

Vägledning för informations- säkerhetsarbete

This document is available in both Swedish and English. The English translation follows directly after the Swedish text.

Innehåll

1	Vägledning för informationssäkerhetsarbete	3
1.1	Syfte	3
1.2	Tillämpningsområde	3
1.3	Identifikation och funktionalitet av ingående system	3
1.4	Koppling mellan system	4
1.5	Organisation	4
1.6	Dokumentation, systembeskrivning	5
1.7	Underhållsrutiner	6
1.8	Förändringsrutiner	6
1.9	Arkivering	7
1.10	Riskhantering	7
1.11	Anskaffande av nytt system samt utveckling av eget system	8
1.12	Checklista för intern och extern revision av dataverksamhet	9
2	Guide for information security work	19
2.1	Purpose	19
2.2	Scope	19
2.3	Identification and functionality of input systems	19
2.4	Linkage between systems	20
2.5	Organisation	20
2.6	Documentation, system description	21
2.7	Maintenance procedures	22
2.8	Change procedures	22
2.9	Archiving	23
2.10	Risk management	23
2.11	Acquisition of new system and development of own system	24
2.12	Checklist for internal and external audits of data operations	25

1 Vägledning för informationssäkerhetsarbete

1.1 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.

1.2 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 webbtjänster (provtagningsanvisningar, folkbokföring, QC)

1.3 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; 7.6, 7.8, 8.1.1, 8.3

ISO 20387; 7.10.1, 7.10.3

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.

1.4 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; 7.6.3

ISO 20387; 7.4.7, 7.5.1, 7.10.3

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.

1.5 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; 5.2.2, 6.2, 6.8, 7.5, 7.6

ISO 20387; 6.2, 6.4, 7.10.3

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.

1.6 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; 7.6.3, 8.3
 ISO 20387; 4.1.4, 7.10.3, 8.3

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.

1.7 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; 6.4, 7.6
ISO 20387; 6.5, 7.10.3

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

1.8 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; 7.6
ISO 20387; 6.5, 7.9, 7.10.3

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.

1.9 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; 8.4
 ISO 20387; 4.1.8, 7.10.6, 8.4

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.

1.10 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; 5.6, 7.6.3, 8.5
 ISO 20387; 4.2, 4.3, 7.10.3, 8.5

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 kringgåås. 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.

1.11 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; 7.6.3

ISO 20387; 6.4, 6.5, 7.9, 7.10.2-7.10.3

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.

1.12 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:	

1. Identifikation och funktionalitet av ingående system	Anteckning
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 ett huvudansvar för validering av hela överföringskedjan?	
☐ 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, epost) ☐ 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 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.	

5. Underhållsrutiner	Anteckning
☐ Finns dokumenterad rutin för förebyggande kontroll, underhåll och övervakning av ☐ maskinvara ☐ diskkapacitet ☐ backup ☐ korrekt överföring mellan system ☐ rapportrutiner (epost, papper)	
☐ Är all datautrustning individmärkt och upptagen i förteckning (dokument eller underhållsdatabas)?	
☐ Finns loggböcker (eller dokument/underhålls-, ärendehanteringssystem) för datautrustning som ☐ server ☐ PC ☐ Skrivare ☐ nätverksutrustning ☐ programvara datasystem ☐ elektronisk överföring av data ☐ Är loggbokssystemet beskrivet i ledningssystemet? ☐ Används loggböckerna? ☐ Går det att identifiera utrustningen? ☐ Är noteringarna daterade och signerade? ☐ Framgår åtgärder?	
☐ Kan man se i systemet eller av dokumentation vilken version som körs.	
☐ Finns underhållsrutiner för kodverk som används vid informationsöverföring. ☐ Är ansvar och befogenheter för underhåll av kodverk dokumenterat i ledningssystemet?	
☐ Finns en skriftlig rutin för all berörd personal (samt eventuella externa leverantörer) att tillämpa vid olika typer av fel i systemet. Rutinen skall inkludera ☐ verksamhetens hantering vid totalt driftstopp. (Reservrutiner, återskapande av system) ☐ verksamhetens hantering vid olika felsituationer tex. avbrott i nätverk, fel på PC, fel på skrivare, programfel, överföringsfel till annat system, fel i epostöverföring. ☐ hur felrapportering, korrigering skall gå till från personal via IT-ansvariga ev. till leverantör ☐ hur dokumentation skall ske av fel och åtgärder. ☐ vem som ansvarar för uppföljning av fel som rapporterats vidare till leverantör. ☐ vem som ansvarar för felsökning i olika delar av kedjan vid överföringsfel till annat system ☐ i händelse av allvarliga programfel som t.ex. förväxling av resultat - åtgärder för att säkra kvalitet - t.ex. extra kontroller av rapportutskriften	
☐ Är rutinen tillgänglig, känd och aktuell?	
☐ 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
☐ 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?	

6. Förändringsrutiner	Anteckning
☐ 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, webbläsare) ☐ 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 ☐ nytt eller ändrat format elektronisk beställning eller elektronisk rapport (meddelande eller web) ☐ ny svarsrapport ☐ 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. ☐ hur provningen skall dokumenteras. Instruktioner eller färdig mall för dokumentation där det skall framgå ☐ vem som provat ☐ när det skett ☐ orsak till provningen ☐ om valideringen skett i test eller driftmiljö ☐ version av testat program/systemversion ☐ referens till eventuella fel. ☐ vilka underlag (utskrifter, skärmdumpar) som skall tas ut ur systemet för att styrka provningen ☐ hur man med olika markeringar i underlagen visar att uppgifter är kontrollerade och korrekta/felaktiga – tex. med streck eller bock vid en kontrollerad uppgift. ☐ Sammanfattande resultat, beslut om drifttagning	

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-viruskyddet 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 resultatinsmatning 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	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?	

9. Anskaffande av nytt system samt egenutveckling	Anteckning
☐ Används en internationell standard som grund	
☐ Föreligger ett tydligt kund - leverantörsförhållande? (Även vid intern utveckling) ☐ Utgår man från överenskomna specifikationer för att klargöra funktionen för alla inblandade parter? ☐ Hur sker godkännande av specifikation och levererad funktion? ☐ Finns en överenskommelse om hur ändringar och tillägg till ursprunglig specifikation skall hanteras? ☐ Finns överenskommelse om acceptansprov? ☐ Finns en överenskommelse om acceptansgranskning av dokumentation? ☐ Är källkods rättigheter klarlagda och framgår i avtal.	
☐ Är en analys gjord över risker och sårbarhet - både tekniska och kompetensmässiga?	
☐ Sker testning enligt planer? Dokumenterar leverantören sin testning?	
☐ Finns bestämda konstruktionsregler för namngivning, kommentering etc?	
☐ Finns det risker med valda utvecklingsverktyg? Är dessa identifierade och överenskomna?	
☐ Uppdateras handböcker efter förändring?	
☐ Sker planering med grundplaner och uppföljning-revidering? Sker avstämning av planer mellan kund-leverantör?	

9. Anskaffande av nytt system samt egenutveckling	Anteckning
☐ Finns avtal med externa utvecklare som täcker behörigheter, befogenheter, kompetenskrav, källkods rättigheter och serviceåtaganden?	
☐ Finns en formaliserad metod eller rutin som täcker de vanligaste typerna av vidareutveckling? ☐ Omfattar den alla led i utvecklingskedjan? ☐ framtagning av specifikationer ☐ design ☐ kodning ☐ testning ☐ validering/verifikation (pkt 6) ☐ dokumentation inklusive handbok, ☐ information ☐ drifttagning ☐ korrigering av eventuella fel ☐ ändringar och tillägg till ursprunglig specifikation ☐ uppdatering av dokumentation efter programändringar	

2 Guide for information security work

2.1 Purpose

The purpose of this document is to provide accredited bodies and bodies seeking accreditation with guidance on improving information security. The document also provides guidance on information security assessment requirements.

The checklist at the end of the document can be used for internal and external audits.

2.2 Scope

The document applies to all types of computer systems and support systems used in the accredited bodies, both direct production systems and support systems for the management system. Examples of such systems with different names in brackets;

- LIS (LIMS, lab computer system, production system)
- Lab Module (POCT, PNA)
- Booking (RIS etc.)
- Order and response
- Image processing (PACS)
- Physiological analysis systems
- Document Management
- Issue, deviation, complaint handling
- Internal Audit Management
- Permission Management (driver's licence)
- Spreadsheet and word processor macros
- Programmable Table Calculators
- Process control (control system, tracks)
- Instrument systems (embedded computers, workstations to instruments)
- External support systems and web services (sampling instructions, population registration, QC)

2.3 Identification and functionality of input systems

Requirement reference: 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; 7.6, 7.8, 8.1.1, 8.3
 ISO 20387; 7.10.1, 7.10.3

As a starting point for the work on information security, the organisation should identify which systems are used, the functionality of each system and the functional connections between the systems.

A reconciliation should then be made with the accreditation standard to see if there are requirements in it that relate to the functionality of the system such as response reporting, document management, measurement of quality indicators, approval of documents, traceability to which changes have been made in results. The starting point is that the requirements for data functions are in line with those for manual paper-based procedures.

The data in the system should be evaluated in order to establish what is a valid original and what copies (electronic and paper) and what handling procedures apply to the latter.

All the staff concerned must have the necessary access to instructions and information for the execution of the work. The operational requirements for system availability and the fallback procedures must therefore be documented.

2.4 Linkage between systems

Requirement reference: 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; 7.6.3
 ISO 20387; 7.4.7, 7.5.1, 7.10.3

All parties to the exchange of information should understand and have documented the potential risks associated with the exchange.

Accredited bodies have a primary responsibility for validating the entire exchange initially and in case of changes occurring in the transmission chain.

The recipient of the information is responsible for carrying out plausibility checks to stop gross misstatements.

2.5 Organisation

Requirement reference: 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; 5.2.2, 6.2, 6.8, 7.5, 7.6
 ISO 20387; 6.2, 6.4, 7.10.3

The data systems of an establishment are subject to equivalent requirements as for other accredited bodies with regard to the competence, competencies, responsibilities and powers of the staff.

The requirements also apply to services and products that the accredited body receives or purchases from both external and internal suppliers. The accredited body is always responsible for ensuring the quality of the services/products purchased through contracts and controls.

For systems that communicate with other systems, both within their own operations and with external ones, cooperation between the different parties responsible for development and operational support should take place with a clearly documented division of responsibility. The allocation of responsibilities should also cover the updating of system descriptions and common procedures.

All users of a system should have received adequate training in the management of the system, as well as procedures and rules for both normal and abnormal operational situations.

The training should be documented and linked to the certificates of competency issued in the management system

The operational support resources should be of sound technical competence, follow quality assurance procedures and be organisationally located at a level commensurate with the use made of the system.

There should be documentation of the decision-making process when dealing with errors or when a new system version is to be commissioned. Competence to become operational or to take decisions on the continued operation of the system despite faults detected, possibly with control measures, should be linked to operational and IT competence. At times when regular data personnel are not available, decision-making personnel should have sufficient competence to assess the consequences of observed data errors and take the necessary measures.

2.6 Documentation, system description

Requirement reference: 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; 7.6.3, 8.3
 ISO 20387; 4.1.4, 7.10.3, 8.3

System description includes documentation of functionality, system platforms and technical solutions necessary for system maintenance and further development. Relevant documentation including the supplier's manual for the management and maintenance of the computer system should be available to the relevant staff.

The system description may consist of external documents from the supplier supplemented with descriptions of local customisations and communication with other systems. All documents must be

document controlled and there must be traceability to which version of the system the description refers.

If the system is unique and owned by the accredited body, it must be ensured that in all future situations a complete copy of the documentation is available to ensure the system's survival.

2.7 Maintenance procedures

Requirement reference: 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; 6.4, 7.6
 ISO 20387; 6.5, 7.10.3

Accredited bodies should have documented procedures for:

- preventive maintenance and monitoring of system functionality.
- situations when the system is not working as intended. The fallback procedures shall include regular work instructions, as well as troubleshooting, error reporting and remediation. Changes, errors and actions should be recorded on paper or electronically

2.8 Change procedures

Requirement reference: 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; 7.6
 ISO 20387; 6.5, 7.9, 7.10.3

The system shall be validated for proper functioning, availability, traceability, transparency and access by unauthorised persons. Validation should be carried out for any system changes in the system platform or application software.

The purpose of validation is to ensure the quality of a system or the exchange of information between systems.

This can be done in different ways or in combination:

- Testing (testing) in a specific test environment or operating environment
- Parallel execution of new system/new version against an existing system/version
- Control of results against orders, manual worklists, raw data, manual calculations or alternative response methods not covered by the change.

- Comparison of data in the respective systems in case of electronic transmission between systems
- Periodic sample testing on systems in operation to ensure that there has been no change, for example, in configuration parameters, vendor patches or in the external communication chain.

Validation should follow a documented procedure covering the entire data flow. The procedure should describe the method of validation in case of changes and ensure that supporting documentation is created. The supporting documentation should include a summary report detailing the reason for the validation, who performed the validation and the time, system version, results and decision. The results should be supported by evidence.

If the accredited body rely on external validation of system changes, the reports of the external validation should be sufficiently detailed to allow for proper decisions to be taken.

When introducing a new computer system or in the event of major changes, the accredited body must contact SWEDAC for planning assessment work.

2.9 Archiving

Requirement reference: 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; 8.4
 ISO 20387; 4.1.8, 7.10.6, 8.4

The archiving requirements of the management system for data in the system must be defined and met. For data stored on a particular system, such as in a previous operating system, a plan must be in place on how the activity intends to ensure the continuity of the computer system during the retention period.

2.10 Risk management

Requirement reference: 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; 5.6, 7.6.3, 8.5
 ISO 20387; 4.2, 4.3, 7.10.3, 8.5

The system must meet basic requirements for security and confidentiality in respect of the authorisation and control systems (BKS), protection against computer viruses and backup.

If the system uses underlying access protection in the operating system, database or word processor to protect the integrity of the data, this must not be able to be circumvented. Supplier's requirements for operating systems and settings must be followed.

The basis for modern information security work is to conduct a documented process analysis of the information flow of the business. As part of the process analysis, the performance of risk analysis includes an assessment of risks related to the accuracy, availability, transparency and traceability of the information flow. The risks found are evaluated against the management system's policy with requirements for the organisation's information security.

Process analysis of information security can usefully be done with a comprehensive view in connection with process analysis of ordinary bodies.

2.11 Acquisition of new system and development of own system

Requirement reference: 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; 7.6.3
 ISO 20387; 6.4, 6.5, 7.9, 7.10.2-7.10.3

Software development should follow the guidelines of international standards. If the supplier is certified according to an international standard, this can be an advantage, otherwise the business should take note of the supplier's routines, such as validation of software, request for changes and correction of found errors.

When developing systems, the work should be quality assured through documented procedures and instructions. Risks should be identified in terms of technical and competency vulnerability. Source code rights and responsibilities for specifications, testing and operations should be clarified.

2.12 Checklist for internal and external audits of data operations

Activity:

Date:

Responsible IT:

Participants:"

Items that are not relevant to the current system are marked as not applicable at the time of the audit.

1. Identification and functionality of input systems	Notes
System Name: Version: Vendor: System Platform: Computer: O/S: dbms: Development Tools: Functionality: Connection to other systems:	
System Name: Version: Vendor: System Platform: Computer: O/S: dbms: Development Tools: Functionality: Connection to other systems:	
System Name: Version: Vendor: System Platform: Computer: O/S: dbms: Development Tools: Functionality: Connection to other systems:	

1. Identification and functionality of input systems	Notes
System Name: Version: Vendor: System Platform: Computer: O/S: dbms: Development Tools: Functionality: Connection to other systems:	

2. Organisation	Note
☐ Is the operating aid organisation described in the management system (e.g. in the form of different roles as system owner, system manager, system operator)? ☐ Is placement shown in organisation chart? ☐ Are there deputies for all functions?	
☐ Does the management system or contract specify the liability of external suppliers? ☐ Is it clear that the operation holds primary responsibility for validating the entire transfer chain when transferring between systems?	
☐ Has the operational support organisation of the system received sufficient and documented training?	
☐ Is the authorisation system (licence) also used for the management of the computer system? ☐ Is there documentation of training and information about the computer system?	
☐ Are internal quality audits of data operations carried out regularly?	
☐ Do the purchasing procedures in the management system also cover computer equipment and services?	

3. Contracts	Notes
Agreements with all parties outside the business (suppliers, customers, group IT department) covering ☐ critical hardware and software support ☐ connections and transfers to external systems (web, EDI, email) ☐ Are all parties clearly described – including subcontractors and third party suppliers? ☐ Is there a requirement to have a contract with any third party, e.g. service for equipment not owned by the business, sub-contractors for programme development, operating support at EDI? ☐ Are the responsibilities/limits and commitments of the different parties in normal management described (who does what, when and how)? ☐ Is the agreed functionality specified? ☐ Is the agreed availability of access to/receipt of information specified? ☐ Is ownership and responsibility for the information stated? ☐ Are contact persons listed? ☐ Are the names and privileges of persons who carry out work on the premises of the establishment or have access to the computer system of the establishment indicated? ☐ Are responsible for updating agreements, system descriptions and common documents listed? ☐ Is a skills guarantee given? ☐ Is there a commitment to comply with documented security and privacy rules and that access/access to the systems is not possible for anyone other than competent staff? ☐ Is there a commitment to record key system events and error actions in the Event Viewer or Case Management System? ☐ Is a description of the fallback procedures for different types of errors available? ☐ Are reporting times specified for operating aid (also in the case of new developments)? ☐ Is Trouble Ticket Availability and Contact Routes Specified?	
Applicable when information is exchanged with other systems, e.g. electronic responses, web access to reports. ☐ Are agreed protocols and platforms for transfers between systems described? ☐ Is a description of each party's monitoring of information exchange available? ☐ Is there a commitment to provide information on events and changes that may affect the exchange of information? ☐ Are plausibility checks which the recipient undertakes to make to stop gross errors, such as data not being sent twice, being transmitted incompletely or incorrectly, described? ☐ Is there a commitment to inform the parties concerned without delay of any suspected errors in the exchange of information? ☐ Is it specified who is responsible for troubleshooting different parts of the chain for transmission failures between systems? ☐ Is there a commitment to verify that information is exchanged correctly following changes in codes, functions, platforms and that the intersystem transfer bodies have a primary responsibility for the validation of the entire chain?	

4. Documentation, system description	Notes
☐ Is a system description available? ☐ Which internal and external documents are included? ☐ Are all document controlled and traceable to the current system version? Is there a list? ☐ Is the documentation sufficient for operational support and development. ☐ If the system is unique, does the business have access to a copy of the detailed documentation in the event of a disaster?	
System documentation indicates ☐ the functions of the computer system. If a standard system is in place, it shall be documented which functions, if any, are not used. ☐ a description - preferably graphic - over ☐ Hardware ☐ system software ☐ network ☐ connections to external systems ☐ information flow ☐ database structure ☐ login protection/access ☐ virus protection ☐ transparency (e.g. firewalls, secure network, encryption, or non-sensitive information) ☐ communication with external systems ☐ transfer formats and mappings ☐ how the information is protected against changes e.g. by checksum calculation, encryption or traceability by matching logs with content before and after processing ☐ logs that information has been transmitted and what has been transmitted during despatch, receipt and retransmission. ☐ how the sender can view sent messages, recovered or saved. ☐ Log monitoring capabilities. Archiving times. ☐ Receipt functions and notifications for information exchange ☐ Is there a user manual (or built-in help system) ☐ Is the user manual document controlled? ☐ Is traceability available for which system version the instruction applies to?	

5. Maintenance Procedures	Notes
☐ Is there a documented procedure for preventive inspection, maintenance and monitoring of: ☐ hardware ☐ disk capacity ☐ backup ☐ correct data transfer between systems ☐ reporting procedures (email, paper)	
☐ Is all IT equipment individually marked and listed in a register (document or maintenance database)?	
☐ Are there logbooks (or documents/maintenance or case management systems) for IT equipment such as: ☐ server ☐ PC ☐ printer ☐ network equipment ☐ software systems ☐ electronic data transfer ☐ Is the logbook system described in the management system? ☐ Are the logbooks used? ☐ Can the equipment be identified? ☐ Are the entries dated and signed? ☐ Are corrective actions recorded?	
☐ Can the current version in use be identified in the system or through documentation?	
☐ Are there maintenance procedures for code sets used in information transfer? ☐ Are responsibilities and authorities for maintenance of code sets documented in the management system?	
☐ Is there a written procedure for all relevant personnel (including any external suppliers) to follow in case of different types of system errors? The procedure shall include: ☐ the organisation's handling of total system downtime (contingency routines, system recovery) ☐ the organisation's handling of various error situations, such as network interruptions, PC failures, printer errors, software faults, transfer errors to another system, email transfer errors ☐ how error reporting and correction shall be carried out from personnel via IT ☐ who is responsible, possibly including suppliers ☐ how errors and corrective actions shall be documented ☐ who is responsible for following up errors reported to the supplier ☐ who is responsible for troubleshooting different parts of the chain in case of transfer errors to another system ☐ in the event of serious software errors, such as mixing of results – actions to ensure quality, e.g. extra verification of report printouts	
☐ Is the procedure available, known, and up to date?	

5. Maintenance Procedures	Notes
☐ Are authorities to implement actions in the event of identified errors documented in the management system (e.g. to put the system in/out of operation, correct errors/order corrections, implement quality control of results)?	

6. Change procedures	Notes
☐ Is the system versioned? (Does version management also include peripheral parts of the system such as response reports, file conversions, instrument interfaces.) ☐ Is the build-up of version management documented? ☐ Indicates the version designation in technical documents, test reports, manuals, error reports.	
☐ Is final validation against locked (frozen) versions of the system?	
☐ Is there a documented procedure for checking reports against basic material? Is this ☐ for all answers routinely ☐ at start-up ☐ in the case of a serious defect.	
☐ Is there a dedicated test environment? ☐ is it documented? ☐ is there a risk that the test environment is used inadvertently or that the test response will be sent to the customer?	
☐ Does the business have access to detailed reports from the supplier's testing?	

6. Change procedures	Notes
☐ Is there a written validation procedure in which it is clear when the validation/verification is to take place, e.g. at ☐ new system version ☐ minor changes/fixes in programme code ☐ upgrade hardware or system software (server and clients, browser) ☐ new instrument ☐ new version of software in instruments ☐ changes to connected external systems or part of the communication chain ☐ new or modified analysis/survey including code works changes ☐ change in calculation functions ☐ new customer or changed customer information such as address/reporting method ☐ new or changed format electronic ordering or electronic report (message or web) ☐ new response report ☐ who is responsible for sufficient testing, who is competent to carry out testing, who approves the test carried out and who takes the decision to put into service ☐ instructions on how to carry out the test. Level of detail sufficient to cover all normal variation and extreme cases and to provide uniform testing even if several persons test. Expected result so that the test can be repeated. ☐ How the testing shall be documented. Instructions or a predefined template for documentation shall include: ☐ who performed the testing ☐ when the testing was conducted ☐ the reason for the testing ☐ whether the validation was carried out in a test or production environment ☐ version of the tested program/system version ☐ reference to any detected errors ☐ which supporting documentation (printouts, screenshots) shall be retrieved from the system to verify the testing ☐ how different markings in the documentation indicate that information has been verified and is correct/incorrect – e.g. by using a line or a check mark next to the verified item ☐ summary of results, decision on commissioning	

7. Archiving	Notes
☐ Is the computer system used solely as an archive for certain data? What archiving times are stated in the management system. Is it described how you intend to secure the archive, etc., platform and skills?	

8. Risk management	Notes
☐ Available written backup routine that covers: ☐ rotation scheme description ☐ media labelling ☐ responsible (and deputy) ☐ management ☐ storage of daily backup and system backup for unique software in other fire zone, fire resistant cabinet ☐ that completed backup and any errors are noted in the logbook ☐ Checks made backup by eg. re-reading? ☐ Is there a documented procedure for re-creation? ☐ Are the responsibilities and powers for the operation and management of the backup system documented in the management system	
☐ Does the system of authorisation provide adequate protection? ☐ Is the rating system documented? ☐ How often does a password change? ☐ How many characters is minimum? ☐ Can passwords be reused?	
☐ Do visitors have access to equipment? Is it possible for unauthorised persons to read on monitors?	
☐ Is regular or continuous anti-virus screening of PC. ☐ Is anti-virus protection documented?	
☐ How is proper transmission between systems ensured? Are checksums and unique sequence numbers used in message transfer? Is there receipt handling?	
☐ Check premises for. ☐ heat and humidity ☐ fire, flood protection ☐ dust ☐ electricity supply ☐ sources of interference ☐ lock access protection?	
☐ Control of manual result input and change of results. Matches issued permissions?	
☐ Control of traceability of a sample: Signoffs, times, changes, link to control sample?	
☐ Checking of time limits. Same time on server and all clients?	
☐ Documented risk analysis available ☐ Covers all use cases such as ☐ Communication terminal<->server, client<->server, server<->server	

8. Risk management	Notes
☐ Communication with external systems e.g. EDI web reports, web ordering, population register ☐ Are information assets classified ☐ There are overall information security policies and guidelines ☐ Is the risk assessment made for deficiencies in the information ☐ accuracy ☐ accessibility ☐ transparency ☐ traceability ☐ Is there an agreed action plan that includes planned measures, bodies, times, responsibilities	
☐ An action plan for post-disaster recovery	
☐ Are there spare equipment or an action plan for non-critical equipment?	

9. Procurement of new systems and in-house development	Notes
☐ An international standard is used as the basis.	
☐ Is there a clearly defined customer-supplier relationship? (Also in the case of internal development) ☐ Are agreed specifications used to clarify the function for all involved parties? ☐ What is the approval process for specifications and delivered functionality? ☐ Is there an agreement on how changes and additions to the original specification should be managed? ☐ Is there an agreement regarding acceptance testing? ☐ Is there an agreement regarding acceptance review of documentation? ☐ Are source code rights clarified and specified in the agreement?	
☐ Has an analysis of risks and vulnerabilities been conducted – both technical and competence-related?	
☐ Is testing carried out according to plans? Does the supplier document their testing?	
☐ Are there defined design rules for naming conventions, commenting, etc.?	
☐ Are there risks associated with the chosen development tools? Have these been identified and agreed upon?	
☐ Are manuals updated after changes?	
☐ Is planning done with baseline plans and follow-up/revision? Are plans coordinated between customer and supplier?	
☐ Are there agreements with external developers covering access rights, authorities, competence requirements, source code rights, and service commitments?	

9. Procurement of new systems and in-house development	Notes
☐ Is there a formalised method or routine that covers the most common types of further development? ☐ Does it cover all stages of the development chain? ☐ Preparation of specifications ☐ Design ☐ Coding ☐ Testing ☐ Validation/verification (see item 6) ☐ Documentation including user manuals ☐ Information ☐ Commissioning ☐ Correction of any errors ☐ Changes and additions to the original specification ☐ Updating of documentation following program changes	