ARBETSFÖRMEDLINGEN
SWEDISH PUBLIC EMPLOYMENT SERVICE

Informationssäkerhet

Hur Arbetsförmedlingen arbetar för att stärka sin informationssäkerhet
Uppdrag 3.2 i Regleringsbrevet

Förord

Denna rapport har tagits fram med anledning av följande uppdrag i Arbetsförmedlingens regleringsbrev för år 2022.

3.2 Informationssäkerhet samt utveckla arbetet med individuella handlingsplaner

Arbetsförmedlingen ska övergripande redogöra för hur myndigheten arbetat för att stärka sin informationssäkerhet och för hur den planerar för att möta framtida behov, bl.a. utifrån aktuella digitaliseringsinitiativ och utifrån reformeringen av myndigheten. Arbetsförmedlingen ska särskilt redogöra för åtgärder för att utveckla den interna styrningen och uppföljningen av informationssäkerhetsarbetet inklusive myndighetsledningens roll i detta. Denna del av uppdraget ska redovisas till Regeringskansliet (Arbetsmarknadsdepartementet) senast den 26 oktober 2022.

Beslut i ärendet har fattats av generaldirektör Maria Mindhammar. Föredragande har varit enhetschef Per Gauffin. Övriga som deltagit i den slutliga handläggningen är it-direktör Krister Dackland, kvalificerade handläggare Leo Berndtson, Per-Anders Ode samt Per-Ola Persson.

Beslutet är fastställt digitalt i Diariet och saknar därför namnunderskrifter.

Maria Mindhammar

Generaldirektör

Per Gauffin

Enhetschef

Af 00009 5.0 (2022-03-28)

Författare: Per Gauffin, Leo Berndtson, Per-Anders Ode, Per-Ola Persson
Datum: 2022-10-26
Diarienummer: Af-2022/0075 2570

Innehåll

1 Sammanfattning

Regeringen har i regleringsbrev för budgetåret 2022 avseende Arbetsförmedlingen begärt beskrivningar för hur myndigheten arbetat för att stärka sin informationssäkerhet och för hur den planerar för att möta framtida behov, bl.a. utifrån aktuella digitaliseringsinitiativ och utifrån reformeringen av myndigheten. Arbetsförmedlingen ska särskilt redogöra för åtgärder för att utveckla den interna styrningen och uppföljningen av informationssäkerhetsarbetet inklusive myndighetsledningens roll i detta. Denna rapport är en redovisning av uppdraget.

Arbetsförmedlingen driver ett större pågående förändringsarbete inom myndighetens informationssäkerhetsarbete. Arbetet utgår från en framtagen och beslutad handlingsplan. Handlingsplanens övergripande syfte är att ytterligare förstärka myndighetens ledningssystem för informationssäkerhet (LIS) som ett integrerat ledningssystem inom myndighetens ordinarie ledningssystem, intern styrning och kontroll.

En central del i LIS-arbetet är det tvärfunktionella kravarbetet, med utgångspunkt i myndighetens arbetsordning, baserat på struktur och förutsägbarhet enligt ISO 27002:2022. Detta arbete ger ytterligare stöd till LIS säkerhetsprocesser som till exempel ständiga förbättringar och ledningens delaktighet. Taktiska och operativa säkerhetsprocesser som t ex incidenthantering, informationssäkerhetsklassificering och informationsägarskap samt riskhantering stödjer det systematiska och riskbaserade arbetssättet.

Det tvärfunktionella arbetet stärker organisationens förmåga inom, strategisk, taktiskt och operativ informationssäkerhet samt tydliggör även ansvar och roller inom cybersäkerhet och dataskydd.

1.1 Strategiska aktivitetsområden

Strategiska aktivitetsområden utifrån regleringsbrevets önskade redogörelser och som ska stärka myndighetens informationssäkerhet

- En tydlig koppling till tvärfunktionella arbetssätt inom myndighetens LIS för att ytterligare förstärka ledningens engagemang på flera nivåer.
- En förstärkt integration av myndighetens LIS inom intern styrning och kontroll. Processer och metoder ska skapa systematik inom verksamhetsplaneringen. Integrationen förstärker förmågan inom ledningens genomgång[1] genom uppföljning, granskning och ständiga förbättringar.
- Förstärkt förmåga kring hotbildsanalys, omvärldsanalys och det riskbaserade arbetssättet på flera nivåer. Lägesbilder under året ger kontinuitet och delredovisningar till ledningens genomgång.

[1] MSBFS 2020:6 14-14 §, Uppföljning av informationssäkerhetsarbetet om myndighetens målsättning och inriktning för informationssäkerhetsarbetet

- Rapportering av lägesbilder till myndighetsledningen förstärks ytterligare vad avser systematik. Rapportering samordnas, sammanställs och återkopplas genom lägesbilder samt ledningens genomgång inom informationssäkerhet, cybersäkerhet och dataskydd.

1.2 Handlingsplanens syfte att stärka Arbetsförmedlingens informationssäkerhet

LIS-arbetet har det övergripande syftet att kontinuerligt utveckla mognadsgraden av myndighetens förmåga och vidareutveckla och förstärka integrationen av LIS inom myndighetens ordinarie ledningssystem. Det övergripande syftet är

Ett, verksamhetsutvecklande, riskbaserat, systematiskt ledningssystem för informationssäkerhet.

Det pågående arbetet är indelat i två aktivitetsområden, säkerhetsåtgärder och säkerhetsprocesser som skapar förutsättningar för en tvärfunktionell ”organisatorisk informationssäkerhetsförmåga” över tid. Med detta avses att hela organisationen har förmågan att ständigt utveckla och förbättra myndighetens LIS.

Grunden i arbetet är att över tid förstärka och förtydliga

- kravhantering, tvärfunktionellt och med utgångspunkt i generaldirektörens arbetsordning
- ett riskbaserat arbetssätt genom processen ”säkerhetsresa för IT initiativ”, metodstöd inom intern styrning och kontroll, hotbilds- och omvärldsanalyser, samt stöd inom informationssäkerhetsklassificering och riskanalysmetoder
- ett systematiskt arbetssätt genom att lägesbilder, hotbilds-, och omvärldsanalys, intern styrning och kontroll och riskhantering inom verksamhetsplanering kopplas till ledningens genomgång på flera nivåer
- den verksamhetsutvecklande förmågan genom ständig utveckling av metod och processtöd baserat på ledningens delaktighet och strategiska styrning.

2 Inledning och uppdrag

Regeringen har i regleringsbrev för budgetåret 2022 avseende Arbetsförmedlingen begärt att myndigheten övergripande ska redogöra för hur man arbetat för att stärka sin informationssäkerhet.

> *Arbetsförmedlingen ska övergripande redogöra för hur myndigheten arbetat för att stärka sin informationssäkerhet och för hur den planerar för att möta framtida behov, bl.a. utifrån aktuella digitaliseringsinitiativ och utifrån reformeringen av myndigheten.*

> *Arbetsförmedlingen ska särskilt redogöra för åtgärder för att utveckla den interna styrningen och uppföljningen av informationssäkerhetsarbetet inklusive myndighetsledningens roll i detta.*
>
> *Denna del av uppdraget ska redovisas till Regeringskansliet (Arbetsmarknadsdepartementet) senast den 26 oktober 2022.*

Arbetsförmedlingen har valt att besvara frågeställningen om informationssäkerhetsarbetet genom att beskriva området under fyra huvudområden (avsnitt 3–6).

- Förutsättningar som påverkar myndighetens arbete med informationssäkerhet
- Myndighetens arbete för att stärka informationssäkerheten och möta framtida behov
- Utveckling av styrning och uppföljning inom informationssäkerhet
- Myndighetsledningens roll inom informationssäkerhet

3 Förutsättningar som påverkar myndighetens arbete med informationssäkerhet

Arbetsförmedlingen genomför ett strategiskt, taktiskt och operativt arbete för att etablera en förmåga att ständigt förbättra ledningssystemet för informationssäkerhet (LIS). Arbetet genomförs med fokus på myndighetens förmåga att över tid arbeta med både kravhantering samt metod- och processutveckling.

Ett långsiktigt arbete pågår för att förtydliga förutsättningarna för hur Arbetsförmedlingens förmåga ska stärkas. Områden med särskilt fokus är organisationens förmåga inom informationssäkerhet, cybersäkerhet och dataskydd.

Arbetsförmedlingens reformering samt digitalisering påverkar ledningssystemet och det systematiska och riskbaserade arbetssättet. Ett arbete som avser att möta upp behoven är att förstärka det tvärfunktionella arbetssättet med att utveckla krav och åtgärder samt även att förtydliga beslutsprocesser enligt ett tvärfunktionellt arbetssätt.

3.1 Informationssäkerhet - ISO 27000 standarder

Standarderna i ISO 27000-serien har beteckningen Ledningssystem för informationssäkerhet (LIS) och bildar grunden för att bedriva ett systematiskt informationssäkerhetsarbete i en organisation. Arbetsförmedlingens LIS utvecklas med stöd av den senaste versionen av standarden ISO 27002:2022.

ISO-standardens struktur utgår i sin tur från fyra åtgärdsområden.

- Organisatoriska åtgärder

- Åtgärder inom personalsäkerhet
- Åtgärder inom fysiskt skydd
- Tekniska åtgärder

I arbetet att förstärka myndighetens LIS utifrån ISO 27000 serien så skapar detta nyttor och förtydliganden som t.ex. förutsägbarhet och strukturer som stödjer upphandling, avtal och leverantörsstyrning. Detta exempel är direkt stödjande (verksamhetsutvecklande) i relation till myndighetens strategiska mål och förändringsarbete.

Kravmassan på 93 åtgärder inom ISO 27002:2022 omfattar inte bara krav och åtgärder utan även krav på att införa, kontrollera och ständigt utveckla förmåga inom metod och processer inom LIS.

Myndighetens arbete med följsamhet och förutsägbarhet till ISO-standarden 27001 samt 27002 omfattar arbete med krav och åtgärder samt att etablera en ”organisatorisk förmåga” över tid, vilket innefattar ett tvärfunktionellt arbetssätt för att ständigt uppdatera regler, stödjande dokument samt process- och metodstöd.

Arbetssättet avser även att förtydliga ansvaret kopplat till arbetsordningen genom att olika organisatoriska delar av myndigheten tar ett aktivt ansvar för att myndigheten har väl avvägda åtgärder inom myndighetens LIS.

Ansvaret för krav, åtgärder, process- och metodstöd, fördelas utifrån arbetsordningen, med stöd av åtgärdsområden i ISO 27002:2022. Arbetet samordnas och bereds i beslutsforum på taktisk och strategisk nivå.

3.2 Digitalisering

Den snabba utvecklingen skapar helt nya möjligheter att komma åt och hantera information. Förändringen är global och drivs i grunden av teknikutveckling som i sin tur skapar nya användarbeteenden och förändrade förväntningar. Dessa förändringar sker mycket brett i samhället, både inom företag och för enskilda individer.

Den digitala kompetensen hos myndighetens kunder och olika samarbetspartners (fristående aktörer, leverantörer, o.s.v.) utvecklas och deras förväntningar på hög tillgänglighet och kvalitet i våra digitala tjänster växer snabbt, vilket leder till höga krav på vår digitala tillgänglighet. Myndighetens tjänster förväntas vara tillgängliga dygnet runt, vara lätta att använda och ska hantera våra kunders information på ett säkert sätt.

För att möta förväntningarna pågår en omfattande digitaliseringstransformation inom myndigheten. I princip förändras hela myndighetens verksamhet för att på ett effektivt sätt kunna fungera i en digital värld. Helt nya arbetsprocesser som ökar kundvärdet utifrån en högre grad av digitalt tillgängliga tjänster gör att nya applikationer byggs på moderna digitala plattformar.

När myndigheten transformeras till digital verksamhet påverkas informationshanteringen i stor omfattning. Det innebär en förflyttning från analog

och manuell informationshantering där myndighetens arbetssätt förändras och där våra sätt att lagra och dela information förändras.

Information, processer och uppföljning blir tydligare knutna till it-systemen och ansvaret för informationen knyts även närmare it-organisationen. Informationssäkerheten blir mer beroende av it-systemens säkerhet och myndighetens förmågor inom cybersäkerhet.

3.3 Reformeringens påverkan av informationssäkerheten

Justeringar i myndighetens uppdrag och inriktning påverkar myndighetens digitala förändring och sättet att utföra uppdraget. Utvecklingen av samarbetet med de fristående aktörerna innebär att stora delar av myndighetens direkta kundkontakter flyttas från myndigheten till de fristående aktörerna med förändringar inom informationshantering.

Delning av kundinformation innebär utmaningar ur ett informationssäkerhetsperspektiv. Personuppgifter behöver hanteras mellan myndigheten och de fristående aktörerna och hanteringen måste följas upp. Ett av målen med LIS är att belysa dessa utmaningar och förtydliga ansvar inom t.ex. informationsöverföring inom processer och verksamhetssystem.

4 Myndighetens arbete för att stärka informationssäkerheten och möta framtida behov

Informationssäkerhet omfattar perspektiven konfidentialitet, riktighet, tillgänglighet och spårbarhet. För att nå detta när omvärldens förväntningar och tekniska förutsättningar kontinuerligt förändras, samtidigt som myndigheten i sig själv transformeras, krävs ett omfattande och målinriktat arbete.

Mycket arbete läggs och har lagts på att skapa medvetenhet och kunskap om informationssäkerhet i alla led på myndigheten. För att nå god informationssäkerhet krävs specialister med djup teknisk kompetens, välutbildade systemutvecklare, hög medvetenhet och kunskap bland handläggare och framför allt en välfungerande, effektiv struktur och kultur som mäter, följer upp och vidareutvecklar god informationssäkerhet.

Arbetsförmedlingen har ett pågående och omfattande arbete för att utveckla ett modernt LIS, som kommer att stötta och styra arbetet med informationssäkerhet på myndigheten. Detta arbete beskrivs mer utförligt i kapitel 5.

4.1 Genomfört och påbörjat arbete

År 2018 bildades en ny enhet inom it-verksamheten med inriktning på informationssäkerhet för myndighetens digitala verksamhet. Syftet var att både stärka myndighetens förmågor inom informationssäkerhet och att implementera en mer effektiv och konstruktiv kultur inom digital säkerhet. Enheten heter Cybersäkerhet och Digital tillit och omfattar idag närmare 60 medarbetare.

En viktig inriktning i arbetet med informationssäkerhet är att skapa en kultur som möjliggör ett effektivt säkerhetsarbete som stöttar utvecklingen av myndighetens digitala tjänster. Arbetet med informationssäkerhet ska inte vara hindrande utan förenkla och möjliggöra nya tjänster och funktioner.

En annan viktig del är att utveckla samarbetet mellan Arbetsförmedlingens övriga säkerhetsfunktioner, verksamhetsområden samt myndighetens rättsavdelning. Stora satsningar har gjorts inom rättsavdelningen för att bygga upp en hög kompetens inom informationssäkerhet och it-juridik som till exempel inom området dataskydd.

Parallellt med byggandet av organisationen och förmågorna togs en målarkitektur fram. Arkitekturen är en strategi och målbild för de tekniska och funktionella förmågorna som krävs för ett effektivt cybersäkerhetsarbete i myndighetens digitaliserade verksamhet. Samtliga system har flyttats över till en ny modern it-miljö med bättre skalskydd och med avgränsade zoner som kraftigt försvårar tillgängligheten för externa angripare.

Den tekniska förmågan har förstärkts med exempelvis sårbarhetsscanningar, övervakningsverktyg och nya behörighetsverktyg med förstärkt åtkomstkontroll. En SOC[2] (Security Operations Center) har byggts upp och egna penetrationstestare[3] har anställts, myndighetens skydd mot överbelastningsattacker (DDOS) har förbättrats samt uppgraderingsrutiner har förtydligats och automatiserats. Kravställningar till och rutiner för uppföljning av underleverantörer har förstärkts och uppdaterats.

Störst arbete har lagts på att höja kompetensen samt bygga tillit inom verksamheten, utanför de specifika säkerhetsfunktionerna och att skapa en kultur med ett riskbaserat arbetssätt grundat på kunskap och goda processer.

Arbetsförmedlingen har etablerat en process, kallad säkerhetsresan, inför att utveckla och upphandla it-produkter. Arbetssättet är en viktig operativ och praktisk del inom myndighetens LIS.

Säkerhetsresan är ett antal aktiviteter som ska genomföras för varje planerad it-produkt som t.ex hot- och riskanalys, informationsklassning eller en laglighetsbedömning. Säkerhetsresan avslutas med en utvärdering från ett tvärfunktionellt informationssäkerhetsråd där det genomförda säkerhetsarbetet godkänns innan produktionssättning eller upphandling.

[2] Security Operations Center (SOC) för övervakning och analys av all datatrafik i realtid med syfte att identifiera och registrera såväl oönskade beteenden som olika typer av attacker
[3] Teknisk cybersäkerhetsspecialist med särskild kompetens att identifiera sårbarheter i system eller applikationer

Ett konkret exempel på kompetensutveckling inom informationssäkerhetsområdet är initiativet ”Agera cybersäkert” som genomförs i enlighet med myndighetens verksamhetsplanering för 2022. Arbetet riktar sig till samtliga medarbetare på myndigheten för att skapa en större kunskap och medvetenhet inom digital informationssäkerhet. Initiativet bygger på grundläggande kunskap och lyfter fram vardagliga situationer och ger exempel på medvetenhet inom säkerhet i relation till god förvaltning.

Då myndighetens digitala verksamhet och behoven på god säkerhet hela tiden växer ökar även behoven på enklare och mer effektiva säkerhetslösningar. Integrerat med arbetet för myndighetens LIS, drivs även ett arbete med att beskriva en ”bas-säkerhet”. Det innebär att skapa en tydlig grundnivå för alla funktioner. Genom att definiera en standardiserad lägstanivå förenklas analys och utredningsarbete och antalet potentiella säkerhetshål kan minimeras.

Det rättsliga perspektivet får allt större inverkan på informationssäkerheten. En god hantering av personuppgifter enligt dataskyddsförordningen ställer krav på informationssäkerhetsarbetet. Myndigheten har gjort stora satsningar på att bygga upp kompetens inom it-rätt och personuppgiftshantering. Rättsavdelningen har ett mycket nära samarbete med it-verksamheten och säkerhetsenheten. Ett nära samarbete mellan säkerhet och juridik är en nödvändig framgångsfaktor för ett gott informationssäkerhetsarbete på en modern, digital myndighet.

5 Utveckling av styrning och uppföljning av informationssäkerhetsarbetet

Centrala mål i LIS-arbetet är att arbetet med etablering av den organisatoriska förmågan inte utgör ett projekt utan avser en etablerad förmåga över tid inom myndigheten. Utgångspunkten är ett organisationsoberoende samordnat arbetssätt. Detta innebär att flera olika organisatoriska delar av myndigheten får ett direkt ansvar för att ständigt förbättra myndighetens LIS och därmed blir ledning och styrning involverad i flera nivåer och inom flera organisatoriska områden.

Övergripande strategiska aktivitetsområden inom LIS-arbetet

- En tydlig koppling till tvärfunktionella arbetssätt inom myndighetens LIS för att ytterligare förstärka ledningens engagemang på flera nivåer.
- En förstärkt integration av myndighetens LIS inom intern styrning och kontroll. Processer och metoder ska skapa systematik inom verksamhetsplaneringen. Integrationen förstärker förmågan inom ledningens genomgång[4] genom uppföljning, granskning och ständiga förbättringar.
- Förstärkt förmåga kring hotbildsanalys, omvärldsanalys och det riskbaserade arbetssättet på flera nivåer. Lägesbilder under året ger kontinuitet och delredovisningar till ledningens genomgång.

[4] MSBFS 2020:6 14-15 §, Uppföljning av informationssäkerhetsarbetet

- Rapportering av lägesbilder till myndighetsledningen förstärks ytterligare vad avser systematik. Rapportering samordnas, sammanställs och återkopplas genom lägesbilder samt ledningens genomgång inom informationssäkerhet, cybersäkerhet och dataskydd.

LIS-arbetet har det övergripande syftet att kontinuerligt utveckla mognadsgraden av myndighetens förmåga och vidareutveckla och förstärka integrationen av LIS inom myndighetens ordinarie ledningssystem. Det övergripande syftet är

Ett, verksamhetsutvecklande, riskbaserat, systematiskt ledningssystem för informationssäkerhet.

1. "Ett" (1)

Ledningssystemet - LIS är myndighetens ledningssystem för informationssäkerhet och utgår ifrån ett tvärfunktionellt arbetssätt.

Ett sammanhållet ledningssystem som samlar, skapar överblick och stödjer ett tvärfunktionellt arbetssätt och gör det ”enklare att göra rätt”. Åtgärder ska vara beskrivna i styrande och stödjande dokument på ett korrekt sätt och i nära samverkan mellan de funktioner där kunskap och ansvar finns. Ett exempel kan vara att regler eller åtgärder inom personalsäkerhet tas fram i nära samverkan med it-verksamheten, personalavdelningen och rättsavdelningen.

2. "Verksamhetsutvecklande"

Myndighetens LIS ska stödja dom strategiska målen för myndigheten. Ledningssystemet ska bidra till att det ska vara "enklare att göra rätt" inom verksamhetsutveckling, produktstyrning eller annat förändringsarbete, till exempel genom att olika verksamhetsutvecklingsprojekt tar med informationssäkerhetsarbete tidigt. Genom ett proaktivt säkerhetsarbete ökar kvaliteten och kan minska kostnader såsom omtag, backa i systemutveckling, eller annat som kan uppstå då säkerhetsbrister upptäcks för sent.

Med verksamhetsutvecklande avses att myndighetens LIS ska stödja myndighetens reformering och strategiska mål att

- över tid uppnå målet, ”enklare att göra rätt” utifrån verksamhetsutvecklade direkta och indirekta stöd inom verksamhetsutveckling och myndighetens reformering
- skapa en organisationsoberoende struktur med en tvärfunktionell förmåga över tid, med utgångspunkt i arbetsordning
- förstärka förmågan inom ledningens (alla nivåer) åtagande, uppföljning och styrning kopplat till ett taktiskt och strategiskt förbättringsarbete över tid.

3. "Systematiskt"

Att myndigheten har ett systematiskt arbetssätt innebär att LIS-arbetet införlivas inom intern styrning och kontroll, riskhantering samt vidare inom verksamhetsplaneringsarbetet.

Ett systematiskt informationssäkerhetsarbete inom ett ledningssystem innebär många olika saker. Övergripande kan arbetet beskrivas utifrån perspektiven planera, genomföra, följa upp & analysera samt förbättra.

4. "Riskbaserat"

Genomförande av riskanalyser och metodstöd för riskanalys stödjer det systematiska informationssäkerhetsarbetet. Genom riskanalyser identifieras hot och oönskade händelser som kan leda till negativa konsekvenser för organisationen. Med stöd av ISO-standarden utformas arbetssätt för att informationssäkerhetsrelaterade risker analyseras och att riskanalysens resultat ligger till grund för val och utformning av säkerhetsåtgärder och det systematiska informationssäkerhetsarbetet.

5. "Ledningssystem"

Ett övergripande mål är att integrera myndighetens LIS inom myndighetens befintliga ledningssystem. Med detta menas att LIS-processer samordnas och integreras inom styrande processer som intern styrning och kontroll, riskhantering samt myndighetens verksamhetsplaneringsarbete.

Genom de beskrivna målen i arbetet har myndigheten metod och grund för ett ledningssystem för informationssäkerhet, tillsammans med LIS- säkerhetsprocesser som är den andra centrala delen i myndighetens säkerhetsförmåga.

5.1 Långsiktigt mål

Det övergripande syftet är *ett sammanhållet, verksamhetsutvecklande systematiskt och riskbaserat arbetssätt* i myndighetens LIS. LIS ska avspegla myndighetens arbete med informationssäkerhet i sin tur anpassat efter övergripande förmåga etc. inom ISO 27000 serien.

Det långsiktiga verksamhetsutvecklande målet i handlingsplanen är att det ska vara ”enklare att göra rätt” genom ett utökat fokus på metod och processer inom LIS, ett LIS som stödjer myndighetens operativa, taktiska och strategiska mål.

Ett tvärfunktionellt arbetssätt inom arbetet med kravhantering ökar inte bara säkerhetsmedvetandet utan också förmågan att över tid i att upprätthålla, ständigt utveckla och förbättra området styrande och stödjande dokument.

Grunden i ISO 27000 serien, - inom en större myndighet eller organisation - är att krav och åtgärder är delegerade och förutsätter ett brett deltagande i flera

organisatoriska enheter inom en organisation i sitt genomförande. I arbetet uttrycks detta utifrån målet med ett organisationsoberoende och tvärfunktionellt arbete. Nyckelintressenter styr och deltar aktivt i arbetet som över tid utvecklar LIS i relation till målet med ständig förbättring.

Rätt sak-kompetens inom den komplexa kravmassan inom ISO 27000-serien och i ett ledningssystem är centralt för att minska förändringsarbetet med förankring och förståelse av myndighetens LIS. Genom detta ökar över tid säkerhetsmedvetandet och kunskapen om myndighetens LIS som ett väl avvägt, pragmatiskt och praktiskt fungerande ledningssystem. Det organisationsoberoende perspektivet avser att myndighetens LIS är något som olika organisatoriska delar ansvarar för inom myndigheten utifrån arbetsordning och delegation.

Målet med att ytterligare förstärka det systematiska och riskbaserade arbetssättet är att fortsätta att förtydliga integrationen av informationssäkerhetsarbetet inom myndighetens ordinarie ledningssystem för intern styrning och kontroll.

Utgångspunkten är att informationssäkerhet är en verksamhetsledningsfråga. Genom fortsatt och förstärkt integration inom intern styrning och kontroll förstärker myndigheten samtidigt övergripande och specifika arbetssätt som exempelvis förmågan att bevaka risk-/hotbilden mot myndigheten. Arbetet med ledningssystemets säkerhetsprocesser inom informationssäkerhet kommer närmare ett organisationsövergripande riskhanteringsperspektiv som också stöds av modeller som COSO[5].

5.2 Tvärfunktionell kravhantering

Arbetet inom LIS och kravhantering, syftar till att etablera ett tvärfunktionellt arbete kring myndighetens styrande och stödjande dokument, ett arbetssätt för att inkludera myndighetens sak-kompetens inom krav/åtgärder med målet att uppnå förmåga ”över tid”. Med detta avses en tvärfunktionell förmåga över tid som inte har arbetsformen av ett projekt eller ett initiativ. Förmågan avser att bibehållas över tid i myndigheten för att ständigt förvalta och utveckla LIS processer och annat metodstöd.

Arbetet med kravhantering följer strukturen inom ISO 27002:2022 med etablering av kravgrupper med sak-kompetens inom de olika säkerhetsåtgärderna.

1 Organisatoriska åtgärder, - 37 säkerhetsåtgärder
2 Person-/Personalsäkerhetsrelaterade åtgärder, - 8 säkerhetsåtgärder
3 Fysiska åtgärder, - 14 säkerhetsåtgärder
4 Tekniska åtgärder, - 34 säkerhetsåtgärder

Kravhanteringsarbetet utförs genom att utse sammankallande roller med representation från nyckelintressenter inom myndighetens LIS. Rättsavdelningen, verksamhetsområde It, HR-avdelningen, förvaltningsavdelningen samt

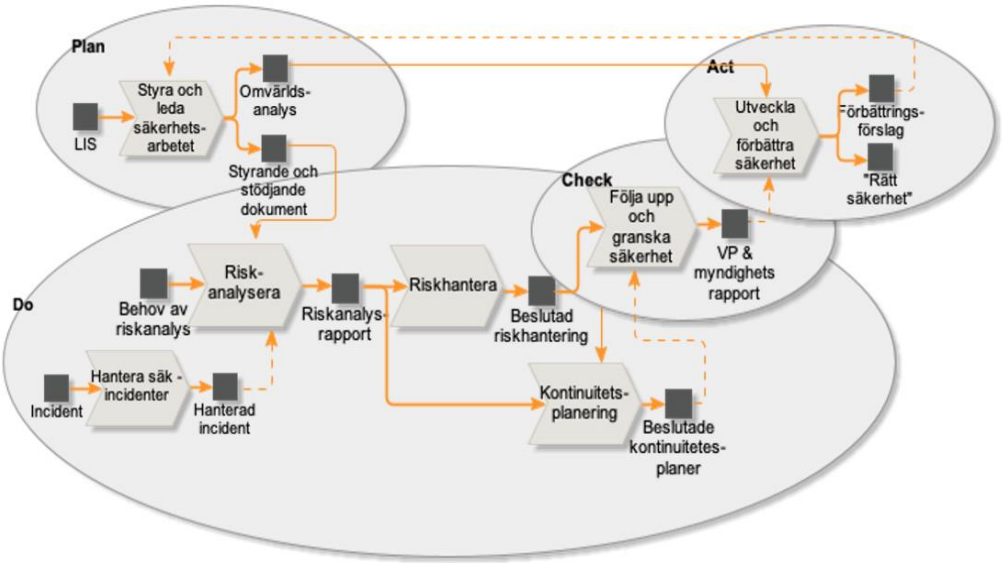
[5] en förkortning för Committee of Sponsoring Organizations, en modell för att utvärdera intern styrning och kontroll,

ledningsstaben är exempel på nyckelintressenter i arbetet vid sidan av representanter från verksamhetens huvudprocesser i linjeverksamheten.

Kravhanteringsarbetet samordnas och förankras inom tvärfunktionella beslutsforum. Genom detta bibehålls förmågan att bereda och ta beslut på olika nivåer, baserat på arbetsordning och delegation. Målsättningen är att kravarbetet resulterar i kontinuerlig uppdatering, förbättring, gallring av styrande och stödjande dokument kopplat till myndighetens LIS. Över tid kan mer fokus överföras till metod och processutveckling för att uppnå det verksamhetsutvecklande målet med myndighetens LIS.

5.3 Ledningssystemets processer för ett systematiskt & riskbaserat arbetssätt

Handlingsplanen för att utveckla myndighetens LIS redovisar aktiviteter som avser att ytterligare förstärka och förtydliga processer inom ett systematiskt och riskbaserat arbetssätt. Dessa processer avser att förstärka arbetssätt som myndigheten redan har på plats inom intern styrning och kontroll. Processerna i det riskbaserade arbetssättet stöds av processer inom verksamhetsplanering som skapar förutsättningar för uppföljning och ständig förbättring. Dessa processer stöds vidare av specifika processer och metoder i informationssäkerhetsarbetet inom myndigheten. Exempel på detta är processer för incident- och kontinuitetshantering.



Figur: 1Handlingsplanens förklaringsmodell - en PDCA-modell (Plan, Do, Check, Act) för ständig förbättring.

Olika processer inom myndighetens LIS:

1 Tvärfunktionell omvärlds- och hotbildsanalys.

2 Metod och processer för riskanalys, - indelad enligt, verksamhetsorienterat, teknikorienterat samt ett organisationsövergripande syfte. Metod för riskanalys innefattar informationssäkerhetsklassificering. Kopplas till avrapportering i verksamhetsplaneringen.
3 Metod och process för riskhantering enligt punkt 2. Riskhantering ska även kopplas till produktstyrning och produktutveckling. Kopplas till avrapportering i verksamhetsplaneringen.
4 Incidenthantering samt kontinuitetshantering. Kopplas till avrapportering i verksamhetsplaneringen.
5 Process och metodstöd inom uppföljning och analys av det systematiska och riskbaserade arbetssättet. (Intern styrning och kontroll samt verksamhetsplanering)
6 Process och metodstöd för att utveckla och förbättra informationssäkerhetsarbetet samt ledningens genomgång. Detta kopplas till avrapportering i verksamhetsplaneringen samt myndighetsövergripande analyser.

Målet för styrning och ansvar i process- och metodperspektivet är att etablera organisatoriska förmågor genom

- tydliga krav och åtgärder för hur LIS processer styrs och tillämpas genom koppling till styrande och stödjande dokument
- etablerade LIS processer/metoder som beskriver arbetets genomförande, med ett tydligt processägarskap som inkluderar process- och metodutveckling
- en tydlig koppling till kompetens och ansvar som stödjer arbetet inom LIS processerna, (processförmåga med tydligt ansvar inom utförande/stödjande)
- ett tydligt verksamhetsansvar i LIS-processernas beslutspunkter med tydlig koppling till myndighetens arbetsordning.

6 Myndighetsledningens roll inom informationssäkerhet

Arbetsförmedlingen är en styrelsemyndighet, det innebär att styrelsen har det yttersta ansvaret för verksamheten. För att styrelsen ska kunna utgöra ett effektivt ledningsorgan delegeras en stor del av styrelsens ansvar och beslutsbefogenheter till generaldirektören, vilket också har skett inom Arbetsförmedlingen. Med myndighetsledning avser vi generaldirektörens ledningsgrupp.

Det kontinuerliga arbetet inom myndighetens LIS, vilket omfattar ovan beskrivna mål och aktiviteter, har det övergripande syftet att förstärka myndighetsledningens styrning genom ett (1) ledningssystem.

Arbetet avser att förstärka perspektivet om ett integrerat ledningssystem utifrån ett systematiskt och riskbaserat arbetssätt med en nära integrerad koppling till myndighetens arbete inom intern styrning och kontroll.

Ovan beskriven förklaringsmodell inom arbetet med handlingsplanen illustrerar en PDCA modell (Plan, Do, Check, Act) för ständig förbättring. LIS är enligt denna förklaringsmodell integrerat inom processer för intern styrning och kontroll samt processer för verksamhetsplanering.

Plan – Styra och leda informationssäkerhetsarbetet, specifikt kravhantering och kravarbete. Arbetet får styrning från ledningens genomgång.

Do – LIS säkerhetsprocesser som motsvarar det systematiska och riskbaserade arbetssättet i genomförande, integrerat inom processer för intern styrning och kontroll i myndighetens ”ordinarie ledningssystem”. Får styrning från styrande och stödjande dokument inom kravhanteringsarbetet.

Check – Uppföljning sker inom verksamhetsplanering. Processerna stödjer uppföljning/planering på olika ledningsnivåer och stödjer rapporteringen till myndighetsledningen.

Act – Ständig förbättring där ledningens genomgång stödjer återkoppling till arbetet med att styra och leda säkerhetsarbetet både på strategisk och taktisk nivå. Detta ger förutsättningar i sin tur till respektive organisatorisk del inom myndigheten kopplat till arbetsordningen. Momentet ledningens genomgång avser att ytterligare förstärka myndighetsledningens delaktighet och strategiska styrning genom ledningssystemet och PDCA-modellen.

Ledningens genomgång är det moment i Arbetsförmedlingens informationssäkerhetsarbete där myndighetsledningen informerar sig om i vilken utsträckning införda säkerhetsåtgärder motsvarar myndighetens behov, om allvarliga risker som inte åtgärdats samt övriga hinder för att uppnå ledningens målsättning med informationssäkerhetsarbetet. I uppbyggnaden utifrån kravhantering samt förtydligande av LIS säkerhetsprocesser förstärks förutsättningarna inom förmågan ledningens genomgång kontinuerligt.

Målsättningen är att skapa tydlighet till verksamhetsansvar i relation till arbetsordningen. Med detta avses att ansvaret följer arbetsordningen och att vissa områden som är centrala inom ledningens genomgång som cybersäkerhet, dataskydd eller annan övergripande förmåga kan avrapporteras specifikt från respektive verksamhet men också sammanhållet i relation till arbetsordningens fördelning av verksamhetsansvar.

Genom modellens beskrivning inom (*Act*) vad avser ständig utveckling och förbättring kan myndigheten strategiskt styra centrala förbättrings- och fokusområden av myndighetens LIS. Genom detta förstärks myndighetsledningens roll kring styrning av ledningssystemet.