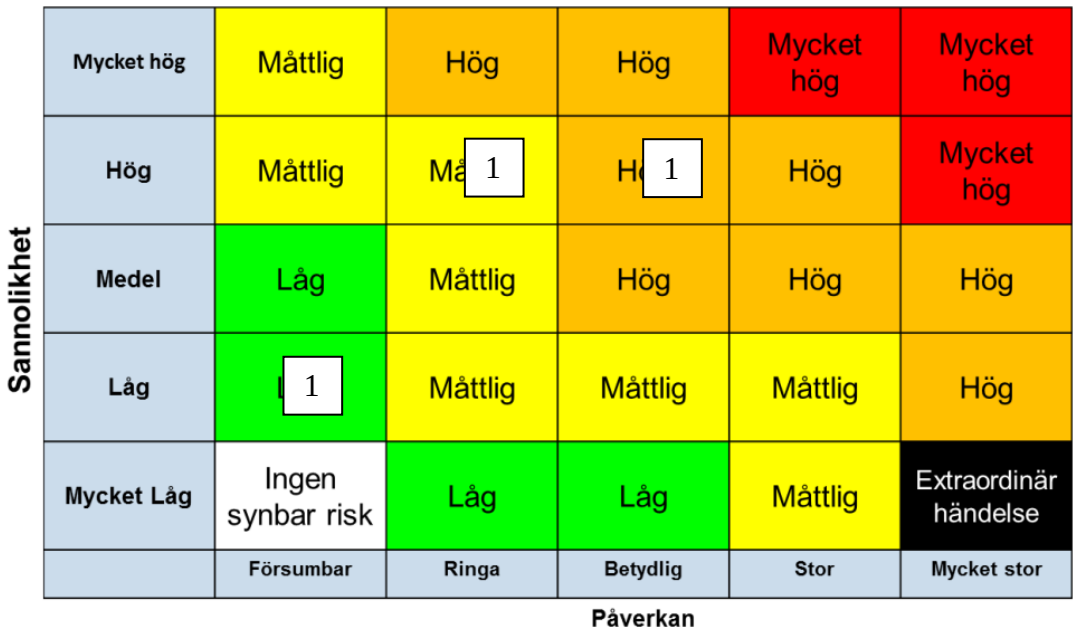


Bild 4.3. Acceptera risk/Försvarsmakten.

Reducera risk (2). Påverkan och/eller sannolikhet för att risken reduceras när detta bedöms vara kostnadseffektivt. De riskreducerande åtgärderna kan t.ex. utgöras av processförbättringar, kompetensutveckling, omfördelning av resurser eller åtgärder för att skapa handlingsberedskap. De kan vara förebyggande och/eller skadebegränsande. Exempel på förebyggande åtgärder är ansvars- och arbetsfördelning, attestregler, omfördelning av resurser och inbyggda kontrollfunktioner i IT-system. Exempel på skadebegränsande åtgärder är inventeringar, avstämningar och resultatanalys.

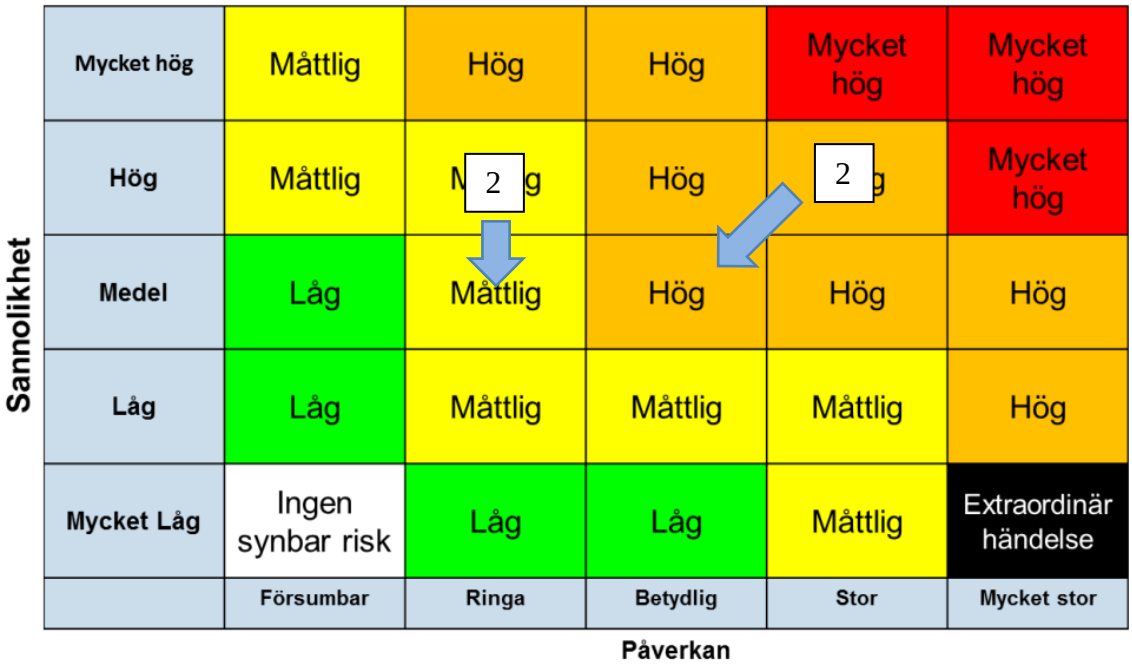


Bild 4.4. Reducera risk/ Försvarsmakten.

Undvika risk (3). Den som tilldelats en uppgift lämnar helt eller delvis tillbaka uppgiften då risken bedöms vara för stor och inte går att reducera till rimlig kostnad. Det kan innebära att ansvarig chef beslutar att helt avstå från att genomföra t.ex. ett projekt. Om risken är kopplad till en tilldelad uppgift, beslutar uppgiftställaren om uppgiften ska utgå.

Överföra (dela) risk (4). Risken överförs helt eller delvis till extern part som har bättre förebyggande och/eller skadebegränsande riskåtgärder och därmed bättre förutsättningar att kostnadseffektivt kunna hantera risken. Risken kan också helt eller delvis överföras genom försäkring till annan part (t.ex. till Kammarkollegiet) som har större ekonomiska förutsättningar att kostnadseffektivt kunna bära risken. En risk kan endast överföras till extern part. Internt sker byte av riskägare, d.v.s. den som har ansvar för uppgiften och de risker som är kopplade till den.

Observera
De risker som hamnar i kategorin *mycket hög* ska hanteras omgående för att kunna reduceras till en lägre risknivå.

5. Åtgärder/riskhantering

Verksamhetsansvariga väljer ut de risker som ska hanteras och vidtar åtgärder. Exempel på riskhantering är att minska förutsättningarna för att risker löser ut, underlätta att göra rätt, genomföra förkontroller och tester samt åtgärder för att upptäcka och korrigera fel som redan gjorts dvs. efterkontroller. Det är väsentligt att tidigt i riskhanteringen arbeta med riskreducerande åtgärder, dels för att minska sannolikheten för att en risk löser ut och dels för att minska konsekvenserna för verksamheten i det fall risken löser ut.

Förebyggande åtgärder kan vara planering, åtgärder för rekrytering, utbildning, utformning av instruktioner och handböcker som underlättar att göra rätt. Exempel på förebyggande åtgärd är spel, analyser samt kontinuitetsplanering i de gemensamma processerna.

Uppföljande åtgärder kan vara både manuella och automatiska. Löpande uppföljning av verksamhetsplaner för att säkerställa att planerad verksamhet har genomförts. Ekonomisk uppföljning av verksamhet är ett sätt att följa upp att budgeten följs. Ett annat exempel är uppföljning av utbetalning av löner och tillägg.

Korrigerande åtgärder innebär att fel rättas till när det upptäcks på ett sätt som säkerställer att det inte uppstår igen, varken där det uppstått eller på annan plats i organisationen. Avvikelsehanteringen fungerar korrigerande då åtgärder vidtas för att oönskade händelser inte ska upprepas. Felet kan till exempel ha sin orsak i att en rutin inte följs på grund av att den inte är känd. Regelverk kan uppdateras för att underlätta att göra rätt. Ett annat exempel är korrigering av felaktigheter i bokföringen.

När verksamheten har prioriterat vilka risker som ska hanteras fastställs hur riskhanteringen för dessa ska utformas. Det ska dokumenteras med beskrivning av åtgärden, vem som ansvarar för att beslutade åtgärder vidtas, tidsplan samt en löpande statusuppdatering. Verksamhetsansvarig chef ska rapportera de mest väsentliga riskerna med tillhörande åtgärder till uppdragsgivaren. Alla risker som omfattar allvarlig skada på personal, materiel eller egendom ska rapporteras.

Referensnummer	
Uppgift/mål	Uppgift eller mål som risken är kopplad till.
Riskområde	1. Påverkan att driva verksamheten effektivt. 2. Påverkan att följa lagar, förordningar, avtal och interna regler och styrningar. 3. Påverkan att rapportera och följa upp verksamhet på ett rättvisande sätt. 4. Påverkan att genomföra verksamhet med god hushållning av statens medel.
Identifierad risk	Beskrivning av risken.
Riskvärde	* Mycket hög * Hög * Måttlig * Låg
Åtgärd	Beskrivning av planerad åtgärd eller åtgärder.
Ansvarig	Ansvarig person för riskhanteringen.
Tidplan	När en åtgärd beräknas vara klar samt när uppföljning ska ske.
Status	Lägesbeskrivning av hur risken hanteras.
Återrapportering	Är risken av väsentlig betydelse ska den rapporteras till uppdragsgivaren.

Bild 5.1. Åtgärdsplanen utformning/Försvarsmakten.

Åtgärdsplanen och de tillhörande rapporteringsrutinerna fungerar som ett sätt att säkerställa att riskanalysen och åtgärderna är tillräckliga för att ligga till grund för bedömningen av den interna styrningen och kontrollen. Åtgärdsplanen är en del av den ordinarie verksamhetsuppföljningen. Mall för åtgärdsplan återfinns i bilaga 1.

6. Uppföljning och utvärdering

Uppföljning och utvärdering av arbetet med den interna styrningen och kontrollen är en förutsättning för att kunna säkerställa att verksamheten fungerar på avsett sätt. Det motiverar även medarbetare till att bli mer riskmedvetna. En kontinuerlig uppföljning möjliggör även för ledningen att tidigt göra korrigeringar av fördelningen av resurser, prioriteringar och ansvar. Den som tilldelats uppgifter och identifierat risker kopplat till dessa ansvarar för att följa upp att åtgärder vidtas för att hantera risken samt att väderingen av risken är aktuell. Riskanalyser och åtgärder som vidtas med anledning av analysen ska dokumenteras i den omfattning som är nödvändig för uppföljning och bedömning av om den interna styrningen och kontrollen är betryggande.

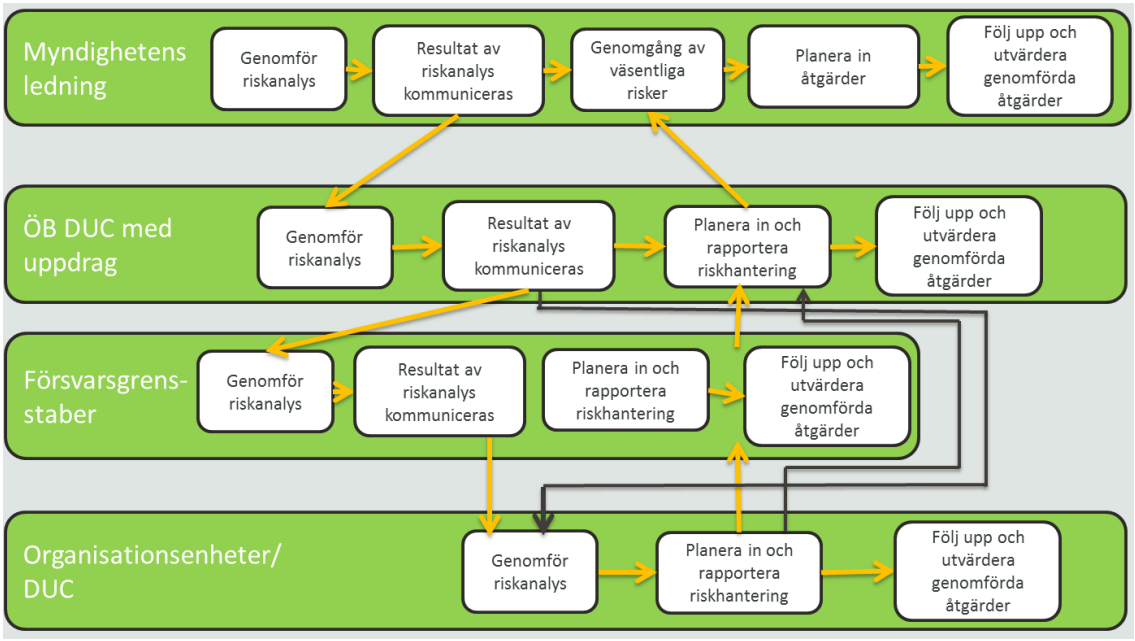


Bild 6.1 Principskiss för riskhantering[4]/Försvarsmakten.

[4] Försvarsmakten inrättar försvarsgrensstaber från 2019. Intill dess att försvarsgrensstabernas styrning och kontroll fullt har etablerats kommer produktionsledningen i tillämpliga delar understödja försvarsgrensstabernas styrning och kontroll av underställda organisationsenheter.

6.1. Uppföljning av riskbedömning

C OrgE och andra verksamhetsansvariga rapporterar löpande de mest väsentliga riskerna inklusive åtgärder till uppdragsgivaren. Analys av inrapporterade risker ska återkopplas. Försvarsgrensstaberna sammanställer återrapporterade väsentliga risker och återrapporterar en sammanvägd bedömning av väsentliga risker till Produktionsledningen. Respektive ÖB DUC sammanställer därefter de inkomna underlagen samt gör en egen bedömning som återrapporteras i månadsredovisningarna till Försvarsmaktsledningen.

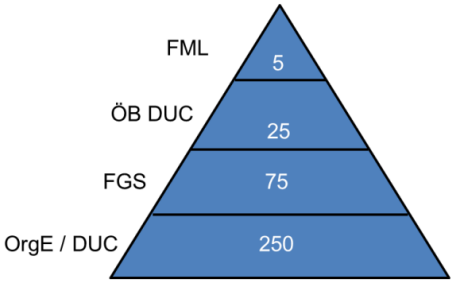


Bild 6.2 Exempel på hur antalet väsentliga risker varierar på olika nivåer/Försvarsmakten.

Försvarsmaktens riskbedömning på myndighetsnivån utgör grunden för överbefälhavarens intygande i årsredovisningen om en betryggande intern styrning och kontroll. Denna bedömning ska säkerställa att:

- Försvarsmakten med hjälp av riskanalyser har identifierat omständigheter som utgör en risk för att myndighetsledningen inte fullgör ansvaret för verksamheten.
- Myndighetens riskanalys är ändamålsenlig och anpassad efter Försvarsmaktens behov.
- Riskanalysen identifierar och värderar risker samt tar ställning till om och hur risken ska hanteras.
- Myndigheten har vid behov uppdaterat genomförd riskanalys för att säkerställa att den omfattar aktuella risker.

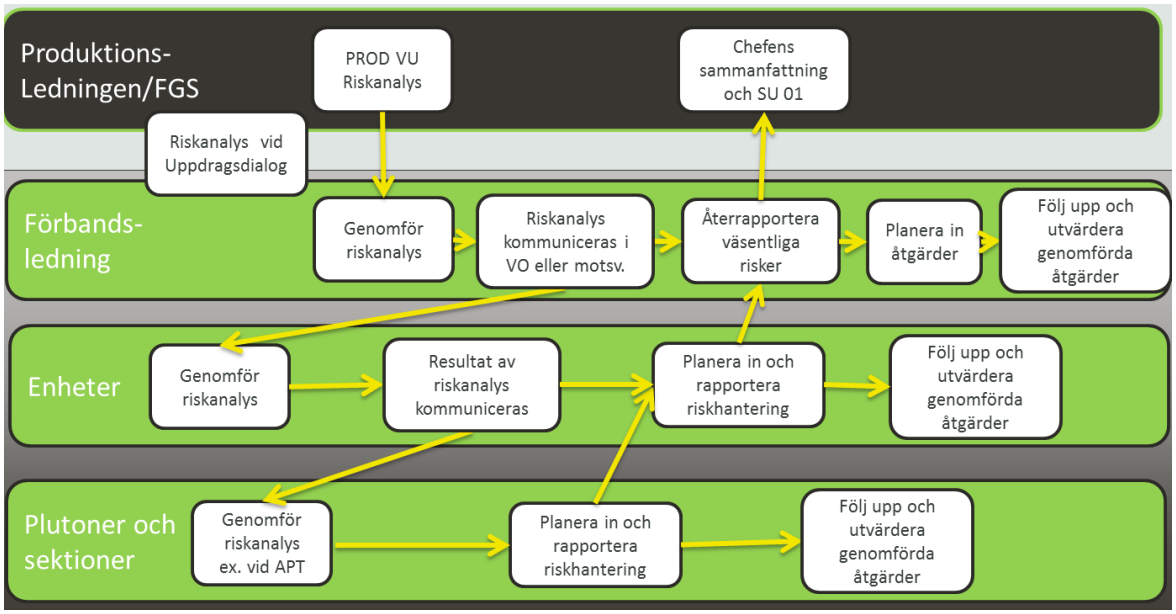


Bild 6.3 Principskiss för riskhantering vid OrgE/Försvarsmakten.

Vid OrgE sker riskhanteringen som en integrerad del vid genomförande av verksamheten. Riskanalyser och åtgärder för att hantera risker ska dokumenteras i den utsträckning som behövs för att kunna följa upp risker och rapportera in väsentliga risker till uppdragsgivaren.

6.2. Utlösta risker

När en risk löser ut eller det inträffar en händelse som kan påverka möjligheten att uppnå givna uppgifter eller uppsatta mål ska det hanteras enligt följande.

1. *Klarlägg vilken uppgift eller vilket mål som den utlösta risken eller inträffade händelsen är kopplad till.*
2. *Beskriv vad som har inträffat som löste ut risken eller incidenten.*
3. *Beskriv riskhistoriken och vilka åtgärder som vidtagits i riskhanteringen*
4. *Beskriv effekten av den utlösta risken eller händelsen.*
5. *Beskriv påverkan på andra identifierade risker*
6. *Identifierade nya risker som uppstår på grund av den utlösta risken*
7. *Utarbeta en åtgärdsplan*
8. *Rapportera att risken löst ut eller händelse inträffat till uppdragsgivaren*

Mall för dokumentation av utlöst risk finns i bilaga 2.

6.3. Uppföljning och utvärdering av ISK-arbetet

För att säkerställa att statusen på arbetet med intern styrning och kontroll i Försvarsmakten är ändamålsenlig bör det årligen genomföras uppföljning och utvärdering. Det görs främst genom självutvärdering ur ett systematiskt perspektiv, där de som tilldelas uppgifter och genomför riskanalys värderar statusen på de egna åtgärderna inom intern styrning och kontroll. Självutvärderingen omfattar en granskning av egna styrdokument, arbetsordningar och verksamhetsplaner, en bedömning av riskhanteringen och genomförandet av åtgärder samt uppnådd effekt. Vidare ska självutvärderingen innehålla en åtgärdslista för hur och när den egna hanteringen av intern styrning och kontroll ska utvecklas. Självutvärderingen ska dokumenteras och följas upp av den som arbetar med riskhanteringen samt kommuniceras med uppdragsgivaren.

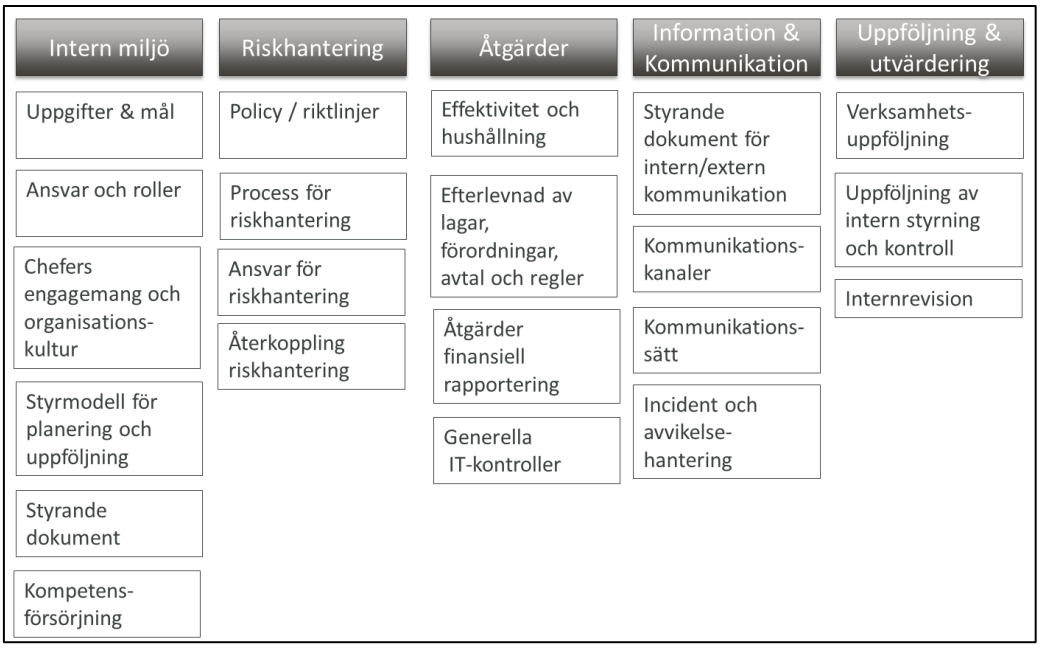


Bild 6.4 Exempel på utvärdering av ISK-status/Försvarsmakten.

Exemplet på bild 6.4 är en modell för självutvärdering. Den beskriver de olika momenten i intern styrning och kontroll och visar vad som ingår under respektive del. Vid självutvärderingen bedöms den egna förmågan inom respektive ruta genom att ställa frågor. Exempel på frågor att ställa i fältet *Uppgifter & mål* kan vara – Är *Uppgifter och mål* tydligt formulerade och är de genomförbara? Frågor och svar i självutvärderingen ska dokumenteras. Resultatet av utvärderingen markeras med färgerna grön, gul och röd i fälten, beroende på hur väl det bedöms fungera. Grön färg används för moment som bedöms fungera bra, gul för moment som kan förbättras och röd färg används för moment med större förbättringsbehov.

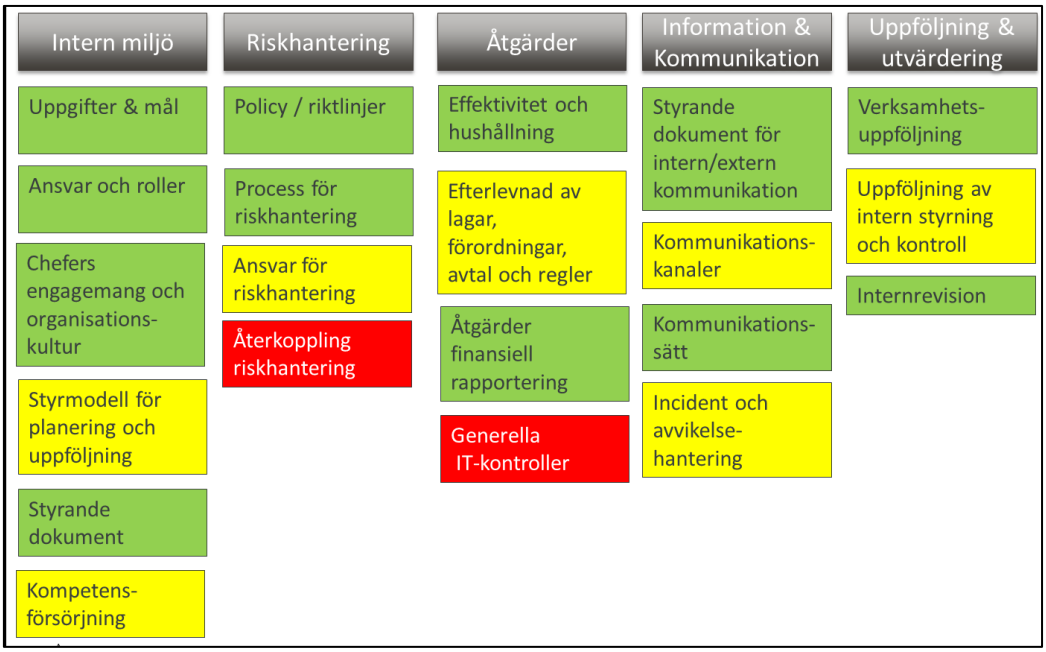


Bild 6.5 Exempel på utvärdering av ISK-status/Försvarsmakten.

När självutvärderingen är genomförd har fälten färgkodats utifrån den bedömda statusen.

Som ett led i självutvärderingen bör ett antal förbättringsområden väljas ut inom de olika momenten som sedan sammanställs i en handlingsplan. Arbetet med förbättringsåtgärder genomförs och resultatet redovisas för ledningen. Resultatet bör återspeglas vid nästa självutvärdering. Uppföljningen bör alltså visa om de införda åtgärderna resulterat i det som avsågs och om angreppsätten och underlaget för värderingen varit lämplig.

6.4. Internrevisionens uppgifter[5]

Försvarsmaktens internrevision ska självständigt granska och lämna förslag till förbättringar av myndighetens arbete inom ramen för intern styrning och kontroll. Vidare ska internrevisionen utifrån en analys av verksamhetens risker självständigt granska om ledningens interna styrning och kontroll är utformad så att Försvarsmakten med rimlig säkerhet kan fullgöra kraven på en betryggande intern styrning och kontroll[6].

7. Myndighetsledningens ansvar

Intern styrning och kontroll är i stor utsträckning fråga om ansvar. Ytterst handlar det om ett ledningsansvar även om medarbetarna deltar i arbetet.

7.1. Myndighetsledningens arbete

Myndighetens ledning ska bilda sig en egen uppfattning om den interna styrningen och kontrollens effektivitet och besluta om vilka som är de väsentligaste riskerna samt vilka åtgärder som ska vidtas. Genom en löpande avrapportering från ÖB DUC och beslut om åtgärder kan myndighetsledningen göra detta.

Myndighetens ledning fokuserar särskilt på fyra områden[7] inom intern styrning och kontroll:

1. *Riskacceptansnivå i Försvarsmakten.* Riskacceptansen är den övergripande nivån på risker som bedöms som godtagbara för verksamheten. Ledningen avgör den risknivå som ska gälla inom myndigheten.

2. *Leda utvecklingen av intern styrning och kontroll.*[8] Myndighetens ledning ansvarar för att riskhanteringen sker på ett systematiskt sätt. Med riskanalys identifieras de omständigheter som kan leda till att myndighetsledningen inte fullgör ansvaret för verksamheten. Riskanalysen ska vara ändamålsenlig och anpassad efter Försvarsmaktens behov samt identifierar, värderar och tar ställning till

[5] 3-4 §§ Internrevisionsförordning (2006:1228)
[6] 3§ Myndighetsförordning (2007:515)
[7] Rekommendation i COSO (Committe of Sponsoring Organizations of the Treadway Commission).
[8] I förordningen (2007:603) om intern styrning och kontroll benämns detta som *Processen för intern styrning och kontroll*.

eventuella åtgärder. Den genomförda riskanalysen uppdateras vid behov för att säkerställa att den är aktuell och relevant.

3. *Risker i förhållande till risknivån.* Utifrån ÖB:s årliga avvägning samt målsättningarna i Försvarsmaktens strategiska inriktning (FMSI) och FMVP, bedöms de väsentligaste riskerna som myndigheten står inför i förhållande till den riskacceptansnivå som fastställts.

4. *Kontinuerlig information om väsentliga risker och hur dessa åtgärdas.* Säkerställa kontinuerliga kommunikationskanaler mellan ÖB DUC och överbefälhavaren för att säkerställa tillförlitlig information i rätt tid.

Myndighetsledningens bedömning av utvecklingen av intern styrning och kontroll baseras på självutvärderingar samt rapporter från intern och extern revision.

7.2. Bedömningen i årsredovisningen

Överbefälhavarens bedömning av den interna styrningen och kontrollen utgår från den dokumentation som upprättats om riskanalys, beslut om åtgärder och uppföljning. Om det förelegat brister i den interna styrningen och kontrollen ska dessa beskrivas i dokumentationen.

Som grund för underskriftsmeningen bör det lämnas en redovisning av de omständigheter som legat till grund för bedömningen av den interna styrningen och kontrollen. Redovisningen kan även omfatta en beskrivning av de väsentligaste riskerna, hur dessa har hanterats samt hur eventuella brister åtgärdats.

8. Regelefterlevnad

Grunden i regelefterlevnad är att utforma reglerna så tydligt att de som vill göra rätt också kan göra rätt. Kontinuerligt arbete genomförs i syfte att förtydliga styrningen samt genomföra informations- och utbildningsinsatser. Målet är att gällande regelverk är tydliga, kommunicerade, förstådda samt accepterade hos Försvarsmaktens chefer och medarbetare. Trots detta arbete uppstår det större eller mindre fel i form av oönskade händelser. När ett fel inträffar är det viktigt att det snabbt upptäcks och korrigeras.

8.1. Tre försvarslinjer

I arbetet med regelefterlevnad tillämpar Försvarsmakten principen om de tre försvarslinjerna[9]. Det innebär i korthet att den första försvarslinjen är en beskrivning av det ansvar som chefer oavsett nivå i Försvarsmakten har för hantering av risker.

Den andra försvarslinjen utgörs av funktioner för riskhantering och regelefterlevnad. Bland annat övervakar, kontrollerar och rapporterar den andra linjen myndighetens risker och hur interna och externa regelverk följs.

I den tredje försvarslinjen utför Internrevisionen, Säkerhetsinspektionen, Militära flyginspektionen samt Försvarsinspektören för hälsa och miljö (FIMH), samt den interna miljörevisionen revision, granskning och kontroll av verksamheten. Syftet är att säkerställa att Försvarsmakten följer lagar, förordningar, avtal och andra regler som garantera säkerhet, effektivitet, miljöhänsyn m.m. Militära flyginspektionen och FIHM utövar dessutom tillsyn. Då tillsyn utövas är Militära flyginspektionen och FIHM inte underställda överbefälhavaren utan lyder direkt under regeringen.

Bortom den tredje försvarslinjen finns den externa revisionen som för Försvarsmaktens del utgörs av Riksrevisionen.

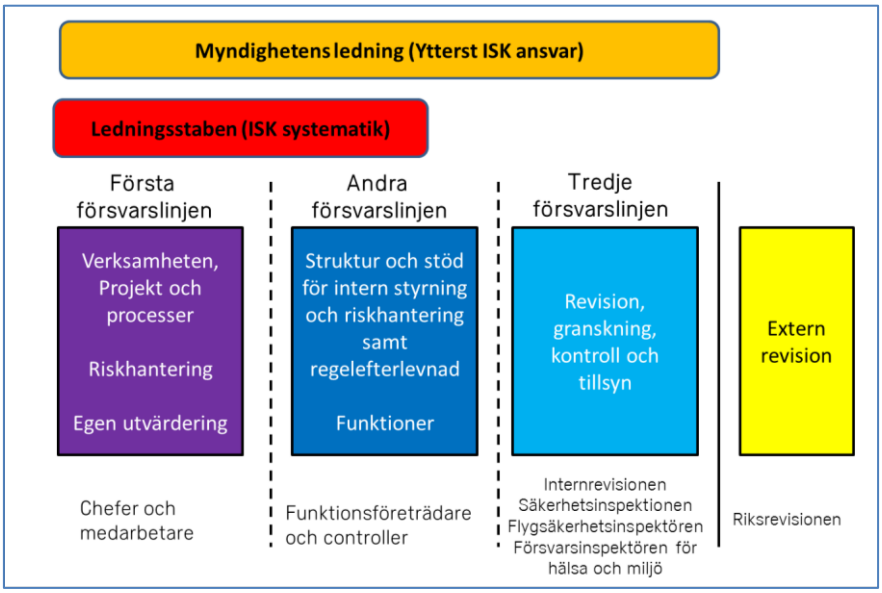


Bild 8.1. Principskiss för tillämpning av de tre försvarslinjerna/Försvarsmakten.

[9] Tillämpning av COSO:s 3:e princip.

9. Förebygga och upptäcka oegentligheter

9.1. Inledning

Statlig verksamhet bygger på förtroende. En viktig del i att upprätthålla det förtroendet är att myndigheterna aktivt arbetar mot oegentligheter. Försvarsmakten har likt andra myndigheter därför ett särskilt fokus på att upptäcka och förebygga oegentligheter.

Oegentligheter är ett samlingsbegrepp för hela gruppen av oönskade beteenden och handlingssätt med konsekvenser för myndighetens anseende och/eller verksamhet. Begreppet oegentlighet omfattar även korruption vilket innebär att nyttja en offentlig ställning för att uppnå otillbörlig vinning för sig själv eller andra.

Den som upptäcker eller misstänker oegentligheter har inte alltid möjlighet att förhindra aktiviteten. Däremot kan han eller hon på olika sätt slå larm om sina misstankar. För att underlätta för den som vill anmäla misstankar finns det en rutin för såväl rapportering som utredning.

Begreppen oegentligheter/korruption brukar innefatta:
− tagande och givande av muta,
− vänskapskorruption, jäv m.m.
− otillbörlig påverkan,
− förtroendeskadliga bisysslor, andra förmåner,
− att gynna sig själv eller någon på arbetsgivarens bekostnad,
− stöld, bedrägeri, förskingring.

Försvarsmakten har reglerat etiska riktlinjer för anställda i Försvarsmakten avseende jäv, bisyssla samt givande och tagande av muta i H JÄV[10],
En grundläggande del i arbetet med att förebygga risken för oegentligheter är att myndigheten har en bild av vilka riskerna är och inom vilka områden de finns. Risker för oegentligheter i Försvarsmakten hanteras enligt följande metod.

9.2. Försvarsmaktens metod för identifiering och hantering av risker för oegentligheter.

Försvarsmaktens metod[11] för utvärdering av risker för oegentligheter i verksamheten baseras på en modell som är framtagen av *Institute of internal auditors* som har anpassats[12] av Ekonomistyrningsverket för att användas i myndigheter. Metoden omfattar fem steg som beskrivs nedan.

9.2.1. Identifiera relevanta risker för oegentligheter.

För att identifiera områden där risk för oegentligheter föreligger behövs kunskap om myndighetens verksamhet och ett öppet sinne. En risk kan öppna upp för flera möjliga upplägg vad gäller oegentligheter. Systematik och kreativitet krävs för att identifiera vilka typer av oegentligheter som sannolikt kan uppstå.

[10] Handbok Jäv, bisyssla och muta 2015.
[11] IPPF - Practice Guide. Internal Auditing and Fraud. The Institute of Internal Auditors December 2009.
[12] Vägledning. Oegentligheter och intern styrning och kontroll. ESV 2016:24

Medvetenhet inom Försvarsmakten om risker i allmänhet och tidigare inträffade händelser med anknytning till oegentligheter är väsentliga faktorer som spelar in när en riskanalys genomför. Ett lågt riskmedvetande är en betydande risk i sig. Det kan medföra att det inte kommer några signaler om oegentligheter trots att det finns en hög risk i verksamheten. Tidigare händelser kan också ha gett kunskaper och insikter som är användbara i arbetet med riskanalysen.

Vad är sannolikheten att en oegentlighet ska uppstå och vad skulle det få för konsekvenser för myndigheten? Utvärdera verksamheten systematiskt och ställ kontrollfrågor som exempelvis:

- Var finns det luckor i Försvarsmaktens kontroller?
- Finns det brister i handläggningsrutinerna?

Vissa processer är mer riskutsatta än andra. Dessa behöver granskas extra noggrant. Exempel på extra utsatta processer:

- Processer där myndigheten fattar beslut med ekonomisk eller personlig påverkan för den som är föremål för beslutet. Det kan till exempel röra sig om beslut kopplade till upphandling av materiel och tjänster.
- Processer där möjlighet ges att direkt komma över pengar eller varor. Exempel på detta kan vara lönetillägg eller inköp.

9.2.2. Identifiera möjliga upplägg för oegentligheter och rangordna dem utifrån risk.

Det är viktigt att ha ett brett perspektiv när möjliga upplägg för oegentligheter ska identifieras. Det finns personer inom Försvarsmakten som har bättre möjligheter att utnyttja luckorna i myndighetens kontroller än andra. Därmed inte sagt att de agerar utifrån möjligheterna. Det är personer i ledande ställning, nyckelpersoner, personer med lång erfarenhet om myndighetens rutiner och personer som ensamma kan fatta beslut om exempelvis beställningar eller utbetalningar. De som kan verksamheten bäst är bäst på att upptäcka och förebygga men de är samtidigt de som har bäst möjlighet att utnyttja systemet.

Det kan uppstå situationer där scenarier väljs bort då de bedöms att de är för långsökta och aldrig har inträffat tidigare. Vissa av de mer ovanliga scenarierna kan dock medföra allvarliga konsekvenser för myndigheten. Det kan exempelvis handla om att myndighetens förmåga att bedriva sin verksamhet under en längre period försvåras. Ett annat scenario är att myndigheten drabbas av en allvarlig förtroendeskada. När så bedöms kunna vara fallet bör det tas med i riskanalysen trots att sannolikheten att det ska inträffa bedöms som låg.

9.2.3. Identifiera vilka kontroller som finns på plats för att förebygga riskerna och om det saknas kontroller som borde finnas.

Tvåsamheten är en grundläggande del av den interna styrningen och kontrollen. Om den utförande och den kontrollerande personen i samarbete kan genomföra en oegentlighet

ökar risken. Detsamma gäller om en anställd har möjlighet att i samarbete med någon utanför myndigheten, exempelvis en leverantör, genomföra ett upplägg.

När riskfaktorer och möjliga upplägg för oegentligheter har identifierats ska det kartläggas vilka kontroller som redan i dag finns på plats för att motverka riskerna. Men innan det görs är det bra att ha skaffat sig en uppfattning om vilka kontroller som borde finnas på plats. Intern styrning och kontroll innefattar policys och rutiner för att hantera risker i organisationens processer. Det kan även handla om att ha extra kontroller av känsligare uppgifter, att ha inbyggda IT-kontroller, spärrlista för behörigheter i PRIO, genomföra informationsvärdering och uppdaterade behörigheter.

9.2.4. Testa effektiviteten i de kontroller som finns på plats.

Testa effektiviteten i de kontroller som finns på plats för att få bekräftat om de motverkar och upptäcker oegentligheter på det sätt som är avsett. Att testa effektiviteten i kontrollerna syftar till att få en uppfattning om kontrollerna fungerar som det är tänkt. Att kontroller har beslutats och att det finns dokumenterade rutiner medför inte med automatik att kontrollerna faktiskt genomförs. De kontroller som har genomförts behöver också vara dokumenterade för att kunna följa upp att kontrollen har genomförts.

Kontrollerna kan indelas i förbyggande och upptäckande för att myndigheten ska kunna få en bild av att det finns en lämplig relation och fördelning mellan förebyggande och upptäckande kontroller. Myndigheten bör även skaffa sig en bild av vilka kontroller som är inbyggda i IT-systemen och om kontrollerna är tvingande.

Det är en del av chefsansvaret att ha kunskap om den interna styrningen och att kontrollen fungerar på avsett sätt inom det egna ansvarsområdet. Därför är det i första hand ansvarig chef som ska se till att det sker en regelbunden uppföljning av effektiviteten i de kontroller som finns för att förebygga och upptäcka oegentligheter.

9.2.5. Dokumentera utvärderingen och rapportera resultatet.

Ovanstående steg i utvärderingen dokumenteras i enlighet med bilaga 1 och rapporteras av organisationsenheter, beroende på lydnadsförhållandena, antingen till FGS eller till PROD. Inom Högkvarteret rapporteras risker för oegentligheter via avdelningar och staber till ledningsstaben. Riskhanteringen följs kontinuerligt upp av den som hanterar risken och för aktiviteter som återstår utses då en ansvarig för genomförande med upprättande av tidsplan.

Den utvärdering som genomförts kan återanvändas och uppdateras nästa gång en övergripande riskvärdering genomförs av området. Det finns ingen anledning att börja om från början utan det är mer effektivt att uppdatera, förbättra och fördjupa den riskutvärdering som redan tagits fram.

10. Exempel på riskhantering inom specifika områden.

Arbetet med riskhantering inom specifika områden kan identifiera risker som har påverkan på uppdrag och uppgifter. De ska i så fall hanteras i enlighet med kapitel 4-6.

Nedan beskrivs några av dessa områden där specifika metoder för riskhantering tillämpas som en del av Försvarsmaktens interna styrning och kontroll.

10.1. Försvarsmaktens gemensamma processer

Riskhantering och kontinuitetsplaneringen i Försvarsmaktens gemensamma processer genomförs enligt anvisningarna på samarbetsytan Verksamhetsutveckling och förvaltningsstyrning som finns på intranätet emilia. Riskhanteringen utgår från de specifika mål och syften i respektive process. Kontinuitetsplaneringen syftar till att kunna använda alternativa tillvägagångssätt vid störningar i verksamheten.

10.2. Insatsverksamhet

För riskhantering vid militära insatser ska Försvarsmaktens gemensamma riskhanteringsmodell användas. Principen för modellen är att inledningsvis fastställa grundvärden utifrån den egna uppgiften och verksamheten. Därefter konkretiseras och bedöms hoten. Till detta identifieras nuvarande skydd och bedömd sårbarhet och med det som grund bedöms risken. När den aktuella risken har analyserats beslutas om åtgärder och en plan för uppföljning.

10.3. Systematiskt arbetsmiljöarbete

Försvarsmaktens systematiska arbetsmiljöarbete hanteras genom interna bestämmelser för myndighetens arbetsmiljöledningssystem (systematiskt arbetsmiljöarbete). Tillämpliga delar av värdegrundsarbete, veteran- och anhörigstödsarbete, jämställdhets- och jämlikhetsarbetet samt försvarspsykologisk verksamhet och friskvård ingår i det systematiska arbetsmiljöarbetet.

Det systematiska arbetsmiljöarbetet syftar till att förebygga ohälsa och olycksfall samt att även i övrigt uppnå en god arbetsmiljö. Rutinerna inom det systematiska arbetsmiljöarbetet är nödvändiga för att säkerställa att målet nås och att Försvarsmakten uppfyller krav i arbetsmiljölagen, jämställdhetslagen, arbetsmiljöförordningar och författningar från bl.a. Arbetsmiljöverket.

10.4. Riskhanteringen vid övningsverksamhet

Reglemente verksamhetssäkerhet (SäkR) har sitt ursprung i det som tidigare benämndes SäkI och innehåller bestämmelser som är gemensamma för Försvarsmakten.

SäkR utgör bestämmelser för att verksamhet ska genomföras med en tolerabel risknivå för personalen och för att minimera skador på materiel, miljö och tredje man. Riskhanteringen vid övningsverksamhet regleras bland annat i Försvarsmaktens säkerhetsbestämmelser. Den syftar till att skapa förutsättningar för att under insats, kunna agera på ett sådant sätt som kan säkerställa verkan och överlevnad.

Riskhantering i övningsverksamhet regleras även i Regler för militär sjöfart (RMS), Regler för militär luftfart (RML) samt andra regler och bestämmelser.

10.5. Hantering av klimatrisker för Försvarsmaktens verksamhet

Riskanalyser och riskhantering av effekter som uppkommer till följd av klimatförändringar sker i enlighet med anvisningar i förordningen (2018:1428) om myndigheters klimatanpassning. En modell för klimat, risk- och sårbarhetsanalyser är under utarbetande 2019 som specificerar metoder och tillvägagångssätt. Riskanalyser ska genomföras för all verksamhet; samtliga försvarsgrenar, organisationsenheter och militärregioner. Bedömningar av konsekvenser och risker från ett förändrat klimat för Försvarsmaktens verksamhet ska inkluderas i långsiktigt strategiskt arbete.

Konsekvenser, risker och sårbarhet av ett förändrat klimat analyseras och bedöms för Försvarsmaktens verksamhet kontinuerligt, och en uppdatering sker minst vart femte år med början 2019. Åtgärdsförslag konkretiseras och prioriteras utifrån riskanalys och riskvärdering.

När riskvärdering är genomförd och åtgärder är prioriterade, beslutas om implementering i en handlingsplan samt en plan för uppföljning och utvärdering. Handlingsplanen ses över årligen men en uppdatering sker minst vart femte år med början 2019.

Syftet är att säkerställa och öka den aktuella och framtida operativa förmågan. Det systematiska klimatarbetet säkerställer Försvarsmaktens och Sveriges måluppfyllelse inom området.

10.6. Systemsäkerhet

Vid planering av materielsystem ställs systemsäkerhetskrav som sedan följer materielsystemet under hela dess livstid. Innan materiel efter anskaffning eller modifiering får tas i bruk inom Försvarsmakten krävs att Högkvarteret har fattat beslut om användning (BOA) för aktuell materiel. Beslut om användning förutsätter att materielbeskrivningar, instruktioner och säkerhetsföreskrifter är framtagna och har delgivits berörda. För att ett sådant beslut ska kunna fattas krävs bl.a. att materielen är säker att hantera och förvara.

10.7. IT-säkerhetstjänst

IT-säkerhetsrisker hanteras i Handbok för Försvarsmaktens säkerhetstjänst, Informationssäkerhet (H SÄK Infosäk). Målgruppen är främst säkerhetschefer och IT-säkerhetschefer samt annan personal som arbetar med informationssäkerhetsfrågor.

Bilaga 1 – Åtgärdsplan riskhantering

FÖRSVARSMAKTEN

Åtgärdsplan riskhantering

Datum Beteckning

Sida 1 (1)

Uppgift/mål	*Ange uppgift eller mål som risken är kopplad till.*
Riskområde	*Ange riskområde*
Identifierad risk	*Beskrivning av risken.*
Riskvärde	*Ange riskvärde*
Åtgärd	*Beskrivning av planerad åtgärd eller åtgärden.*
Ansvarig	*Ange ansvarig person för riskhanteringen.*
Tidplan	*När en åtgärd beräknas vara klar samt när uppföljning ska ske.*
Status	*Lägesbeskrivning av hur risken hanteras.*
Återrapportering	*Är risken av väsentlig betydelse ska den rapporteras till uppdragsgivaren.*

Åtgärdsplanen används för riskhantering i enlighet med H ISK.

Bild B1.1 Mall för åtgärdsplan riskhantering/Försvarsmakten.

Bilaga 2 – Hantering av utlöst risk

FÖRSVARSMAKTEN

Hantering av utlöst risk

Datum Beteckning

Sida 1 (1)

Uppgift/mål	*Ange uppgift eller mål som risken är kopplad till.*
Utlöst risk / Inträffad händelse	*Ange benämningen på risken samt vad som har inträffat.*
Riskhistorik och vidtagna åtgärder	*Beskrivning vidtagna åtgärder för hantering av risken.*
Effekt på mål	*Konsekvensbeskrivning av påverkan på given uppgift eller uppsatt mål.*
Påverkan på andra identifierade risker	*Beskriv vilka andra identifierade risker som påverkas samt utveckla åtgärdsplan vid respektive risk utifrån denna påverkan.*
Identifierade nya risker	*Beskriv nya identifierade risker som uppstått samt upprätta åtgärdsplan för respektive risk.*
Åtgärdsplan	*Beskriv vilka åtgärder som ska vidtas för att hantera konsekvenserna av den utlösta risken.*

Hantering av utlöst risk används i enlighet med H ISK.

Bild B2.1 Mall för hantering av utlöst risk/Försvarsmakten.

Bilaga 3 – Mall för utvärdering av ISK-status

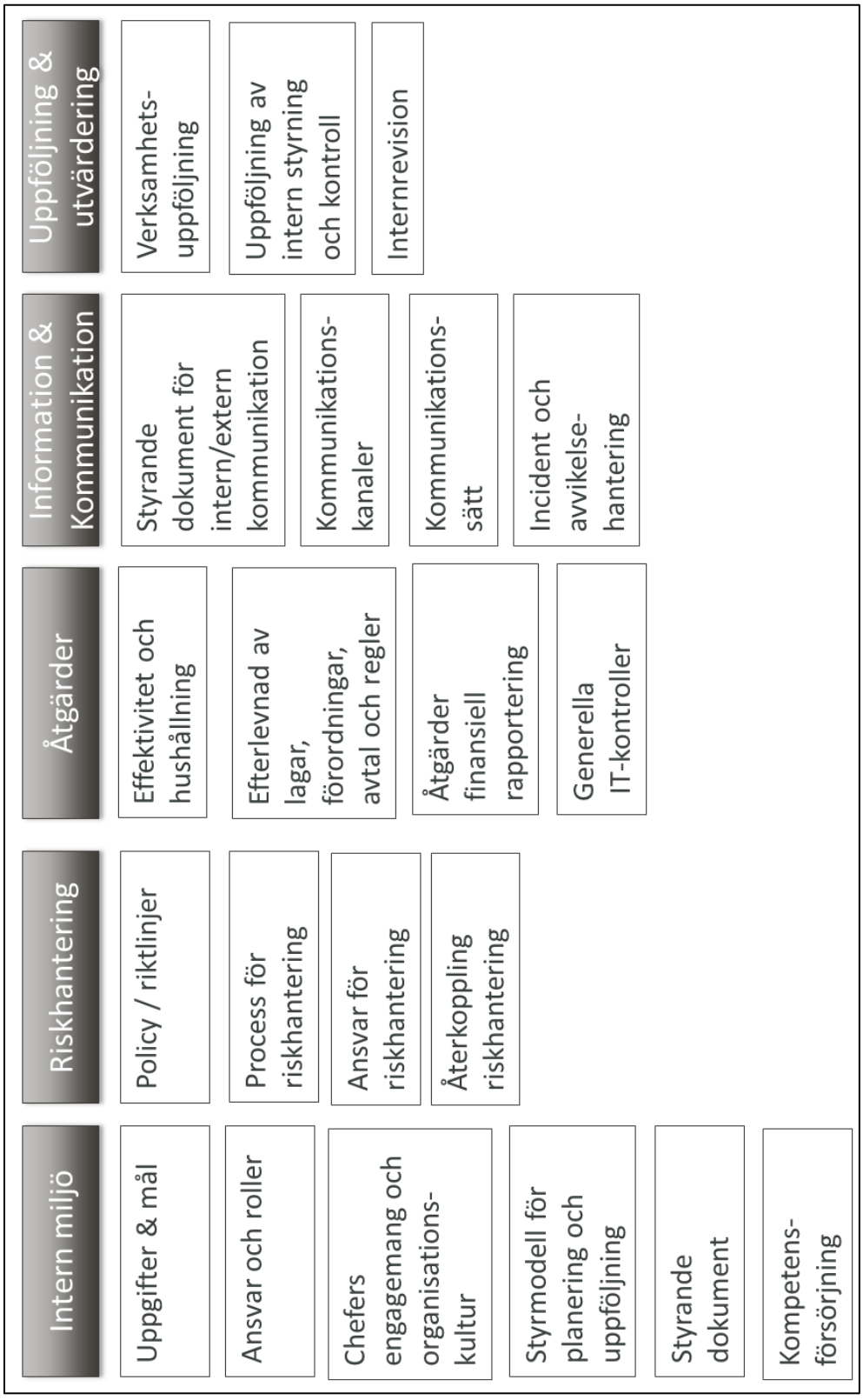


Bild B3.1 Exempel på utvärdering av ISK-status/Försvarsmakten

Redaktionell information

Denna utgåvas text är en revidering av Handbok Intern styrning och kontroll med utgivningsår 2016.

Det huvudsakliga redaktörsarbetet har utförts av Hampe Klein och Pär Mohlin HKV LEDS PLANEK U/A.

Arbetsgång under 2019:

Remissversion skickades ut till HKV ledningar och staber 2019-01-25 med sluttid för återkoppling 2019-02-08. Remissynpunkter har inarbetats i den slutliga utgåvan.

Bakgrund till större förändringar i H ISK 2018:

Försvarsmaktens systematik för arbetet med intern styrning och kontroll har utvecklats sedan den första utgåvan av H ISK kom ut 2016. Vidare har styrande förordningar ändrats varvid de nya lydelserna har inarbetats i Handboken. Begreppen intern miljö samt information och kommunikation bar beskrivits. Ett nytt kapitel om myndighetens arbete med att förebygga och upptäcka oegentligheter har tillkommit.

Bildförteckning

Kapitel 1-8

Bild nr	Illustration	Notering
1.1	Ekonomistyrningsverket	Skriftligt medgivande.
4.1	Ekonomistyrningsverket	Skriftligt medgivande.
4.2	Försvarsmakten	
4.3	Försvarsmakten	
4.4	Försvarsmakten	
5.1	Försvarsmakten	
6.1	Försvarsmakten	
6.2	Försvarsmakten	
6.3	Försvarsmakten	
6.4	Försvarsmakten	
6.5	Försvarsmakten	
8.1	Försvarsmakten	

Bilaga 1

Bild nr	Illustration	Notering
1.1	Försvarsmakten	

Bilaga 2

Bild nr	Illustration	Notering
2.1	Försvarsmakten	

Bilaga 3

Bild nr	Illustration	Notering
3.1	Försvarsmakten	

Litteratur/Källförteckning

Committe of Sponsoring Organizations of the Treadway Commission. (2013). *Internal Control - Integrated Framework COSO.* American Institute of Certified Accountants.

Committe of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise Risk Management - Integrated Framework.* American Institute of Certified Accountants.

Ekonomistyrningsverket. (2011). *Idéskrift Systematiserat sunt förnuft.* Stockholm: Ekonomistyrningsverket.

Ekonomistyrningsverket (2016) *Vägledning. Oegentligheter och intern styrning och kontroll. ESV 2016:24.* Stockholm: Ekonomistyrningsverket.

Försvarets materielverk. (2014). *Intern styrning och kontroll Enterprise Risk Management i FMV.* Stockholm: Försvarets Materielverk.

Försvarsmakten. (2009). *Försvarsmaktens gemensamma riskhanteringsmodell.* Stockholm: Försvarsmakten.

Försvarsmakten. (2015) *Handbok Jäv, bisyssla och muta.* Stockholm: Försvarsmakten

Försvarsmakten. (2017). *Handbok Systematiskt arbetsmiljöarbete.* Stockholm: Försvarsmakten.

Försvarsmakten. (2017). *Reglemente – Verksamhetssäkerhet Gemensam.* Stockholm: Försvarsmakten.

The Institute of Internal Auditors. (2009). *IPPF- Practice Guide. Internal Auditing and Fraud*. The Institute of Internal Auditors.

Regeringen. (u.d.). *Förordningen (2007:603) om intern styrning och kontroll.*

Regeringen. (u.d.). *Internrevisionsförordning (2006:1228).*

Regeringen. (u.d.). *Myndighetsförordning (2007:515).*

Svensk standard (2015) *Miljöledningssystem – Krav och vägledning (ISO 14001:2015)* Stockholm: Swedish Standard Institute

Svensk Standard (2018) *Riskhantering - vägledning (ISO 31000:2018, IDT).* Stockholm: Swedish Standard Institute

Wikland, T. (2012). *Intern styrning och kontroll - både lönsamt och säkert.* Stockholm: FAR Akademin.

Regler, bestämmelser och handböcker som påverkat innehållet i denna handbok

FIB 2018:6 Försvarsmaktens interna bestämmelser med arbetsordning för Försvarsmakten (FMArbO)

Reglemente -

Manual -

Handbok *Försvarsmaktens gemensamma riskhanteringsmodell.* (2009).

Denna handbok beskriver Försvarsmaktens systematiserade arbetsätt för intern styrning och kontroll.

Allt arbete med intern styrning och kontroll inom myndigheten syftar till att Försvarsmakten ska kunna lösa uppgifter och nå de mål som riksdagen och regeringen satt upp. Den främsta uppgiften för Försvarsmakten är att upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp.

Intern styrning och kontroll är en integrerad del av Försvarsmaktens verksamhet och syftar till att ge en rimlig försäkran om att givna uppgifter löses samt att uppsatta mål uppfylls.

FÖRSVARSMAKTEN

107 85 STOCKHOLM
www.forsvarsmakten.se