**Vägledning för aktiv systemförvaltning**

Innehåll

[1 Inledning 4](#_Toc423017627)

[1.1 Bakgrund 4](#_Toc423017628)

[1.2 Syfte med dokumentet 4](#_Toc423017629)

[1.3 Mål med dokumentet 4](#_Toc423017630)

[1.4 Avgränsning 4](#_Toc423017631)

[2 Basfakta 6](#_Toc423017632)

[2.1 Giltighet och revision 6](#_Toc423017633)

[2.2 Referenser 6](#_Toc423017634)

[2.3 Begrepp och förkortningar 6](#_Toc423017635)

[3 Vägledning 7](#_Toc423017636)

[3.1 Definition av aktiv förvaltning 7](#_Toc423017637)

[3.2 Mål med aktiv systemförvaltning 7](#_Toc423017638)

[3.2.1 Effekter av aktiv systemförvaltning 8](#_Toc423017639)

[3.3 Organisation 8](#_Toc423017640)

[3.3.1 Roller och ansvar 8](#_Toc423017641)

[4 Process för aktiv systemförvaltning 10](#_Toc423017642)

[4.1 Exempelscenario 10](#_Toc423017643)

[4.1.1 Beskrivning av System X 10](#_Toc423017644)

[4.2 Omvärldsbevakningsfas 11](#_Toc423017645)

[4.2.1 Målgrupp 11](#_Toc423017646)

[4.2.2 Periodicitet 11](#_Toc423017647)

[4.2.3 Metod 11](#_Toc423017648)

[4.2.4 Ingångsvärde 11](#_Toc423017649)

[4.2.5 Resultat 11](#_Toc423017650)

[4.2.6 System X 12](#_Toc423017651)

[4.3 Analysfas 13](#_Toc423017652)

[4.3.1 Målgrupp 13](#_Toc423017653)

[4.3.2 Periodicitet 13](#_Toc423017654)

[4.3.3 Metod 13](#_Toc423017655)

[4.3.4 Ingångsvärde 13](#_Toc423017656)

[4.3.5 Resultat 13](#_Toc423017657)

[4.3.6 System X 14](#_Toc423017658)

[4.4 Åtgärdsfas 15](#_Toc423017659)

[4.4.1 Målgrupp 15](#_Toc423017660)

[4.4.2 Periodicitet 15](#_Toc423017661)

[4.4.3 Metod 15](#_Toc423017662)

[4.4.4 Ingångsvärde 15](#_Toc423017663)

[4.4.5 Resultat 15](#_Toc423017664)

[4.4.6 System X 16](#_Toc423017665)

[4.5 Uppföljningsfas 17](#_Toc423017666)

[4.5.1 Målgrupp 17](#_Toc423017667)

[4.5.2 Periodicitet 17](#_Toc423017668)

[4.5.3 Metod 17](#_Toc423017669)

[4.5.4 Ingångsvärde 17](#_Toc423017670)

[4.5.5 Resultat 17](#_Toc423017671)

[4.5.6 System X 17](#_Toc423017672)

# Inledning

FMV designar, utvecklar, levererar och förvaltar system för Försvarsmaktens räkning. Efter leverans befinner sig systemet i en vidmakthållandefas. I nuläget används tilldelade betalningsmedel i stor utsträckning till nyanskaffning istället för åtgärder som skulle kunna optimera och förlänga systemets livscykel.

För att ett system skall vara av nytta för verksamheten krävs att dess systemcykel optimeras under hela dess livslängd. Genom att arbeta med systemförvaltning aktivt värderas systemet utifrån satta perimetrar samt med återkommande intervall. Detta skapar en kostnadseffektiv förvaltning samt bibehållen säkerhetsnivå för systemet.

Att införa aktiv systemförvaltning innebär att via ökad omvärldsbevakning identifiera, hantera och åtgärda förändringar som kan påverka systemet med syfte att förlänga systemets livscykel. Det kan gälla förändrad hotbild för verksamheten såväl som förändringar i verksamheten, men även sårbarheter och tekniska förändringar i system. Aktiv systemförvaltning bidrar till enkel och effektiv kommunikation inom verksamheten samt genomförande av förändringar i systemen.

För FMV som tekniskt förvaltningsansvarig innebär detta att vidmakthållandefasen innehåller IT-säkerhetsarbete. Detta arbete måste således beställas och prioriteras av FM för att förlänga systemlivscykel för aktuellt system.

## Bakgrund

Bakgrund till detta dokument är:

* ISD processen har utvecklats av FMV med syfte att på ett strukturerat sätt kvalitetssäkra leveranser av säkra och godkända IT-system till Försvarsmakten
* FM ska prioritera och beställa aktiv systemförvaltning från FMV där IT-säkerhetsaspekten ingår
* I framtiden uppnå en gemensam förvaltning med FM inom vidmakthållandeuppdraget
* FMV (Tekniskt förvaltningsansvarig) har totalansvar för de levererade system som FMV har designansvar för.
* Säkerställa att informationssäkerhetsfrågor hanteras i verksamhetens IT-utveckling.

## Syfte med dokumentet

Det här dokumentet beskriver en arbetsgång för den del av FMVs aktiva systemförvaltning som hanterar IT-säkerhetsarbete i syfte att förlänga systemlivscykeln.

## Mål med dokumentet

Målet med detta dokument är:

* Dokumentera en vägledning för aktiv systemförvaltning avseende IT-säkerhet som en del av FMVs vidmakthållandeuppdrag

## Avgränsning

Det är inte hela förvaltningsprocessen som beskrivs i detta dokument utan enkom IT-säkerhetsarbetet avseende vidmakthållande och ej driftåtgärder som gör sig gällande för levererade system.

De system som innefattas av denna vägledning är de som FMV har *designansvar* för, dvs. icke PRIO eller liknande.

Dokumentet behandlar inte heller eventuella akuta driftsåtgärder, dessa hanteras inom ramen för befintliga processer.

# Basfakta

## Giltighet och revision

| **Datum** | **Utgåva** | **Status** | **Beskrivning** | **Handläggare** | **Fastställd av** |
| --- | --- | --- | --- | --- | --- |
| 2015-06-24 | 1.0 | Leverabel | Slutjusteringar för leverans | Dan Olofsson | Ej fastställd |

## Referenser

| **Ref.** | **Dokumentnamn** | **Dok. id.** |
| --- | --- | --- |
| *
 | FMV vägledning för ISD och SE | 13FMV5921-1:3 |
| *
 | Direktiv för Försvarsmaktens informationsteknikverksamhet (DIT04) |  |

## Begrepp och förkortningar

|  |  |
| --- | --- |
| **Begrepp** | **Definition/förklaring** |
| Aktiv systemförvaltning | Att under återkommande intervall och med utsatta perimetrar värdera ett systems status för att förlänga dess livscykel |
| ISD-processen | FMVs process för att på ett strukturerat sätt kvalitetssäkra leveranser av säkra och godkända IT-system till Försvarsmakten |

# Vägledning

## Definition av aktiv förvaltning

Aktiv systemförvaltning innebär att upprätthålla ett systems fortsatta utveckling i verksamheten även efter leverans. Genom att införa denna form av systemförvaltning under vidmakthållandeuppdraget förlängs livscykeln för systemet, och kvalitéten i tjänsten/produkten upprätthålls. En förutsättning för aktiv systemförvaltning är att arbetet utförs enligt en fastställd periodicitet (se bild nedan).



*Bild 1: Säkerhetsnivå och förlängd livcykel genom aktiv systemförvaltning.*

En del av aktiv systemförvaltning innebär att ständigt vara uppdaterad kring de förändringar som ett system ställs inför. Detta uppnås genom att utföra omvärldsanalyser. Dessa kan innefatta både logiska och praktiska förändringar. Att analysera den omvärld som systemet befinner sig i ger ett helhetsperspektiv över systemet under hela dess livscykel och ger stor verksamhetsnytta då informationssäkerhetsbrister identifieras och åtgärdas snabbare. Identifikation av brister och sårbarheter för åtgärd utförs i samråd med verksamheten i form av förvaltningsforum där brukarmöten hålls på regelbunden basis.

Aktiv systemförvaltning ska införa förbättringar och justeringar som tar höjd för identifierade förändringar, och införa dessa i systemet enligt överenskommen vidmakthållandeprocess.

## Mål med aktiv systemförvaltning

Målen med införande av aktiv systemförvaltning är:

* Förlänga systemets livscykel utifrån ett kvalitets- och IT-säkerhetsperspektiv
* Säkerställa en verksamhetsdriven och, ur ett informationssäkerhetsperspektiv, en säker vidmakthållandeprocess
* Bidra till förbättrad förvaltningsstyrning

### Effekter av aktiv systemförvaltning

Effekterna av att införa aktiv systemförvaltning är att tydliggöra och etablera:

* *Styrning* - Ansvar, roller, mandat, forum och arbetssätt relaterade till förvaltning
* *Ekonomi* - Hantering av ekonomi och finansiering av förändringar med budgetering och uppföljning
* *Samverkan* - Hantering av ändringar som påverkas vid förändring av arbetssätt eller IT-tjänster såsom; styrande dokument, utbildning, kommunikation och masterdata
* *Gränssnitt* - Försvarsmakten och FMV har arbetssätt som bland annat resulterar i ett antal myndighetsgemensamma flöden respektive IT-tjänster som nyttjas av båda myndigheterna. Förvaltningsstyrningen ska omhänderta kravställning på dessa IT-tjänster
* *Ärendehantering* - Optimerat ärendeflöde och form för samverkan vid förändringar
* *Enhetlighet* - mallar för förvaltningsplaner, utbildningsplaner, behovsframställan och uppdrag
* *Säkerhetsnivå* – genom aktiv systemförvaltning bibehålls fortlöpande en högre säkerhetsnivå och ger en förlängd livscykel för systemet.

## Organisation

Den aktiva systemförvaltningen bygger på en samverkan mellan olika aktörer där FMV med det tekniska ansvaret är en del av helheten.

När förvaltningsteamen blir mer aktiva finns en tydligare ”kanal” till tekniskt ansvarig för snabbare åtgärder i förbättringssyfte. I förvaltningsforum där brukarmöten hålls på regelbunden basis blir omvärldsbevakningen aktualiserad i den aktiva förvaltningsprocessen. Detta leder i sin tur till en tätare dialog med verksamheten och ger bättre verksamhetsnytta.

### Roller och ansvar

Förvaltingsansvarig (FA):

* Försvarsmakten (FM)
* Systemägare
* Leder och planerar vidmakthållandet.
* Egen budget. Saknas anslag måste FA lyfta ut aktuellt uppdrag till nytt projekt.

Driftansvariga:

* Försvarsmakten (FM)
* Sköter driften, och förbättrar systemet.
* Leder och planerar brukarmöten inom ett visst driftområde.

Tekniskt förvaltningsansvar:

* FMV
* Leder och planerar IT-säkerhetsarbetet inom ramen för vidmakthållandeprocessen.
* Ansvarar för framtagna och utvecklade produkter.



*Bild 2. Översikt roller och ansvar för aktiv systemförvaltning*

Bilden visar en ansvarsfördelning för aktiv systemförvaltning. Den beskriver de olika delar av organisationen som är delaktiga i vidmakthållandeuppdraget.

# Process för aktiv systemförvaltning

Nedan följer en beskrivning av de periodiska genomgångarna av ett system, dvs. den aktiva systemförvaltningsprocessen. Bilden illustrerar aktiv systemförvaltnings fyra delfaser:

* Omvärldsbevakningsfas
* Analysfas
* Åtgärdsfas
* Uppföljningsfas

****

*Bild 3: Aktiv systemförvaltning med dess faser.*

## Exempelscenario

För att tydliggöra aktiv systemförvaltning presenteras här ett exempelscenario, härmed kallat System X.

System X exemplifierar varje fas i aktiv systemförvaltning utifrån ett resultatperspektiv i avsnitt 4.2.6, 4.3.6, 4.4.6 och 4.5.6.

### Beskrivning av System X

System X är ett autentiseringssystem för att säkerställa säker inloggning i ett FMV system.

FM har inkommit med nya krav på system X gällande funktion för logganalys. Denna funktionalitet måste införas i loggsystemet samt i de system som ligger inom dess omgivning.

För att avgöra huruvida lösningen är genomförbar inom befintlig förvaltning, eller om den ska hanteras som ett nytt projekt, hanteras kraven den aktiva systemförvaltningens fyra faser:

* Omvärldsbevakning
* Analys
* Åtgärd
* Uppföljning

## Omvärldsbevakningsfas

Omvärldsbevakningen skall fånga upp eventuella förändringar i verksamhet eller teknik som kan ha påverkan på systemet och dess livscykel. Omvärldsbevakningen identifierar brister i befintlig lösning, uppkomna risker samt hot och sårbarheter. Sårbarheter och brister kan även upptäckas via verksamheten samt incidenthanteringsprocessen. Genom omvärldsbevakning av produkter/system fångas sårbarheter och brister upp i ett tidigt skede.

### Målgrupp

Omvärldsbevakningen utförs av förvaltningsteamet på uppdrag av systemägaren.

### Periodicitet

Omvärldsbevakning bör genomföras minst en gång per månad.

### Metod

Omvärldsbevakningen skall fånga upp eventuella förändringar i verksamhet eller teknik som kan ha påverkan på systemet och dess livscykel. Omvärldsbevakningen identifierar brister i befintlig lösning, uppkomna risker samt hot och sårbarheter.

Omvärldsbevakningen innehåller således följande steg:

* Nulägesanalys:
* Uppföljning från föregående möte
* Aktuell status för systemet
* Genomförda åtgärder
* Planerade åtgärder
* Åtgärder som ej blivit hanterade i förra omgången
* Identifierade verksamhets- och tekniska förändringar
* Incidenter (uppkomna problem, sårbarheter)
* Brukarmötesprotokoll, där användarproblem med aktuellt system tas upp och dokumenterats

### Ingångsvärde

* Nulägesanalys: aktuell status för systemet, genomförda åtgärder, planerade åtgärder, uppföljning från föregående möte, åtgärder som ej blivit hanterade i förra omgången, identifierade verksamhets- och tekniska förändringar
* Incidenthanteringsprocessen (uppkomna problem, sårbarheter)
* Brukarmötesprotokoll, där användarproblem med aktuellt system tas upp och dokumenteras
* Uppföljnings/åtgärdsprotokollet

###  Resultat

Omvärldsbevakningen resulterar i en dokumenterad krav- och förändringslista där ursprung och riskområde på aktuellt system dokumenteras. Denna lista är ännu *ej* prioriterad.

### System X

Omvärldsbevakningen påvisade förändringar i verksamheten som kravställer system X:s logganalysfunktion. FM har infört en tätare periodicitet för revision av behörigheter inom verksamheten vilket leder till att System X måste ha en bättre logganalysfunktionalitet inbyggd.

*Exempel på krav- och förändringslista:*

|  |  |  |  |
| --- | --- | --- | --- |
| Nr | Krav/förändring | Ursprung | Riskområde |
| 1 | System X ska ha en funktion för logganalys | Omvärldsanalys | Spårbarhet, riktighet, konfidentialitet |

## Analysfas

Under analysfasen evalueras sårbarheter, brister och eventuella förändringar (t ex tekniska) som upptäckts i omvärldsanalysen. Evalueringen utförs ur ett informationssäkerhetsperspektiv, genom hot-, risk- och sårbarhetsanalys (HRS) för att kunna identifiera eventuella åtgärder i systemen. Utgångsvärdet från analysfasen utgör även en grund för beslutsfattande i efterföljande åtgärdsfas.

### Målgrupp

Förvaltningsteamet genomför hot-, risk- och sårbarhetsanalysen.

### Periodicitet

Analysen bör genomföras en gång per månad.

### Metod

Hot och riskanalysen (HRS) innehåller följande 3 steg:

1. Hotbildanslys: i workshopformat får deltagarna bidra med eventuella informationssäkerhetsrisker och hot som finns i relation till systemet. Även kvalitetsfrågor och övriga hot och risker bör tas med. Hot och risker bör grupperas för att göra antalet hot och risker mer hanterbara.
2. Hot och risker värderas enligt riskvärdesmatris. Varje punkt diskuteras utifrån sannolikhet och konsekvens. Eventuellt kan man behöva sätta ihop sammanhang till scenario.
3. Åtgärder föreslås som underlag för steg 4.3 (se nedan).

### Ingångsvärde

Input till hot, risk och sårbarhetsanalys är

* Krav- och förändringslista från omvärldsbevakningen.

HRS utförs med fördel i workshopformat inom förvaltningsteamet. Deltagande parter bör vara:

* Systemansvarig
* Systemförvaltare/Drift
* Informationssäkerhetrepresentant
* Verksamhetsrepresentanter
* Tekniskt förvaltningsansvarig

### Resultat

Output från HRS är en prioriterad hot och risklista, samt beslutsunderlag för eventuella åtgärder.

### System X

Hot och riskanalysen identifierar en risk för försämrad spårbarhet om logganalys ej är möjligt att utföra.

Rutiner och verktyg för logganalys behöver vidareutvecklas och implementeras i system X.

*Exempel på hotkatalog efter HRS*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID  | Scenario/konsekvens | Hanterar kravnr | Sannolikhet | Konsekvens | Risk-värde | Åtgärdsförslag |
| HRS1 | Ett eventuellt intrång identifieras i efterhand. Pga. svårigheter att analysera informationen i loggfilerna riskerar fler intrång att upptäckas för sent. Konsekvensen av detta blir således en försämrad spårbarhet och bristfällig möjlighet att upptäckt intrång | 1 | H | M | 4 | Vidareutveckla och implementera rutiner och verktyg för logganalys i system X |

## Åtgärdsfas

Åtgärdsfasen utgör en besluts- och åtgärdsfas för förvaltningen. Alla hot/risker/sårbarheter tilldelas en ansvarig som ansvarar för att åtgärden blir utförd.

### Målgrupp

Beroende på beslutad åtgärd kan följande roller vara involverade:

* FA
* Driftsansvarig
* Tekniskt ansvarig
* Ev. projektledare

### Periodicitet

Åtgärder sker enligt åtgärdslista/protokoll från HRS.

### Metod

Efter analysfasen åtgärdas de identifierade sårbarheterna och bristerna. De punkter som enligt HRS-resultatet ska åtgärdas beslutas. När ska respektive punkt åtgärdas, påverkar det andra delar av systemet. Ryms detta inom budget, behöver verksamheten förändras?

* Varje åtgärd får en ansvarig utsedd som återkopplar till systemägare
* I varje förslag på åtgärd ska nyttoeffekter samt estimerade kostnader för respektive åtgärd finnas med.
* Åtgärderna bör även definieras som antingen kortsiktiga eller långsiktiga och därefter tidsestimeras.

Åtgärderna införs via ändringshanteringsprocessen och/eller incidenthanteringsprocessen.

### Ingångsvärde

* HRS-protokollet

### Resultat

* Åtgärdslista/protokoll – prioritering och åtgärdsförslag redovisas.
	+ Åtgärder som ryms inom befintlig verksamhetsbudget hanteras enligt befintliga incident- samt ändringsprocesser.
	+ Åtgärder som hamnar utanför budgetram skickas på remiss till systemägare för vidare hantering och eventuell uppstart av nytt projekt i enlighet med ISD-processen.

### System X

Efter diskussion om vilka åtgärder som bör utföras för att säkra en bättre logganalysfunktionalitet i System X bestämdes följande:

* FMV bör vidareutveckla logganalysfunktionaliteten i System X så att överenstämmelse med nya krav uppnås.
* Nya rutiner kring användning och rapportering med hjälp av den nya funktionaliteten ska implementeras.

*Exempel på åtgärdslista/protokoll*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Åtgärdsförslag | Prio. | Hanterar riskID | Kostnad | Hanteras av | Ansvarig | Åtgärd utförd J/N |
| Å1 | Vidareutveckla och implementera rutiner och verktyg för logganalys i system X | 1 | HRS1 |  | ÄP (ändrings-hanterings-process) | NN |  |
| Å2 | Genomföra omkonfiguration av brandväggsregler | 1 | HRS1 |  | IP (incident-hanterings-processen) | NN |  |
| Å3 | Utveckla och implementera mobilaccess till system X | 2 | R5 |  | ISD | System-ägare |  |

## Uppföljningsfas

Efter åtgärd återkopplar ansvarig för förändring till förvaltningsgruppen som dokumenterar genomförd åtgärd. Åtgärdsprotokollet utgör sedan input till nästa förvaltningsforums omvärldsbevakning.

###  Målgrupp

FA ansvarar för att uppföljning av genomförda åtgärder.

### Periodicitet

Uppföljning sker fortlöpande mellan mötena. Dessa ska dokumenteras och vara en del av nästa mötes omvärldsbevakning.

### Metod

Systemägaren:

* Följer upp åtgärdsprotokollet kontinuerligt
* Uppdaterar protokollet med de åtgärder som är utförda.
* Eventuella icke utförda åtgärder noteras och följs upp i nästa förvaltningscykel.

Resultatet blir ett uppdaterat åtgärdsprotokoll som blir input till nästa omvärldsbevakningsfas.

### Ingångsvärde

Åtgärdsprotokollet

### Resultat

Uppdaterat åtgärdsprotokoll

### System X

Efter beslutad åtgärd för att System X ska efterleva de nya logganalyskraven har FA följt upp vidareutvecklingen av systemet. Avstämningar dokumenteras i åtgärdsprotokollet.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Åtgärdsförslag | Prio. | Hanterar riskID | Budget | Hanteras av | Ansvarig | Åtgärd utförd J/N |
| Å1 | Vidareutveckla och implementera rutiner och verktyg för logganalys i system X | 1 | HRS1 |  | ÄP (ändrings-hanterings-process) | NN |  |
| Å2 | Genomföra omkonfiguration av brandväggsregler | 1 | HRS1 |  | IP (incident-hanterings-processen) | NN |  |
| Å3 | Utveckla och implementera mobilaccess till system X | 2 | R5 |  | ISD | System-ägare |  |