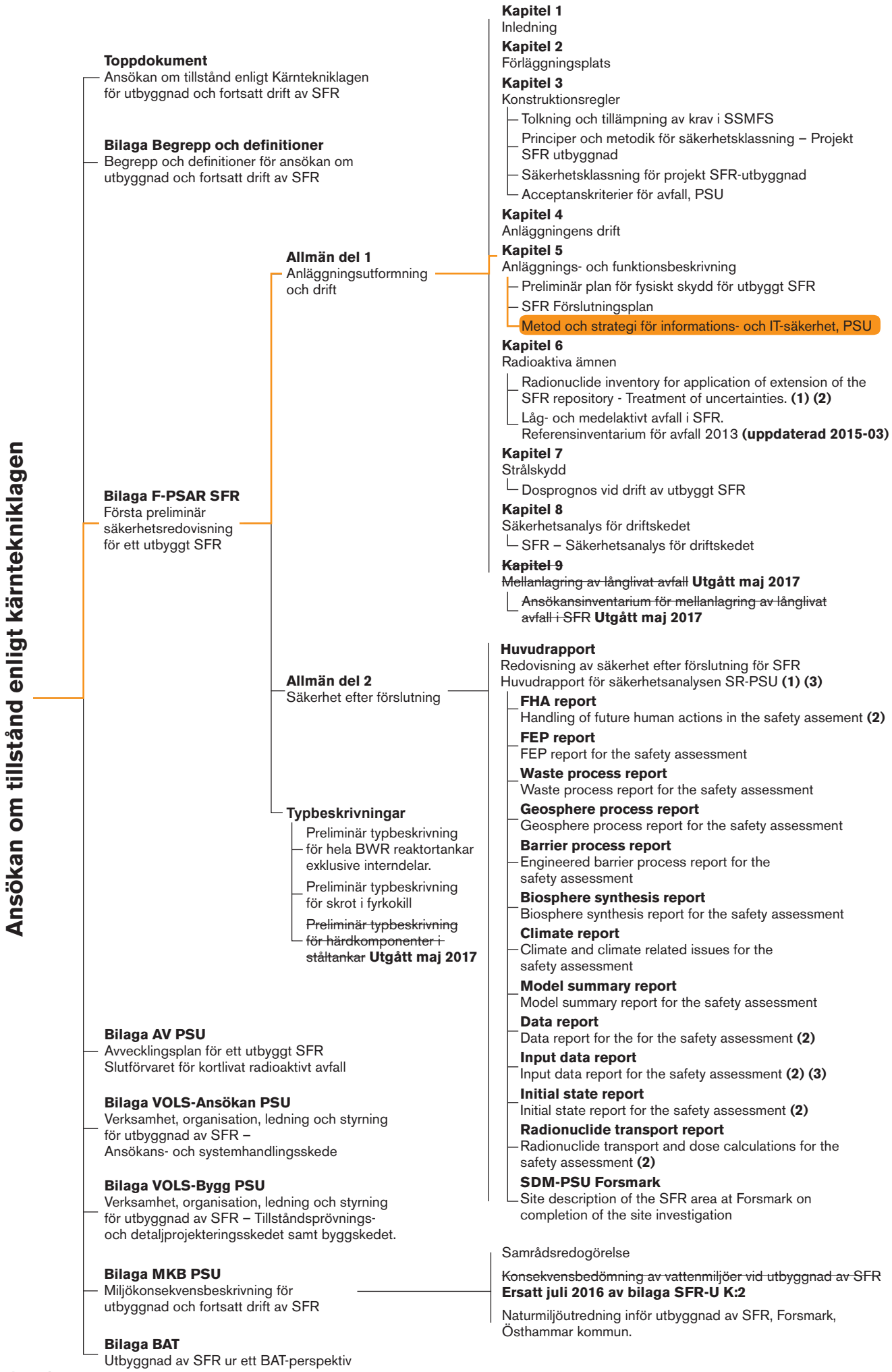


Kompletteringar

(1) September 2015 – Svensk version av *Huvudrapport SR-PSU* i allmän del 2 samt ny version (3.0) av *Radionuclide inventory* i allmän del 1 kapitel 6
(2) Oktober 2015 – Fem uppdaterade rapporter i allmän del 2 samt ny version (4.0) av *Radionuclide inventory* i allmän del 1 kapitel 6
(3) Oktober 2017 – Uppdatering av *Huvudrapport SR-PSU* och *Input data report*

Öppen

Metodbeskrivning

DokumentID	Version	Status	Reg nr	Sida
1429738	1.0	Godkänt		1 (14)
Författare Thomas Bengtsson Mikael Hammarström Björn Rüden			Datum 2014-02-24	
Kvalitetssäkrad av Therese Adusjö (KG)			Kvalitetssäkrad datum 2014-03-19	
Godkänd av Peter Larsson			Godkänd datum 2014-03-19	
Kommentar Granskning är utförd enligt granskningsprotokoll SKBdoc 1431669				

Metod och strategi för informations- och IT-säkerhet PSU

Innehållsförteckning

Svensk Kärnbränslehantering AB
Box 250, 101 24 Stockholm
Besöksadress Blekholmstorget 30
Telefon 08-459 84 00 Fax 08-579 386 10
www.skb.se
556175-2014 Säte Stockholm

1 Inledning

1.1 Bakgrund

Säker information är en viktig tillgång för Svensk Kärnbränslehantering AB (SKB). Otillbörlig påverkan på eller förlust av informations-tillgångar kan innebära stora konsekvenser för företaget. Det kan även innebära ett brott mot institutionella krav som lagar, förordningar och föreskrifter.

Mot bakgrund av detta ska SKB systematiskt och behovsanpassat arbeta med att trygga informations-tillgångarna ur de säkerhetsaspekter som företaget fastställt. Detta arbete är en angelägenhet för hela organisationen.

SKB:s ledningssystem för informationssäkerhet (LIS) är den del av ledningssystemet som styr informationssäkerheten i verksamheten. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att alla organisationens verksamheter tillämpar det styrande regelverket.

SKB:s LIS tar sin utgångspunkt i de etablerade internationella och nationella standarder som stödjer arbetet med informationssäkerhet och som har samlats i standardserien ISO/IEC 27000 (SIS, 2014). Standarderna är strukturerade i tre nivåer: krav, riktlinjer och stöd.

Projekt SFR-utbyggnads informationssäkerhetsstrategi beskriver övergripande informationssäkerhetsprocessen och förhåller sig till:

- SKB:s Ledningssystem för Informationssäkerhet, LIS
- Myndigheten för samhällsskydd och beredskap (MSB) anvisningar för informationssäkerhet
- Standardserien ISO/IEC 27000
- Projekt SFR-utbyggnads tids- och aktivitetsplan

Den beskrivna informationssäkerhetsprocessen ska ge erforderlig informationssäkerhet genom att Projekt SFR-utbyggnad ska:

- Förhålla sig till SKB:s Ledningssystem för Informationssäkerhet och andra styrande dokument
- Utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet inom projektet
- Klassificera sina informationstillgångar med utgångspunkt från säkerhetsaspekterna:
    - nukleär säkerhetspåverkan
    - konfidentialitet
    - riktighet
    - tillgänglighet
    - spårbarhet
- Använda riskanalyser för att bestämma hur risker ska hanteras samt vilka åtgärder som ska vidtas
- Införa fastställda säkerhetsåtgärder
- Genomföra och dokumentera kontroller
- Införa förbättringar

Dessutom ska projektets ledning hålla sig informerad om arbetet och minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet.

För att informationssäkerhetsarbetet ska vara framgångsrikt är det av stor vikt att det förankras i projektet, att tillräckliga resurser avdelas och att det bedrivs som en del av övrigt projektarbete.

1.2 Syfte

Syftet med detta dokument är att beskriva informationssäkerhetsstrategin för Projekt SFR-utbyggnad.

Informationssäkerhetsstrategin omfattar Projekt SFR-utbyggnads alla skeden från inledande projektering till och med provdrift av färdig anläggning, dvs. tills dess att färdig anläggning överlämnas till driftsorganisationen. ”Projekt SFR-utbyggnad” innefattar, i detta dokument, även anläggningsändringar på SFR 1.

Arbetet med informationssäkerhet syftar till att skydda projektets informationstillgångar, som kan vara av både analog och digital karaktär, mot otillbörlig påverkan ur fysiska, logiska och administrativa perspektiv.

Strategin innehåller fyra olika huvuddelar:
- Övergripande process- och metodbeskrivning för informationssäkerhetsarbetet
- Beskrivning av processteg under projektets livscykel
- Aktiviteter och leveranser kopplade till de olika processtegen
- Övergripande aktiviteter och leveranser kopplade till projektets projektplan

1.3 Målgrupp

Denna strategi är ett styrande dokument för Projekt SFR-utbyggnads informationssäkerhetsarbete och kan även utvisa för andra intressenter och kravställare hur projektets informationssäkerhetsarbete bedrivs.

Strategin ska kunna användas av SKB i övergripande projektansökningar till Strålsäkerhetsmyndigheten för att redovisa det informationssäkerhetsarbete som ska genomföras i Projekt SFR-utbyggnad, både avseende projektarbetet och färdig anläggning.

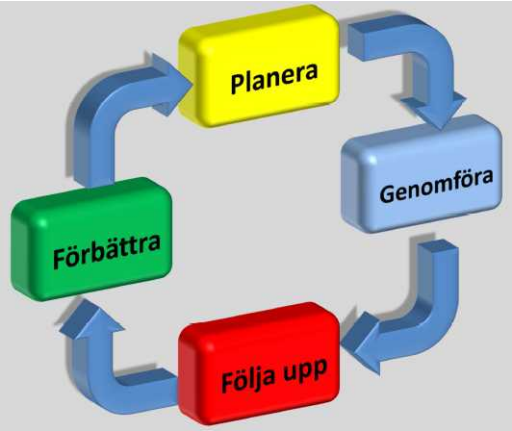
1.4 Avgränsningar

Vilka säkerhetsåtgärder enligt ISO/IEC 27002 som är tillämpbara på Projekt SFR-utbyggnad är inte beskrivna i detta dokument.

2 Informationssäkerhetsarbete inom Projekt SFR-utbyggnad

2.1 Allmänt

Information är en av SKB:s viktigaste tillgångar och utgör en förutsättning för att SKB ska kunna bedriva sin verksamhet. Därför måste information, informationssystem och processnära IT-system skyddas med avseende på nukleär säkerhetspåverkan, konfidentialitet[1], riktighet, spårbarhet och tillgänglighet så att SKB:s och externa parters verksamheter, tillgångar och relationer inte skadas.



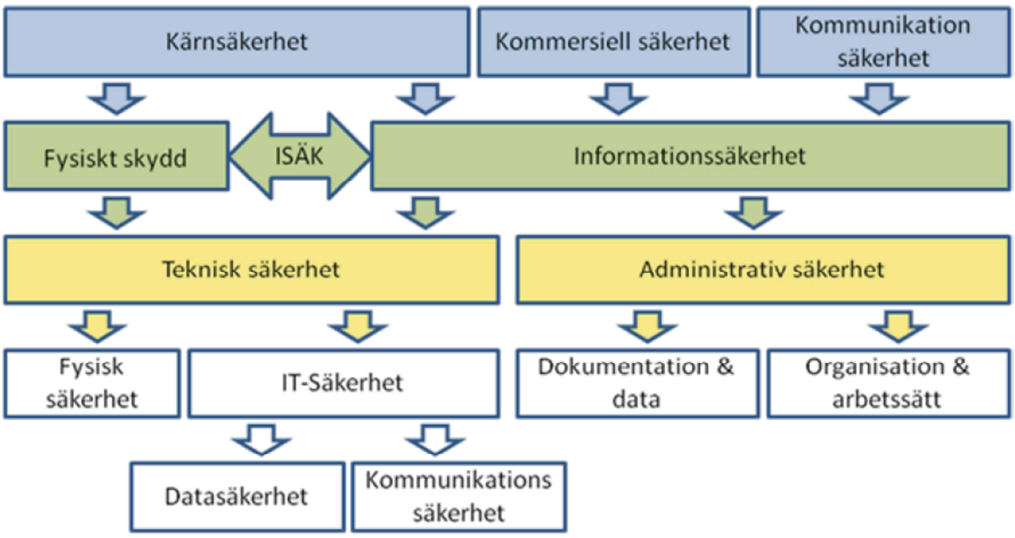
Figur 1 *Utvisande PDCA-modellen*

Genom Projekt SFR-utbyggnads arbete med informationssäkerhet ska projektet motsvara uppdragsgivares och samhällets förväntningar samt uppfylla författningar och myndigheters krav.

Arbetet med informationssäkerheten ska bedrivas fortlöpande enligt den s.k. PDCA (Plan Do Check Act)-modellen, se figur 1. Modellen etablerar ett arbetssätt som syftar till att skapa erforderligt skydd för informationstillgångar ur administrativa, logiska och fysiska perspektiv, under projektets livstid.

Projektets arbete med informationssäkerheten grundar sig på de rutiner som utarbetats av SKB för informationssäkerhet vilka i sin tur baseras på standardserien ISO/IEC 27000.

Omfattningen av begreppet ”Informationssäkerhet” för SKB definieras enligt figur 2.



Figur 2 *Utvisande säkerhetsstrukturen för SKB*

[1] Benämns i vissa SKB-dokument som sekretess

2.2 Säkerhetsorganisation

Ansvarsförhållanden och rollfördelning för säkerhetsarbetet i projektet ska vara tydliga och uttalade vad avser säkerhetsskydd, informationssäkerhet och fysisk säkerhet.

För Projekt SFR-utbyggnad ska följande roller finnas:

- Säkerhetsskyddssamordnare:
  - Samordnare för informations- och IT-säkerhet
  - Samordnare för fysisk säkerhet

Beroende på omfattning av säkerhetsarbetet kan rollerna vara explicita eller tillikabefattningar.

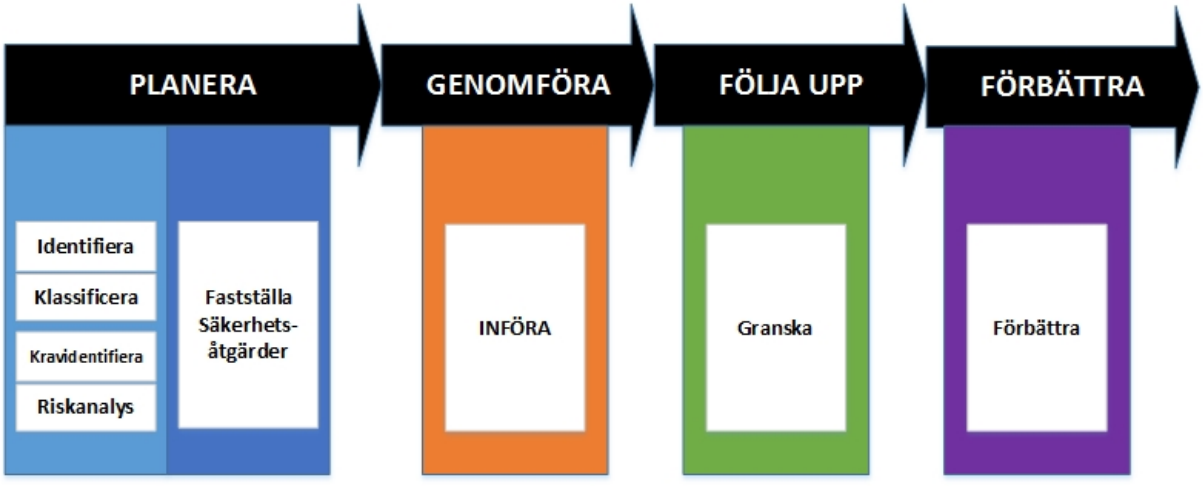
Projektets säkerhetsorganisation och rollernas ansvarsområde ska utformas så att de har okomplicerade kopplingar till SKB:s centrala säkerhetsorganisation och dess roller.

3 Processbeskrivning

För att informationssäkerhetsarbetet ska bli framgångsrikt krävs en process som är väl utvecklad och har sina rötter i beprövade metoder för informationssäkerhetsarbete. Den process projektet ska använda för att bedriva ett systematiskt informationssäkerhetsarbete har därför sin grund i MSB:s process (MSB, u å) för införande av LIS (Ledningssystem för Informationssäkerhet), standardserien ISO/IEC 27000 samt de riktlinjer för informationssäkerhet som sedan tidigare utarbetats centralt inom SKB.

Processen ska användas för det övergripande informationssäkerhetsarbetet men även för delmoment under projektets livstid, se figur 3.

Processen innebär att Projekt SFR-utbyggnad initialt gör en inventering av informationstillgångarna som sedan klassificeras utifrån hur skyddsvärda de är. Därefter identifieras påverkande krav och projektet genomför en riskanalys för att identifiera risker för projektets informationstillgångar. Med detta som grund kan projektet därefter fastställa säkerhetsåtgärder för att skydda informations-tillgångarna innan de fastställs och införs. I det avslutande steget tas de erfarenheter som erhållits under processen tillvara, för att förbättra och utveckla informationssäkerhetsarbetet.



Figur 3 *Utvisande processen för Projekt SFR-utbyggnads informationssäkerhetsarbete*

4 Processteg

4.1 Planera

4.1.1 Identifiera och klassificera

Arbetet med informationssäkerheten syftar till att skydda projektets och den färdiga anläggningens informationstillgångar, som kan vara av både analog och digital karaktär, mot hot[2]. Informationstillgångarna är i varierande grad känsliga och kritiska och vissa tillgångar kan behöva utökat skydd eller särskild hantering. För att kunna veta vilka tillgångar som behöver skyddas ska dessa tidigt identifieras.

Identifieringsarbetet leder till en dokumenterad och strukturerad förteckning över informations-tillgångarna vilken utgör en grund för det fortsatta arbetet.

När identifieringen av informationstillgångarna är gjord ska dessa klassificeras efter begreppen *nukleär säkerhetspåverkan*, *konfidentialitet*, *riktighet, tillgänglighet* och *spårbarhet*. Informationsklassificeringen ska ske enligt av SKB framtagen modell för klassificering av information och ska dokumenteras i enlighet med modellen för upprättande av informationshanteringsplan.

PSU ska likt ovan även identifiera och klassificera sina informations- och IT-system med dess applikationer. Dessa ska förtecknas i system- och applikationslistor för Projekt SFR-utbyggnad och färdig anläggning.

Klassificering av informationstillgångarna ska ses över före det att dessa ska delges utanför projektet, till exempel i form av ett förfrågningsunderlag. Klassificeringsarbetet ska då ligga till grund för att rätt säkerhetsåtgärder vidtas och kommuniceras innan informationen delges utanför projektet.

Leverans

- Informationshanteringsplan färdig anläggning
- Informationshanteringsplan PSU

Informationshanteringsplanen består av uppgifter om hur informationshanteringen sker under dess livscykel, från att dokument och data skapas, genom hantering i lagringsplatser och arkiv till bevarande eller gallring. En informationshanteringsplan består av två delar, en som styr dokumenthantering och en som styr datahantering.

Informationshanteringsplanen ska, där det är tillämpligt, ta hänsyn till Projekt SFR-utbyggnads system- och applikationslistor samt upprättas och revideras i SKB:s databas DOCplan.

Informationsägaren ansvarar för att upprätta informationshanteringsplanerna och för att rätt kompetens från det aktuella verksamhetsområdet är representerat vid klassificeringsarbetet. Klassificeringsarbetet kan även genomföras med stöd av SKB:s informationssäkerhetssamordnare.

4.1.2 Kravidentifiera

När informationstillgångarna är identifierade och klassificerade ska projektet identifiera de krav som ställs på både färdig anläggning och projektet och som kan ha påverkan på hanteringen av informationstillgångarna. Dessa krav utgörs av lagar och förordningar, föreskrifter och koncernens styrande regelverk.

[2] Hoten kan till exempel utgöras av antagonistiska hot, bestå av olyckslaster, naturlaster eller mänskliga fel

SKB beskriver centralt de krav som gäller internt inom området informations- och IT-säkerhet. Denna beskrivning omfattar en ”basnivå” av krav som gäller för alla verksamheter och projekt. ”Basnivån” utgår från en samlad analys av externa krav. Vid kravidentifiering kopplas dessa krav samman med berörd informationstillgång. Detta innebär att ett aktivt ställningstagande måste ske vid bedömning av kravens tillämpbarhet i projektet.

Tillämpbara krav och eventuella avsteg ska dokumenteras enligt fastställd modell.

Projektet ska fortlöpande stämma av styrande krav med SKB:s informationssäkerhetssamordnare.

Leverans

- Dokumentation utvisande alla för färdig anläggning styrande krav
- Dokumentation utvisande alla för PSU styrande krav

Projektet ska utifrån förteckning av SKB:s basnivå för informationssäkerhet och ovan angivna dokument upprätta dokumentation över tillämpliga krav och eventuella avsteg som gäller för projektet. Detta genomförs av projektets säkerhetsorganisation med stöd av SKB:s informationssäkerhets-samordnare och i enlighet med gällande bestämmelser.

4.1.3 Riskanalys

Riskanalysens syfte är att identifiera risker för projektets skyddsvärden, där informationstillgångarna är en av dessa. När skyddsvärdena är identifierade ska hot och sårbarheter mot dessa analyseras.

Hoten kan vara aktördrivna (antagonistiska) och av fysisk eller logisk karaktär, bestå av olyckslaster, naturlaster (väderfenomen, sjukdomar) eller mänskliga fel (slarv eller felhantering på grund av okunskap). Hoten kan påverka informationstillgångarnas konfidentialitet, riktighet, tillgänglighet och spårbarhet vilket bland annat kan leda till nukleär säkerhetspåverkan.

Sårbarheterna kan vara logiska, fysiska eller administrativa. När sårbarheterna är identifierade ska säkerhetsåtgärder föreslås som ger det skyddsvärda ett adekvat skydd vilket minskar risken till en acceptabel nivå. Säkerhetsåtgärderna ska fastställas i en säkerhetsplan (se avsnitt 4.1.1).

Projekt SFR-utbyggnad ska göra riskanalyser enligt SKB:s modell för riskhantering.

Leverans

För Projekt SFR-utbyggnad ska två grundläggande riskanalyser tas fram:

- Riskanalys färdig anläggning.
  Analysen ska identifiera hot och sårbarheter mot den färdiga anläggningen. Detta för att projektet ska kunna projektera ett adekvat skydd ur både logiska och fysiska perspektiv för anläggningens skyddsvärden[3] baserat på riskanalys och styrande krav.

- Riskanalys Projekt SFR-utbyggnad inkluderande Anläggningsändringar SFR 1.
  Analysen ska identifiera hot och sårbarheter mot projektet och dess informationstillgångar ur både logiska och fysiska perspektiv. Analysen ligger till grund för projektspecifika säkerhetsåtgärder.

Resultatet från riskanalyserna ska protokollföras och godkännas av informationsägaren.

[3] Skyddsvärdena innefattar även andra tillgångar än informationstillgångar

4.1.4 Fastställa säkerhetsåtgärder

Baserat på tidigare processteg ska ett antal säkerhetsåtgärder tas fram för att minska de risker och omhänderta de krav som tidigare identifierats.

Säkerhetsåtgärderna ska balanseras enligt principen risk, nytta och kostnad. Med detta avses att identifierade risker ska reduceras i förhållande till nyttan säkerhetsåtgärderna innebär och kostnaden de medför.

Säkerhetsåtgärderna som tas fram ska även baseras i tillämpliga delar på standarden ISO/IEC 27002 och SKB:s ”basnivå”. Där det är möjligt ska säkerhetsåtgärderna utformas enligt SKB:s princip för djupledsförsvar som består av fysiska och logiska skyddszoner.

Säkerhetsåtgärderna ska dokumenteras i en säkerhetsplan. Säkerhetsplanen ska upprättas med stöd av SKB:s produktionsanvisning och ska redovisa hur skyddet är utformat ur fysiska-, logiska- och administrativa perspektiv. Den färdiga säkerhetsplanen ska godkännas av informationsägaren.

Fastställda säkerhetsåtgärder, enligt säkerhetsplanerna, ska där de är tillämpbara hanteras under projektets alla faser. Säkerhetsåtgärderna påverkar då fortlöpande bl.a. Projekt SFR-utbyggnads systembeskrivningar och annan teknisk dokumentation.

Leverans

- Säkerhetsplan färdig anläggning
    - Plan fysiskt skydd
    - Plan för informationssäkerhet

Säkerhetsplanen för färdig anläggning består av två delar. Plan fysiskt skydd beskriver de säkerhetsåtgärder som ska vidtas i färdig anläggning vad avser fysiskt skydd. Plan för informationssäkerhet beskriver övriga informationssäkerhetsåtgärder som ska vidtas vid färdig anläggning.

Tillämpliga rubriker 6-15 i ISO/IEC 27002 används som utgångspunkt för säkerhetsåtgärderna.

- Säkerhetsplan PSU inkluderande Anläggningsändringar SFR 1
    - Plan fysiskt skydd
    - Plan för informationssäkerhet

Säkerhetsplanen består av två delar. Plan fysiskt skydd beskriver de säkerhetsåtgärder som ska vidtas för projektet vad avser fysiskt skydd. Plan för informationssäkerhet beskriver övriga informationssäkerhetsåtgärder som ska vidtas för projektet.

Tillämpliga rubriker 6-15 i ISO/IEC 27002 används som utgångspunkt för säkerhetsåtgärderna.

4.2 Genomföra

4.2.1 Införa säkerhetsåtgärder

För att omsätta säkerhetsplanerna till praktisk nytta behöver olika aktiviteter initieras; medarbetare utbildas och fysiska-, logiska- samt administrativa säkerhetsåtgärder införas.

Vid införandet av säkerhetsåtgärder för projektet ska roller och ansvarsområden vara tydliga och uttalade. Projektet ska även där det är tillämpligt genomföra en förenklad riskanalys för införandet av säkerhetsåtgärderna. Detta för att vara förberedd och medveten om de risker som finns för införandet. Projektet kan då snabbt vidta åtgärder för att komma vidare i införandeprocessen om problem uppstår.

Projektets informationssäkerhetsansvarige ska i samråd med informationsägare och delprojektledare medverka i framtagande av utbildningsplan för berörda anställda. Utbildningsplanen är en del av plan för införande av säkerhetsåtgärden.

Det åligger även projektet att kommunicera säkerhetsåtgärderna i den omfattning det krävs för att medvetandegöra målen med säkerhetsåtgärderna hos medarbetarna och medarbetarnas roll i dessa.

När nya säkerhetsåtgärder eller aktiviteter införs kan det även finnas behov av att skapa nya, för PSU, styrande dokument eller revidera befintliga.

Plan för införande av säkerhetsåtgärder ska följa de riktlinjer som finns centralt hos SKB.

Leverans

- Plan för införande av säkerhetsåtgärder för färdig anläggning
- Plan för införande av säkerhetsåtgärder för PSU inkluderande Anläggningsändringar SFR 1

Införandeplanerna ska för varje identifierat leveransobjekt definiera vem som är införandeansvarig, vilka aktiviteter som är knutna till säkerhetsåtgärden, utbildningsbehov för säkerhetsåtgärden samt hur kommunikation ska ske kring detta. Införandeplanerna ska även identifiera de olika insatser som krävs för att alla beslutade säkerhetsåtgärder ska följas av berörda medarbetare och få praktisk nytta i verksamheten.

4.3 Följa upp

4.3.1 Granska

Projekt SFR-utbyggnad ska genomföra interna kontroller av informationssäkerheten med planerade intervall. Syftet är att avgöra om alla beslutade säkerhetsåtgärder för projektet existerar, följs och fungerar tillfredsställande. Vidare syftar kontrollarbetet även till att skapa förutsättningar för att kunna upptäcka och utvärdera påverkan på informationstillgångarna i form av bristande konfidentialitet, riktighet, tillgänglighet och spårbarhet, vilket bland annat kan leda till nukleär säkerhetspåverkan.

Förutom de planerade kontrollerna ska löpande övervakning ske med fokus på informations-tillgångarnas säkerhet. För Projekt SFR-utbyggnad innebär detta t ex. att säkerställa spårbarhet i bevakningstekniska informations- och IT-system. För Projekt SFR-utbyggnad ska arbetet med övervakning ske kontinuerligt genom PDCA-modellen och enligt av SKB fastställd modell för informationssäkerhetsarbetet.

När granskningen visar någon form av avvikelse ska den hanteras enligt av SKB framtagen modell för hantering av avvikelser.

Vidare ska projektet även granska dokumentation innan denna fastställs och distribueras externt,

exempelvis förfrågningsunderlaget (FU) inför en upphandling.
Det finns ur ett säkerhetsperspektiv flera syften med granskningen. Det ena syftet är att granska dokumentationen för att säkerställa att projekteringen tagit hänsyn till de säkerhetskrav som ställts på anläggningen. Det andra syftet är att granska dokumentationen för att säkerställa att klassificeringen är korrekt gjord mot bakgrund av de redovisade säkerhetsaspekterna.

Slutligen ska granskning av säkerhetsrelaterade byggdelar under byggnationen ske. Syftet med detta är att säkerställa att de ställda säkerhetskraven verkställs under produktionen av färdig anläggning.
När anläggningen tas i provdrift ska projektet även genomföra regelbundna kontroller av informationssäkerheten enligt en i förväg uppgjord kontrollplan. Detta arbete överlämnas sedan till driftorganisationen då Projekt SFR-utbyggnad avvecklas.

Granskning relaterad till informationssäkerhet ska genomföras inom ramen för Projekt SFR-utbyggnads ordinarie granskningsarbete.

Leverans

- Kontrollplan för interna kontroller Projekt SFR-utbyggnad, bilaga till Säkerhetsplan Projekt SFR-utbyggnad
- Kontrollplan för färdig anläggning i provdrift, bilaga till Säkerhetsplan färdig anläggning
- Rapport efter genomförd kontroll med åtgärdsförslag för identifierade avvikelser

Kontrollplanerna ska minst utvisa vad som ska kontrolleras, vem som ansvarar för kontrollen och när den ska vara utförd. Rapporten ska dokumentera identifierade avvikelser så att de kan åtgärdas på ett strukturerat sätt.

Detta genomförs av projektets säkerhetsorganisation med stöd av SKB:s informationssäkerhets-samordnare och i enlighet med gällande bestämmelser.

5 Aktiviteter och leveranser kopplade till projektets olika faser

5.1 Allmänt

För projektet kommer arbetet med informationssäkerheten att bedrivas enligt tidigare redovisad process och metod.

Inledningsvis inriktas informationssäkerhetsarbetet mot att identifiera och klassificera informationstillgångar samt att införa tillämpliga skyddsåtgärder för dessa. När det inledande arbetet är genomfört ska informationssäkerheten vidmakthållas för att möta de informationssäkerhets-påverkande förändringar som sker under projektets livstid.

För projektet kommer förändringar av förhållanden som har påverkan på informationssäkerheten att ske fortlöpande.

Dessa förändringar kan vara:

- Förändringar av externa och interna krav (tillkommande krav eller icke längre gällande krav)
- Förändringar av informationstillgångar (tillkommande eller avgående informationstillgångar)
- Förändringar av personal (tillkommande personal, avgående personal, förändrade arbetsuppgifter etc.)
- Förändringar av informationshanteringssystem (införande av nya system, avveckling av system etc.)
- Förändringar av lokaler (nya arbetsplatser, avveckling av arbetsplatser, samlokalisering etc.)

Då förändringar som har påverkan på informationssäkerhetsarbetet sker är det nödvändigt att vidta åtgärder för att säkerställa att rätt nivå på säkerheten hålls. Ett praktiskt exempel kan vara att en ny kravidentifiering sker vid förändringar av lagar som rör verksamheten.

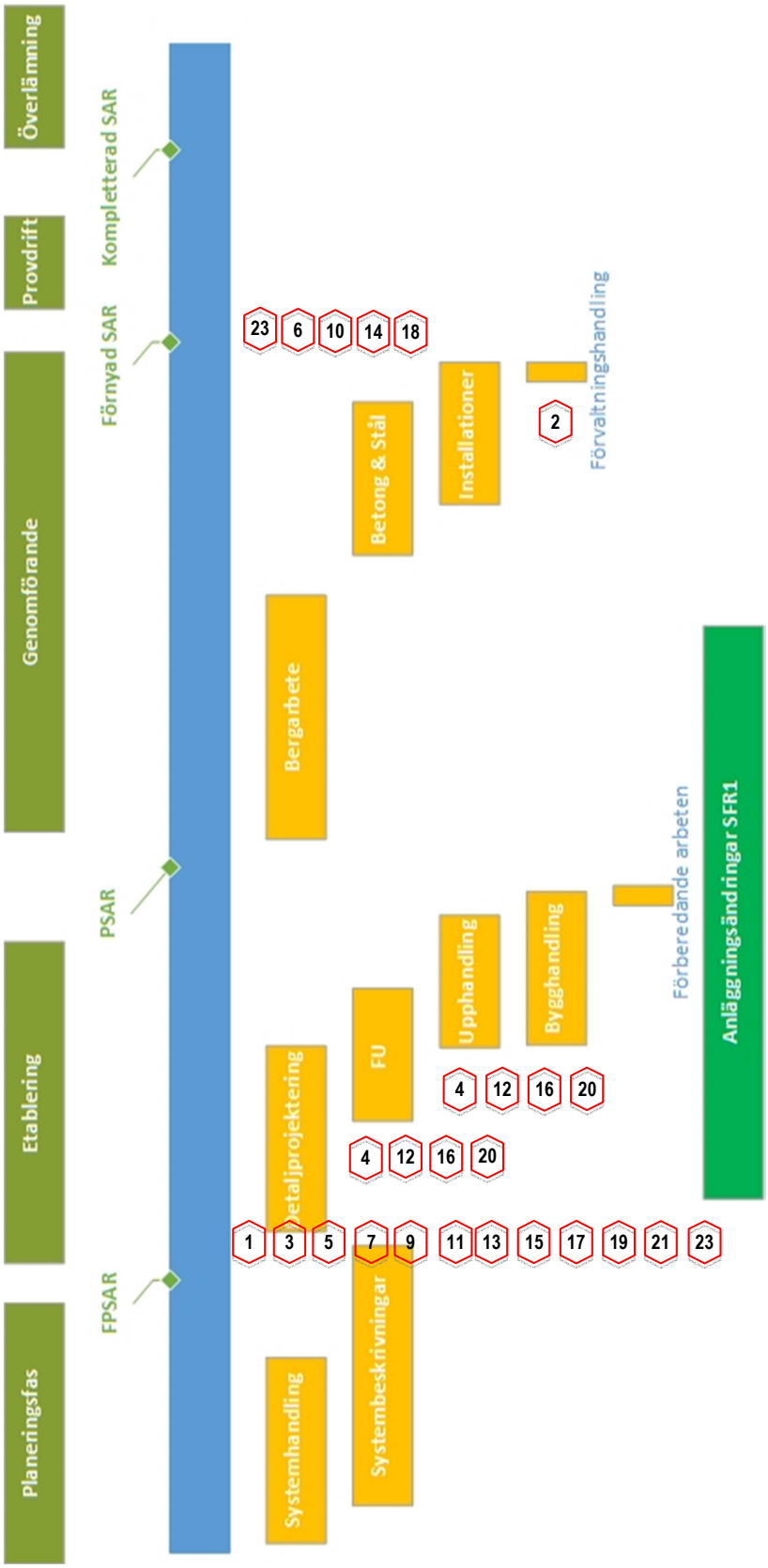
För Projekt SFR-utbyggnad sker en informationsklassificering inför projektets början samt när projektet övergår till förvaltning. Ny klassificering av information under projektets livslängd bör göras vid sådana förändringar i verksamheten som påverkar informationstillgångarna.

Vid större verksamhetsändringar i projektet bör en förnyad grundläggande riskanalys genomföras alternativt genomförs en separat riskanalys för den specifika verksamheten. Då en riskanalys påverkas av yttre förändringar ska den revideras med jämna mellanrum.

Säkerhetsåtgärder ska tas fram, dokumenteras och fastställas innan detaljprojekteringen startar. Detta för att skydda projektets informationstillgångar under hela projektets livstid. Med utgångspunkt i skyddsbehovet fastställs de mål och säkerhetsåtgärder som krävs för en balanserad informationssäkerhet.

Vid större förändringar i det grundläggande säkerhetsarbetet måste tillämpliga säkerhetsåtgärder enligt rubrikerna 6-15 i ISO/IEC 27002 revideras.

5.2 Grafisk figur utvisande leveranser



Figur 3, *Utvisande informationssäkerhetsrelaterade leveranser kopplade till PSU:s övergripande tids- och aktivitetsplan.*

Redovisade leveranser utgör exempel på, men begränsas inte till, vad som behöver göras i säkerhetsarbetet utöver det grundläggande säkerhetsarbetet i projektets olika faser. Leveranserna beskrivs i p. 4.3 Matris utvisande leveranser

5.3 Matris utvisande leveranser

Leverans-nr	Referens i dok	Aktiviteter för informationssäkerhetsarbetet
1	4.1.1.1	Informationshanteringsplan färdig anläggning (Upprättad)
2		Informationshanteringsplan färdig anläggning (Revideras)
3	4.1.1.1	Informationshanteringsplan PSU (Upprättad)
4		Informationshanteringsplan PSU (Revideras)
5	4.1.2.1	Kravuppfyllnadsmatris utvisande alla för färdig anläggning styrande krav (Upprättad)
6[4]		Kravuppfyllnadsmatris utvisande alla för färdig anläggning styrande krav (Revideras)
7	4.1.2.1	Kravuppfyllnadsmatris utvisande alla för PSU styrande krav (Upprättad)
8[5]		Kravuppfyllnadsmatris utvisande alla för PSU styrande krav (Revideras)
9	4.1.3.1	Riskanalys färdig anläggning (Upprättad)
10		Riskanalys färdig anläggning (Revideras)
11	4.1.3.1	Riskanalys PSU inkluderande Anläggningsändringar SFR 1 (Upprättad)
12		Riskanalys PSU inkluderande Anläggningsändringar SFR 1 (Revideras)
13	4.1.4.1	Säkerhetsplan färdig anläggning (Upprättad)
14		Säkerhetsplan färdig anläggning (Revideras)
15	4.1.4.1	Säkerhetsplan PSU inkluderande Anläggningsändringar SFR 1 (Upprättad)
16		Säkerhetsplan PSU inkluderande Anläggningsändringar SFR 1 (Revideras)
17	4.2.1.1	Plan för införande av säkerhetsåtgärder för färdig anläggning (Upprättad)
18		Plan för införande av säkerhetsåtgärder för färdig anläggning (Revideras)
19	4.2.1.1	Plan för införande av säkerhetsåtgärder för PSU inkluderande Anläggningsändringar SFR 1 (Upprättad)
20		Plan för införande av säkerhetsåtgärder för PSU inkluderande Anläggningsändringar SFR 1 (Revideras)
21	4.3.1.1	Kontrollplan för interna kontroller PSU, bilaga till Säkerhetsplan PSU (Upprättad)
22[6]		Kontrollplan för interna kontroller PSU, bilaga till Säkerhetsplan PSU (Revideras)
23	4.3.1.1	Kontrollplan för färdig anläggning i provdrift, bilaga till Säkerhetsplan färdig anläggning (Upprättad)
24[7]		Kontrollplan för färdig anläggning i provdrift, bilaga till Säkerhetsplan färdig anläggning (Revideras)
25[8]	4.3.1.1	Rapport efter genomförd kontroll med åtgärdsförslag för identifierade avvikelser (Upprättad)

[4] Genomförs då styrande krav förändras, dock senast enligt grafisk bild utvisande övergripande tids- och aktivitetsplan.
[5] Ej inlagd på grafisk bild utvisande övergripande tids- och aktivitetsplan då denna genomförs då styrande krav förändras.
[6] Ej inlagd på grafisk bild utvisande övergripande tids- och aktivitetsplan då denna genomförs efter genomförd kontroll.
[7] Ej inlagd på grafisk bild utvisande övergripande tids- och aktivitetsplan då denna genomförs efter genomförd kontroll.
[8] Upprättas i samband med genomförande av kontroll. Baserat på denna revideras kontrollplanen.

6 Referenser

MSB, u å. Metodstöd. Myndigheten för samhällsskydd och beredskap. Tillgänglig: https://www.informationssakerhet.se/sv/Metodstod/Metodstod

SIS, 2014. SS-ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO / IEC 27000:2014, IDT). Stockholm: Swedish Standards Institute.