SWEDAC DOC 10:5

SWEDAC

2019-01-21
Utgåva 3

Vägledning för informationssäkerhetsarbete

Innehåll

1. Syfte

Syftet med detta dokument är att ge ackrediterade verksamheter och verksamheter som söker ackreditering vägledning vid förbättring av informationssäkerhet. Dokumentet ger också vägledning till de krav som ställs vid bedömning av informationssäkerhet.

Checklistan i slutet av dokumentet kan med fördel användas vid interna och externa revisioner.

2. Tillämpningsområde

Dokumentet gäller för alla typer av datasystem och datastöd som används i den ackrediterade verksamheten, såväl direkta produktionssystem som stödsystem för ledningssystemet. Exempel på sådana system med olika benämningar inom parentes;

- LIS (LIMS, labdatasystem, produktionssystem)
- Labmodul (POCT, PNA)
- Bokning (RIS mm)
- Beställning och svar
- Bildbehandling (PACS)
- Fysiologiska analyssystem
- Dokumenthantering
- Ärende, avvikelse-, klagomålshantering
- Internrevisionshantering
- Behörighetshantering (körkorts-)
- Makron i kalkylark och ordbehandlare
- Programmerbara bordskalkylatorer
- Processtyrning (styrsystem, banor)
- Instrumentsystem (inbyggda datorer, arbetsstationer till instrument)
- Externa stödsystem och webtjänster (provtagningsanvisningar, folkbokföring, QC)

3. Identifikation och funktionalitet av ingående system

Kravreferens: ISO/IEC 17025; 8.1.1, 8.3
ISO/IEC 17020; 8.2.1, 8.2.2, 8.2.5, 8.3.1 ISO/IEC 17021; 10.3.1, 10.3.3
ISO/IEC 17065; 8.2.1, 8.2.2, 8.2.5, 8.3.1
ISO/IEC 17024; 4.4
ISO 15189; 4.2, 4.3, 5.10

Verksamheten bör som en utgångspunkt för arbetet med informationssäkerhet kartlägga vilka system som används, respektive systems funktionalitet och vilka funktionella samband som finns mellan systemen.

En avstämning bör därefter göras mot ackrediteringsstandarden för att se om det finns krav i denna som berör systemets funktionalitet som exempelvis svarsrapportering, dokumenthantering, mätning av kvalitetsindikatorer, godkännande av dokument, spårbarhet till vilka ändringar som har gjorts i resultat. Utgångspunkten är att kraven på datafunktioner är i nivå med de som gäller för manuella pappersbaserade rutiner.

Data i systemet bör utvärderas för att fastlägga vad som är giltigt original respektive kopior (elektroniskt och papper) och vilka hanteringsrutiner som gäller för de senare.

All berörd personal måste ha nödvändig tillgång till instruktioner och information för arbetets genomförande. Verksamhetens krav på systemets tillgänglighet samt reservrutiner måste därför vara dokumenterade.

4. Koppling mellan system

Kravreferens: ISO/IEC 17025; 7.11.6, 7.11.2
ISO/IEC 17020; 6.2.13
ISO/IEC 17021; 10.3.3
ISO/IEC 17065; 4.5
ISO/IEC 17024; 4.4.1, 4.4.3
ISO 15189; 5.10.3

Alla parterna i informationsutbytet bör vara införstådda med och ha dokumenterat de eventuella risker som är förknippade med utbytet.

Den ackrediterade verksamheten har ett huvudansvar för validering av hela utbytet initialt och vid förändringar som sker i överföringskedjan.

Mottagaren av informationen har ett ansvar för att utföra rimlighetskontroller så att grova felaktigheter stoppas.

5. Organisation

Kravreferens: ISO/IEC 17025; 6.2, 6.6.2, 7.10.1
ISO/IEC 17020 ; 5.2.7, 6.1.1, 6.1.4, 6.1.5, 6.1.10, 6.2.14, 7.1.8
ISO/IEC 17021; 6.1, 7.1, 7.2, 7.5, 9.1.3, 9.2.2
ISO/IEC 17065; 5.1, 6.1, 6.2, 7.3, 7.4.2
ISO/IEC 17024; 4.2.4
ISO 15189; 4.1.1.4, 4.6, 4.9, 5.1, 5.10

På en verksamhets datasystem ställs motsvarande krav som på annan ackrediterad verksamhet med avseende på personalens kompetens, behörigheter, ansvar och befogenheter.

Kraven gäller även för tjänster och produkter som den ackrediterade verksamheten erhåller eller köper från såväl extern som intern leverantör. Verksamheten ansvarar alltid för att säkerställa kvaliteten på inköpta tjänster/produkter genom avtal och kontroller.

För system som kommunicerar med andra system, såväl inom den egna verksamheten som med externa, bör samarbetet mellan de olika parter som svarar för utveckling och driftstöd ske med en tydligt dokumenterad ansvarsfördelning. Ansvarsfördelningen bör även täcka uppdatering av systembeskrivning och gemensamma rutiner.

Alla användare av ett system bör ha fått tillräcklig utbildning i systemets hantering samt rutiner och regler för såväl normala som onormala driftsituationer.

Utbildningen bör vara dokumenterad och knuten till utfärdade behörighetsbevis i ledningssystemet

Resurserna för driftstöd bör ha fullgod teknisk kompetens, följa kvalitetssäkringsrutiner och vara organisatoriskt placerade på en nivå som motsvarar systemets användning.

En dokumentation bör finnas av beslutsordning vid hantering av fel eller när en ny systemversion skall tas i drift. Behörighet att ta i drift eller fatta beslut om systemets fortsatta drift trots konstaterat fel, eventuellt med kontrollåtgärder, bör vara kopplat till såväl verksamhets som datateknisk kompetens. Vid tidpunkter när ordinarie datapersonal inte är tillgänglig bör beslutsfattande personal har tillräcklig kompetens för att bedöma konsekvenserna av observerade datafel och vidta nödvändiga åtgärder.

6. Dokumentation, systembeskrivning

Kravreferens: ISO/IEC 17025; 8.3.1
ISO/IEC 17020; 8.2.4
ISO/IEC 17021; 10.3.3
ISO/IEC 17065; 8.2.4
ISO/IEC 17024; 4.2, 4.6
ISO 15189; 4.3, 5.10.3

Systembeskrivning omfattar den dokumentation över funktionalitet, systemplattformar och tekniska lösningar som är nödvändig för systemets skötsel och vidareutveckling. Relevant dokumentation inklusive handbok från leverantören för hantering och skötsel av datasystemet bör vara tillgänglig för berörd personal.

Systembeskrivningen kan utgöras av externa dokument från leverantör kompletterat med beskrivning över lokala anpassningar och kommunikation med andra system. Alla dokument måste vara dokumentstyrda och det måste finnas spårbarhet till vilken version av systemet som beskrivningen avser.

Är systemet unikt och ägs av den ackrediterade verksamheten måste man ha försäkrat sig om att i alla situationer framledes ha tillgång till en komplett kopia av dokumentationen för att garantera systemets fortlevnad.

7. Underhållsrutiner

Kravreferens: ISO/IEC 17025; 7.11, 6.4
ISO/IEC 17020; 6.2.5, 6.2.13
ISO/IEC 17021; 10.3.3
ISO/IEC 17065; 8.3
ISO/IEC 17024; 4.4
ISO 15189; 5.3.1, 5.10.3

Verksamheten bör ha dokumenterade rutiner för

- förebyggande underhåll och övervakning av systemets funktionalitet.
- situationer när systemet inte fungerar som avsett. Reservrutinerna skall omfatta såväl anvisningar för ordinarie arbete som felsökning, felrapportering och åtgärdande. Förändringar, fel och åtgärder bör noteras på papper eller elektroniskt

8. Förändringsrutiner

Kravreferens: ISO/IEC 17025; 7.11
ISO/IEC 17020; 6.2.13
ISO/IEC 17021; 10.3.3
ISO/IEC 17065; 8.3
ISO/IEC 17024; 4.4
ISO 15189; 5.10.3

Systemet skall vara validerat med avseende på korrekt funktion, tillgänglighet, spårbarhet samt insyn och åtkomst för obehöriga. Validering bör ske vid alla systemförändringar i systemplattform eller applikationsprogramvara.

Syftet med validering är att kvalitetssäkra ett system eller utbyte av information mellan system.

Detta kan ske på olika sätt eller i kombination:
- Provning (testning) i särskild testmiljö eller i driftmiljö
- Parallell körning av nytt system/ny version mot ett befintligt system/version
- Kontroll av resultat mot beställningar, manuella arbetslistor, rådata, manuella beräkningar eller alternativt svarssätt som inte omfattas av förändringen.
- Jämförelse av data i respektive system vid elektronisk överföring mellan system
- Regelbundna stickprov i system som är i drift för att säkerställa att inte förändringar skett t ex. i konfigurationsparametrar, leverantörspatchar eller i extern kommunikationskedja.

Validering bör ske enligt en dokumenterad rutin som omfattar hela dataflödet. Rutinen bör beskriva valideringsmetod vid olika förändringar och säkerställa att styrkande dokumentation skapas. Den styrkande dokumentationen bör innehålla en sammanfattande rapport som anger orsak till valideringen, vem som utfört valideringen och tidpunkt, systemversion, resultat och beslut. Resultaten bör styrkas med underlag.

Förlitar den ackrediterade verksamheten sig på extern validering av systemförändringar bör rapporterna från den externa valideringen vara så detaljerade att dessa kan ligga till grund för korrekta beslut.

Vid införande av nytt datasystem eller vid större förändringar skall verksamheten ta kontakt med SWEDAC för planering av bedömningsinsats.

9. Arkivering

Kravreferens: ISO/IEC 17025; 8.4
ISO/IEC 17020; 7.3, 7.4, 8.4.1,
ISO/IEC 17021; 10.3.4
ISO/IEC 17065; 8.4.1
ISO/IEC 17024; 4.6.2
ISO 15189; 4.13

Ledningssystemets arkiveringskrav på data i systemet måste vara definierade och uppfyllas. För data som arkiveras i särskilt system, exempelvis i ett tidigare driftsystem, måste en plan finnas över hur verksamheten avser att säkerställa datasystemets fortlevnad under arkiveringstiden.

10. Riskhantering

Kravreferens: ISO/IEC 17025; 7.11, 8.5
ISO/IEC 17020; 6.2.13, 8.8.1
ISO/IEC 17021; 10.3.3
ISO/IEC 17065; 8.8.1
ISO/IEC 17024; 4.6.1
ISO 15189; 4.14.6, 5.0.3

Systemet måste uppfylla basala krav på säkerhet och sekretess när det gäller behörighets- och kontrollsystem (s.k. BKS), skydd mot datavirus och backup.

Om systemet använder sig av underliggande åtkomstskydd i operativsystem, databas eller ordbehandlare för att skydda integriteten av data får detta inte kunna kringgås. Leverantörens ev. krav på operativsystem och inställningar måste följas.

Grunden för modernt informationssäkerhetsarbete är att genomföra en dokumenterad processanalys av verksamhetens informationsflöde. Som en del i processanalysen ingår utförandet av riskanalys

med en bedömning av risker när det gäller informationens riktighet, tillgänglighet, insyn samt spårbarhet. De funna riskerna värderas mot ledningssystemets policy med ställda krav på organisationens informationssäkerhet.

Processanalys av informationssäkerhet kan med fördel göras med totalsyn i samband med processanalyser av ordinarie verksamhet.

11. Anskaffande av nytt system samt utveckling av eget system

Kravreferens: ISO/IEC 17025; 7.11
ISO/IEC 17020; 6.2.13, 7.1.8
ISO/IEC 17021;10.3.3
ISO/IEC 17065; 8.3
ISO/IEC 17024; 4.4.3
ISO 15189; 5.10.3

Utveckling av programvara bör följa riktlinjer i internationella standarder. Är leverantören certifierad enligt en internationell standard kan detta vara en fördel, annars bör verksamheten ta del av leverantörens rutiner, t ex validering av programvara, begäran om ändringar samt åtgärdande av funna fel.

Vid egen utveckling av system bör man kvalitetssäkra arbetet genom dokumenterade rutiner och anvisningar. Risker bör vara identifierade när det gäller teknisk och kompetensmässig sårbarhet. Källkodsrättigheter samt ansvar för specifikationer, testning och drifttagning bör vara klarlagda.

Checklista för intern och extern revision av dataverksamhet

Verksamhet:
Datum:
Ansvariga IT:
Deltagare:’

Punkter som inte är relevanta för aktuellt system markeras vid revisionen som ej tillämplig.

1. Identifikation och funktionalitet av ingående system	Anteckning
Namn på system: Version: Leverantör: Systemplattform: Dator: O/S: dbms: Utvecklingsverktyg: Funktionalitet: Koppling till andra system:	
Namn på system: Version: Leverantör: Systemplattform: Dator: O/S: dbms: Utvecklingsverktyg: Funktionalitet: Koppling till andra system:	
Namn på system: Version: Leverantör: Systemplattform: Dator: O/S: dbms: Utvecklingsverktyg: Funktionalitet: Koppling till andra system:	
Namn på system: Version: Leverantör: Systemplattform: Dator: O/S: dbms: Utvecklingsverktyg: Funktionalitet: Koppling till andra system:	

2. Organisation	Anteckning
❑ Är driftstödsorganisationen beskriven i ledningssystemet (t.ex. i form av olika roller som systemägare, systemförvaltare, systemansvarig)? ❑ Framgår placering i organisationsschema? ❑ Finns ställföreträdare för alla funktioner?	
❑ Framgår externa leverantörers ansvar i ledningssystemet eller avtal? ❑ Framgår att verksamheten vid överföring mellan system	
❑ Har systemets driftstödsorganisation erhållit tillräcklig och dokumenterad utbildning?	
❑ Används behörighetssystem (körkort) även för hantering av datasystemet? ❑ Finns dokumentation av genomförd utbildning och information om datasystemet?	
❑ Görs interna kvalitetsrevisioner av dataverksamheten regelbundet??	
❑ Täcker inköpsrutinerna i ledningssystemet även datautrustning och datatjänster?	

3. Avtal	Anteckning
❑ **Finns avtal med alla parter utanför verksamheten (leverantörer, kunder, koncern IT-avdelning) som täcker** ❑ support för kritisk maskinvara och programvara ❑ kopplingar och överföringar till externa system (web, EDI, mail) ❑ Är alla parter tydligt beskrivna – även underleverantörer och tredjepartsleverantörer? ❑ Framgår krav på att ha avtal gentemot ev. tredjepart t.ex. service för utrustning som ej ägs av verksamheten, underleverantörer vid programutveckling, driftstöd vid EDI? ❑ Är ansvarsområden/gränser och åtaganden för de olika parterna vid normal förvaltning beskrivna (vem som gör vad, när och hur)? ❑ Anges överenskommen funktionalitet? ❑ Anges överenskommen tillgänglighet för åtkomst till/mottagande av information? ❑ Är ägandeskap och ansvar för informationen angiven? ❑ Är kontaktpersoner angivna? ❑ Är namn och befogenheter för personer som utför arbete inom verksamhetens lokaler eller har åtkomst till verksamhetens datasystem angivna? ❑ Är ansvariga för uppdatering av avtal respektive systembeskrivning och gemensamma dokument angivna? ❑ Ges kompetensgaranti? ❑ Finns utfästelse att följa dokumenterade regler för säkerhet och sekretess samt att att tillträde/åtkomst till systemen ej är ej är möjlig för andra än kompetent personal? ❑ Finns utfästelse att notera viktiga systemhändelser och felåtgärder i loggbok eller system för ärendehantering? ❑ Finns beskrivning av reservrutiner för olika typer av fel? ❑ Anges inställelsetider för driftstöd (även i samband med nyutveckling)? ❑ Är tillgänglighet för felanmälan och kontaktvägar angivna?	
❑ **Tillämpbart när information utbyts med andra system, tex. elektroniska svar, webåtkomst till rapporter.** ❑ Är överenskommet protokoll och plattformar vid överföring mellan system beskrivna? ❑ Finns en beskrivning av respektive parts bevakning av informationsutbyte? ❑ Finns utfästelse att informera om händelser och förändringar som kan påverka informationsutbyte? ❑ Är rimlighetskontroller som mottagaren åtar sig att göra så att grova felaktigheter stoppas, ex.vis att data inte sänds dubbelt, överförs ofullständigt eller fel, beskrivna? ❑ Finns utfästelse att utan dröjsmål underrätta berörda parter vid misstanke om fel i informationsutbytet? ❑ Är det angivet vem som ansvarar för felsökning i olika delar av kedjan vid överföringsfel mellan system? ❑ Finns en utfästelse att verifiera att information utbyts korrekt efter förändringar i koder, funktioner, plattformar och att verksamheten vid överföring mellan system har ett huvudansvar för validering av hela kedjan?	

4. Dokumentation, systembeskrivning	Anteckning
❑ Finns en systembeskrivning? ❑ Vilka interna och externa dokument ingår? ❑ Är alla dokumentstyrda och spårbara till aktuell systemversion? Finns förteckning? ❑ Är dokumentationen tillräcklig för driftstöd och utveckling. ❑ Om systemet är unikt – har verksamheten tillgång till en kopia av detaljdokumentationen i händelse av katastrof?	
❑ **Framgår det av systemdokumentationen** ❑ Vilka funktioner som datasystemet har. Om man har ett standardsystem skall det vara dokumenterat vilka funktioner som man eventuellt inte använder. ❑ en beskrivning – gärna grafisk - över ❑ maskinvara ❑ systemprogramvara ❑ nätverk ❑ kopplingar till externa system ❑ informationsflöde ❑ databasstruktur ❑ inloggningsskydd/åtkomst ❑ virusskydd ❑ insyn (tex brandväggar, säkert nät, kryptering, alt. ej känslig information) ❑ kommunikation med externa system ❑ överföringsformat och mappningar ❑ hur informationen skyddas mot förändringar t.ex. genom checksummeberäkning, kryptering eller att spårbarhet finns genom matchning av loggar med innehåll före och efter bearbetningar ❑ loggar över att information har överförts och vad som har överförts vid avsändning, mottagning och vidaresändning. ❑ hur avsändaren kan visa skickade meddelanden, återskapade eller sparade. ❑ bevakningsfunktioner för loggar. Arkiveringstider. ❑ kvittensfunktioner och -meddelanden över informationsutbyte ❑ Finns användarhandbok (eller inbyggt hjälpsystem) ❑ Är användarhandboken dokumentstyrd? ❑ Finns pårbarhet för vilken systemversion som instruktionen gäller för?	

5. Underhållsrutiner	Anteckning
❑ Finns en systembeskrivning? ❑ Vilka interna och externa dokument ingår? ❑ Är alla dokumentstyrda och spårbara till aktuell systemversion? Finns förteckning? ❑ Är dokumentationen tillräcklig för driftstöd och utveckling. ❑ Om systemet är unikt – har verksamheten tillgång till en kopia av detaljdokumentationen i händelse av katastrof?	
❑ **Framgår det av systemdokumentationen** ❑ Vilka funktioner som datasystemet har. Om man har ett standardsystem skall det vara dokumenterat vilka funktioner som man eventuellt inte använder. ❑ en beskrivning – gärna grafisk - över ❑ maskinvara ❑ systemprogramvara ❑ nätverk ❑ kopplingar till externa system ❑ informationsflöde ❑ databasstruktur ❑ inloggningsskydd/åtkomst ❑ virusskydd ❑ insyn (tex brandväggar, säkert nät, kryptering, alt. ej känslig information) ❑ kommunikation med externa system ❑ överföringsformat och mappningar ❑ hur informationen skyddas mot förändringar t.ex. genom checksummeberäkning, kryptering eller att spårbarhet finns genom matchning av loggar med innehåll före och efter bearbetningar ❑ loggar över att information har överförts och vad som har överförts vid avsändning, mottagning och vidaresändning. ❑ hur avsändaren kan visa skickade meddelanden, återskapade eller sparade. ❑ bevakningsfunktioner för loggar. Arkiveringstider. ❑ kvittensfunktioner och -meddelanden över informationsutbyte ❑ Finns användarhandbok (eller inbyggt hjälpsystem) ❑ Är användarhandboken dokumentstyrd? ❑ Finns pårbarhet för vilken systemversion som instruktionen gäller för?	

6. Underhållsrutiner	Anteckning
❑ Är systemet versionshanterat? (Inkluderar versionshanteringen även perifera delar av systemet som t.ex. svarsrapporter, filkonverteringar, instrumentinterface.) ❑ Är uppbyggnaden av versionshanteringen dokumenterad? ❑ Framgår versionsbeteckningen i tekniska dokument, testrapporter, handledningar, felrapporter.	
❑ Sker slutvalidering gentemot låsta (frysta) versioner av systemet?.	
❑ Finns en dokumenterad rutin för rapportkontroll mot grundunderlag? Används denna ❑ för alla svar rutinmässigt ❑ i samband med driftstart ❑ vid konstaterat allvarligt fel.	
❑ Finns en särskild testmiljö? ❑ är den dokumenterad? ❑ finns risk för att testmiljön används av misstag eller att testsvar går ut till kund?	
❑ Har verksamheten tillgång till detaljrapporter från leverantörens provning?	
❑ Finns en skriftlig valideringsrutin där det framgår när validering/verifiering skall ske t.ex. vid ❑ ny systemversion ❑ mindre förändringar/rättningar i programkod ❑ uppgradering maskinvara eller systemprogramvara (server och klienter, webläsare) ❑ nytt instrument ❑ ny version av programvara i instrument ❑ förändringar i anslutna externa system eller del av kommunikationskedja ❑ ny eller ändrad analys/undersökning inkl. kodverksändringar ❑ ändrade beräkningsfunktioner ❑ ny kund eller ändrade kunduppgifter som adress/rapportsätt ❑ ny fax hos kund ❑ nytt eller ändrat format elektronisk beställning eller elektronisk rapport (meddelande eller web) ❑ ny svars/faxrapport ❑ vem ansvarar för att provning görs i tillräcklig omfattning, vem som är behörig att utföra provning, vem som godkänner genomförd provning och vem som fattar beslut att ta i drift ❑ instruktioner hur provningen skall genomföras. Detaljnivå tillräcklig för att täcka all normalvariation och extremfall och ge enhetlig provning även om flera personer provar. Förväntat resultat så att provningen går att upprepa.	

7. Arkivering	Anteckning
❑ Använder man enbart datorsystemet som arkiv för vissa uppgifter? Vilka arkiveringstider är då uppgivna i ledningssystemet. Är det beskrivet hur man avser att säkerställa arkivet m.a.p plattform och kompetens?	

8. Riskhantering	Anteckning
❑ Finns skriftlig backuprutin som täcker: ❑ beskrivning av rotationsschema ❑ mediamärkning ❑ ansvarig (och ställföreträdare) ❑ handhavande ❑ förvaring av daglig backup och systembackup för unik programvara i annan brandzon, brandsäkert skåp ❑ att genomförd backup och eventuella fel noteras i loggbok ❑ Görs kontroll av gjord backup genom tex. återläsning? ❑ Finns en dokumenterad rutin för återskapande? ❑ Är ansvar och befogenheter för backupsystemets funktion och skötsel dokumenterade i ledningssystemet	
❑ Ger behörighetssystemet tillräckligt skydd? ❑ Är behörighetssystemet dokumenterat? ❑ Hur ofta byts lösenord? ❑ Hur många tecken är minimum? ❑ Kan lösenord återanvändas?	
❑ Har besökare tillgång till utrustning? Är det möjligt för ej behöriga att läsa på bildskärmar?	
❑ Görs regelbunden eller kontinuerlig anti-viruskontroll av PC. ❑ Är anti-virusskyddet dokumenterat?	
❑ Hur säkerställs korrekt överföring mellan system? Används checksummor och unika sekvensnummer vid meddelandeöverföring? Förekommer kvittenshantering?	
❑ Kontrollera lokaler med avseende på. ❑ värme och fuktighet ❑ brand-, översvämningsskydd ❑ damm ❑ elförsörjning ❑ störkällor ❑ lås-åtkomstskydd?	
❑ Kontroll av manuell resultatinmatning och ändring av resultat. Stämmer med utfärdade behörigheter?	
❑ Kontroll av spårbarhet för ett prov. Signeringar, tidpunkter, ändringar, koppling till kontrollprov?	
❑ Kontroll av tidsangivelser. Samma tid på server och alla klienter?	

8. Riskhantering, forts	Anteckning
❑ Finns en dokumenterad riskanalys ❑ Täcker den alla användningsfall som ex.vis ❑ Kommunikation terminal<->server, klient<->server, server<->server ❑ Kommunikation med externa system ex.vis EDI- webrapporter, webbeställning, befolkningsregister,?? ekonomisystem ❑ Är informationstillgångar klassificerade ❑ Finns övergripande policy och riktlinjer för informationssäkerhet ❑ Är riskbedömning gjord för brister i informationens ❑ riktighet ❑ tillgänglighet ❑ insyn ❑ spårbarhet ❑ Finns beslutad handlingsplan som inkluderar planerade åtgärder, aktiviteter, tider, ansvar	
❑ Finns en handlingsplan för återskapande av systemet efter katastrof	
❑ Finns reservutrustning eller en handlingsplan för ej kritisk utrustning?	

SWEDAC

Besöksadress: Österlånggatan 9, 503 31 Borås
Postadress: Box 878, 501 15 Borås

0771-99 09 00 registrator@swedac.se www.swedac.se