

# Vägledning för informationssäkerhetsarbete

## Innehållsförteckning

Kap 1	Syfte	Sid 3
Kap 2	Tillämpningsområde	Sid 3
Kap 3	Identifikation och funktionalitet av ingående system	Sid 3
Kap 4	Koppling mellan system	Sid 4
Kap 5	Organisation	Sid 4
Kap 6	Dokumentation, systembeskrivning	Sid 5
Kap 7	Underhållsrutiner	Sid 5
Kap 8	Förändringsrutiner	Sid 5
Kap 9	Arkivering	Sid 6
Kap 10	Riskhantering	Sid 6
Kap 11	Anskaffande av nytt system samt utveckling av eget system	Sid 7
Annex	Checklista för extern och intern revision av dataverksamhet	Sid 8

## Vägledning för informations säkerhetsarbete

### 1 Syfte

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

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 analysystem
- 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 webbtjänster (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 informations säkerhet kartlägga vilka system som används, respektive systems funktionalitet och vilka funktionella samband som finns mellan systemen.

En avstämning bör därefter göras mot ackrediteringsstandarderna 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 ha 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. Källkods rättigheter 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
<input type="checkbox"/> Är driftstödsorganisationen beskriven i ledningssystemet (t.ex. i form av olika roller som systemägare, systemförvaltare, systemansvarig)? <input type="checkbox"/> Framgår placering i organisationsschema? <input type="checkbox"/> Finns ställföreträdare för alla funktioner?	
<input type="checkbox"/> Framgår externa leverantörers ansvar i ledningssystemet eller avtal? <input type="checkbox"/> Framgår att verksamheten vid överföring mellan system har ett huvudansvar för validering av hela överföringskedjan?	
<input type="checkbox"/> Har systemets driftstödsorganisation erhållit tillräcklig och dokumenterad utbildning?	
<input type="checkbox"/> Används behörighetssystem (körkort) även för hantering av datasystemet? <input type="checkbox"/> Finns dokumentation av genomförd utbildning och information om datasystemet?	
<input type="checkbox"/> Görs interna kvalitetsrevisioner av dataverksamheten regelbundet?	
<input type="checkbox"/> Täcker inköpsrutinerna i ledningssystemet även datautrustning och datatjänster?	

3 Avtal	Anteckning
<p><input type="checkbox"/> <b>Finns avtal med alla parter utanför verksamheten (leverantörer, kunder, koncern IT-avdelning) som täcker</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> support för kritisk maskinvara och programvara</li> <li><input type="checkbox"/> kopplingar och överföringar till externa system (web, EDI, mail)</li> <li><input type="checkbox"/> Är alla parter tydligt beskrivna – även underleverantörer och tredjepartsleverantörer?</li> <li><input type="checkbox"/> 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?</li> <li><input type="checkbox"/> Är ansvarsområden/gränser och åtaganden för de olika parterna vid normal förvaltning beskrivna (vem som gör vad, när och hur)?</li> <li><input type="checkbox"/> Anges överenskommen funktionalitet?</li> <li><input type="checkbox"/> Anges överenskommen tillgänglighet för åtkomst till/mottagande av information?</li> <li><input type="checkbox"/> Är ägandeskap och ansvar för informationen angiven?</li> <li><input type="checkbox"/> Är kontaktpersoner angivna?</li> <li><input type="checkbox"/> Är namn och befogenheter för personer som utför arbete inom verksamhetens lokaler eller har åtkomst till verksamhetens datasystem angivna?</li> <li><input type="checkbox"/> Är ansvariga för uppdatering av avtal respektive systembeskrivning och gemensamma dokument angivna?</li> <li><input type="checkbox"/> Ges kompetensgaranti?</li> <li><input type="checkbox"/> Finns utfästelse att följa dokumenterade regler för säkerhet och sekretess samt att tillträde/åtkomst till systemen ej är ej är möjlig för andra än kompetent personal?</li> <li><input type="checkbox"/> Finns utfästelse att notera viktiga systemhändelser och felåtgärder i loggbok eller system för ärendehantering?</li> <li><input type="checkbox"/> Finns beskrivning av reservrutiner för olika typer av fel?</li> <li><input type="checkbox"/> Anges inställelsetider för driftstöd (även i samband med nyutveckling)?</li> <li><input type="checkbox"/> Är tillgänglighet för felanmälan och kontaktvägar angivna?</li> </ul>	
<p><input type="checkbox"/> <b>Tillämpbart när information utbyts med andra system, tex. elektroniska svar, webåtkomst till rapporter.</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Är överenskommet protokoll och plattformar vid överföring mellan system beskrivna?</li> <li><input type="checkbox"/> Finns en beskrivning av respektive parts bevakning av informationsutbyte?</li> <li><input type="checkbox"/> Finns utfästelse att informera om händelser och förändringar som kan påverka informationsutbyte?</li> <li><input type="checkbox"/> 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?</li> <li><input type="checkbox"/> Finns utfästelse att utan dröjsmål underrätta berörda parter vid misstanke om fel i informationsutbytet?</li> <li><input type="checkbox"/> Är det angivet vem som ansvarar för felsökning i olika delar av kedjan vid överföringsfel mellan system?</li> </ul>	

<input type="checkbox"/> 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
<input type="checkbox"/> Finns en systembeskrivning? <input type="checkbox"/> Vilka interna och externa dokument ingår? <input type="checkbox"/> Är alla dokumentstyrda och spårbara till aktuell systemversion? Finns förteckning? <input type="checkbox"/> Är dokumentationen tillräcklig för driftstöd och utveckling. <input type="checkbox"/> Om systemet är unikt – har verksamheten tillgång till en kopia av detaljdokumentationen i händelse av katastrof?	
<p><b>Framgår det av systemdokumentationen</b></p> <input type="checkbox"/> Vilka funktioner som datasystemet har. Om man har ett standardsystem skall det vara dokumenterat vilka funktioner som man eventuellt inte använder. <input type="checkbox"/> en beskrivning – gärna grafisk - över <ul style="list-style-type: none"> <li><input type="checkbox"/> maskinvara</li> <li><input type="checkbox"/> systemprogramvara</li> <li><input type="checkbox"/> nätverk</li> <li><input type="checkbox"/> kopplingar till externa system</li> <li><input type="checkbox"/> informationsflöde</li> <li><input type="checkbox"/> databasstruktur</li> </ul> <input type="checkbox"/> inloggningskydd/åtkomst <ul style="list-style-type: none"> <li><input type="checkbox"/> viruskydd</li> <li><input type="checkbox"/> insyn (tex brandväggar, säkert nät, kryptering, alt. ej känslig information)</li> </ul> <input type="checkbox"/> kommunikation med externa system <input type="checkbox"/> överföringsformat och mappningar <ul style="list-style-type: none"> <li><input type="checkbox"/> hur informationen skyddas mot förändringar t.ex. genom checksummeberäkning, kryptering eller att spårbarhet finns genom matchning av loggar med innehåll före och efter bearbetningar</li> <li><input type="checkbox"/> loggar över att information har överförts och vad som har överförts vid avsändning, mottagning och vidareändning.</li> <li><input type="checkbox"/> hur avsändaren kan visa skickade meddelanden, återskapade eller sparade.</li> <li><input type="checkbox"/> bevakningsfunktioner för loggar. Arkiveringstider.</li> <li><input type="checkbox"/> kvittensfunktioner och -meddelanden över informationsutbyte</li> </ul> <input type="checkbox"/> Finns användarhandbok (eller inbyggt hjälpsystem) <input type="checkbox"/> Är användarhandboken dokumentstyrd? <input type="checkbox"/> Finns spårbarhet för vilken systemversion som instruktionen gäller för?	

5 Underhållsrutiner	Anteckning
<input type="checkbox"/> Finns dokumenterad rutin för förebyggande kontroll, underhåll och övervakning av <ul style="list-style-type: none"> <li><input type="checkbox"/> maskinvara</li> <li><input type="checkbox"/> diskkapacitet</li> <li><input type="checkbox"/> backup</li> <li><input type="checkbox"/> korrekt överföring mellan system</li> <li><input type="checkbox"/> rapportrutiner (fax, papper)</li> </ul>	
<input type="checkbox"/> Är all datautrustning individmärkt och upptagen i förteckning (dokument eller underhållsdatasystem)?	
<input type="checkbox"/> Finns loggböcker (eller dokument/underhålls-, ärendehanteringssystem) för datautrustning som <ul style="list-style-type: none"> <li><input type="checkbox"/> server</li> <li><input type="checkbox"/> PC</li> <li><input type="checkbox"/> Skrivare</li> <li><input type="checkbox"/> nätverksutrustning</li> <li><input type="checkbox"/> programvara datasystem</li> <li><input type="checkbox"/> elektronisk överföring av data</li> </ul> <input type="checkbox"/> Är loggbokssystemet beskrivet i ledningssystemet? <input type="checkbox"/> Används loggböckerna? <input type="checkbox"/> Går det att identifiera utrustningen? <input type="checkbox"/> Är noteringarna daterade och signerade? <input type="checkbox"/> Framgår åtgärder?	
<input type="checkbox"/> Kan man se i systemet eller av dokumentation vilken version som körs.	
<input type="checkbox"/> Finns underhållsrutiner för kodverk som används vid informationsöverföring. <input type="checkbox"/> Är ansvar och befogenheter för underhåll av kodverk dokumenterat i ledningssystemet?	
<input type="checkbox"/> Finns en skriftlig rutin för all berörd personal (samt eventuella externa leverantörer) att tillämpa vid olika typer av fel i systemet. Rutinen skall inkludera <ul style="list-style-type: none"> <li><input type="checkbox"/> verksamhetens hantering vid totalt driftstopp. (Reservrutiner, återskapande av system)</li> <li><input type="checkbox"/> verksamhetens hantering vid olika felsituationer tex. avbrott i nätverk, fel på PC, fel på skrivare, programfel, överföringsfel till annat system, fel i faxöverföring.</li> <li><input type="checkbox"/> hur felrapportering, korrigerande skall gå till från personal via IT-ansvariga ev. till leverantör</li> <li><input type="checkbox"/> hur dokumentation skall ske av fel och åtgärder.</li> <li><input type="checkbox"/> vem som ansvar för uppföljning av fel som rapporterats vidare till leverantör.</li> <li><input type="checkbox"/> vem som ansvarar för felsökning i olika delar av kedjan vid överföringsfel till annat system</li> <li><input type="checkbox"/> i händelse av allvarliga programfel som t.ex. förväxling av resultat - åtgärder för att säkra kvalitet - t.ex. extra kontroller av rapportutskriften</li> </ul>	
<input type="checkbox"/> Är rutinen tillgänglig, känd och aktuell?	
<input type="checkbox"/> Är befogenheter att införa åtgärder vid konstaterat fel dokumenterade i ledningssystemet (tex. ta system i/ur drift, rätta fel/beställa rättning, införa kvalitetskontroll av svar)	

6 Förändringsrutiner	Anteckning
<input type="checkbox"/> Är systemet versionshanterat? (Inkluderar versionshanteringen även perifera delar av systemet som t.ex. svarsrapporter, filkonverteringar, instrumentinterface.) <input type="checkbox"/> Är uppbyggnaden av versionshanteringen dokumenterad? <input type="checkbox"/> Framgår versionsbeteckningen i tekniska dokument, testrapporter, handledningar, felrapporter.	
<input type="checkbox"/> Sker slutvalidering gentemot låsta (frysta) versioner av systemet?	
<input type="checkbox"/> Finns en dokumenterad rutin för rapportkontroll mot grundunderlag? Används denna <ul style="list-style-type: none"> <li><input type="checkbox"/> för alla svar rutinmässigt</li> <li><input type="checkbox"/> i samband med driftstart</li> <li><input type="checkbox"/> vid konstaterat allvarligt fel</li> </ul>	
<input type="checkbox"/> Finns en särskild testmiljö? <ul style="list-style-type: none"> <li><input type="checkbox"/> är den dokumenterad?</li> <li><input type="checkbox"/> finns risk för att testmiljön används av misstag eller att testsvar går ut till kund?</li> </ul>	
<input type="checkbox"/> Har verksamheten tillgång till detaljrapporter från leverantörens provning?	
<input type="checkbox"/> Finns en skriftlig valideringsrutin där det framgår när validering/verifiering skall ske t.ex. vid <ul style="list-style-type: none"> <li><input type="checkbox"/> ny systemversion</li> <li><input type="checkbox"/> mindre förändringar/rättningar i programkod</li> <li><input type="checkbox"/> uppgradering maskinvara eller systemprogramvara (server och klienter, webläsare)</li> <li><input type="checkbox"/> nytt instrument</li> <li><input type="checkbox"/> ny version av programvara i instrument</li> <li><input type="checkbox"/> förändringar i anslutna externa system eller del av kommunikationskedja</li> <li><input type="checkbox"/> ny eller ändrad analys/undersökning inkl. kodverksändringar</li> <li><input type="checkbox"/> ändrade beräkningsfunktioner</li> <li><input type="checkbox"/> ny kund eller ändrade kunduppgifter som adress/rapportsätt</li> <li><input type="checkbox"/> ny fax hos kund</li> <li><input type="checkbox"/> nytt eller ändrat format elektronisk beställning eller elektroniskt rapport (meddelande eller web)</li> <li><input type="checkbox"/> ny svars/faxrapport</li> </ul> <input type="checkbox"/> 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 <input type="checkbox"/> 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.	

<input type="checkbox"/> hur provningen skall dokumenteras. Instruktioner eller färdig mall för dokumentation där det skall framgå <ul style="list-style-type: none"> <li><input type="checkbox"/> vem som provat</li> <li><input type="checkbox"/> när det skett</li> <li><input type="checkbox"/> orsak till provningen</li> <li><input type="checkbox"/> om valideringen skett i test eller driftmiljö</li> <li><input type="checkbox"/> version av testat program/systemversion</li> <li><input type="checkbox"/> referens till eventuella fel.</li> <li><input type="checkbox"/> vilka underlag (utskrifter, skärmdumpar) som skall tas ut ur systemet för att styrka provningen</li> <li><input type="checkbox"/> hur man med olika markeringar i underlagen visar att uppgifter är kontrollerade och korrekta/felaktiga – tex. med streck eller bock vid en kontrollerad uppgift.</li> <li><input type="checkbox"/> Sammanfattande resultat, beslut om drifttagning</li> </ul>	
---	--

7 Arkivering	Anteckning
<input type="checkbox"/> 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
<input type="checkbox"/> Finns skriftlig backuprutin som täcker: <ul style="list-style-type: none"> <li><input type="checkbox"/> beskrivning av rotationsschema</li> <li><input type="checkbox"/> mediamärkning</li> <li><input type="checkbox"/> ansvarig (och ställföreträdare)</li> <li><input type="checkbox"/> handhavande</li> <li><input type="checkbox"/> förvaring av daglig backup och systembackup för unik programvara i annan brandzon, brandsäkert skåp</li> <li><input type="checkbox"/> att genomförd backup och eventuella fel noteras i loggbok</li> </ul> <input type="checkbox"/> Görs kontroll av gjord backup genom tex. återläsning? <input type="checkbox"/> Finns en dokumenterad rutin för återskapande? <input type="checkbox"/> Är ansvar och befogenheter för backupsystemets funktion och skötsel dokumenterade i ledningssystemet	
<input type="checkbox"/> Ger behörighetssystemet tillräckligt skydd? <ul style="list-style-type: none"> <li><input type="checkbox"/> Är behörighetssystemet dokumenterat?</li> <li><input type="checkbox"/> Hur ofta byts lösenord?</li> <li><input type="checkbox"/> Hur många tecken är minimum?</li> <li><input type="checkbox"/> Kan lösenord återanvändas?</li> </ul>	
<input type="checkbox"/> Har besökare tillgång till utrustning? Är det möjligt för ej behöriga att läsa på bildskärmar?	
<input type="checkbox"/> Görs regelbunden eller kontinuerlig anti-viruskontroll av PC. <input type="checkbox"/> Är anti-viruskyddet dokumenterat?	
<input type="checkbox"/> Hur säkerställs korrekt överföring mellan system? Används checksummor och unika sekvensnummer vid meddelandeöverföring? Förekommer kvittenshantering?	

<input type="checkbox"/> Kontrollera lokaler med avseende på. <ul style="list-style-type: none"> <li><input type="checkbox"/> värme och fuktighet</li> <li><input type="checkbox"/> brand-, översvämningsskydd</li> <li><input type="checkbox"/> damm</li> <li><input type="checkbox"/> elförsörjning</li> <li><input type="checkbox"/> störkällor</li> <li><input type="checkbox"/> lås-åtkomstskydd</li> </ul>	
<input type="checkbox"/> Kontroll av manuell resultatinput och ändring av resultat. Stämmer med utfärdade behörigheter?	
<input type="checkbox"/> Kontroll av spårbarhet för ett prov. Signeringar, tidpunkter, ändringar, koppling till kontrollprov??.	
<input type="checkbox"/> Kontroll av tidsangivelser. Samma tid på server och alla klienter?	
<input type="checkbox"/> Finns en dokumenterad riskanalys <input type="checkbox"/> Täcker den alla användningsfall som ex.vis <ul style="list-style-type: none"> <li><input type="checkbox"/> Kommunikation terminal&lt;-&gt;server, klient&lt;-&gt;server, server&lt;-&gt;server</li> <li><input type="checkbox"/> Kommunikation med externa system ex.vis EDI- webrapporter, webbeställning, befolkningsregister,?? ekonomisystem</li> </ul> <input type="checkbox"/> Är informationstillgångar klassificerade <input type="checkbox"/> Finns övergripande policy och riktlinjer för informationssäkerhet <input type="checkbox"/> Är riskbedömning gjord för brister i informationens <ul style="list-style-type: none"> <li><input type="checkbox"/> riktighet</li> <li><input type="checkbox"/> tillgänglighet</li> <li><input type="checkbox"/> insyn</li> <li><input type="checkbox"/> spårbarhet</li> </ul> <input type="checkbox"/> Finns beslutad handlingsplan som inkluderar planerade åtgärder, aktiviteter, tider, ansvar	
<input type="checkbox"/> Finns en handlingsplan för återskapande av systemet efter katastrof	
<input type="checkbox"/> Finns reservutrustning eller en handlingsplan för ej kritisk utrustning?	

9 Anskaffande av nytt system samt egenutveckling	Anteckning
<input type="checkbox"/> Används en internationell standard som grund	
<input type="checkbox"/> Föreligger ett tydligt kund - leverantörförhållande? (Även vid intern utveckling) <input type="checkbox"/> Utgår man från överenskomna specifikationer för att klargöra funktionen för alla inblandade parter? <input type="checkbox"/> Hur sker godkännande av specifikation och levererad funktion? <input type="checkbox"/> Finns en överenskommelse om hur ändringar och tillägg till ursprunglig specifikation skall hanteras? <input type="checkbox"/> Finns överenskommelse om acceptansprov? <input type="checkbox"/> Finns en överenskommelse om acceptansgranskning av dokumentation? <input type="checkbox"/> Är källkods rättigheter klarlagda och framgår i avtal.	
<input type="checkbox"/> Är en analys gjord över risker och sårbarhet - både tekniska och kompetensmässiga?	
<input type="checkbox"/> Sker testning enligt planer? Dokumenterar leverantören sin testning?	
<input type="checkbox"/> Finns bestämda konstruktionsregler för namngivning, kommentering etc?	
<input type="checkbox"/> Finns det risker med valda utvecklingsverktyg? Är dessa identifierade och överenskomna?	
<input type="checkbox"/> Uppdateras handböcker efter förändring?	
<input type="checkbox"/> Sker planering med grundplaner och uppföljning-revidering? Sker avstämning av planer mellan kund-leverantör?	
<input type="checkbox"/> Finns avtal med externa utvecklare som täcker behörigheter, befogenheter, kompetenskrav, källkods rättigheter och serviceåtaganden?	
<input type="checkbox"/> Finns en formaliserad metod eller rutin som täcker de vanligaste typerna av vidareutveckling? <input type="checkbox"/> Omfattar den alla led i utvecklingskedjan? <ul style="list-style-type: none"> <li><input type="checkbox"/> framtagning av specifikationer</li> <li><input type="checkbox"/> design</li> <li><input type="checkbox"/> kodning</li> <li><input type="checkbox"/> testning</li> <li><input type="checkbox"/> validering/verifikation (pkt 6)</li> <li><input type="checkbox"/> dokumentation inklusive handbok,</li> <li><input type="checkbox"/> information</li> <li><input type="checkbox"/> drifttagning</li> <li><input type="checkbox"/> korrigerig av eventuella fel</li> <li><input type="checkbox"/> ändringar och tillägg till ursprunglig specifikation</li> <li><input type="checkbox"/> uppdatering av dokumentation efter programändringar</li> </ul>	