SVENSK STANDARD
SS-ISO/IEC 27036-3:2014

Fastställd/Approved: 2014-05-05
Publicerad/Published: 2017-03-06
Utgåva/Edition: 1
Språk/Language: svenska/Swedish, engelska/English
ICS: 01.140.30; 04.050; 33.040.40; 35.020; 35.040; 35.080

Informationsteknik – Säkerhetstekniker – Informationssäkerhet vid leverantörsrelationer – Del 3: Riktlinjer för informations- och kommunikationssäkerhet i leverantörskedjor (ISO 27036-3:2013, IDT)

Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security (ISO 27036-3:2013, IDT)

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Den internationella standarden ISO/IEC 27036-3:2014 gäller som svensk standard. Detta dokument innehåller den svenska versionen av ISO/IEC 27036-3:2014 följd av den officiella engelska språkversionen.

The International Standard ISO/IEC 27036-3:2014 has the status of a Swedish Standard. This document contains the Swedish language verson of ISO/IEC 27036-3:2014 followed by the official English version.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

Denna standard är framtagen av kommittén för Informationssäkerhet, SIS/TK 318.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Innehåll

Sida

Förord

ISO (Internationella standardiseringsorganisationen) och IEC (Internationella elektrotekniska kommissionen) utgör det specialiserade systemet för internationell standardisering. Nationella organ som är medlemmar i ISO eller IEC deltar i utvecklingen av internationella standarder genom medverkan i tekniska kommittéer inom respektive organisationer med uppgift att behandla avgränsade tekniska områden. De tekniska kommittéerna inom ISO och IEC samarbetar inom områden av gemensamt intresse. Andra internationella organisationer, statliga eller privata, som samarbetar med ISO och IEC, deltar också i arbetet. Inom området informationsteknik har ISO och IEC bildat en gemensam teknisk kommitté, ISO/IEC JTC 1.

Internationella standarder utformas i enlighet med de regler som anges i ISO/IEC Directives, Part 2.

Den gemensamma tekniska kommitténs främsta uppgift är att utarbeta internationella standarder. Förslag till internationell standard som antagits av den gemensamma tekniska kommittén sänds till medlemmarna för omröstning. Publicering som internationell standard kräver godkännande av minst 75 % av röstande medlemmar.

Det bör framhållas att vissa delar av detta dokument kan omfattas av patenträtter. ISO och IEC frånsäger sig ansvaret för att identifiera några eller alla sådana patenträtter.

ISO/IEC 27036-3 utformades av ISO/IEC JTC 1, *Information technology, SC 27, Security techniques*.

ISO/IEC 27036 består av följande delar, under titeln *Informationsteknik – Säkerhetstekniker – Informationssäkerhet vid leverantörsrelationer:*

– *Del 1: Översikt och begrepp*

– *Del 2: Allmänna krav*

– *Del 3: Riktlinjer för informations- och kommunikationssäkerhet i leverantörskedjor*

Följande del är under framtagande:

– *Del 4: Guidelines for security of cloud services*

Orientering

Informations- och kommunikationstekniska produkter och tjänster utvecklas, integreras, och levereras globalt genom djupgående och fysiskt spridda leverantörskedjor. ICT-produkter byggs upp av många komponenter från många leverantörer. Genom hela leverantörskedjan levereras ICT-tjänster genom flera lager av utkontraktering och leveransförsörjning. Beställare har inte djupare insyn i hårdvaru-, mjukvaru- och tjänsteleverantörers processer än till den första länken eller möjligen den andra i leverantörskedjan. Med den kraftiga ökningen av antalet organisationer och människor som ”rör vid” en ICT-produkt eller tjänst, så har insynen i dessa processer minskat dramatiskt. Denna brist på insyn, transparens, och spårbarhet i ICT-leverantörskedjorna innebär risker för beställande organisationer.

Nationell anmärkning: Förkortningen IKT används ibland på svenska, men i denna standard har den engelska förkortningen ICT behållits.

Denna standard ger vägledning för beställare och leverantörer av ICT-produkter och ICT-tjänster för att reducera eller hantera informationssäkerhetsrisker. Denna standard identifierar de affärsmässiga argumenten för säkerhet inom ICT-leverantörskedjan, specifika risker och affärsmässiga relationer samt stöd för organisatorisk förmåga att hantera informationssäkerhetsaspekter och att anamma ett livscykelperspektiv för att hantera risker, i form av specifika säkerhetsåtgärder och rutiner. Efterlevnad av standarden förväntas resultera i:

– ökad insyn och spårbarhet i ICT-leverantörskedjan för att förstärka informationssäkerhetsförmågan,

– ökad förståelse hos beställare rörande varifrån deras produkter och tjänster kommer, och rörande processen för att utveckla, integrera eller använda dessa produkter eller tjänster, allt för att främja implementeringen av informationssäkerhetskrav,

– tillgång till information om vad som kan ha hänt och vilka som kan ha varit inblandade vid eventuella informationssäkerhetshändelser.

Denna internationella standard är tänkt att användas av alla typer av organisationer som beställer eller levererar ICT-produkter och ICT-tjänster inom ICT-leverantörskedjan. Vägledningen riktar primärt in sig på den första länken mellan beställare och leverantör, men de principiella stegen bör tas genom hela kedjan, från det att den första leverantören ändrar sin roll till att bli en beställare osv. Denna förändring av roller och att tillämpa samma steg för varje ny länk mellan beställare och leverantör är den huvudsakliga intentionen bakom standarden. Genom att följa denna internationella standard möjliggörs kommunikation kring informationssäkerhetsrelaterade följder bland organisationerna i leverantörskedjan. Detta hjälper till att identifiera informationssäkerhetsrisker samt deras orsaker så att transparensen genom hela kedjan ökas. Osäkerheter gällande informationssäkerhet relaterade till leverantörsrelationer förekommer i en mängd olika scenarion. Organisationer som önskar förstärka tilliten inom sin ICT-leverantörskedja bör specificera gränserna för sin tillit, utvärdera riskerna med sina aktiviteter inom leverantörskedjan, och sedan specificera och implementera lämplig riskidentifiering och åtgärdsförfaranden för att reducera risken för att sårbarheter uppstår i deras ICT-leverantörskedja.

Ramverket och säkerhetsåtgärderna i ISO/IEC 27001 och ISO/IEC 27002 ger en användbar startpunkt för identifikation av lämpliga krav för beställare och leverantörer. ISO/IEC 27036 ger ytterligare detaljer om specifika krav att använda vid etablering och uppföljning av leverantörsrelationer.

1 Omfattning

Denna del av ISO/IEC 27036 ger beställare och leverantörer av produkter och tjänster inom ICT-leverantörskedjan vägledning om:

a) att få insyn i och att hantera de informationssäkerhetsrisker som orsakas av att ha fysiskt spridda ICT-leverantörskedjor i flera lager,

b) att svara upp mot risker som härstammar från den globala ICT-leverantörskedjan för ICT-produkter och ICT-tjänster som kan ha informationssäkerhetspåverkan på organisationer som använder dessa produkter och tjänster. Dessa risker kan vara relaterade till organisatoriska såväl som tekniska aspekter (t.ex. införande av skadlig kod eller närvaro av förfalskade informationstekniska produkter),

c) att integrera informationssäkerhetsprocesser och rutiner i system och mjukvarors livscykelprocesser, som beskrivs i ISO/IEC 15288 och ISO/IEC 12207, och samtidigt stödja informationssäkerhetsåtgärder, som beskrivs i ISO/IEC 27002.

Denna del av ISO/IEC 27036 omfattar inte kontinuitetsplanering eller aktiviteter relaterade till återhämtningsförmåga omfattande ICT-leverantörskedjan. ISO/IEC 27031 handlar om kontinuitetsplanering.

2 Normativa hänvisningar

Detta dokument hänvisar till följande dokument som är nödvändiga när detta dokument ska tillämpas. För daterade hänvisningar gäller endast den utgåva som anges. För odaterade hänvisningar gäller senaste utgåvan av dokumentet (inklusive alla tillägg).

ISO/IEC 27000, *Information technology – Security techniques – Information security management systems - Overview and vocabulary*

ISO/IEC 27036-1, *Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts*

ISO/IEC 27036-2, *Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements*

3 Termer och definitioner

För tillämpning av detta dokument gäller de termer och definitioner som anges i ISO/IEC 27000, ISO/IEC 27036-1 och de som följer nedan.

3.1
tillförlitlighet
egenskap hos ett system och dess delar att kunna utföra sitt uppdrag korrekt och utan avbrott eller betydande brister i funktion

Svensk anmärkning: I SIS-TR 50:2015 ”Terminologi för informationssäkerhet” anges följande definition: ’mått på i vilken grad ett informationssystem levererar kravställd informationskvalitet’.

3.2
systemelement
del av en uppsättning element som tillsammans utgör ett system

Anm. 1 till termpost: Ett systemelement är en separat del av ett system som kan implementeras för att uppfylla specificerade krav. Ett systemelement kan vara hårdvara, program, data, människor, processer (t.ex. processer för att tillhandahålla kravställning på funktionalitet till användare), rutiner (t.ex. operatörsinstruktioner), lokaler, material och naturligt förekommande substanser (t.ex. vatten, organismer, mineraler), eller någon kombination av dessa.

[KÄLLA: ISO/IEC 15288:2008, definition 4.32]

3.3
transparens
egenskap hos ett system eller en process som medför öppenhet och ansvarighet

3.4
spårbarhet
egenskap som tillåter spårning av aktiviteter utförda av en identitet, process eller ett element genom hela leverantörskedjan

Svensk anmärkning: I SIS-TR 50:2015 ”Terminologi för informationssäkerhet” anges följande definition: ’entydig härledning av utförda aktiviteter till en identifierad användare’.

3.5
validering
bekräftelse, genom tillhandahållande av objektiva bevis, av att kravställningen för ett specifikt tänkt användningsområde eller en applikation har uppfyllts

Anm. 1 till termpost: Validering är en uppsättning aktiviteter som bekräftar och säkerställer att ett system kan uppnå sitt tänkta användningsområde och mål (dvs. att möta intressenternas krav) i den tänkta driftsmiljön.

[KÄLLA: ISO/IEC 15288:2008, definition 4.37]

3.6
verifiering
bekräftelse, genom tillhandahållande av objektiva bevis, av att specificerade krav har uppfyllts

Anm. 1 till termpost: Verifiering är en uppsättning aktiviteter som jämför ett system eller systemelement med de kravställda egenskaperna. Detta kan inkludera, men är inte begränsat till, specificerade krav, designbeskrivning och systemet självt.

[KÄLLA: ISO/IEC 15288:2008, definition 4.38]

Svensk anmärkning: I SIS-TR 50:2015 ”Terminologi för informationssäkerhet” anges följande definition: ’fastställande av någots riktighet, med avseende på specifikation’.

4 Denna standards struktur

Denna standard är strukturerad för att harmonisera med ISO/IEC 15288 och ISO/IEC 12207. Avsnitt 6 motsvarar livscykelprocesserna som beskrivs i dessa två standarder. Denna standard är också harmoniserad med ISO/IEC 27002 och ger referenser till relevanta informationssäkerhetsåtgärder inom livscykelprocesserna med hjälp av tabellen över samband i bilaga B.

Dokumenten som omnämns i denna standard är generiska och behöver inte vara omfattande eller ens separata dokument. Organisationer bör använda existerande dokument för att integrera säkerhet relaterat till ICT-leverantörskedjan.

5 Nyckelbegrepp

5.1 Affärsmässiga argument för informationssäkerhet inom ICT-leverantörskedjan

Organisationer beställer ICT-produkter och ICT-tjänster från många olika leverantörer som i sin tur kan köpa komponenter från andra leverantörer. Informationssäkerhetsriskerna som är associerade med dessa spridda ICT-leverantörskedjor i flera led kan hanteras genom tillämpning av riskhantering och relationer med betrodda partner så att insynen, spårbarheten och transparensen i ICT-leverantörskedjan ökar.

Ökad insyn i ICT-leverantörskedjan fås t.ex. genom att adekvata informationssäkerhets- och kvalitetskrav specificeras samt att uppföljning av leverantörer och deras produkter och tjänster sker löpande när väl en leverantörsrelation har upprättats. Att identifiera och hålla kontakt med de individer som är ansvariga för

kvalitet och säkerhet för kritiska delar i leveransen ökar spårbarheten. Att etablera avtalsmässiga krav och förväntningar, såväl som att granska processer och rutiner ger den transparens som så väl behövs.

Beställare bör verka för förståelse inom sina organisationer rörande de risker som är kopplade till ICT-leverantörskedjan och deras möjliga påverkan på verksamheten. Särskilt ledningen hos beställar-organisationen bör vara medveten om att rutiner hos leverantörer genom hela leverantörskedjan kan påverka huruvida de slutliga produkterna och tjänsterna går att lita på när det gäller att skydda beställarens verksamhet, information och informationssystem.

5.2 Risker inom ICT-leverantörskedjan och angränsande hot

Styrning av informationssäkerhet i en enskild organisation (beställare eller leverantör) är inte tillräckligt för att uppnå informationssäkerhet för ICT-produkter eller ICT-tjänster genom leverantörskedjan. Beställarens styrning av urvalet av ICT-leverantörer, ICT-produkter och ICT-tjänster är kritisk för informationssäkerheten.

Köp av ICT-produkter och ICT-tjänster leder till speciella risker för beställare när det gäller hantering av informationssäkerhetsrisker. När globala ICT-leverantörskedjor blir mer fysiskt spridda och går över ett flertal internationella och organisatoriska gränser, blir det svårare att spåra specifika tillverknings- och driftsrutiner för individuella ICT-element (produkter, tjänster och deras komponenter) och även att identifiera individer som är ansvariga för kvalitet och säkerhet för dessa element. Detta skapar en generell brist på spårbarhet genom hela ICT-leverantörskedjan vilket i sin tur leder till högre risker för

– äventyrande av beställarens informationssäkerhet och därmed också av verksamheten genom avsiktliga händelser såsom införande av skadlig kod och närvaro av förfalskade produkter i ICT-leverantörskedjan,

– oavsiktliga händelser, såsom bristfälliga rutiner omkring mjukvaruutveckling.

Såväl avsiktliga som oavsiktliga händelser skulle kunna äventyra beställarens data och drift genom stöld av immateriell egendom, informationsläckage och reducerad förmåga hos beställare att utföra sina affärs-processer. Vilken som helst av dessa händelser skulle, om de inträffade, kunna skada organisationens rykte, vilket i sin tur skulle kunna leda till ytterligare negativ påverkan, såsom förlust av affärer.

5.3 Typer av relationer mellan beställare och leverantör

Beställare och leverantörer av ICT-produkter och ICT-tjänster kan involvera ett flertal enheter i en mängd olika leverantörskedjebaserade relationer, vilket inkluderar men inte begränsas till:

a) stöd för förvaltning av ICT-system där systemen ägs av beställaren och förvaltas av leverantören,

b) leverantörer av ICT-system eller tjänster där system eller resurser ägs och förvaltas av leverantören,

c) produktutveckling, design, teknik- och systembyggande där leverantören tillhandahåller hela, eller delar av, tjänsten associerad(e) med att skapa ICT-produkter,

d) leverantörer av kommersiella färdigprodukter,

e) leverantörer och distributörer av produkter med öppen källkod.

Beställares risknivå och därmed behov av tillit inom leverantörsrelationer ökar när de ger en leverantör en ökad tillgång till beställarens information och informationssystem och även beställarens beroende av de levererade ICT-produkterna och ICT-tjänsterna. Att t.ex. köpa stöd för förvaltning av ICT-system är ibland förenat med högre risk än att köpa produkter med öppen källkod eller kommersiella färdigprodukter. Sett från leverantörens perspektiv så kan allt äventyrande av beställarens information skada leverantörens rykte och tillit från den specifika beställare vars information och informationssystem har äventyrats.

För att underlätta hanteringen av osäkerheten samt riskerna kopplade till leverantörsrelationer bör beställare och leverantörer etablera en dialog och komma överens om ömsesidiga förväntningar gällande skydd av varandras information och informationssystem.

5.4 Organisatorisk förmåga

För att kunna hantera riskerna kopplade till ICT-leverantörskedjan genom hela livscykeln för ICT-produkter och ICT-tjänster bör beställare och leverantörer implementera en organisatorisk förmåga för att hantera informationssäkerhetsaspekter gällande leverantörsrelationer. Denna förmåga bör etablera och följa upp beställarorganisationens säkerhetsmål gällande ICT-leverantörskedjan, övervaka uppfyllnad av dessa mål och inkludera minst följande:

a) Specificera, bestäm och implementera strategin för hantering av informationssäkerhetsrisker orsakade av sårbarheter inom ICT-leverantörskedjan:

   1) Etablera och underhåll en plan för att identifiera potentiella sårbarheter relaterade till ICT-leverantörskedjan innan de utnyttjas; utöver detta, ha en plan för att lindra negativa effekter.

   2) Identifiera och dokumentera de informationssäkerhetsrisker som är kopplade till de hot, sårbarheter och konsekvenser som är relaterade till ICT-leverantörskedjan (se avsnitt 6.3.4).

b) Etablera och följ grundläggande informationssäkerhetsåtgärder som en förutsättning för robusta leverantörsrelationer (se bilaga B för sambandet mellan avsnitt 6 och ISO/IEC 27002).

c) Etablera och följ grundläggande livscykelprocesser och rutiner för system och program för att fastställa robusta leverantörsrelationer gällande hantering av informationssäkerhetsrisker kopplade till ICT-leverantörskedjan (se avsnitt 6).

d) Utarbeta en uppsättning grundläggande informationssäkerhetskrav som gäller för alla leverantörsrelationer och anpassa dem till specifika leverantörer vid behov.

e) Etablera en repeterbar och testbar process för att fastställa informationssäkerhetskrav kopplade till nya leverantörsrelationer, hantering av existerande leverantörsrelationer, verifiering och validering av att leverantörer följer beställarens informationssäkerhetskrav samt för att avsluta leverantörsrelationer.

f) Etablera förändringsprocesser för att säkerställa att förändringar som möjligen kan påverka informationssäkerheten godkänns och görs vid rätt tillfällen.

g) Specificera metoder för att identifiera och hantera incidenter relaterade till eller förorsakade av ICT-leverantörskedjan och för att sprida information om incidenter till leverantörer respektive beställare.

5.5 Livscykelprocesser för system

Livscykelprocesser kan hjälpa till att specificera förväntningarna mellan beställare och leverantörer gällande stringens och ansvar för informationssäkerhet. Beställare kan implementera livscykelprocesser internt för att öka stringensen i att etablera och hantera leverantörsrelationer. Leverantörer kan implementera livscykelprocesser för att kunna påvisa sin stringens i system- och mjukvaruprocesser gällande leverantörsrelationer. Även om det kommer att underlätta för både beställare och leverantörer att från början ta sig an risker relaterade till ICT-leverantörskedjan bör ytterligare säkerhetsaktiviteter gällande ICT-leverantörskedjan integreras med dessa processer.

System och mjukvaror för med sig många av riskerna inom ICT-leverantörskedjan. Att tillämpa ett livscykelperspektiv, såsom det beskrivs i ISO/IEC 15288 och ISO/IEC 12207, ger ett etablerat sätt att hantera de riskerna. Båda dessa standarder beskriver hur samma uppsättning processer gäller specifikt för system eller program. ISO/IEC 12207 beskriver en speciell tillämpning av ISO/IEC 15288. Båda standarderna tillåter användning av viken livscykel eller livscykelmodell som helst och beskriver en uppsättning processer som kan användas inom den livscykel eller livscykelfas där de passar bäst. Till exempel kan processen för konfigurationshantering användas både under utvecklingsfasen av system eller program och i livscykelfaserna för drift och underhåll. Denna standard tillämpar samma tillvägagångssätt som de två standarderna och beskriver varje process på översiktlig nivå genom ett uttalande om syftet och bryter sedan ner varje process till praxis.

Avsnitt 5.8 innehåller en sammanfattning av specifik praxis för ICT-leverantörskedjan. Avsnitt 6 innehåller sambandet mellan dessa säkerhetsaktiviteter för ICT-leverantörskedjan för varje livscykelprocess. Beställare och leverantörer bör välja de aktiviteter som är relevanta för deras respektive organisation med avseende på leverantörsrelationer generellt sett, såväl som på individuella leverantörsrelationer, baserat på de risknivåer som har specificerats av leverantörer eller beställare, såsom det beskrivs i avsnitt 5.1.

5.6 LIS-processer i förhållande till livscykelprocesser

ISO/IEC 27001 beskriver en riskbaserad process för att implementera ett ledningssystem för informationssäkerhet (LIS) för en specificerad omfattning. Att det finns ett LIS hos såväl beställarorganisationen som hos leverantörsorganisationen underlättar för beställare och leverantör att börja hantera riskerna inom ICT-leverantörskedjan och att inse behovet av de särskilda informationssäkerhetsåtgärder och informationssäkerhetsprocesser som behövs för att hantera dessa risker.

ANM. Detta förutsätter att omfånget för LIS:et inkluderar den specifika del av organisationen som etablerar och underhåller beställar- och leverantörsrelationer.

Om en organisation identifierar risker inom ICT-leverantörskedjan, så bör säkerhetsåtgärder väljas så att dessa risker begränsas, eventuellt med utökade säkerhetsåtgärder för att säkerställa att organisationen tar tillräcklig hänsyn till riskerna. Avsnitt 5.5 behandlar tillämpning av informationssäkerhetsåtgärder. Bilaga B mappar specifika informationssäkerhetsåtgärder mot de individuella livscykelprocesserna i avsnitt 6.

Leverantörer kan genom efterlevnad av ISO/IEC 27001 bevisa för beställare att de håller en viss nivå av stringens.

När beställare och leverantörer inför ett LIS enligt ISO/IEC 27001, så bör informationen som tas fram användas för att kommunicera statusen för styrning av informationssäkerhet mellan beställaren och leverantören. Detta kan inkludera:

a) omfånget för LIS,

b) uttalande om tillämplighet,

c) rutiner för riskanalyser,

d) revisionsplan,

e) medvetenhetsprogram,

f) incidenthantering,

g) mätprogram,

h) informationsklassningsmodell,

i) förändringshantering,

j) andra relevanta säkerhetsåtgärder som har vidtagits.

5.7 Informationssäkerhetsåtgärder från LIS relaterade till ICT-leverantörskedjan

ISO/IEC 27002 inkluderar ett antal säkerhetsåtgärder som specifikt riktar sig mot externa parter, inklusive leverantörer. Avsnitt 15 i ISO/IEC 27002 ger särskild vägledning för leverantörsrelationer. Dessa och ytterligare utökade säkerhetsåtgärder kan användas i livscykelsammanhang för att hjälpa beställare att validera särskild leverantörspraxis så att informationssäkerhet för beställarens information och informationssystem säkerställs.

Bilaga B mappar specifika säkerhetsåtgärder från ISO/IEC 27002 mot individuella livscykelprocesser.