Öppen

Rapport

DokumentID	Version	Status	Reg nr	Sida
1390012	1.0	Godkänt		1 (11)
Författare Mikael Andersson Erik Bernsland			Datum 2013-04-04	
Kvalitetssäkrad av Saida Engström Olle Olsson Tomas Rosengren			Kvalitetssäkrad datum 2013-06-26 2013-06-26 2013-06-27	
Godkänd av Anders Ström			Godkänd datum 2013-06-27	

Principer för informations- och IT-säkerhet för inkapslingsanläggningen och slutförvaret för använt kärnbränsle och kärnavfall

Innehåll

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 Metodik för informations- och IT-säkerhet

Kapitel 1 beskriver på en principiell nivå SKB övergripande metodik för informations- och IT-säkerhet.

1.1 Översikt

SKB har etablerat en företagsövergripande metodik inom området informationssäkerhet som ett gemensamt stöd för att möta externa krav samt hot som kan ha påverkan på SKB:s verksamhet. Avsikten är att upprätthålla ett balanserat och enhetligt skydd för bl a känslig information och informationssystem. Metoden grundar sig på standarder inom ISO 27000-serien vilket innebär att den är avgränsad till att säkerställa en systematisk kravhantering för området informations- och IT-säkerhet. De styrande dokument som omfattas av metoden är integrerade i SKB:s ordinarie ledningssystem.

Metodiken baseras i huvudsak på två bakomliggande analyser:

- Externa krav och hot - påverkan på SKB.
- Interna krav - påverkan på tillgångar[1].

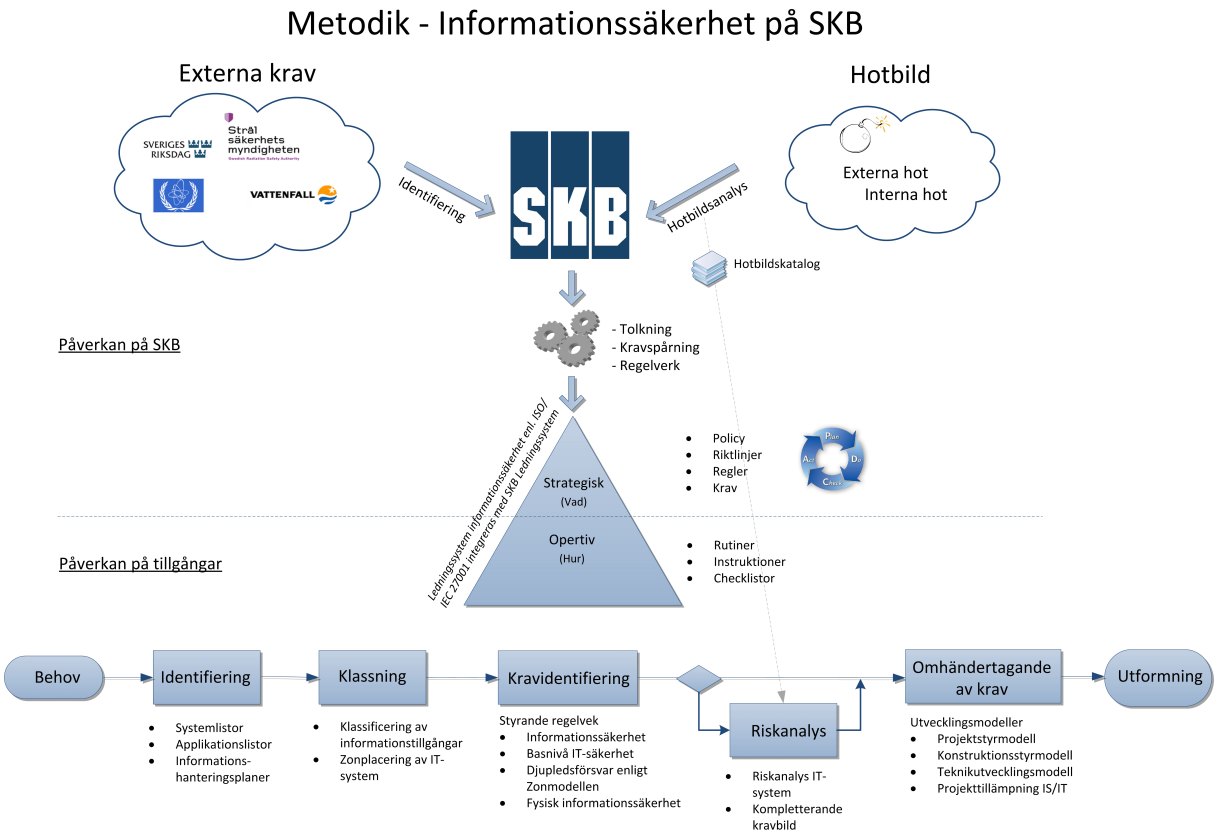
De externa kraven och identifierade hot analyseras, bearbetas och sammanvägs till företagsgemensamma riktlinjer och regelverk som utgör stöd för tillämpning inom alla verksamhetsområden. Det löpande arbetet med uppföljning och förbättring baseras på ett kontinuerligt kvalitetsarbete (PDCA[2]).

De interna regelverken består av styrande dokument och beskriver gemensamma krav och regler som ska tillämpas internt inom SKB. Gemensamma rutiner ger ytterligare stöd på operativ nivå i ledningssystemet där även verksamhetsspecifika rutiner placeras.

Hur de interna kraven påverkar berörda tillgångar utgör nästa analysfas och sker med stöd av ett strukturerat flöde där identifiering av dessa tillgångar utgör en grundläggande aktivitet. Resultat av detta arbete genererar ett informationssäkerhetsanpassat kravunderlag som tillförs övriga krav vid utformning av administrativ eller teknisk lösning. Figur 1 nedan visar en översikt.

[1] Allt som ur ett informationssäkerhetsperspektiv har betydelse för verksamheten. Exempel på tillgångar: information, databaser, programvaror, lokaler, datamedia, avtal, personal etc.

[2] Plan Do Check Act – etablerad metodik för systematiskt förbättringsarbete, här tillämpat inom området informationssäkerhet.



***Figur 1**. Metodik för informationssäkerhet.*

1.2 Hotbildsanalys

1.2.1 Översikt

Hotbildsanalysens resultat ska fungera som ett underlag för planering av det strategiska och företagsövergripande informationssäkerhetsarbetet. Den företagsövergripande delen av hotbildsanalysen resulterar i en hotbildskatalog som på en övergripande nivå beskriver möjliga hot mot organisationen. Analysens resultat ligger även till grund för interna regelverk på strategisk och operativ nivå. Genom riskanalyser på operativ nivå, baserad på den företagsövergripande hotbildskatalogen, bidrar analysarbetet även till den interna kravhanteringen för utformning av informations- och IT-säkerhetsskydd, se figur 1. Analysresultatet för informationssäkerhet ska komplettera hotbildsanalyser som är genomförda för fysiskt skydd.

Genom hotbildsanalysarbetet säkerställas:

- Att det upprättas och förvaltas en företagsövergripande hotbildskatalog för området informationssäkerhet.
- Att riskanalys för skyddsvärda tillgångar genomförs utifrån relevant hotbild.
- Att fysiska och logiska hot kombineras och värderas ur ett samlat riskperspektiv med syfte att upprätthålla ett sammantaget säkerhetsskydd.

1.2.2 Metodbeskrivning

Tillämpad metodik för hotbildsanalys ska vara förenlig med SKB:s regelverk och metoder för området informationssäkerhet. Analys- och bearbetningsarbetet genomförs som strukturerade workshops och enligt ISO 27001-metodiken.

Under analys- och bearbetningsfasen sker löpande avstämningar i syfte att säkerställa kvalitet och inriktning. Arbetet delas in i fyra steg vilka är insamling/avgränsning, bearbetning/analys, avstämning och överlämning.

Hoten i katalogen baseras på och underbyggs av information från intervjuer, befintliga riskanalyser, incidentrapportering, nationella och internationella hotbildskataloger samt erfarenheter. Identifierade informationssäkerhetshot utgår från faktorerna *tillgänglighet*, *riktighet*, *sekretess* och *spårbarhet*.

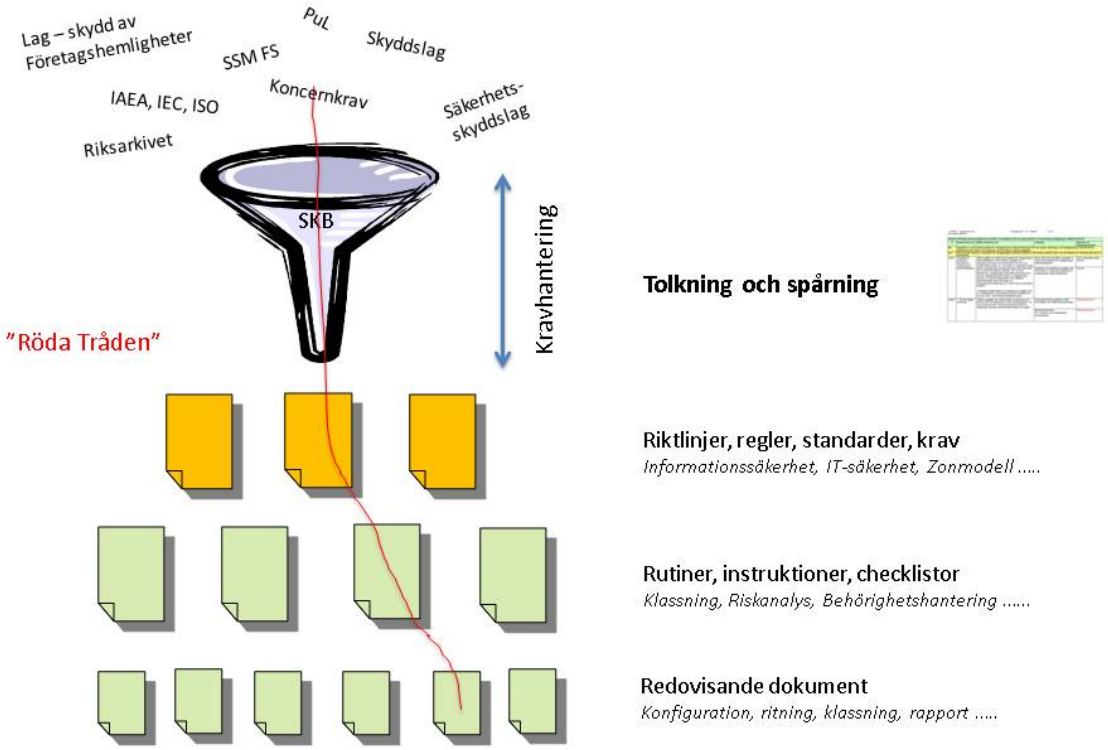
Hotbildskatalogen ligger därefter till grund för att identifiera vilka av de skyddsvärda tillgångar inom SKB som kan påverkas av hoten. Genom att hoten kategoriseras enligt SKB:s definierade riskområden, t ex personal, teknik, ekonomi och finans, kan SKB använda dessa olika hotbilder inom organisationen för att genomföra riskanalyser inom respektive ansvarsområde. Efter genomförd riskanalys identifieras skyddsåtgärder och behov av säkerhetsmekanismer.

1.3 Externa krav

1.3.1 Översikt

De externa kraven omhändertas på ett systematiskt sätt i flera steg. Detta ger en tydlighet i spårbarhet och underlättar hantering vid kompletteringar eller förändringar i den externa kravbilden. De centrala aktiviteterna omfattar bl a kravtolkning, verifiering och validering av krav samt beskrivning i interna styrande dokument och rutiner.

Funktionsområdesansvarig för informationshantering är ansvarig för att krav som berör informationssäkerhet omhändertas vilket bl a sker genom att nedan beskrivna aktiviteter genomförs, granskas, godkänns och dokumenteras i ledningssystemet.



Figur 2. *Omhändertagande av externa krav.*

1.3.2 Metodbeskrivning för identifiering och tolkning av krav

Identifiering av krav

Den externa kravbilden som påverkar området informationssäkerhet baseras på:

- Lagar och förordningar.
- Myndigheters föreskrifter.
- Koncernriktlinjer och krav.

Identifiering av berörda krav dokumenteras i ledningssystemet samt synkroniseras med SKB överordnad kravförteckning.

Tolkning av krav

Tolkning av identifierade externa krav innebär en nedbrytning och förtydligande av kraven till stöd för formulering och beskrivning av interna krav och regler (styrande dokument). Tolkningar och styrande dokument nås via ledningssystemet.

Normalisering mot ISO 27002

Den externa kravbilden är relativt omfattande. För att kunna hantera detta på ett rationellt sätt används en modell där de externa kraven struktureras utifrån standarden ISO/IEC 27002. Denna ger ett bra stöd för att strukturera de externa kraven och samtidigt ge ett normerat stöd för de interna regelverken vilket bidrar till ökad spårbarhet vid tillämpning av de interna kraven. Förankring mot ISO/IEC 27002 underlättar bl a vid genomförande av oberoende granskningar.

Figur 3. *Projicering av externa krav mot ISO/IEC 27002 kontroller och SKB interna regelverk.*

Kravspårning och regelverk

Den detaljerade kravspårningen utgör ett vitalt underlag för att kunna koppla externa krav mot interna regelverk. Här utgör projicering och normalisering mot ISO/IEC 27002 en viktig komponent och komplement till den detaljerade beskrivningen. Genom kravspårningen dokumenteras hur varje externt krav, via ISO-standarden, omhändertas i en eller flera interna regelverk och avsnitt i dessa. Denna metodik innebär att de interna regelverken beskriver de gemensamma interna kraven för att möta och omhänderta den samlade externa kravbilden inom området informationssäkerhet.

Företagsövergripande rutiner

Rutiner och instruktioner utgör underlag på operativ nivå för att möta kraven på genomförande av specifika aktiviteter. Merparten av dessa tillhör berörda verksamhetsområden och kan t ex utgöra del i beskrivningen av en viss arbetsprocess. Några är av gemensam natur och beskrivna för att kunna tillämpas av samtliga verksamheter.
Till dessa hör:

- Klassning av information och IS/IT-system.
- Riskanalys – information och IS/IT.
- Hanteringsregler för sekretessklassad information.
- IT-säkerhetshandbok för användare.
- Uppföljning av efterlevnad – informationssäkerhet.

1.4 Omhändertagande av interna krav

1.4.1 Översikt

De interna regelverken för informations- och IT-säkerhet används som gemensam bas för ingående krav vid utveckling eller förändring av informations- och IT-system. Analyser som tillämpas i samband med omhändertagande av interna krav baseras bl a på klassificering och riskanalys, vilket ger underlag för specificering av ingående säkerhetsrelaterade krav. Dessa säkerhetskrav kompletterar övriga krav för den aktuella lösningen och omhändertas vidare enligt berörd utvecklingsmodell för aktuell verksamhet.

1.4.2 Metodbeskrivning för omhändertagande av interna krav

Identifiering av behov

I visst läge uppstår ett behov av att utforma en lösning baserat på exempelvis ny eller förändrad kravbild, funktionalitet, verksamhet eller arbetssätt. Behovet formuleras och bereds exempelvis i ett ändringsärende eller projektdirektiv.

Identifiering av berörda tillgångar

Utformning av nya system, applikationer, processer eller arbetssätt medför att berörda tillgångar identifieras och dokumenteras i t ex systemlistor, applikationslistor eller informationshanteringsplaner. Dessa underlag identifierar vilka informationssystem/objekt som påverkas av interna krav och hot mot informationssäkerheten. Befintliga tillgångar behandlas enligt samma princip vilket bl a medför genomgång av befintliga underlag vid ändringar på grund av nya eller förändrade förutsättningar för visst system eller process.

Klassificering

Klassificering av identifierade tillgångar (information, IS/IT, ICS) genomförs med avseende på informationssäkerhet baserat på tillgångens påverkan och betydelse för verksamheten avseende sekretess, tillgänglighet, riktighet, spårbarhet samt systemets betydelse för kärnteknisk säkerhet.

Riskanalys

Baserat på resultatet från genomförd klassificering görs en bedömning om genomförande av en riskanalys. Riskanalysen syftar till att identifiera kritiska händelser och risken för att dessa inträffar. Här utgör hotbildsanalysen en viktig grund för att identifiera sådana händelser. Ett resultat av riskanalysen omfattar identifiering av behov av kompletterande krav och skyddsåtgärder för att hantera identifierade risker.

Kravidentifiering

SKB:s regelverk inom området informations- och IT-säkerhet beskriver de krav och regler som gäller internt, baserat på samlad analys av externa krav och hot. Regelverken beskriver den basnivå som gäller för alla verksamheter och projekt. Vid kravidentifiering kopplas dessa krav samman med berörd tillgång. Detta innebär att ett aktivt ställningstagande måste ske vid bedömning av kravens tillämpbarhet samt behov av kompletterande eller förstärkta krav baserat på genomförd riskanalys. Tillämpbara krav och eventuella avsteg dokumenteras.

Omhändertagande av krav

Identifierade informations- och IT-säkerhetskrav kompletterar övriga krav på funktion, gränssnitt, miljö, säkerhet m m vilka tillsammans utgör den sammantagna kravbilden inför utformning av aktuell lösning. Omhändertagande av de olika kraven beskrivs i berörda styrmodeller för projekthantering och utveckling/konstruktion av tekniska system.

Utformning

Utformning av teknisk och administrativ lösning sker i enlighet med ledningssystemets modeller för genomförande av projekt samt utveckling av administrativa och tekniska system.

2 Utformning av informations- och IT-säkerhetsskydd

Kapitel 2 beskriver på en principiell nivå utformningen av informations- och IT-säkerhetsskyddet för slutförvaret för använt kärnbränsle och kärnavfall vilket hanters inom projekt Kärnbränsleförvaret.

2.1 Översikt

Med stöd av gällande regelverk i SKB:s ledningssystem tillämpar projekt Kärnbränsleförvaret redovisad metod vid utformning av skyddet för informations- och IT-säkerhet. Aktuellt regelverk är under revidering inom projekt ISÄK[3], vars resultat successivt kommer ersätta befintliga styrande dokument för att därefter kunna tillämpas inom projekt Kärnbränsleförvaret.

Själva utformningsarbetet genomförs inom ramen för projekt Kärnbränsleförvarets tids- och aktivitetstidsplan vilket gör att arbetet sker successivt och i takt med projektets berörda aktiviteter. Den interna kravhanteringen för informations- och IT-säkerhet ingår således som en del i projektets totala kravhanteringsarbete.

I enlighet med redovisad metod har en företagsövergripande hotbildsanalys genomförts med syfte att, i ett första skede, upprätta en företagsgemensam hotbildskatalog. Katalogen kommer i ett nästa skede fungera som hotbeskrivning i samband med att projekt Kärnbränsleförvaret genomför riskanalyser inom skyddsvärda tillgångar; informationsmängder och datoriserade system. Detta som en del av projektets interna kravhantering för utformning av den planerade slutförvarsanläggnings totala säkerhetsskydd (fysiskt- och logiskt skydd).

2.2 Skyddsvärd information

Den information som projektet upprättar förtecknas i form av informationstyper i en informationshanteringsplan. Planen omfattar bl a en klassificering, där informationen värderas utifrån aspekterna *sekretess*, *riktighet*, *spårbarhet* och *tillgänglighet*. Planen ligger till grund för hur information får hanteras under projekttiden.

Informationens klassificeringsresultat fungerar också som underlag vid kravställning i samband med utformningen av skyddet för informationsbehandlande IT-system.

2.3 Datoriserade system av betydelse för anläggningens säkerhet

Utformningen av Informations- och IT-säkerhetsskyddet för den planerade anläggningens datoriserade system, kommer successivt att kravställas i enlighet med redovisad metod och med stöd av styrande dokument. En klassificering av anläggningssystem är genomförd vars resultat ligger till grund för kommande riskanalys (hotbildsanalys) och IT-säkerhetskravställning utifrån basnivån för IT-säkerhet.

Utformningen av informations- och IT-säkerhetsskyddet grundar sig på en djupledsförvarsprincip som omfattas av ett zonindelat datornätverk och baskrav för IT-säkerhet samt en modell för applikationssäkerhet.

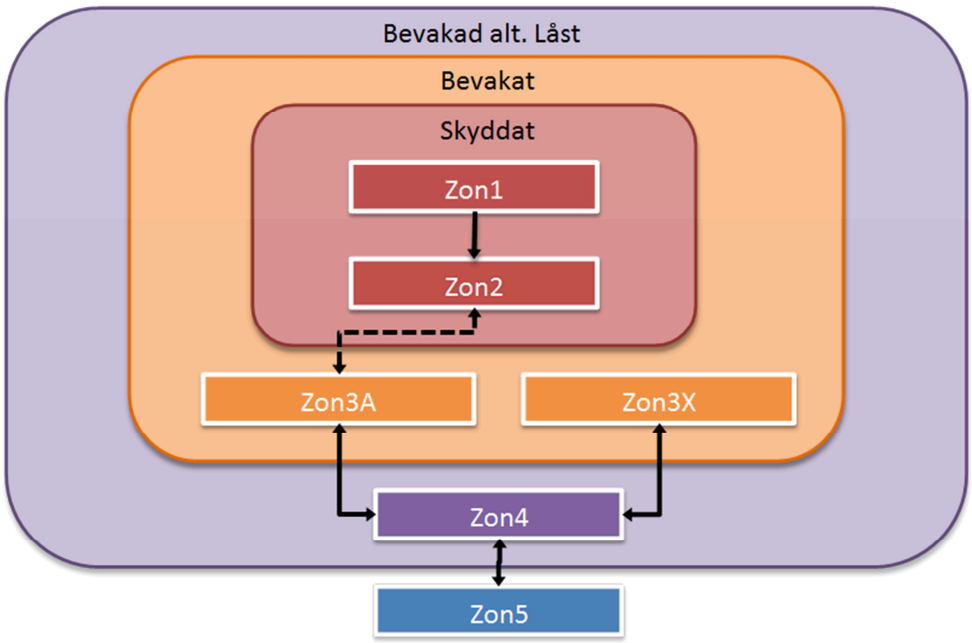
2.3.1 Skyddsprinciper för zonindelat datornätverk

Inom SKB pågår ett arbete med att införa en så kallad zonmodell som förstärker informations- och IT-säkerheten inom företagets befintliga anläggningar. Zonmodellen är en grundläggande skyddsprincip

[3] Företagsövergripande projekt med syfte att i samverkan med berörda verksamhetsområden utveckla informationssäkerheten inom SKB. Projektet består av tre huvudområden som var för sig omfattar ett flertal delområden och aktiviteter för att nå projektets målsättning. Projektets tre huvudområden: a) Ingående krav och interna regelverk, b) Klassificering av IT-system och c) Realisering av zonmodell för djupledsförsvar.

och komponent inom djupledsförsvaret och motsvarar den modell som tillämpas hos svenska kärnkraftverk. Principen ska även tillämpas i samband med utformningen av informations- och IT-säkerhetsskyddet för SKB:s planerade anläggningar, bl a slutförvarsanläggningen.

Genom ett zonindelat datornätverk separeras anläggningens skyddsvärda datoriserade system från t ex administrativa IT-system. En tillämpning av zonmodellen bildar tillsammans med det fysiska skyddet ett sammantaget säkerhetsskydd för de datoriserade system som anses ha betydelse för anläggningens säkerhet. Zonmodellens logiska skyddsbarriärer kompletterar anläggningens fysiska skydd, figur 4.



Figur 4. *Modell för logiska och fysiska skyddszoner.*

Nätverk och system för bevakning och tillträdeskontroll tillämpar SKB:s skyddsprinciper för IT-system inklusive zonmodellen för att möta höga krav på skydd mot obehörig åtkomst, manipulering och störningar.

Generella regler och förutsättningar

Zonmodellen beskriver regler som omfattar skyddsprinciper inom och mellan de zoner som omfattas av modellen. Den grundläggande skyddsprincipen för kommunikation mellan zoner är att varje zon ska skyddas från angränsande zon med en säkerhetslösning som förhindrar obehörig kommunikation mellan olika zoner. Tillåten kommunikation måste terminera i angränsande zon och får aldrig direkt passera två zongränser.

Zonövergångar ska tillämpa skyddsprinciper som säkerställer att integrationer mellan IT-system inte kan tillämpas för annat ändamål än integrationens syfte. Zonövergångar ska med andra ord ha ett skydd som förhindrar dataintrång. Även integrationens informationsflöde ska skyddas så att t ex informationens riktighet vidmakthålls. Dessa grundprinciper är centrala skyddskrav mellan och inom zoner för att säkerställa IT-systemets tillgänglighet ur ett logiskt perspektiv.

Den generella regeln vid tillämpning av zonmodellen medför att IT-system med direkt eller indirekt påverkan på en kärnteknisk anläggnings säkerhet placeras i zon 1 eller 2. Exempel på sådana system är manuella och automatiska säkerhetssystem samt processövervakningssystem (SCADA-systems). IT-system som har liten eller ingen betydelse för anläggningens säkerhet, men betydelse för t ex anläggningens drifttillgänglighet, placeras i zon 3. Exempel på sådana system är underhållssystem,

dokumenthanteringssystem och konstruktionssystem. I zon 4 placeras administrativa IT-system, t ex standardarbetsplatser, e-postserver och skrivare.

Eftersom zon 3 angränsar till zon 2 blir denna logiska skyddsbarriär en extra känslig gränsyta (zonövergång). Detta ställer därför krav på särskilda skyddsmekanismer för att skydda IT-system som är placerade i zon 2 och som har någon form av integration till IT-system placerade i zon 3.

Integration mellan IT-system i olika zoner

System som behöver kommunicera med IT-system i zon 2 ska vara placerade i dedikerad subzon, 3.A inom zon 3. Övriga IT-system i zon 3 (som inte har kommunikation med IT-system i zon 2) ska placeras utanför denna subzon. Med andra ord får det inte finnas någon elektronisk dataöverföring mellan IT-system utanför zon 3.A och IT-system i zon 2.

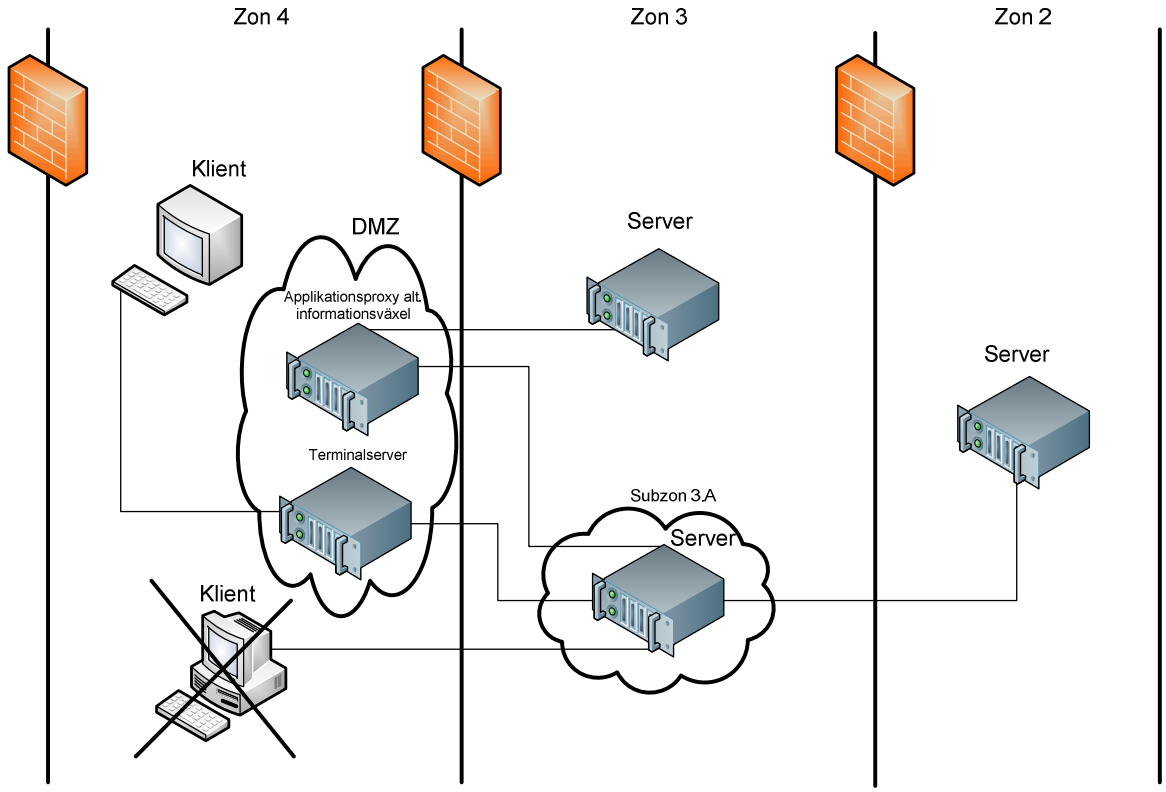
Den logiska skyddsbarriären, som skiljer zonerna åt, ska vara baserad på brandväggsteknik. Mellan zon 2 och zon 3 samt mellan zon 1 och zon 2 ska anpassade brandväggslösningar tillämpas för att tillmötesgå de krav som reglerar respektive zonövergång. Dessa brandväggar kan vara av typen datadiod, datapump eller datasluss.

Subzon 3.A

Utbyte av data mellan IT-system som är placerade i zon 3.A och IT-system placerade i övriga delar av zon 3 (3.X) och zon 4, ska förutom trafikreglering genom brandvägg även styras med hjälp av extra säkerhetstekniska lösningar. Ingen direktkommunikation är tillåten mellan zon 3.A och zon 3 eller zon 4. IT-system i zon 4 som är direkt anslutna till IT-system i zon 3.A via enbart brandvägg är därför inte tillåtet. Vid systemintegrering (server till server) ska datautbyte styras via dedikerad lösning, t ex applikationsproxy[4] eller informationsväxel i server, placerad på DMZ[5] för infrastruktur. Klienter som är placerade i zon 3 (zon 3.X) och zon 4 ska inte ha någon direkt åtkomst till IT-system som är placerade i zon 3.A. I detta fall krävs också extra säkerhetstekniska lösningar, t ex terminalserverlösningar placerade i DMZ för infrastruktur. Regler och exempel åskådliggörs i figur 5.

[4] Proxyserver som kan agera på de högre nivåerna i OSI-modellen. Vilket omfattar de tillämpningsorienterade protokollen för den aktuella systemintegrationen. OSI-modellen (ISO/IEC 7498) är en konceptuell sjuskiktad modell för datorkommunikation.

[5] DMZ, DeMilitarized Zone (demilitariserad zon), är ett isolerat datornätverk (”delnärverk”) som placeras utanför det skyddade ”ordinarie” datornätverket.



Figur 5. *Regler för integration genom subzon 3.A.*