Myndigheten för samhällsskydd och beredskap

Terminologi och begrepp inom informationssäkerhet

Hur man skapar en språkgemenskap

MSB:s kontaktpersoner:
Tom Andersson, 010-240 42 10

Publikationsnummer MSB976 - februari 2016
ISBN 978-91-7383-644-9

Förord

Syftet med den här studien är att utvärdera svensk terminologi på informationssäkerhetsområdet med fokus på frågor om målgrupper och grundläggande begrepp. Denna rapport redovisar målgruppsstrategier för ett löpande terminologiarbete baserat på en fallstudie där experter från olika yrkeskategorier har fått definiera en uppsättning grundläggande begrepp.

Studien är finansierad och gjord på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB). Studien har genomförts av docent Annika Andersson, professor Karin Hedström och professor Fredrik Karlsson från Handelshögskolan, Örebro universitet.

Innehållsförteckning

Sammanfattning

Syftet med den här studien är att utvärdera svensk terminologi på informationssäkerhetsområdet med fokus på frågor om målgrupper och grundläggande termer. Baserat på en Delphi-studie, där experter från olika yrkeskategorier har fått definiera en uppsättning grundläggande begrepp, har vi utvärderat både experternas definitioner och processen med att ta fram definitionerna. Vi har identifierat flera problem med svensk terminologi på informationssäkerhetsområdet. För att stödja arbetet med att utveckla svensk terminologi för informationssäkerhet beskriver vi i rapporten förslag på hur arbetet kan bedrivas vidare. De problem vi har identifierat är bl.a. att begrepp som inte finns med i rådande styrdokument blir otydliga och svårtolkade för experter inom området och att det är problematiskt med två olika styrdokument (HB550 och SIS-TR50:2015) i användning med delvis olika definitioner av samma begrepp. Vi har även sett att olika yrkeskategorier ofta definierar begreppen utifrån sin specifika profession, vilket kan innebära att det finns ett behov av att säkerhetsbegrepp kontextualiseras utifrån yrkesroller. Processen med att arbeta med experter enligt Delphi-metoden gav ett bra underlag för att analysera och diskutera olika definitioner av centrala begrepp inom informationssäkerhetsområdet. Dessutom har experterna varit mycket engagerade i processen. Vi föreslår att framtida begreppsutredningar använder sig av denna metod eller varianter av den och att det är experterna, de som i sitt dagliga yrke handhar informationssäkerheten, som ska vara de som skapar definitionerna. Vi ser också ett stort behov av större, effektivare och mer samordnade former för framtida begreppsutredningar.

1. Inledning

1.1 Bakgrund och syfte

Syftet med den här studien är att utvärdera svensk terminologi på informationssäkerhetsområdet med fokus på frågor om målgrupper och grundläggande begrepp. Denna rapport redovisar målgruppsstrategier för ett löpande terminologiarbete baserat på en fallstudie där experter från olika yrkeskategorier har fått definiera en uppsättning grundläggande begrepp.

De styrdokument för definitionerna vi har använt oss av är SIS handbok HB550 (SIS, 2013) och SIS tekniska rapport SIS-TR 50:2015 (SIS, 2015). HB550 utvecklades mellan år 2000 och 2003 som ett internt projekt inom SIS/TK 456 Informationsskydd och -säkerhet, och med stöd av TK318 och Terminologicentrum (TNC). Den utgåva vi har använt oss av under analysen är nr. 3 från 2011. Handbokens målgrupp är "personer med intresse för informationssäkerhetsområdet, t.ex. i samband med användning, upphandling, specifikation av såväl dator- och kommunikationssystem som enskilda säkerhetsprodukter. Den är också tänkt att kunna användas i utbildningssammanhang" (SIS, 2013, s. 3).

SIS-TR 50:2015 (SIS, 2015) utvecklades 2014 som ett internt projekt inom SIS/TK 318 vilket också fick stöd från TNC. Detta nya styrdokument har utgått från HB550, men nya begrepp har tillkommit och andra har reviderats. Det har även lagts till en ny del som ger en översikt av internationella standarder. Tanken med SIS-TR 50:2015 (SIS, 2015) är att den ska ersätta HB550 (SIS, 2013), men vid studiens ingång så salufördes båda dokumenten av SIS och båda används i praktiken[1]. Vad gäller de definitioner som finns i HB550 (SIS, 2013) och SIS-TR 50:2015 (SIS, 2015) så har vi även jämfört dessa med de engelska begrepp som ISO använder. Vi har utgått från SS-ISO IEC 27000:2014 - "Information technology - Security techniques - Information security management systems - Overview and vocabulary" (ISO, 2014), samt webbtjänsten "ISO concept database"[2] som ISO tillhandahåller.

[1] Under studiens gång plockade SIS bort HB550 för försäljning – något vi även hade tänkt rekommendera i rapporten.
[2] https://www.iso.org/obp/ui/

2. Genomförande av fallstudien

2.1 Delphi-metoden

Den här studien bygger på en Delphi-metod (Delbecq, Van de Ven, & Gustafson, 1975; Schmidt, 1997; Schmidt, Lyytinen, Keil, & Cule, 2001). Delphi-metod används för att förutsäga, identifiera och prioritera olika aspekter, vilket sedan ligger till grund för konceptuell och teoretisk utveckling. En Delphi-undersökning innebär att frågor ställs till experter i omgångar vid olika tillfällen. I vårt fall har vi använt Delphi-metoden för att låta experter inom olika yrkeskategorier definiera centrala begrepp inom informationssäkerhet. Delphi-metoden anses vara mycket användbar för forskning om beslutsfattande när det är brist på enighet eller samsyn, eller där den gemensamma kunskapsbasen är ofullständig (Delbecq et al., 1975). Metoden har använts mycket frekvent inom informatikforskning (Okoli & Pawlowski, 2004). Ett sådant exempel är studier där forskare velat förutse förändringar inom affärsområden, då de försökt identifiera kritiska faktorer för systemutveckling eller tagit fram modeller för organisatoriska förändringsstrategier (Okoli & Pawlowski, 2004).

Vi baserar oss på Schmidt et al. (2001) som utgångspunkt för designen av den här undersökningen. Datainsamlingen och analysen grundas på Schmidt (Schmidt, 1997; Schmidt et al., 2001) och vi delar in Delphi-metoden i fyra faser, vilka presenteras närmare i Tabell 1.

Fas	**Beskrivning**
1. Val av deltagare och uppbyggnad av paneler	Experterna delas in i paneler som ska arbeta med begreppen. Indelningen görs baserat på yrkeskategori.
2. Ta fram de viktigaste informationssäkerhetsbegreppen	Varje paneldeltagare rankar de fem viktigaste informationssäkerhetsbegreppen baserat på en lista som tidigare tagits fram i samarbete med Myndigheten för samhällsskydd och beredskap (MSB).
3. Beskriva och ge definitioner på de framtagna säkerhets-begreppen	Varje paneldeltagare definierar de fem mest centrala begreppen inom informationssäkerhet (de begrepp som blev resultatet av fas 2).
4. Samsyn och konsensus kring definitionerna av begreppen	Feedback och återkoppling från paneldeltagarna avseende de definitioner som de olika paneldeltagarna har gett samt rankning av den mest lämpliga definitionen.

Tabell 1. Delphi-studiens fyra faser.

Under den första fasen grupperade vi experterna i panelgrupper. I den andra fasen tog vi fram de begrepp som panelgrupperna skulle arbeta vidare med. Den tredje fasen handlar om att beskriva och definiera de centrala begreppen, och den fjärde och sista fasen handlar om att utveckla samsyn och konsensus kring definitionerna av de ingående begreppen.

2.1.1 Fas 1: Val av deltagare och uppbyggnad av paneler

En Delphi-studie bygger på experter som deltar i paneler och förlitar sig på den insikt, kompetens och erfarenhet som paneldeltagarna innehar. Att välja ut rätt experter att delta anses vara den mest kritiska delen när en Delphi-studie genomförs (Okoli & Pawlowski, 2004). Delbecq et al. (1975) förespråkar att paneldeltagare väljs baserat på att de: 1) känner sig personligt engagerade i det undersökta problemet; 2) har relevant information att delge; 3) är tillräckligt motiverade för att genomföra sin del av studien, och 4) att de känner att resultatet av studien är värdefullt för dem.

Urvalet av paneldeltagare för denna studie skedde i samråd med Myndigheten för samhällsskydd och beredskap (MSB). Inbjudan till att delta i studien skickades ut till statliga myndigheter, landsting, kommuner samt relevanta nätverk och föreningar. Inbjudan låg även öppen på MSB:s hemsida där ett antal privata aktörer anmälde sig. För att delta använde vi kriteriet att deltagarna skulle ha minst ett års erfarenhet av arbete med frågor om informationssäkerhet, dataskydd, systemsäkerhet, IT-säkerhet, säkerhetsfrågor i informationsförvaltning eller informationshantering. Sammanlagt anmälde sig 85 personer till att delta i studien och efter det första utskicket var 74 deltagare aktiva. Panelerna byggdes upp efter deltagarnas expertkunskap, och totalt 64 personer svarade på enkäterna. För att kunna sortera deltagarna baserat på deras expertis/yrkesroll så gick vi ut med en fråga om vilka typer av säkerhetsfrågor deltagarna arbetat mest med. Detta gjorde vi för att få så homogena paneler som möjligt. Enligt Delbecq et al. (1975) räcker det om panelen består av 10-15 deltagare om gruppen är homogen. Vi valde dock att i de flesta fall ha färre deltagare i våra paneler för att minska arbetsbördan och tidsåtgången för deltagarna när de skulle arbeta med panelens samtliga definitioner. I en panel om sju experter där fem begrepp ska definieras blir det totalt 35 definitioner (7 experter x 5 begrepp) att arbeta med. Tabell 2 visar de yrkesgrupper som deltog, antalet paneler inom varje yrkesgrupp, samt hur många deltagare varje panel bestod av.

Yrkesområde	Paneler	Antal
Juridik och regelverk	Panel J:1	7
	Panel J:2	7
Informationsförvaltning och dokumenthantering	Panel I:1	7
	Panel I:2	7
Systemutveckling och förvaltning	Panel S:1	7
Säkerhetsteknik	Panel T:1	11
Ledning och samordning	Panel L:1	7
	Panel L:2	7
	Panel L:3	7
	Panel L:4	7

Tabell 2. Paneler och antal deltagare under studien.

2.1.2 Fas 2 till 4: Datainsamling

Syftet med Delphi-studien var att få beslutsunderlag för myndighetssamordning av insatser om svensk terminologi inom informationssäkerhet. Med bakgrund i detta fick experterna välja ut vad de ansåg vara de mest centrala begreppen inom informationssäkerhetsområdet. Därefter har experterna tillhandahållit oss definitioner av dessa begrepp som input för en kvalitativ analys.

Under tidsperioden 2015-09-30 till 2015-10-28 genomfördes faserna 2 till 4, där en internetbaserad enkät distribuerades till experterna i varje fas. Experterna hade cirka tio dagar på sig att genomföra respektive fas, och en påminnelse per enkät skickades ut. I den första fasen fick experterna ranka de fem viktigaste begreppen inom informationssäkerhet, begrepp som de senare skulle arbeta med att definiera. Denna rankning gjordes utifrån en lista med begrepp som 18 experter inom informationssäkerhetsområdet rankat fram som de tio viktigaste informationssäkerhetsbegreppen under ett terminologipass på konferensen ”Informationssäkerhet för offentlig sektor”[3]. De begrepp experterna valde ut var: ansvar, informationsklassning, informationssäkerhet, konfidentialitet, riktighet, risk, sekretess, spårbarhet, säkerhet, och tillgänglighet.

Dessa tio begrepp gick ut till samtliga deltagare i Delphi-studien som rankade vilka fem av dessa som de skulle jobba vidare med i panelerna. Rankingen gjordes genom att experterna fick poängsätta begreppen med värden från ett till tio. Resultatet av rankningen i fas 2 presenteras i Tabell 3. Rangordningen är gjord fallande, där medelvärde är avrundat till närmsta tiondel.

[3] https://www.msb.se/sv/Start1/Kalender/Konferens-Informationssakerhet-for-offentlig-sektor-1-2-september-2015/

Ranking	Begrepp	Medelvärde
1	Informationssäkerhet	7,7
2	Ansvar	6,4
3	Tillgänglighet	6,2
4	Informationsklassning	6,1
5	Risk	5,6
6	Riktighet	5,5
7	Säkerhet	5,5
8	Sekretess	5,5
9	Konfidentialitet	4,2
10	Spårbarhet	3,0

Tabell 3. Rankade begrepp efter fas 2.

De begrepp som vi gick vidare med till tredje fasen var de fem högst rankade: informationssäkerhet, ansvar, tillgänglighet, informationsklassning och risk. Den andra enkäten bestod av en lista som innehöll dessa fem begrepp där vi bad paneldeltagarna att definiera dem. Då vi var intresserade av hur deltagarna definierar dessa begrepp i sin arbetssituation så ställde vi frågan utifrån hur de skulle definiera dem för en nyanställd person.

I studiens fjärde fas distribuerade vi paneldeltagarnas definitioner till hela panelen och bad dem att ranka vilken definition som de ansåg vara mest lämplig. Experterna fick ange sitt första-, andra- och tredjehandsval för varje begrepp. I enkäten erbjöds deltagarna även möjlighet att kommentera den genomförda rankningen och/eller göra andra förtydliganden i en kommentarruta.

Sammantaget så har svarsfrekvensen varit hög. Sett till hela studien var 75 % (64 av 85 experter) av de som anmälde sig till studien aktiva genom de flesta faserna av datainsamlingen. Tabell 4 visar svarsfrekvensen för varje fas. För den andra fasen var svarsfrekvensen 87 %, och för de två efterföljande faserna var svarsfrekvensen 86 %. Detta visar att paneldeltagarna har varit mycket engagerade genom hela studien.

Fas	Enkät	Svarsfrekvens
2	Enkät 1 - Fackspråk på Informationssäkerhetsområdet, ranking av initiala begrepp	87 % (74 svar av 85 utskick)
3	Enkät 2 - Fackspråk på Informationssäkerhetsområdet, definiera begrepp	86 % (64 svar av 74 utskick)
4	Enkät 3 - Fackspråk på Informationssäkerhetsområdet, ranking av definitioner	86 % (64 svar av 74 utskick)

Tabell 4. Total svarsfrekvens under studien.

Tabell 5 visar detaljer över svarsfrekvensen för de olika yrkesgrupperna efter sista svarsomgången. Experterna inom yrkeskategorin

”Informationsförvaltning och dokumenthantering” uppnår högst svarsfrekvens med 100 %, och den lägsta (men fortfarande höga) svarsfrekvensen med 73 % återfinns i yrkeskategorin ”Säkerhetsteknik”.

Yrkeskategori	**Svarsfrekvens**
Informationsförvaltning och dokumenthantering	100 % (14 svar från 14 deltagare)
Ledning och samordning	89 % (25 svar från 28 deltagare)
Systemutveckling och förvaltning	86 % (6 svar från 7 deltagare)
Juridik och regelverk	79 % (11 svar från 14 deltagare)
Säkerhetsteknik	73 % (8 svar från 11 deltagare)

Tabell 5. Svarsfrekvens för varje yrkeskategori i sista svarsomgången.

2.2 Analys

Varje fas i datainsamlingen kopplades till en separat analys. Analysen i fas 2 syftade till att bestämma vilka begrepp som skulle ingå i den fortsatta studien. För detta ändamål beräknade vi medelvärdet baserat på de poäng som deltagarna hade gett de olika begreppen. De fem begrepp med högst medelvärde gick vidare till fas 3. Resultatet av den analysen är presenterad i Tabell 3.

Under den tredje fasen samlade vi ihop de begreppsdefinitioner som varje paneldeltagare gett och distribuerade dem till samtliga paneldeltagare. Detta innebar att en panel bestående av sju paneldeltagare fick ta ställning till 35 olika definitioner (7 experter x 5 begrepp). I den här fasen bestod analysen av att säkerställa att endast text rörande definitionerna gick vidare till nästa fas.

Analysen i den fjärde fasen syftade till att ta fram de högst rangordnade definitionerna i respektive panel, samt att genomföra jämförande analyser. För den första delen av analysen använde vi en metod där vi gav varje deltagares förstahandsval 3 poäng, andrahandsval 2 poäng och tredjehandsval 1 poäng. Därefter summerades poängen för varje definition. Således fick den definition som experterna föredrog mest högst poäng. I de fall där två definitioner fick samma poängsumma valdes den definitionen som hade flest förstahandsval. På så vis erhölls en definition per panel som användes för de jämförande analyserna. För den som är intresserad av att ta del av samtliga föreslagna definitioner och dess rankning inom varje panel så återfinns dessa i Bilaga 1.

De innehållsmässiga analyserna var av tre typer. Den första analysen handlade om att jämföra begreppsdefinitioner inom yrkeskategorin, d.v.s. att analysera om och i vilken grad definitionen av ett specifikt begrepp är samstämmigt eller ej inom en viss yrkeskategori. Den andra typen av analys handlade om att

jämföra definitioner mellan olika yrkeskategorier. Den tredje och sista analysen fokuserade jämförelse mellan de olika yrkeskategorierna och SIS:s begreppsdokument HB550 (SIS, 2013) och SIS-TR 50:2015 (SIS, 2015). I samtliga dessa analyser arbetade vi med det textuella innehållet för att avgöra skillnader i hur yrkeskategorierna samt varje panel avgränsade begreppen.

För att få ett mått på hur överens experterna var inom de olika panelerna avseende den högst rankade definitionen skapade vi måttet grad av konsensus. Måttet är beräknat på hur många procent av den teoretiska max-poängen som den högst rankade definitionen hade. Den teoretiska max-poängen är 3 poäng (högst betyg) x antal paneldeltagare som utdelat poäng. En högre procentsats för definitionen betyder då att fler var nöjda med definitionen.

Slutligen genomfördes en jämförelse mellan definitionerna i de svenska styrdokumenten och de som används internationellt, i det här fallet de som ges ut av ISO (ISO, 2014). Även här arbetade vi med det textuella innehållet för att avgöra hur begrepp avgränsades samt vilka aspekter som lyftes fram (Bilaga 2).

3. Resultat

Vi kommer att beskriva resultatet i tre delar. Först analyserar vi innehållet i panelernas definitioner och jämför dessa med definitionerna i HB550 (SIS, 2013) och SIS-TR 50:2015 (SIS, 2015). Därefter analyserar vi graden av konsensus inom panelerna och yrkesgrupperna vad gäller de olika definitionerna. Den tredje delen rör styrdokumenten i relation till internationellt språkbruk. Avslutningsvis reflekterar vi kring själva processen med att ta fram definitioner i en Delhi-studie och hur den fungerade.

3.1 Innehållsmässig analys av definitionerna

Nedan följer den innehållsmässiga analysen av de högst rankade definitionerna, där jämförelser görs med definitionerna i HB550 (SIS, 2013) och SIS-TR 50:2015 (SIS, 2015). I Bilaga 3 finns en lista över dessa definitioner och en jämförelse över hur väl de matchar mot centrala begrepp i de båda styrdokumenten. Intressant att notera är även att två av begreppen som panelerna hade valt ut som centrala – ”informationsklassning” och ”ansvar” – inte finns beskrivna i varken HB550 (SIS, 2013) eller SIS-TR 50:2015 (SIS, 2015). När det gäller ”ansvar” finns det liknande begrepp att luta sig emot (se diskussion nedan). För begreppet ”informationsklassning” finns det dock ingen motsvarighet till detta i de undersökta styrdokumenten.

3.1.1 Informationssäkerhet

I HB550 definieras informationssäkerhet som ”säkerhet för **informationstillgångar** avseende förmågan att upprätthålla önskad **konfidentialitet**, **riktighet** och **tillgänglighet** (även **ansvarighet** och **oavvislighet**)” (SIS, 2013). I SIS-TR 50:2015 beskrivs informationssäkerhet som ”bevarande av **konfidentialitet, riktighet** och **tillgänglighet** hos **information”** (SIS, 2015).

Konfidentialitet, riktighet och tillgänglighet återkommer också i de flesta panelers definitioner. Ett exempel är följande:

> *”Informationssäkerhet är de åtgärder som vidtas för att förhindra att information: görs tillgänglig för eller i övrigt kommer obehöriga till del (konfidentialitet), förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning (riktighet), och information ska kunna utnyttjas i förväntad utsträckning och inom önskad tid (tillgänglighet)”.* (Ledning och samordning, L:4)

Det enda av dessa kriterier som någon gång fallit bort är ”tillgänglighet”. Detta har hänt i en panel med experter från ”Informationsförvaltning och dokumenthantering” och en från ”Ledning och samordning”. Dessa definitioner har fokuserat mer på hotet och att skydda:

> *”Systematisk planering för att information ska skyddas mot obehörig åtkomst (både intrång av extern part och behörighetsstyrning inom organisationen) samt mot förvanskning (d.v.s. informationens autenticitet garanteras)”.* (Informationsförvaltning och dokumenthantering, I:2)

> *”Samtliga tekniska och regelmässiga åtgärder som skyddar organisationens information”.* (Ledning och samordning, L:2)

Att definiera informationssäkerhet som mer än bara teknik är något som lyfts fram tydligt i kommentarerna till definitionerna av informationssäkerhet i både HB550 (SIS, 2013) och SIS-TR 50:2015 (SIS, 2015). Detta sätt att tänka lyfts också av flera av panelerna, där det i flera av definitionerna trycks på att informationssäkerhet gäller både manuella och digitala system. Utöver detta påpekar flera paneler att informationssäkerhet gäller både de tekniska delarna såväl som de administrativa:

> *”Informationssäkerhet är den övergripande säkerheten som omfattar både tekniskt (IT-säkerhet) och administrativt (regler och rutiner) skydd och syftar till att informationen alltid skall vara korrekt, tillgänglig som avsett och skyddad från obehörigt tillträde”.* (Säkerhetsteknik, T:1)

En övergripande reflektion från vår sida vad gäller definitionerna av informationssäkerhet är huruvida det är ”information” eller ”informations**tillgångar**” som är i fokus. I HB550 (SIS, 2013) handlar informationssäkerhet om att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet hos informationstillgångar. Det är en skillnad gentemot SIS-TR 50:2015 (SIS, 2015), där samma formulering finns, men då för ”information”. Vi menar att informationstillgångar skiljer sig åt från information, där begreppet informationstillgångar tydligare pekar på information som är skyddsvärd. Enbart för att information finns inom en organisation behöver den inte vara en tillgång eller ha ett skyddsvärde. Dessutom kan ”informationstillgångar” även inkludera de resurser som tillhandahåller informationen. Panel J:2, i yrkeskategorin ”Juridik och regelverk” skriver att ”… med informationstillgångar avses all information och informationshanterande resurser såsom manuella och IT-baserade informationssystem”. Citatet illustrerar hur all information ses som informations-tillgångar, och vi ser därför ett behov av att problematisera, och framförallt skilja på, begreppen ”information” och ”informationstillgångar”. Detta skulle driva fram en diskussion om vilken information som är skyddsvärd och därmed ligga till grund för olika typer av prioriteringar av arbetet med informationssäkerhet.

3.1.2 Ansvar

”Ansvar” som enskilt begrepp finns inte definierat i vare sig HB550 (SIS, 2013) eller SIS-TR 50:2015 (SIS, 2015). I HB550 (SIS, 2013) finns begreppet

”ansvarighet” definierat och i SIS-TR 50:2015 (SIS, 2015) finns begreppet ”ansvarsskyldighet”.

”Ansvarighet” enligt HB550 innebär ”att en individ givits och påtagit sig visst ansvar och att därvid denne i efterhand kan ställas till svars för sitt handlande” (SIS, 2013). Det handlar således om en princip kopplad till individ, en människa, som också kan komma att stå till svars för sitt handlande. På liknande sätt har SIS-TR 50:2015 definierat ”ansvarsskyldighet” som ”principen att stå till svars och ta ansvar för **konsekvenserna** av beslut och aktiviteter inför **organisationens styrande organ,** rättsliga myndigheter och inför **intressenter** i allmänhet” (SIS, 2015). Ansvar i dessa dokument är m.a.o. kopplat till frågan om skyldigheten att ta på sig skulden om något inte blir rätt utfört. Vikten av att något blir rätt utfört, eller vad som innebär med ”rätt utfört”, är m.a.o. inte kopplat till ansvar i ovanstående styrdokument. Vad som är att anse som ”rätt utfört” är således något som måste definieras inom varje organisation, och en diskussion som ständigt bör vara aktuell.

I samtliga definitioner som panelerna har gett har de sett att ”ansvar” är kopplat till en individ eller mer specifikt till en viss roll, exempelvis enligt följande:

> *”Person eller funktion inom organisationen som har en roll att genomföra vissa specifika aktiviteter eller att följa upp att vissa specifika aktiviteter blir genomförda”.* (Informationsförvaltning och dokumenthantering, I:2)

> *”Ansvar tilldelas en person eller roll och innebär att denne är ålagd att tillse att arbetet sker enligt de regler som har fastställts och innebär att personen/rollen också har mandat att fatta beslut och leda arbetet inom ansvarsområdet”.* (Säkerhetsteknik, T:1)

Vad gäller att stå till svars för sitt handlande så var det bara två paneler (en från ”Ledning och samordning” och en från ”Juridik och regelverk”) som enades om en sådan definition. Ett exempel är:

> *”Skyldighet att se till att något utförs på angivet sätt inom ett avgränsat område. Till ansvaret hör befogenheter och beslutsmandat samt att stå till svars för om något inte utförts på angivet sätt”.* (Ledning och samordning, L:1)

Det är många experter som kommenterat att ”ansvar” i sig är ett ganska abstrakt och komplicerat begrepp, och att det var svårt att definiera för ”det beror på”. Ett exempel på en sådan kommentar är:

> *”Frågan är lurig och, vill jag påstå, lite dåligt ställd. Avses "ansvar" som begrepp i största allmänhet? Eller i ett visst sammanhang? Jag har bara hittat en definition som jag tycker ramar in vad ansvar innebär. Den är rankad som nr 1. Inga andra passar alls om inte frågan förtydligas. Ett (ännu bättre) alternativ till är: "Skyldighet att*

> *vara den som ser till att något blir rätt utfört (och får ta på sig skulden om så inte blir fallet)" (Hämtat från Wikipedia)".* (Ledning och samordning, L:2)

Ytterligare en indikation på att begreppet upplevs som abstrakt och komplext kan vara att två experter i panelen Ledning och samordning L:4 hoppade över att definiera detta begrepp, vilket kan jämföras med att samtliga experter annars skrivit något om alla andra begrepp. Det kan alltså finnas anledning att inkludera, och tydligt definiera, begreppet ”ansvar” i styrdokumenten. Begrepp som inte finns med i rådande styrdokument blir otydliga och svårtolkade för experter inom området.

3.1.3 Tillgänglighet

I HB550 definieras ”tillgänglighet” som ett ”[s]kyddsmål där **informationstillgångar** skall kunna utnyttjas i förväntad utsträckning och inom önskad tid” (SIS, 2013). Tillgänglighet handlar alltså om både *utsträckning* (mängd) och om *tid*. Även i SIS-TR 50:2015 finns tidsaspekten med, men med ett tillägg om *vem* (behörig) som ska ha åtkomst: ”**åtkomst** för behörig person vid rätt tillfälle” (SIS, 2015). De flesta paneler följer i stora drag definitionen i HB550 (SIS, 2013), även om tre paneler inte nämner tidsaspekten i sina definitioner. Att åtkomsten ska gälla *behörig* person lyfts av experterna från ”Ledning och samordning” och ”Informationsförvaltning och dokumenthantering”. Ett exempel är:

> *”Tillgång till informationstillgång(ar) för **behöriga** användare i förväntad utsträckning och inom önskad tidsrymd”.*
> (Informationsförvaltning och dokumenthantering, I:1)

En intressant möjlig utvidgning av begreppet ”tillgänglighet” görs av en panel med experter från ”Ledning och samordning”. Förutom utsträckning och tid så lägger de till plats – d.v.s. *var* behöriga har tillgång till dessa informationstillgångar:

> *”I informationssäkerhetssammanhang avses [tillgänglighet] möjlighet att komma åt information när och **där** den behövs”.*
> (Ledning och samordning, L:4)

Att panelen lägger till i definitionen att behöriga ska kunna komma åt informationen *där* den behövs kan indikera ett förtydligande som kan behövas i dagens samhälle med mobila enheter och t.ex. ambulerande sjukvårdspersonal.

I arbetet med att definiera ”tillgänglighet” syns det tydligt att den profession experterna har påverkar hur de talar om begreppet och vilka aspekter i definitionen de anser är viktiga att lyfta fram. Ett sådant exempel är hur yrkeskategorierna ”Säkerhetsteknik” och ”Systemutveckling och förvaltning” trycker på kriterier som liknar klassisk användbarhet och design. Experterna från ”Systemutveckling och förvaltning”, S:1, nämner att informationen ska

”vara åtkomlig på ett enkelt sätt” och experterna på säkerhetsteknik, T:1, uttrycker vikten av att ”informationen är nå- och användningsbar”. Vidare lyfter experterna i panel I:2, från ”Informationsförvaltning och dokumenthantering”, fram vikten av att information har ”bibehållen kvalitet och autenticitet”, något som är centralt sett till att informationen ska kunna hämtas fram efter lång tids arkivering.

Vi kan också se att experterna inom yrkeskategorin ”Juridik och regelverk” håller sig relativt nära definitionerna som återfinns i HB550 (SIS, 2013) respektive SIS-TR 50:2015 (SIS, 2015), vilket följer den specifika professionens logik där definitioner ses som en del av ett regelverk. Panel J:1 i yrkeskategorin ”Juridik och regelverk” definierar ”tillgänglighet” som ”att beskriva i vilken grad användare kan nå önskad information vid ett givet tillfälle eller tidpunkt”, och panel J:2 definierar begreppet enligt följande: ”[m]ed tillgänglighet menas att informationstillgångar kan nyttjas efter behov i förväntad utsträckning och inom önskad tid”.

3.1.4 Informationsklassning

Begreppet ”informationsklassning” finns inte definierat i vare sig HB550 (SIS, 2013) eller SIS-TR 50:2015 (SIS, 2015). Det är nog anledningen till att panelernas definitioner varierat mycket och att definitionerna ofta är ganska svävande. När vi sökt på SIS och ”informationsklassning” så finns ett dokument från konferensen ”Rätt säkerhet” från 2009 (Veriscan, 2009). I detta dokument framgår det att ”[k]lassning är sätt att bedöma vilken nivå av skydd som är lämpligt med tanke informations värde och de hot som omger den” och att de kriterier som ska ingå i informationsklassning är sekretess, tillgänglighet, spårbarhet och riktighet. Dessa kriterier har flera av panelerna fått med, men många definitioner är mer vaga. Panel I:2 med experter inom ”Informationsförvaltning och dokumenthantering” skriver exempelvis:

”För mig är informationsklassning två begrepp: 1. Klassning efter ämne t.ex. i en diarieplan eller kontoplan, 2. Säkerhetsklassning, dvs. vem som ska tillgång till vilken information och hänger samman med sekretessregler.”
(Informationsförvaltning och dokumenthantering, I:2)

Av citatet framgår att det inte är entydigt vad som menas med informationsklassning och stor vikt läggs vid just sekretess. En annan expert svarade att ”jag har ingen aning”. Ytterligare ett belägg för svårigheten att definiera begreppet syns i definitionen från panel L:3 med experter från yrkeskategorin ”Ledning och samordning”. De ger en längre definition, vilket ger vid handen att de olika aspekterna behöver förtydligas:

> *”Informationsklassning är ett sätt att säkerställa att information erhåller en lämplig skyddsnivå med hänsyn tagen till informationens värde och de risker som omger den. Information klassas i termer av rättsliga krav, värde, verksamhetsbetydelse och känslighet för obehörigt röjande eller modifiering. Som hjälp används kriterierna konfidentialitet, riktighet, spårbarhet och tillgänglighet. Med*

> *konfidentialitet avses att informationen inte får göras tillgänglig eller avslöjas för obehöriga. Med riktighet avses att informationen inte ska kunna förändras och förvanskas av misstag eller av någon obehörig. Med tillgänglighet avses att informationen ska finnas till hands för behöriga användare då den behövs. Resultatet från de olika klassificeringarna skall utgöra det samlade kravet på nivån för skyddet av den aktuella informationen eller IT-systemet".* (Ledning och organisation, L:3)

Detta är ett exempel på hur flera experter har ett behov av att förtydliga och exemplifiera och kontextualisera de informationssäkerhetsbegrepp de använder. Vidare ser vi ett gemensamt mönster tillsammans med de svårigheter experterna hade att definiera begreppet ”ansvar”. När begrepp inte finns med i styrdokumenten blir de otydliga och svårtolkade. Således finns här ett behov av att inkludera, och tydligt definiera ”informationsklassning” i styrdokumenten.

De tydligaste definitionerna av ”informationsklassning” kom, inte så överraskande, från panelerna med experter som ofta jobbar med denna aktivitet, såsom yrkeskategorierna ”Säkerhetsteknik” och ”Systemutveckling och förvaltning”. Ett sådant exempel är:

> *”Informationsklassning är en process som syftar till att bedöma informationens värde och skyddsbehov så att rätt åtgärder kan vidtas för att informationen skall få rätt hantering och skydd".* (Säkerhetsteknik, T:1)

3.1.5 Risk

I HB550 definieras risk som en ”kombination av sannolikheten för att ett givet **hot** realiseras och därmed uppkommande **skadekostnad**” (SIS, 2013). Risk sätts alltså i samband med sannolikheten för att något ska ske och här nämns även de negativa effekterna – den ”uppkommande skadekostnaden”. I SIS-TR 50:2015 definieras risk som ”osäkerhetens effekt på **mål**” (SIS, 2015) och förtydligar då att risk, hot och kostnad måste ställas i förhållande till vilka mål en organisation har.

Vad gäller panelernas definitioner av risk så är de alla, förutom panelen S:1 inom yrkeskategorin ”Systemutveckling och förvaltning”, starkt kopplade till definitionen i HB550. Även om definitionerna inte är exakt ordagranna så är relationen tydlig, exempelvis:

> *”En sammanvägning av sannolikheten för att en händelse ska inträffa och de konsekvenser händelsen kan leda till".* (Informationsförvaltning och dokumenthantering, I:1)

och

> *”Risk är sannolikheten för att en oönskad händelse inträffar och konsekvenserna som detta i så fall skulle innebära”.* (Juridik och regelverk, J:2)

Den panel som avviker var S:1, från ”Systemutveckling och förvaltning”. I denna panel ges följande:

> *”[r]isk beskriver i vilken grad information, fysiska objekt, personal och omgivning kan råka ut för olika hot, som på något sätt skadar, förändrar eller förstör objektet.”*

Fokus i ovanstående definition är på hot och skador, men de har inte kopplat risk till *sannolikheten* av att det kan hända. En annan skillnad i definitionernas formulering är hur de fyra panelerna med Ledning och samordning ger beskrivningar med mer processfokus. De beskriver risk som i innebörden ”riskanalys”. Ett exempel är följande:

> *”Säkerhets**arbetet** [vår fetning] är riskbaserat. Det innebär att skyddsåtgärder regelbundet ska bedömas och anpassas utifrån hur verksamheten förändras eller när det uppstår ändrade förutsättningar i omvärlden (både internt som externt) som har eller kan ha påverkan”. (Ledning och samordning, L:3)*

Kopplingen till mål, som görs i SIS-TR 50:2015 (SIS, 2015) har endast en panel, L:1 från ”Ledning och samordning, nämnt. Det innebär att experterna i övriga paneler mer kopplar ”risk”-begreppet till hur riskanalyser genomförs, och inte till affärs- och verksamhetsvärden som ska uppnås. Exempel på denna mer operationella syn på risk syns i ordval såsom ”sammanvägning”, ”risk är sannolikheten” och ”i vilken grad” vilket går att knyta till arbetet med att göra riskbedömningar.

3.2 Grad av konsensus mellan definitionerna, panelerna och yrkeskategorierna

Till att börja med kan vi konstatera att av 64 experter som har gett definitioner av de fem begreppen så fann vi inga dubbletter, även om flera definitioner är snarlika. Det innebär att vi har 64 olika definitioner av samma begrepp (se Bilaga 1).

En analys av måttet grad av konsensus för varje begrepp och varje panel visar att det egentligen inte finns konsensus i begreppets sanna innebörd, d.v.s. att det finns övervägande enighet mellan deltagarna i en panel. Tabell 6 visar resultaten för respektive panel och begrepp, och där är graderna av konsensus relativt låga. I tabellen indikerar en högre procentsats en högre grad av enighet inom respektive panel.

Yrkeskategori	Panel	Grad av konsensus för begrepp				
		Informations-säkerhet	Ansvar	Tillgänglighet	Informations-klassning	Risk
Informationsförvaltning och dokumenthantering	I:1	76 %	48 %	48 %	57 %	52 %
	I:2	62 %	43 %	71 %	52 %	86 %
Ledning och samordning	L:1	76 %	62 %	67 %	48 %	57 %
	L:2	62 %	52 %	62 %	57 %	52 %
	L:3	61 %	67 %	61 %	67 %	78 %
	L:4	53 %	47 %	40 %	67 %	40 %
Systemutveckling och förvaltning	S:1	44 %	67 %	56 %	67 %	50 %
Juridik och regelverk	J:1	92 %	75 %	92 %	92 %	83 %
	J:2	62 %	76 %	57 %	52 %	52 %
Säkerhetsteknik	T:1	62 %	75 %	75 %	83 %	67 %

Tabell 6. Grad av konsensus för varje enskilt begrepp baserat på de olika panelerna

De delvis låga graderna av konsensus kan hänföras till den metodmässiga begränsningen i studien, där fler iterationer kunde ha ökat graden av konsensus. Tabellen visar dock att yrkeskategorierna har haft olika svårt att enas om de olika begreppsdefinitionerna, givet samma antal iterationer. Exempelvis ser vi att när de gällde att definiera begreppet ”informationssäkerhet” så hade panelen i yrkeskategorin ”Systemutveckling och förvaltning” svårt att enas om en definition, medan båda panelerna i yrkeskategorin ”Juridik och regelverk” fann detta enklare. Graden av konsensus, givet varje panels egna definitioner, sträcker sig från 40 % (Ledning och samordning, L:4) till 92 % (Juridik och regelverk, J:1). En tolkning är att deltagarna i sin tolkning av begreppet utgår från hur de brukar närma sig problem baserat på sin yrkesroll. Experterna inom ”Juridik och regelverk” arbetar med regelföljande och har därmed i högre grad än andra grupper vana av att definiera begrepp utifrån från verksamhetens regelverk. En annan tolkning är att denna grupp kan vara relativt homogen.

Som diskuterats tidigare ligger definitionen som deltagarna i panelerna för ”Juridik och regelverk” använder sig av nära hur begreppet ”informationssäkerhet” definieras i styrdokumenten SIS-TR 50:2015 (SIS, 2015) och HB550 (SIS, 2013). I SIS-TR 50:2015 definieras ”informationssäkerhet” som ”bevarande av konfidentialitet, riktighet och tillgänglighet hos information” (SIS, 2015). Exempelvis definierar experter i panel J:2 ”informationssäkerhet” som

> *”att upprätthålla: - Konfidentialitet, informationstillgångar är tillgängliga endast för behöriga. - Riktighet, informationstillgångar förändras eller påverkas inte oönskat eller utom kontroll. -*

Tillgänglighet, informationstillgångar kan nyttjas efter behov i förväntad utsträckning och inom önskad tid".

Deltagarna i panelen S:1, i yrkeskategorin ”Systemutveckling och förvaltning”, hade en mer verksamhetsinriktad definition. De skriver om ”informationssäkerhet” enligt följande:

”[i]nformationssäkerhet omfattar både administrativa rutiner med policys och riktlinjer samt tekniskt skydd med bland annat brandväggar och kryptering. Det handlar om att ta ett helhetsgrepp och skapa en fungerande långsiktig process för att ge organisationens kritiska information det skydd det förtjänar. Informationssäkerhet syftar till att upprätthålla önskad nivå av konfidentialitet, riktighet och tillgänglighet för våra informationstillgångar".

Skillnaderna i definitioner kan tolkas som att experter i den senare panelen i högre grad än experterna från J:2 (”Juridik och regelverk”) kontextualiserar sin tolkning av begreppet ”informationssäkerhet”, samt att dessa personer arbetar inom/gentemot många olika typer av verksamheter och då kan utgöra en relativt heterogen grupp. Sammantaget kan det leda till lägre samstämmighet inom panelen.

Ett annat exempel på tydliga skillnader mellan yrkeskategorierna rör begreppet ”ansvar”. Graden av konsensus, givet panelernas egna definitioner, sträcker sig från 22 % (Informationsförvaltning och dokumenthantering, I:2) till 38 % (Juridik och regelverk, J:1 och J:2, samt Säkerhetsteknik, T:1). Här är det tydligt att panelerna I:1 och I:2, från yrkeskategorin ”Informationsförvaltning och dokumenthantering”, fann detta begrepp svårare att definiera än panelen T:1 från yrkeskategorin ”Säkerhetsteknik”. Jämför vi inom varje panel ser vi även här skillnader mellan vilka definitioner som de hade lättare att komma överens om. Tar vi panelen I:2, i yrkeskategorin ”Informationsförvaltning och dokumenthantering” som exempel så framgår det att de tyckte det var lättare att definiera ”risk” än ”informationsklassning”. Panelen L:4, i yrkeskategorin ”Ledning och samordning”, tyckte tvärtom – att det var lättare att gå mot en gemensam definition av ”informationsklassning” än ”risk”.

Graden av konsensus i Tabell 6 har endast kunnat beräknas inom respektive panel, då de enbart haft tillgång till panelens egna definitioner. Således kan inte måttet användas för att mäta konsensus över yrkeskategorierna. Däremot visar den innehållsmässiga analysen ovan att det finns skillnader mellan hur de olika yrkeskategorierna väljer att definiera begreppen, där olika experter fokuserar på olika aspekter. När experter från panelerna i ”Systemutveckling och förvaltning” och ”Säkerhetsteknik” definierar tillgänglighet lägger de till kvalitetsaspekter gällande design av system. Det ska vara ”enkelt” och ”användbart” när behöriga ska ha tillgång till information. När panelen ”Systemutveckling och förvaltning” definierar begreppet ”informationssäkerhet” så exemplifierar de med brandväggar och kryptering.

I panelen ”Ledning och samordning” syns ett management-perspektiv och här präglas språkbruket av att dessa personer arbetar med styrning och ledning av verksamheter.. De skriver exempelvis att ”[i]nformationssäkerhet handlar om hur vi på ett *förtroendefullt* och säkert sätt…” eller hur ”[a]nsvar och styrning ur ett informationsperspektiv behövs för att säkerställa att informationen *är anpassad till samtliga intressenters behov…”*. Panelerna inom ”Informationsförvaltning och dokumenthantering” använder däremot i sina beskrivningar begrepp som ”klassning efter ämne” och exemplifierar med ”diarieplan” och ”kontoplan”. Experter från panelerna inom ”Juridik och regelverk” använder begrepp som ”påföljd” och gör förtydliganden om hur man ska ”följa gällande lagar, förordningar, styrdokument etc.”.

Sammantaget ser vi att det är tydligt att säkerhetsbegrepp diskuteras utifrån den profession som experterna har, vilket borde leda till minskad konsensus mellan de olika yrkesgrupperna. Förutom att begreppsbilden ser olika ut så ser vi att de i sina definitioner också vill exemplifiera och kontextualisera utifrån sitt eget yrke, dvs. sin egen expertis.

3.3 Definitionerna i relation till internationellt begreppsbruk

Analysen av definitionerna i de svenska styrdokumenten med de som används inom ISO (ISO, 2014) (Bilaga 2) visar att definitionerna i SIS-TR 50:2015 (SIS, 2015) är mycket mer samstämmiga med definitionerna från ISO jämfört med HB550 (SIS, 2013). Detta är säkerligen ett medvetet val med många fördelar när till exempel översättningar av standarder görs. Det som också framgår av denna jämförelse är att de begrepp som deltagarna i den här studien saknade – ”ansvar” och ”informationsklassning” – inte heller finns beskrivna i styrdokumentet från ISO. Att dessa begrepp saknas i internationella styrdokumenten kan då vara en möjlig förklaring till att de saknas i de svenska dokumenten. Angående diskussionen om skillnaden mellan ”informationstillgångar” (så som begreppet används i HB550) och ”information” så ser vi här att ISO (ISO, 2014) i sin definition av informationssäkerhet håller sig till det bredare begreppet ”information” istället för ”information assets”.

3.4 Metoden att komma fram till definitionerna

Ett syfte med den här studien var att undersöka om en Delphi-metod, d.v.s. att jobba fram definitioner i paneler, är ett fungerande arbetssätt för framtida begreppsarbete. Det korta svaret på detta är: ja. Vi blev positivt överraskade över den höga svarsfrekvensen, panelernas uthållighet och hur engagerade experterna har varit i denna begreppsutredning. Dessutom ser vi stora fördelar med att engagera så många experter som möjligt med olika bakgrund. Dels då experternas gemensamma kunnande leder till bättre kvalitet på definitionerna – ju fler som bidrar desto fler aspekter belyses och fler idéer får bollas. Dels

även för att definitionerna kommer att stämma mer överens med hur människor som i sin vardag arbetar med informationssäkerhet tänker. Det är svårt för några få personer, oavsett hur kunniga, att skapa definitioner som alla känner igen sig i. I denna studie ingick 64 experter jämfört med HB550 (SIS, 2013) där sex experter är namngivna som utvecklare av rapporten och i SIS-TR50:2015 (SIS, 2015) fem experter.

Däremot så ser vi flera förbättringsområden vad gäller implementationen av metoden. En tydlig förbättring är att panelerna skulle behöva åtminstone ytterligare en iteration. För att nå högre grad av konsensus kring definitionerna borde deltagarnas kommentarer på varandras definitioner ha integrerats i definitionerna och sedan skickas ut i ytterligare en iteration tillsammans med frågan ”stämmer det här bättre in på hur ni ser på begreppet?”. Som tidigare redovisats i Tabell 6 så varierade graden av konsensus över definitionerna mycket mellan de olika panelerna. Högst grad av samstämmighet kring definitionerna hade panelerna inom yrkeskategorierna ”Juridik och regelverk” och minst samstämmighet hade panelen inom yrkeskategorin ”Systemutveckling och förvaltning”. Även viss variation inom yrkeskategorierna fanns vad gäller graden av konsensus. Exempelvis var det en (L:4) av fyra paneler inom ”Ledning och organisation” som hade absolut lägst konsensus av alla paneler (se Tabell 6).

För att förtydliga vårt resonemang angående antal iterationer som behövs så exemplifierar vi med en panel från ”Juridik och regelverk” (J:2). De var på god väg med slutjusteringar av definitionerna. Kommentarer rörde exempelvis saker som att byta ut ord: ”*Lagligt borde vara legalt. Gillar formuleringen Informationssäkerhet utgår från att information är en viktig tillgång som behöver skyddas*” eller ”*Roll bättre än person. Behöriga användare bättre än roll*”. Andra ändringar i denna panel har varit tillägg och förtydligande som behövs: ”*Tillägg att det inte enbart är användare utan även behöriga system eller processer behövs*” och ”*Spårbarhet bör INTE finnas med i själva klassningen. Spårbarheten hanteras i åtgärderna som införs*”. En panel som kommit så här pass långt skulle behöva en iteration till för att få synpunkter på de sista kommentarerna.

Om vi reflekterar kring processen utifrån de enskilda begreppen ser vi även att vissa begrepp kan behöva flera iterationer. Ett exempel från samma panel rör begreppet risk, där en paneldeltagare inte tycker att någon av de erbjudna definitionerna var bra: ”*Här var vi inte bra… Väldigt stor tro på ’mätbar’ risk.*” I detta fall skulle diskussionen behövas kanske två till tre iterationer till. Här är det metodmässigt viktigt att låta de enskilda begreppen ta den tid de tar för att närma sig konsensus. En annan reflektion är att vissa paneler kan behöva hjälp med att hitta ett urval av bra definitioner att börja med. En deltagare hörde av sig till oss e-postledes och tyckte att det var svårt att rangordna definitionerna då samtliga, inklusive de egna, var för dåliga.
En annan förbättring kring implementationen av metoden skulle vara att tydligt peka på att ”nu är det skarpt läge”, nu jobbar ni som experter för att skapa verkliga definitioner. Vårt upplägg med att experterna uppmanades förklara begreppen för en nyanställd blev lite förvirrande ibland. Anledningen

till att vi formulerade frågan i termer av att de skulle förklara begreppen för en nyanställd var att vi ville komma förbi risken att experterna bara slår upp en definition av begreppet och använder den definitionen. Vi ville komma mer nära hur de i en vardaglig situation definierar de utvalda begreppen. Vårt tillvägagångssätt skapade dock ibland lite osäkerhet kring på vilken nivå definitionerna skulle skrivas på. Exempelvis funderade en expert på hur ”byråkratisk” definitionerna ska vara:

> *”Man kan möjligen fundera över orden ’konfidentialitet’ och ’informationstillgångar’. Låter byråkratiskt och svårt att greppa för en som inte är insatt i ämnet”.* (Ledning och samordning, L:1)

En annan expert kommenterade:

> *”Ibland måste man skilja på formella och informella definitioner. Formella definitioner är viktiga när det gäller att skapa tydlighet och stringens i regelverk, i dialog med ’professionen’, i avtal etc. Den informella definitionen, ’lekmannadefinitionen’ är viktig i dialogen med medarbetaren. Ibland funkar den formella definitionen även i informella sammanhang, men långt ifrån alltid. Jag skulle t.ex. i en utbildningssituation med medarbetare i möjligaste mån använda den formella definitionen med en lekmannaöversättning som komplement. I exemplet med ’informationssäkerhet’ så har jag rankat den bästa formella definitionen som nr 1, och den bästa informella definitionen som nr 2. Nr 3 är också en bra informell definition”.* (Ledning och samordning, L:2)

Det är följaktligen viktigt att experterna vet för vem de skriver definitionerna, och i vilket sammanhang de ska användas. Som experten i den sista kommentaren nämner så kan det också finnas goda skäl att skilja på formella och mer informella definitioner. Detta är en rekommendation som vi kommer att utveckla i diskussionen nedan.

Delphi-metoden har flera styrkor, vilket diskuterats ovan. I den här studien hade vi mycket gott engagemang genom hela datainsamlingen, vilket visas i tabellerna 4 och 5. Engagemang är ofta kopplat till arbetsbelastning, och här bör påpekas att arbetsbelastningen snabbt stiger när antalet paneldeltagare och/eller begrepp ökas. Antalet definitioner som varje paneldeltagare ska arbeta med utgörs av antal paneldeltagare x antal begrepp. Det gör att varje panel inte kan arbeta med för många begrepp åt gången, samt att panelerna bör begränsas i storlek.

4. Diskussion och rekommendationer för framtiden

Utifrån vår analys kan vi se både problem och möjligheter inför det fortsatta arbetet med ett gemensamt fackspråk inom informationssäkerhetsområdet. Vi redogör för dessa innan vi presenterar våra rekommendationer.

En svaghet vi har identifierat är att begrepp, såsom ”ansvar” och ”informationsklassning”, som ses av experter som centrala informations-säkerhetsbegrepp helt saknas i styrdokumenten SIS-TR 50:2015 (SIS, 2015) och HB550 (SIS, 2013). Vi finner det också olyckligt att definitionerna av begrepp i de två styrdokumenten skiljer sig åt. Särskilt tydligt är det vad gäller begreppen ”tillgänglighet” och ”risk”, där HB550 definierar ”tillgänglighet” som ”[s]kyddsmål där informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid” (SIS, 2013) och SIS-TR 50:2015 definierar det som ”åtkomst för behörig person vid rätt tillfälle” (SIS, 2015). Begreppet ”risk” definieras i HB550 som ”[k]ombination av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad” (SIS, 2013) och i SIS-TR 50:2015 ses ”risk” som ”osäkerhetens effekt på mål” (SIS, 2015). Ytterligare ett exempel är att om ”risk” ska vara kopplat till mål så borde detta förtydligande finnas med i båda dokumenten. Vidare vore det också önskvärt att båda dokumenten beskriver informationssäkerhet med referens till såväl ”information” som till ”informationstillgångar” och att detta görs på ett enhetligt sätt.

Att dokumenten är enhetliga skulle underlätta betydligt för yrkesverksamma experter inom området. I nuvarande situation är båda dessa dokument styrande, vilket istället kan leda till osäkerhet och svårigheter för ledning och styrning av informationssäkerhetsarbetet. Det som skulle kunna underlätta ännu mer är om det bara fanns ett dokument att använda sig av. Som framgår av Bilaga 3, som återger panelernas definitioner, så ligger de flesta definitioner mer i linje med HB550 (SIS, 2013) än SIS-TR50:2015 (SIS, 2015). Av 32 definitioner som vi kunde göra jämförelser med så innehöll 26 av dem centrala koncept från HB550:s definitioner, och endast 11 innehöll centrala koncept från SIS-TR50:2015. Vi kan bara spekulera kring vad detta beror på. Antingen så känner experterna sig mer bekväma med definitionerna i HB550 eller så beror det på att SIS-TR 50:2015 är ett mycket nyare dokument och att HB550 är det dokument där definitionerna internaliserats hos experterna. Ett exempel på hur välförankrade HB550:s definitioner är kan vi se på användningen av begreppen “risk” och “tillgänglighet”. Dessa två begrepp är de som bäst stämmer överens mellan panelerna och i jämförelse med HB550. Ingen definition är exakt likadan som HB550, men de är mycket snarlika. Att experternas definitioner ligger närmare HB550 indikerar indirekt också att de avviker mer från definitionerna i ISO än om de anslutit mer till SIS-TR50:2015.

Detta baseras på att analysen av HB550 och SIS-TR50:2015 där vi fann att det senare styrdokumentet ansluter med till det internationella styrdokumentet från ISO (ISO, 2014).

En annan aspekt som tydligt framkom under analysen är att många experter har ett behov av att förtydliga, utveckla och kontextualisera definitionerna som ges i HB550 (SIS, 2013) och SIS-TR 50:2015 (SIS, 2015). Vi ser att definitionerna i dessa styrdokument oftast är mer allmänna och mindre detaljerade än de som ges av experterna. Om vi använder begreppet informationssäkerhet som exempel så ser vi att i HB550 ges definitionen:

> *”säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet (även ansvarighet och oavvislighet)”* (SIS, 2013)

I SIS-TR 50:2015 ges en ännu kortare definition:

> *”bevarande av konfidentialitet, riktighet och tillgänglighet hos information”* (SIS, 2015)

När dessa definitioner jämförs med panelernas definitioner ser vi att experterna utvecklar och förtydligar sina definitioner mer. Ett exempel är följande:

> *”Med detta menas hur vi tar hand om och skyddar den information vi hanterar inom myndigheten. Detta med utifrån informationens tillgänglighet, riktighet, konfidentialitet och spårbarhet. Tillgänglighet innebär att informationen ska vara nåbar när vi behöver den. Riktighet att innehållet i informationen är korrekt och autentisk och inte förvanskad. Konfidentialitet att informationen bara kan nås av eller delges den eller de personer som har behörighet att ta del av den. Spårbarheten är viktig för att säkerställa att informationen inte ändrats, eftersökts eller lämnats ut till någon som inte har behörighet att ta del av den”.* (Informationsförvaltning och dokumenthantering, I:1)

Vår analys visade också att experterna i flera fall kontextualiserar definitionerna genom att använda exempel från den egna professionen. Sammantaget visar detta behov av att utvidga och kontextualisera definitionerna, där experter skulle vara behjälpta av att ha egna sektorspecifika definitioner förutom de allmänna och generella. Vi föreslår, som några av paneldeltagarna har varit inne på, att det arbetas fram en fast uppsättning rena och stringenta definitioner, såsom i HB550 (SIS, 2013) eller SIS-TR 50:2015 (SIS, 2015), som skulle kunna kallas formella definitioner, och att varje sektor sedan jobbar fram en mer detaljerad och kontextspecifik definition – liknande de ”technical reports” som skrivs som tillägg för olika standarder.

Vi rekommenderar att yrkesverksamma experter inom området använder sig av en Delphi-metod för att komma fram till konsensus kring 1) de gemensamma, generella definitionerna, och 2) därefter dela upp gruppen baserat på yrkesgrupper eller organisatoriska enheter för att enas om de sektor-specifika definitionerna. Vi grundar detta i att vi under vårt arbete med panelerna sett att olika yrkesgrupper har behov att förtydliga begreppen utifrån sin verksamhet.

Vad gäller de gemensamma, generella, definitionerna ser vi ett stort behov av att experterna även är med i detta arbete. Dels för att det är de som i sitt dagliga arbete praktiskt handhar organisationers och samhällets informationssäkerhet och då måste vara målgruppen för terminologin. Då bör målgruppen känna igen sig i de definitioner som tas fram. Dessutom skulle detta öka kvalitén på definitionerna då det är många som tänker och risken minskar för att väsentliga aspekter missas. Bara genom denna fallstudie har vi fått flera uppslag till nya intressanta aspekter att beakta. Exempelvis när panelerna diskuterade begreppet ”tillgänglighet” så kom det upp frågor om användbarhet är en viktig aspekt att ta hänsyn till eller om platsen är viktig. Det visar på vad som händer om fler personer deltar i arbetet med begrepp.

Vi föreslår löpande, kontinuerliga paneler (t.ex. med 2 års mellanrum) då nya begrepp dyker upp och gamla byter betydelse. Med tanke på hur engagerade och noggranna deltagarna var under denna studie så känns det inte som orimligt att engagera 70-80 experter till detta arbete vartannat år. Däremot bör man vara försiktig med hur många begrepp som behandlas av varje panel sett till att arbetsbelastningen snabbt kan öka.

Våra rekommendationer kan summeras enligt följande:

- Ett enhetligt styrdokument med definitioner av informationssäkerhetsbegrepp skapas. Detta dokument ersätter de två dokument som finns nu och där definitionerna i flera fall skiljer sig åt.
- Skapandet av detta enhetliga styrdokument görs av yrkesverksamma experter som i sitt dagliga verk arbetar med informationssäkerhetsfrågor.
- Arbetet med att ta fram definitioner följer Delphi-metoden såsom beskrivet i denna rapport (inklusive de förbättringsförslag som ges).
- Att arbetet med att ta fram definitioner görs återkommande då nya begrepp dyker upp och gamla byter betydelse.
- Utöver skapandet av en gemensam, generell, begreppsapparat även låter olika sektorer (yrken eller organisationer) skriva sektor-specifika tillägg (motsvarande standarders ”technical reports” där förtydliganden och kommentarer finns).
- Att all framtida begreppsutveckling utgår ifrån de yrkesverksamma experternas behov och dessa tillfrågas om vilka begrepp som behöver definieras. På detta sätt kan det säkerställas att begrepp som experterna saknar, såsom ”informationsklassning” och ”ansvar” i denna studie, inte uteblir i styrande dokument.
- Att all framtida begreppsutveckling effektiviseras och tydligt samordnas mellan olika aktörer.

5. Referenser

Delbecq, A. L., Van de Ven, A. H., & Gustafson, D. H. (1975). *Group Techniques for Program Planning. A guide to nominal group and delphi processes*. Glenview, Illinois, USA: Scott, Foresman and Company.

ISO. (2014). ISO/IEC 27000:2014, Information technology — Security techniques — Information security management systems — Overview and vocabulary: International Organization for Standardization (ISO).

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information and Management, 42*, 15-29.

Schmidt, R. (1997). Managing Delphi Surveys Using Nonparatetric Statistical Techniques. *Decision Sciences 28*(3), 763-773.

Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: an international Delphi study. *Journal of Management Information Systems, 17*(4), 5-36.

SIS. (2013). *SIS Handbok 550 - Terminologi för informationssäkerhet* (Vol. 3). Stockholm: SIS Förlag.

SIS. (2015). Terminologi för informationssäkerhet. In SIS (Ed.), (1 ed., pp. 112): SIS.

Veriscan. (2009). Informationsklassning. *Rätt Säkerhet* Retrieved November 23, 2015, from http://www.sis.se/pdf/Fia_Ewald.pdf

Bilaga 1: Samtliga experters föreslagna definitioner och hur de rankats inom varje panel.

Varje deltagares förstahandsval har fått 3 poäng, andrahandsvalet 2 poäng och tredjehandsvalet 1 poäng. Således har den definition som experterna föredrog mest fått högst poäng.

Informationsförvaltning och dokumenthantering, panel I:1

Begrepp	*Definitioner*	*Poäng*
Informations-säkerhet	Med detta menas hur vi tar hand om och skyddar den information vi hanterar inom myndigheten. Detta med utifrån informationens tillgänglighet, riktighet, konfidentialitet och spårbarhet. Tillgänglighet innebär att informationen ska vara nåbar när vi behöver den. Riktighet att innehållet i informationen är korrekt och autentisk och inte förvanskad. Konfidentialitet att informationen bara kan nås av eller delges den eller de personer som har behörighet att ta del av den. Spårbarheten är viktig för att säkerställa att informationen inte ändrats, eftersökts eller lämnats ut till någon som inte har behörighet att ta del av den.	16
	Att skydda information så att den alltid finns när den behövs, man kan lita på att den är korrekt och inte manipulerad och förstörd samt att endast behöriga personer får ta del av den.	8
	Säkerhet för alla informationstillgångar oavsett om informationen hanteras manuellt eller digitalt och oberoende av dess form eller miljö den förekommer i. Omfattar främst konfidentialitet, tillgänglighet och riktighet samt spårbarhet och oavislighet.	7
	Informationssäkerhet är bevarandet av informationens riktighet, tillgänglighet och sekretess. Syftet är att skydda informationstillgångarna oavsett var de finns och hur de används.	6
	Arbete med att förhindra att myndighetens information försvinner eller förvanskas samt är tillgänglig i framtiden.	2
	Att veta vilken information som finns, var den finns, i vilket skick den är och hur den ska hanteras.	2
	Informationssäkerhet handlar om hur vi hanterar vår information. Att vi har regler och rutiner som gör att informationen inte kan hanteras av obehöriga.	1
Ansvar	Den som ansvarar för en verksamhet ansvarar också	10

	för informationssäkerheten för den information som hanteras i verksamheten.	
	Alla som på något sätt arbetar med information om det så är med att skapa den, bevara eller tillgängliggöra den, har ett ansvar att göra detta på ett säkert sätt. Ansvaret gäller så väl den enskilde medarbetare som myndigheten i stort.	9
	En fastställd fördelning per befattning avseende hantering av informationstillgång(ar).	6
	Ansvar betyder att det finns uppgifter som någon eller några ska åtgärda, kontrollera att det följs eller fungerar.	6
	Ansvar definierar vad man har rätt (och härmed också inte rätt) att göra.	4
	Att ur infosäkperspektiv känna till vad som gäller för hantering och användning av olika typer av information (öppen/publik, intern och konfidentiell information).	4
	Myndighetschefen	3
Tillgänglighet	Tillgång till informationstillgång(ar) för behöriga användare i förväntad utsträckning och inom önskad tidsrymd.	10
	Att informationen finns att tillgå i förväntad utsträckning och inom önskad tid.	10
	Informationen ska finnas tillgänglig när vi behöver den. För att detta ska kunna ske på ett säkert sätt är det viktigt att informationens innehåll identifieras och bedöms utifrån informationssäkerhetens andra tre grundprinciper.	7
	Att information ska kunna nyttjas över tid och oberoende av databärare.	6
	Att det går att söka och hitta information när jag behöver tillgång till den.	5
	Tillgänglighet innebär säkerställande att behöriga användare vid behov har tillgång till informationen, och tillhörande tillgångar.	4
	Tillgänglighet betyder att man har tillgång till något.	0
Informations-klassning	Att bestämma vilka säkerhetskrav som ska gälla för en informationstillgång, utifrån vilka konsekvenser som kan uppstå om informationen inte hålls tillgänglig, riktig och konfidentiell.	12
	Metodik för att indela informationstillgång(ar) så att definierad skyddsnivå kan uppnås avseende konfidentialitet, tillgänglighet och riktighet.	11
	Informationsklassning är en metod för att fastställa informationens värde och grunden för att ge	10

	informationstillgången rätt skyddsnivå för att tillvara ta detta värde.	
	En metod att klassificera olika typer av information som öppen/publik, intern och konfidentiell information. Klassningen styr hur vi hanterar och delar information internt och externt.	5
	Krävs för att man t ex ska kunna tillgängliggöra information på ett säkert sätt. Den som jobbar på t ex en myndighet har varken användning för eller skäl till att ta del av all information som förvaras inom denna. Det är först genom en informationsklassning som man kan vara säker på att man har förutsättningar att leva upp till informationssäkerhetens grundprinciper.	3
	För att veta hur vi ska hantera vår information måste vi klassa den utifrån ett antal kriterier. Det handlar om vilket värde och betydelse informationen har för ägaren, men också om juridiska krav, såsom sekretess och PuL.	1
	Kartläggning av processer.	0
Risk	En sammanvägning av sannolikheten för att en händelse ska inträffa och de konsekvenser händelsen kan leda till.	11
	Risk är kombination av sannolikheten för att ett givet hot realiseras och den därmed uppkommande skadekostnaden.	11
	Produkten av sannolikheten för att ett hot ska inträffa och potentiell skadekostnad.	8
	Information som inte skyddas på ett säkert sätt och uppfyller kraven på tillgänglighet, riktighet, konfidentialitet och spårbarhet utgör en risk. Risken kan ligga på individnivå eller mer övergripande samhällsnivå beroende på vilken typ av information som har brister i hanteringen av den. ex. för dig som handläggare Information som inte finns tillgänglig ex en allmän handling som inte går att hitta när en person begär ut den pga av att någon lagt den under fel diarienummer eller klassat den fel i ett e-arkiv, utgör en risk. Information som t ex konverterats eller migrerats in i ett nytt system och där man inte gjort autenticitetskontroller med eventuell informationsförlust eller förvanskning som resultat, utgör en risk. Information som inte klassats och märkts upp och tilldelas åtkomstbehörighet utgör en risk eftersom vem som helst då kan komma åt känsligt innehåll t ex uppgifter om skyddad identitet. Det är därför oerhört viktigt att det går att följa informationen	3

	och de eventuella ändringar som görs i den, hur, när och till vem den tillhandahålls, spårbarheten helt enkelt.	
	Risk är kombination av sannolikheten för att ett givet hot realiseras och den härmed uppkomna skadekostnaden om så sker.	3
	Hur stor är risken att viss informationen försvinner eller förvanskas och vad händer.	0
	Risk är något som är negativt, att det finns konsekvenser för något.	0

Informationsförvaltning och dokumenthantering, panel I:2

Begrepp	*Definitioner*	*Poäng*
Informations-säkerhet	Systematisk planering för att information ska skyddas mot obehörig åtkomst (både intrång av extern part och behörighetsstyrning inom organisationen) samt mot förvanskning (d.v.s. informationens autenticitet garanteras).	13
	Regler och rutiner för att behålla informationens integritet, autenticitet, spårbarhet och äkthet. Och att eventuell sekretess bibehålls så länge det krävs.	12
	Jag anser att det ligger tre olika uttydningar av begreppet. 1. Att vi har ett tillförlitligt digitalt system/nät med brandväggar, lösenord mm eller att analoga handlingar förvaras betryggande så att de inte utsätts för stöld eller annan skada. 2. Att vi kan bevara viktig digital och analog information över lång tid och att den inte förvanskas. 3. Att vi kan lita på att informationen är riktig och vilken version som är den slutliga.	9
	Information, oberoende av media, ska hanteras och förvaras på ett säkert sätt så att regelverk och avtal följs samt att samarbetspartner, allmänhet och medarbetare ska känna sig trygga med att information hanteras på rätt sätt.	6
	Säkerhet rörande all information vi hanterar. Inte bara personuppgifter utan även arbetsmaterial innan beslut med mera.	2
Ansvar	Person eller funktion inom organisationen som har en roll att genomföra vissa specifika aktiviteter eller att följa upp att vissa specifika aktiviteter blir genomförda.	9
	Innebär att varje del i informationskedjan har en ägare	9

	som ser till att rutiner och regelverk följs och som har mandat att påverka informationshanteringen.	
	Aktivitet där man ser till att en arbetsuppgift blir korrekt utförd.	8
	Var och en har ansvar för att känna till vilket regelverk (lagar, förordningar, föreskrifter, interna riktlinjer och policys mm.) som gäller för medarbetaren i tjänsteutövningen.	8
	Ansvar finns i olika nivåer, det du personligen har ansvar för som din inpasseringsbricka, din dator ditt lösenord o s v. Sen finns det ansvar för egendom, ansvar för verksamhet och ansvar för personal.	6
	Ett systematiskt arbetssätt till syfte att säkerställa att information förblir tillgänglig, riktig, konfidentiell och spårbar.	3
	Ansvar innebär att man tar ansvar för den tjänst man har och sköter den. Man ska komma i tid både till jobbet och sammanträden man ska ansvara för sina tilldelade arbetsuppgifter så att de utförs på bästa möjliga sätt och håller tidsramarna. Ansvar innebär också att bry sig om sina arbetskamrater och deras väl och ve och att vara lojal mot arbetsgivaren i så motto att man följer de regler som är vedertagna på arbetsplatsen.	1
Tillgänglighet	Information går att återsöka och ta del av för personer med rätt behörighet, med bibehållen kvalitet och autenticitet.	15
	Att rätt information, vid behov, finns att hämta och läsa.	12
	Möjlighet att kunna använda informationen på ett enkelt och intuitivt sätt där organisationen vet hur den ska hitta information och kunna dela den med olika intressenter.	6
	Alla medborgare ska kunna ta del av myndighetens verksamhet och service på lika villkor. Oavsett funktionshinder, språk mm.	4
	Inom offentliga myndigheter (som jag tillhör) ska man vara tillgänglig varje dag om möjligt. Man kan begränsa tillgängligheten genom att ha telefontider. Telefontider, semester, sjukdom, tjänsteresor ska framgå av telefonsvar och e-post med hänvisning till annan person som kan gå in i ens ställe om bortovaron är mer än en dag. Telefontider bör också kännas till av receptionen och läggas in på myndighetens webbplats.	3
	När information ska vara tillgänglig och för vilka. Kan	2

	även vara när vi ska vara tillgängliga för besök/frågor.	
Informations-klassning	För mig är informationsklassning två begrepp: 1. Klassning efter ämne t.ex. i en diarieplan eller kontoplan, 2. Säkerhetsklassning, dvs. vem som ska tillgång till vilken information och hänger samman med sekretessregler.	11
	Information klassificeras med hänsyn till aktuellt skyddsbehov inriktat på tillgänglighet, konfidentialitet, riktighet och spårbarhet.	10
	Ett sätt att värdera information utifrån krav på sekretess och integritet, men också ett sätt ett redovisa informationen i ett sammanhang t.ex. vilken verksamhet som ansvarar för informationen.	9
	Information klassificeras utifrån en fördefinierad struktur, t.ex. efter ämnesområde (dossierplan) eller verksamhetsprocess (klassificeringsstruktur), alternativt märks upp med fördefinierade nyckelord.	5
	Kategorisering av information i klasser av olika nivåer av skyddsbehov.	4
Risk	Risk innebär en kalkylerad sårbarhet som organisationen måste planera för och ha en plan för att möta konsekvenserna som risken kan innebära.	18
	Sannolikheten att en omständighet leder till en oönskad händelse.	11
	Något fenomen som kan hota informationens autenticitet eller tillgänglighet, eller som kan medföra obehörig åtkomst.	6
	I arkivet är stöld, förvanskning, brand, angrepp, översvämning och obehörig åtkomst olika exempel på risker. Risker finns inom alla områden t.ex. IT där det gäller buggar, förlust av information, intrång mm. Hot och våld kan förekomma inom myndigheten.	4
	Att bedöma information utifrån hur viktig den är, hur stor skada en förlust kan innebära.	3
	Det finns många typer av risker, personalen brukar räknas som en av de största riskerna utifrån deras beteende och ibland dåliga insikt i säkerhetsfrågor. Risker är även hot om sabotage av olika slag.	2
	Utan informationssäkerhet kan det finnas risk för att information hanteras på ett otillåtet sätt.	1

Juridik och regelverk, panel J:1

Begrepp	*Definitioner*	*Poäng*
Informations-säkerhet	Information är uttryck för din, min och organisationens kunskap. Säkerhet för information är att säkerställa att kunskapen är A) tillgänglig B) endast känd av behöriga C) riktig.	11
	Hur vi säkerställer att information är tillgänglig riktig, skyddad och tillgänglig.	7
	Information är något värdefullt som behöver skyddas efter behov. Behovet definieras av de lag- och verksamhetskrav som finns på informationen. Genom att klassa informationen som hanteras i våra processer och system får vi kunskap om vilka krav som gäller för respektive informationsmängd. Genom att jämföra hur vår nuvarande hantering stämmer överens med de krav som finns på hanteringen av informationen kan vi ta fram förbättringsförslag. Åtgärdsförslagen kan handla om såväl tekniska som administrativa åtgärder.	6
Ansvar	Ansvar för informationssäkerhet innebär att du som individ och anställd ska bruka den information du är anförtrodd och kommer i kontakt med på ett tillräckligt säkert sätt.	9
	En uppgift som är definierad för en person och att det blir påföljd om man inte följer den.	9
	Det systematiska arbetet handlar bl.a. om att följa upp och kontinuerligt identifiera sårbarheter i vår hantering av informationen. Det är viktigt att det finns tydliga roller med ansvar, mandat och resurser för att agera på identifierade brister. Det behövs också ett uttalat ansvar för andra roller inom det systematiska informationssäkerhetsarbetet, ex. uppdatering av policys och hanteringsregler, uppföljning av efterlevnad m.m.	6
Tillgänglighet	Tillgänglighet är att beskriva i vilken grad användarna kan nå önskad information vid ett givet tillfälle eller tidpunkt.	11
	Att informationen finns och att det fungerar att använda den när den behövs.	9
	Krav på tillgänglighet är utöver riktighet, konfidentialitet och spårbarhet en av de fyra viktiga informationssäkerhetsegenskaperna. Statliga myndigheter har särskilda tillgänglighetskrav reglerat i	4

	olika författningar, bl.a. i sin hantering av allmänna handlingar.	
Informations-klassning	En process för att ge informationen rätt behandling i avseende sekretess, spårbarhet, riktighet och tillgänglighet.	11
	Informationsklassning är ett beslutsunderlag för hur skyddsvärd given information är utifrån kvantitativa och/eller kvalitativa beskrivningar av informationens behov av tillgänglighet, konfidentialitet och riktighet.	7
	Informationsklassning handlar om att kartlägga vilken information som flödar genom och lagras i våra processer och system. Klassningen sker genom att genom att vi ställer oss vissa frågor, ex. är informationen allmän handling eller arbetsmaterial? Innehåller den personuppgifter och är det i så fall fråga om strukturerad eller ostrukturerad behandling? Finns det känslig information, ex. sådan som rör rikets säkerhet eller är sekretessklassat enligt offentlighet- och sekretesslagen? Finns det några gallringsföreskrifter från Riksarkivet som gäller för informationen? Finns det några krav från den interna verksamheten på informationshanteringen? Svaren, tillsammans med vägledning från tillämpliga lagar, hjälper oss att upprätta en samlad kravbild på informationshanteringen.	6
Risk	Risk är bedömning av sannolikhet att en given händelse inträffar och dess konsekvenser.	10
	De negativa konsekvenserna av en framtida händelse som kan beräknas ifråga om sannolikhet och skada.	8
	Risker identifieras huvudsakligen i samband informationsklassning och riskanalys. Identifierade risker kan hanteras på olika sätt, antingen genom att elimineras, reduceras eller accepteras. Oförutsedda risker identifieras även löpande i verksamheten, ex. i samband med inträffade incidenter.	6

Juridik och regelverk, panel J:2

Begrepp	*Definitioner*	*Poäng*
Informations-säkerhet	Med informationssäkerhet avses att upprätthålla: • Konfidentialitet, informationstillgångar är tillgängliga endast för behöriga • Riktighet, informationstillgångar förändras eller påverkas inte oönskat eller utom kontroll • Tillgänglighet, informationstillgångar kan nyttjas efter behov i förväntad utsträckning och inom önskad tid. Med informationstillgångar avses all information och informationshanterande resurser såsom manuella och IT-baserade informationssystem.	13
	Informationssäkerhet handlar om att den information, inklusive de system och verktyg som innehåller och behandlar den, ska skyddas så att den är riktig och tillgänglig för enbart de personer, system eller processer som den avsedd för. = Säker hantering av information.	7
	Att säkerställa att information och informationssystem har ett ändamålsenligt skydd avseende konfidentialitet, tillgänglighet och riktighet baserat på hot- och riskanalys.	7
	Omfattar dina och myndighetens åtgärder och system för att skydda din och myndighetens information från obehörig åtkomst eller förvanskning och att den blir tillgänglig på avsett sätt.	5
	"Ett tillstånd som innebär skydd med avseende på konfidentialitet, riktighet och tillgänglighet." Det är oerhört viktigt att spårbarhet inte finns med i den definitionen om den ska användas. Alternativt ska definitionen enligt SIS RT 50:2015 användas där även autenticitet, ansvarsskyldighet, oavvislighet och auktorisation finns med.	4
	Uppnås genom att identifiera vilket lagligt skydd och vilka risker det finns när vi hanterar olika typer av information. När vi vet informationens behov av skydd inför vi de tekniska åtgärder, rutiner och arbetssätt som gör att informationen är tillräckligt skyddad, tillgänglig och inte förstörs genom olycka eller slarv.	4
	Informationssäkerhet utgår ifrån att information är en viktig tillgång som behöver skyddas. Informationssäkerhet består av hörnstenarna tillgänglighet, riktighet, konfidentialitet och spårbarhet.	2
Ansvar	Ansvaret för informationssäkerheten följer verksamhetsansvaret. Är man ansvarig för en verksamhet är man också ytterst ansvarig för	16

	säkerställandet av verksamhetens information. Som medarbetare har hen ett ansvar att inom sitt ansvarsområde informera sig om och följa gällande lagar, förordningar, styrdokument etc samt aktivt arbeta för ökad säkerhet och rapportera brister och svagheter.	
	Varje medarbetare har ett personligt ansvar för att följa policy och regler för informationssäkerhet och att bedöma sin informations skyddsvärde och utifrån detta hantera informationen.	9
	Att följa de styrande regelverken. Krävs goda förutsättningar för att möjliggöra att en medarbetare ska kunna ta sitt ansvar samt uppföljning.	5
	För att informationen ska skyddas, vara tillgänglig och inte förstöras måste alla ta sitt ansvar och följa de rutiner och arbetssätt som är bestämda. De som arbetar med att ta fram rutiner och arbetssätt har särskilt ansvar för att dessa blir användbara och uppfyller syftet.	4
	Ansvar innebär att en person har ett åliggande.	3
	En skyldighet att stå till svars för något.	3
	Ansvar, är att följa det regelverk som finns. För gemene man handlar det främst om medvetenhet och delaktighet. Om man stöter på något som bryter säkerheten (incident) så meddelar man det. För någon som har ansvar för ett system ansvar man också för att rätt skydd finns för systemet.	2
Tillgänglighet	Med tillgänglighet menas att informationstillgångar kan nyttjas efter behov i förväntad utsträckning och inom önskad tid (med informationstillgångar avses all information och informationshanterande resurser såsom manuella och IT-baserade informationssystem).	12
	Med tillgänglighet avses att informationen ska finnas till hands för behöriga användare då den behövs.	10
	Tillgänglighet är att informationen ska finnas åtkomlig för den behörige när den begärs.	5
	Beskrivning av hur och när information är eller bör vara åtkomlig för att kunna nyttjas i avsedda processer.	4
	Bedömning av behovet av att viss roll har tillgång till information i en viss situation eller tidpunkt.	3
	Står för att informationen ska finnas åtkomlig för den person som har behov av den, när behovet finns. Rätt information, i rätt tid till rätt person.	2

	Det ska vara möjligt att hantera information när det behövs.	0
Informations-klassning	Innebär att man bedömer informationens betydelse för verksamheten samt de krav (såväl interna som externa) som finns på informationen för att på så sätt tydliggöra skyddsbehovet för informationen.	11
	Informationsklassning är bedömning av information eller den samlade informationsmängden i ett system med avseende på konfidentialitet, riktighet, tillgänglighet och behov av spårbarhet, för att förse informationen eller systemet med ett lämpligt anpassat skydd.	9
	Är en värdering av informationen, som ska ge svar på vilka skyddsåtgärder som behöver vidtas. Informationsklassningen utgår ifrån tillgänglighet, riktighet, konfidentialitet och spårbarhet.	7
	Metod för att genom att riskbedöma vilka skador obehörig åtkomst, otillgänglighet och felaktig information orsakar organisationen, samverkanspartner och samhälle.	3
	Informationsklassning skall göras för att informationen skall ges en lämplig skyddsnivå utifrån kriterierna konfidentialitet, riktighet, spårbarhet och tillgänglighet.	3
	Att klassificera information avseende konfidentialitet, tillgänglighet och riktighet utifrån en fastställd normskala avseende konsekvenser av hot och risker som faller ut.	2
	Klassa information med utgångspunkt i konfidentialitet, riktighet och tillgänglighet. Det är oerhört viktigt att spårbarhet inte finns med i den definitionen.	1
Risk	Risk är sannolikheten för att en oönskad händelse inträffar och konsekvenserna som detta i så fall skulle innebära.	11
	En sammanvägning av sannolikheten för att en viss händelse ska inträffa och de negativa konsekvenser som händelsen kan leda till.	7
	Sätt att beskriva konsekvens och sannolikhet för att något oönskat inträffar tex att uppsatta mål inte nås eller att informationen inte skyddas tillräckligt.	7
	Effekter av händelser, företeelser eller omständigheter som kan påverka en verksamhets mål eller möjlighet att bedriva sin verksamhet kan preciseras som risker.	6

	Sannolikhet och konsekvens av att ett hot realiseras.	4
	Risk är möjligheten för en tänkt skadehändelse att inträffa.	1
	Möjlighet att en negativ händelse ska inträffa.	0

Ledning och samordning, panel L:1

Begrepp	*Definitioner*	*Poäng*
Informations-säkerhet	Informationssäkerhet handlar om hur vi på ett förtroendefullt och säkert sätt kan hantera den information inom vår verksamhet och som vi har i såväl pappersdokument som i våra digitala system.	16
	Informationssäkerhet handlar om organisationens förhållande till den information vi hanterar oavsett form och kanal.	8
	De säkerhetsåtgärder vi inför för att bevara informationens konfidentialitet, riktighet och tillgänglighet i en verksamhet.	5
	Konfidentialitet, riktighet och tillgänglighet hos information.	5
	Riskhantering beträffande verksamhetens informationstillgångar.	4
	De policys/rutiner/åtgärder som företaget har för att säkerställa att verksamhetens information hanteras rätt.	3
Ansvar	Skyldighet att se till att något utförs på angivet sätt inom ett avgränsat område. Till ansvaret hör befogenheter och beslutsmandat samt att stå till svars för om något inte utförts på angivet sätt.	13
	Finns olika typer av ansvar. Jag tänker på det ansvar som förenas med någon form av uppgift och där eftergift/sanktion kan utkrävas i de fall ansvaret brister hos den som tilldelats uppgiften.	8
	Alla verksamma har ansvar för att verksamheten ska upprätthålla god informationssäkerhet.	6
	Ansvar innebär att man som person och i sin roll som medarbetare är medveten om skeenden som man påverkar och har klar bild av hur agerandet berör andra. I verksamheten finns även olika ansvarsnivåer som bygger på ekonomiska mandat och lagregleringar.	6
	Att vara skyldig till att något utförs/genomförs.	5
	Utpekat vad respektive roll har för ansvar, vad	4

	förväntas av dig?	
Tillgänglighet	Att informationstillgångar är tillgängliga i förväntad utsträckning och inom önskad tid för behöriga användare.	14
	Att informationen/systemet är tillgängligt för behörig användare när denna behöver informationen.	10
	Ur ett infosäkperspektiv; att informationen är tillgänglig när den behövs för den som har rätt att ta del av den.	9
	Att behörig aktör har åtkomst till information vid önskat tillfälle.	5
	Din rätt till information som du behöver för att kunna utföra ditt arbete vid rätt tillfälle.	3
	Tillgänglighet handlar om hur vi kan nås och hur information är åtkomlig. Det är ett vitt begrepp som används med olika betydelser beroende av behov. Tre exempel: 1. Du nås via telefon eller besök på tider som kommunicerats. 2. Information som vi hanterar i verksamheten är nåbar på den tid som kund/medborgare har behov av. 3. Kunder/medborgare kan använda nätet utan avbrott.	1
Informations-klassning	Att klassa information utifrån de konsekvenser som kan uppkomma vid brister eller förlust av konfidentialitet, riktighet och tillgänglighet hos information.	10
	Klassning av information innebär att vi värderar information som finns i vår verksamhet utifrån hur känslig den är för en persons integritet eller andra säkerhetsaspekter. Värderingen är en grund för hur man sedan hanterar t.ex. åtkomst, utlämnande och sekretess.	6
	Klassning av information för att ta reda på dess skyddsvärde utifrån rättsliga krav, värde och verksamhets betydelse.	6
	En metod för identifiering av rimligt skydd för verksamhetens information och de resurser den används i, baserat på interna och externa krav.	6
	Dessa informationstillgångar har vi och så här värderar vi dem utifrån konfidentialitet, riktighet och tillgänglighet.	5
	En form av riskanalys i syfte att identifiera, analysera och värdera informationens skyddsvärde.	3

Risk	Tänkbar och oönskad händelse som, om den inträffar, bedöms hindra eller försvåra att mål nås. En risk uttrycks ofta som en kombination av sannolikheten att händelsen inträffar och de konsekvenser den bedöms kunna medföra.	12
	Den negativa effekt en händelse kan få på vår verksamhet. I denna bedömning ingår att bedöma en händelses sannolikhet och konsekvens.	7
	Sannolikheten för att något oönskat ska inträffa.	6
	Bedömning av risker i vår verksamhet handlar om att ta ställning till hur vårt agerande påverkar andra parter. Skada för annan? Vad blir konsekvenserna? Hur minskar vi dem? Hur stor är sannolikheten? osv.	6
	Möjlig negativ konsekvens av framtida händelse.	5
	Ponerade riskscenarier för verksamheten har lyfts och beaktats.	0

Ledning och samordning, panel L:2

Begrepp	*Definitioner*	*Poäng*
Informations-säkerhet	Samtliga tekniska och regelmässiga åtgärder som skyddar organisationens information.	13
	System och arbetssystematik för att klassificera, kategorisera, upprätta och hantera data, information och kommunikationsobjekt på ett korrekt och säkert sätt.	7
	Tillgänglighet, riktighet, sekretess.	6
	Bevarande av (önskad/beslutad) tillgänglighet, riktighet och konfidentialitet hos information.	6
	Säkerhet kring all information som du som anställd hanterar i din roll oavsett om informationen finns i din dator, mobiltelefon, på papper eller i ditt huvud.	5
	Regelverk och åtgärder för att säkerställa tillgänglighet, integritet och sekretess avseende organisationens informationstillgångar.	3
	Informationssäkerhet går att del upp i två delar. Tekniska lösningar för att säkerställa exempelvis drift och tillgänglighet. Den andra delen handlar om att skapa en informationssäker kultur där alla är medvetna om riskerna.	2
Ansvar	Tydligt ägande och innehavande av processens, inom	11

	tilldelade områden, förutsättningar, händelser och effekter.	
	Avser vem som är ansvarig för att skydda och hantera information på ett säkert sätt.	7
	Att ta stå för och ta konsekvenser av fattade beslut, att sanktioner kan utkrävas om ansvaret inte upprätthålls/arbetsuppgifterna inte utförs korrekt.	7
	Ansvaret för att upprätthålla informationssäkerheten och vidta åtgärder om någon incident inträffar åvilar i första hand den som är närmast den verksamhet som äger/hanterar informationen.	7
	Vad för väntas av dig i ditt arbete gällande hantering av info.	4
	Du är ansvarig för att hantera information enligt gällande lagar och regler.	3
	Ansvar för vadå? Informationssäkerhet? Då skulle jag säga att det är ett mycket oklart vem som ansvarar för informationssäkerheten då det rör både drift och kultur. IT-chef, verksamhetschef?	2
Tillgänglighet	Att informationen är tillgänglig för den som har behov och rätt till åtkomst till den när den behövs.	13
	Egenskapen hos en informationsmängd att vara användbar (åtkomlig) av en behörig person (eller enhet) vid rätt tid.	11
	Rätt information ska vara tillgänglig när du behöver den.	6
	Fysisk och digital möjlighet att leverera, ge access till och tillåta upplevelsen av ett utbud.	5
	Att ha tillgänglighet till de verktyg som används i vardagen. Servrar, tjänster, system osv. Viktigt att det är lätt att tillgå de system och tjänster annars kommer personalen hitta genvägar. Tillgänglighet handlar även om att begränsa användarnas befogenheter.	4
	Tillgängligheten anger hur långa avbrott som kan accepteras i ett informationssystem utan att organisationen drabbas av allvarliga konsekvenser.	3
	Hur och när behöver du ha tillgång till info.	0
Informations-klassning	En metod för att kategorisera en informationsmängd utifrån dess behov av skydd avseende tillgänglighet, riktighet och konfidentialitet. Till varje klass knyter man en uppsättning skyddsåtgärder.	12
	Informationsklassning används för att klassa	10

	känsligheten hos en organisations information och ska ses som vägledning för hur olika typer av information ska hanteras.	
	Informationen som hanteras i en process eller i ett system ska klassificeras utifrån de fyra skydden tillgänglighet, riktighet, sekretess och spårbarhet. Klassificeringen avgör hur känslig informationen är med tanke på om något de fyra skydden fallerar.	10
	Ett sätt att klassificera informationen utifrån hur känslig den är.	5
	Hur känslig är informationen och vilken skyddsnivå ska det ligga i.	4
	Kategorisering/klassificering av objekt och dess innehåll.	1
Risk	En sammanvägning av sannolikheten för att en oönskad händelse ska inträffa och konsekvensen av den.	11
	Risk är osäkerhet om framtida händelsers negativa påverkan på en organisation.	9
	En risk betyder att något negativt riskerar att inträffa. Det är inte en händelse utan en teoretisk händelse.	9
	Sannolikhet x konsekvens är det enkla svaret.	5
	Sannolikheten för att en händelse ska inträffa multiplicerat med konsekvensen (negativ eller positiv) av att händelsen inträffar.	4
	Negativ konnotation till möjliga effekter som kan uppstå i varje isolerad eller sammantagen händelse.	3
	Sannolikhet och konsekvens.	1

Ledning och samordning, panel L:3

Begrepp	*Definitioner*	*Poäng*
Informations-säkerhet	Informationssäkerhet är ytterst en kvalitetsfråga och inbegriper alla delar av myndighetens verksamhet. Oavsett vilken form informationen har, eller på vilket sätt den överförs eller lagras, måste den få ett tillräckligt skydd avseende korrekthet och fullständighet, tillgänglighet, skydd mot obehörig åtkomst, tillgrepp, skada och förstörelse och kunna spåras och återskapas.	11
	Information är en viktig och strategisk tillgång i alla organisationer/myndigheter. Informationssäkerhet är	10

	de åtgärder som vidtas för att säkerställa att information inte läcker ut, förvanskas eller förstörs samt för att information ska vara tillgänglig när den behövs. För en organisation/myndighet kan det handla om att skydda information mot hot för att säkerställa verksamhetens kontinuitet, minimera verksamhetens risker och maximera avkastningen på investeringar och affärsmöjligheter. Informationen som ska skyddas kan vara tryckt på papper, vara lagrad elektroniskt, överföras med post eller med elektroniska hjälpmedel, visas på film eller yttras i en konversation. I organisationens/myndighetens ledningssystem för informationssäkerhet beskrivs de säkerhetsåtgärder som gäller för säkerhetsarbetet. Ledningssystemet omfattar organisationsstruktur, policyer, planeringsaktiviteter, ansvar, praxis, rutiner, processer och resurser. Det övergripande ledningssystemet, baserad på en metodik för verksamhetsrisk, syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra säkerheten.	
	Informationssäkerhet är kombinationen av administrativ säkerhet, it-säkerhet och fysisk säkerhet.	5
	Vikten och betydelsen att följa de regler som gäller för informationssäkerheten för skydd av företagets/myndighetens goodwill, varumärke samt affärer och konkurrens.	4
	De åtgärder som vidtas för att uppnå önskad nivå på skydd av informationstillgångar. Hantering av risker kopplat till tillgången information.	3
	Är de åtgärder som vidtas för att hindra att information läcker ut, förvanskas eller förstörs och för att informationen ska vara korrekt.	3
Ansvar	Oavsett roll i organisationen så har man som medarbetare ansvar för den verksamhet man arbetar med avseende informationssäkerhet. Ansvaret finns innan, under och efter anställning. Personalansvarig chef ansvarar för att informera om vad som specifikt gäller för dina arbetsuppgifter vad gäller avseende skyddet och ansvaret för informationen avseende dina arbetsuppgifter.	12
	Som anställda har du ansvar för att skydda känslig information.	7
	Förväntas ta hand om.	5
	Ansvaret för att en god säkerhet upprätthålls i organisationen/myndigheten ligger hos styrelsen, nämnder, motsvarande som har det yttersta ansvaret för att ett aktivt säkerhetsarbete bedrivs samt att	4

	säkerhetsarbetet fastställs och organiseras utifrån verksamhetens mål, skyddsvärda objekt samt det fastställda ledningssystemet. Ansvaret för informationssäkerheten ligger i linjen, som allt annat chefsansvar, vilket innebär att varje chef ansvarar för säkerheten inom det egna ansvarsområdet och att personalen är informerad. Varje medarbetare har ett egenansvar, vilket innebär att arbeta aktivt för ökad säkerhet och för att påpeka brister i säkerheten till närmaste chef. Dessutom finns utsedda specialistroller inom säkerhetsområdet, bl a informationssäkerhetschef, IT-säkerhetschef, personuppgiftsombud.	
	Skyldighet.	3
	Vem som har befogenhet att göra vad.	2
Tillgänglighet	Att använda informationen ska kunna motiveras ur arbetssynpunkt, d v s bara för att man har behörighet så har man inte automatiskt rätt att tillgängliggöra sig den. Med andra ord så ska informationen vara tillgänglig och användas enkom av dem som är behöriga att ta del av den samt när behovet finns för att lösa arbetsuppgiften.	11
	Informationen ska vara tillgänglig när den behövs för att klara arbetsuppgiften. Detta kan variera över tiden.	8
	Med tillgänglighet avses att information, system och tjänster vid behov är tillgängliga för de som är behöriga och bedöms behöva resurserna för att utföra sitt arbete. Det innebär möjligheten att utnyttja informationstillgångar efter behov i förväntad utsträckning och inom önskad tid. Organisationen/myndigheten identifierar i riskanalys verksamhetskrav rörande tillgänglighet av informationssystem.	6
	Åtkomligt, möjligt att använda eller nyttja.	5
	Åtkomlig.	5
	Behovsanpassning/styrning.	1
Informations-klassning	Informationsklassning är ett sätt att säkerställa att information erhåller en lämplig skyddsnivå med hänsyn tagen till informationens värde och de risker som omger den. Information klassas i termer av rättsliga krav, värde, verksamhetsbetydelse och känslighet för obehörigt röjande eller modifiering. Som hjälp används kriterierna konfidentialitet, riktighet, spårbarhet och tillgänglighet. Med konfidentialitet avses att informationen inte får göras tillgänglig eller avslöjas för	12

	obehöriga. Med riktighet avses att informationen inte ska kunna förändras och förvanskas av misstag eller av någon obehörig. Med tillgänglighet avses att informationen ska finnas till hands för behöriga användare då den behövs. Resultatet från de olika klassificeringarna skall utgöra det samlade kravet på nivån för skyddet av den aktuella informationen eller IT-systemet.	
	För att säkerhetsställa att informationen har ett tillräckligt skydd så ska den klassas avseende krav på konfidentialitet, riktighet, tillgänglighet samt spårbarhet.	11
	Bedömning och gruppering av informations betydelse för verksamheten.	6
	Bedömning av information i syfte identifiera ett rimligt skydd.	5
	All information ska sekretessklassas enligt de regler som gäller.	1
	Vet hur olika info-mängder ska/kan hanteras.	1
Risk	Säkerhetsarbetet är riskbaserat. Det innebär att skyddsåtgärder regelbundet ska bedömas och anpassas utifrån hur verksamheten förändras eller när det uppstår ändrade förutsättningar i omvärlden (både internt som externt) som har eller kan ha påverkan.	14
	En risk är att något oförutsett kan hända som har konsekvenser för organisationen/myndigheten. En risk syftar på en osäker händelse som kan leda till en olycka eller kris, det måste dock inte ske en olycka för att det skall finnas en risk. Vi är hela tiden omgivna av risker i vår vardag, vi möts ständigt av varningsskyltar och nyhetsartiklar om olika risker. En del risker är vi medvetna om och kan göra något åt medan andra är mer diffusa och svåra att hantera. Risk är de skadliga konsekvenserna av till tidpunkt och utsträckning eller utformning okända framtida händelser. Ibland, framför allt i vetenskapliga sammanhang, avses med risk ett mått på risken i fråga, men när sådana mått inte är tillgängliga måste man föra ett kvalitativt resonemang. En risk är produkten av sannolikheten för att ett hot realiseras och därmed för orsakar skadekostnader. Riskanalys används som process för att identifiera säkerhetsrisker, bestämma deras betydelse och identifierar skyddsåtgärder. Informationssäkerhetsarbetet bedrivs i huvudsak som en riskhantering.	9

	Skadliga konsekvenserna av till tidpunkt och utsträckning eller utformning okända framtida händelser.	3
	Osäkerhetens effekt på mål.	3
	Möjlighet att något oönskat inträffar.	3
	Risker för informationsförluster, som du som nyanställd kan råka ut för.	3

Ledning och samordning, panel L:4

Begrepp	*Definition*	*Poäng*
Informations-säkerhet	Informationssäkerhet är de åtgärder som vidtas för att förhindra att information: görs tillgänglig för eller i övrigt kommer obehöriga till del (konfidentialitet), förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning (riktighet), och information ska kunna utnyttjas i förväntad utsträckning och inom önskad tid (tillgänglighet).	8
	Bevarande av konfidentialitet, riktighet och tillgänglighet hos information. Informationssäkerhet är en kombination av administrativ och teknisk säkerhet, där fysisk och IT-säkerhet ingår i den tekniska säkerheten	6
	Det som står i SIS HB550: ”Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet (även ansvarighet och oavvislighet).	6
	1. Ett tillstånd där all typ av information (såväl analog och digital som den kunskap som innehas av enskilda eller organisationen) är säkrad utifrån kända hot/händelser. Dessa är i sin tur noga framtagna och bedömda utifrån kvalitetssäkrade riskanalyser. 2. Informationen enligt ovan är skyddad avseende tillgänglighet, riktighet, sekretess och spårbarhet samt att det finns framtagna kontinuitetsplaner för att undvika händelser som leder till verksamhetshinder vad avser informationen. 3. Informationssäkerhet jämförs ofta med IT-säkerhet som mer avser det tekniska skyddet av informationen. Informationssäkerhet täcker som nämnts i p1 alla information och handlar mer om utbildning och information för att höja säkerherhetsmedvetandet, skapa regelverk och rutiner, följa upp och göra kontroller avseende informationstillgången.	4

	Ett tillstånd då rätt och korrekt information är tillgänglig för rätt person i önskad utsträckning och att det i efterhand går att återskapa detta skeende.	2
	Informationssäkerhet har ett mål att skydda information så att den finns när den behövs (tillgänglighet), att informationen är korrekt och inte manipulerad eller förstörd (riktighet), att endast behöriga personer får ta del av den (insynsskydd/konfidentialitet) och att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet). Detta stämmer väl både privat och i tjänsten.	1
	Informationssäkerhet – både teknik och administration av system med användare.	0
Ansvar	Ansvar och styrning ur ett informationsperspektiv behövs för att säkerställa att informationen är anpassad till samtliga intressenters behov samt till gällande regler och riktlinjer.	7
	Det som står i SIS HB550 – ”Ansvarighet – princip innebärande att en individ givits och påtagit sig visst ansvar och att därvid denne i efterhand kan ställas till svars för sitt handlande”.	7
	skyldighet att stå till svars, att ha uppsikt och kontroll (med eller utan egen arbetsinsats) över en arbetsuppgift eller ett definierat (ansvars-) område.	6
	Du som användare av vår information har ett ansvar att upprätthålla de skyddsåtgärder vi har valt för att skydda den.	4
	Ett begrepp som inom området beskriver att en person/funktion har ett tydligt uttalat uppdrag som leder till en negativ konsekvens om det inte utförs på angivet sätt.	3
Tillgänglighet	Att information finns då när den behövs. Den brukar handla om tre företeelser: - vardagsrobusthet - krav på tillgång till information i dagligt arbete; - återställning av information efter förlust - krav på att få tillbaka information efter en incident eller katastrof, det brukar handla om krav på backupper; - tillgång till information i framtiden - krav på arkivering.	6
	I informationssäkerhetssammanhang avses möjlighet att komma åt information när och där den behövs.	6
	Det som står i SIS HB550 – ”skyddsmål där informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid”.	4
	Mätetal eller värdering av hur tillgänglighet eller otillgänglighet till information påverkar verksamheten.	3

	Här blir det ju helt avhängt i vilket sammanhang ordet används... tillgänglighet inom informationssäkerhetsområdet definierar jag som information som kan utnyttjas/användas i förväntas utsträckning och inom önskad tid.	3
	Egenskapen att vara åtkomlig och användbar vid begäran av en behörig enhet.	3
	Tillgänglighet är ett mått på hur väl vi har åtkomst till vår information när vi så önskar.	2
Informations-klassning	Att genom konsekvensanalys värdera sin information utifrån aspekterna konfidentialitet, riktighet och tillgänglighet.	10
	En process för att identifiera och värdera vår information.	5
	En grundläggande aktivitet för att information och resurser ges nödvändiga skydd. Informationen klassificeras utifrån den funktion och betydelse den har för verksamheten och de konsekvenser det medför om informationen till exempel skulle hanteras felaktigt, försvinna eller komma i orätta händer.	5
	Informationsklassning är framtagning av krav som en viss informationsmängd ställer på tillgänglighet, riktighet, insynsskydd och spårbarhet (krav på oavvislighet mm kan tillkomma). Man värderar konsekvenser av att informationen inte är tillgänglig, manipulerat/ej korrekt, röjd och spårbarheten saknas. Konsekvenser kan påverka verksamhet, kunder, användare mm samt ha juridisk karaktär. Det är viktigt att analysera konsekvenserna under informationens hela livscykel. Konsekvenser brukar uppskattas i skala mellan 1 och 4, där 1 är ingen påverkan och 4 är mycket alvarlig påverkan.	5
	Bedömning av aspekterna: Tillgänglighet, Riktighet, Sekretess.	1
	Information värderas utifrån känslighet om den kan nås av obehöriga. Vad blir konsekvensen om det inträffar (menbedömning).	0
Risk	Sannolikheten och konsekvensen av att ett hot/en händelse inträffar.	6
	Risk kan ses som en funktion av sannolikheten för att en viss händelse inträffar och konsekvensen av att denna händelse inträffar. D.v.s. en sammanvägning av sannolikhet och konsekvens.	6
	Kombination av sannolikheten för att ett givet hot realiseras och dess konsekvenser.	5

	Sammanvägningen av konsekvensen av en oönskad händelse med sannolikheten för att den skulle inträffa.	5
	Risk är en uppskattning av att en potentiell skada inträffar. Under en riskanalys identifierar man eventuella händelser som negativt kan påverka hantering av informationen. När man har gjort klassificering av information då har man gjort halva jobbet - man har uppskattat konsekvenser. Under riskanalysen uppskattar man även sannolikheten att de eventuella händelserna inträffar (uppskattas i en skala mellan 1 och 4, där 1 är en låg sannolikhet och 4 är mycket hög sannolikhet). Produkten av konsekvens och sannolikhet ger en risk. För att minska risker strävar man att minska sannolikheten och/eller konsekvensen av händelserna.	4
	Det som står i SIS HB550 – ”kombination av sannolikheten för ett givet hot realiseras och därmed uppkommande skadekostnad”.	3
	Relation mellan skada och konsekvens.	0

Systemutveckling och förvaltning, panel S:1

Begrepp	*Definitioner*	*Poäng*
Informations-säkerhet	Information är en grundläggande byggsten i vår organisation. Informationssäkerhet omfattar både administrativa rutiner med policys och riktlinjer samt tekniskt skydd med bland annat brandväggar och kryptering. Det handlar om att ta ett helhetsgrepp och skapa en fungerande långsiktig process för att ge organisationens kritiska information det skydd den förtjänar. Informationssäkerhet syftar till att upprätthålla önskad nivå av konfidentialitet, riktighet och tillgänglighet för våra informationstillgångar.	8
	Informationssäkerhet är ett övergripande begrepp som täcker in både digital och analog informationshantering.	8
	De åtgärder som säkerställer att informationen är oförvanskad, oåtkomlig för obehöriga och hanteras endast av behöriga användare. Det gäller både i IT-system och alla andra sammanhang.	8
	Innebär att man på olika sätt skyddar information som hanteras oavsett om den hanteras manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.	7
	Hur man hanterar viktig information på ett säkert sätt oavsett om den är talad, på papper eller digital.	5

	Åtgärder som vidtas för att skydda information som klassificerats som känslig och som inte får lämnas till andra personer som inte har behov av den i sitt dagliga arbete.	0
	Att se till att man har tillräckligt med kunskap för att kunna surfa säkert.	0
Ansvar	Detta är de skyldigheter och uppgifter en person har att fullgöra. Ett ansvar kan aldrig delegeras, däremot uppgifter kopplade till ansvaret.	12
	Att följa de riktlinjer och regler som gäller för hantering av information som personen kommer i kontakt med i sitt arbete. Ansvara för att information inte utan vidare lämnas ut till obehöriga.	9
	Ansvar, inom informationssäkerhet, är ett begrepp som beskriver i första hand förhållandet mellan VAD och VEM.	6
	Med befogenhet och resurser för en uppgift personligen säkerställa att uppgiften blir utfört på rätt sätt.	5
	Svagaste länken i en kedja är ofta människan. Därför är det mycket viktigt att alla tar sitt ansvar för den information man hanterar.	2
	Alla anställda har ett ansvar.	2
	Att ta ansvar för att inte bidra till att virus, etc., kommer in i organisationen.	0
Tillgänglighet	Information som behövs ska vara åtkomlig på ett enkelt men ändå kontrollerat sätt. Information ska vara åtkomlig utan onödig fördröjning.	10
	Att information alltid finns när vi behöver den (tillgänglighet).	8
	Hög tillgänglighet innebär att du från olika platser och på olika sätt ges möjlighet att på ett säkert sätt nå den information som du är behörig till.	7
	Tillgänglighet är ett av de fyra mätområden vid informationsklassning. Den talar om nivå av viktighetsgrad att funktionen i fråga går att nyttja.	6
	Att (information) går att ta fram när den behövs.	4
	Detta beskriver i vilken mån exempelvis information skall kunna ses eller kunna användas av behörig användare.	1
	Att arbeta för att så mycket data som möjligt är tillgängligt för så många som möjligt. Att information såväl som data ska vara fri.	0

Informations-klassning	Informationsklassning är en hjälp för informationssäkerhetsansvariga och informationsägare att vidta skyddsåtgärder för att uppnå rätt nivå av informationssäkerhet. Informationsklassning mäts enligt: konfidentialitet, tillgänglighet, riktighet och spårbarhet.	12
	All information behöver klassificeras i olika informationsklasser. Det är företagets ansvar att information åsätts den informationsklassning som är relevant för aktuell information. Informationsklasser kan vara - Top Secret - Secret - Confidential - Restricted - Open Ovanstående uppdelning medför att all information blir klassificerad. Till varje informationsklass finns regler får åtkomst, spridning, vilket skydd som ska åsättas. Informationsklassen ska med regelbundenhet kontrolleras och i förekommande fall ändras. Ansvaret för informationsklassificering åligger informationsägaren.	7
	Innebär att man klassificerar information genom att beskriva vilka konsekvenser det skulle innebära om informationen hamnar i orätta händer, är felaktig, ej nåbar eller att det saknas loggar. Hög klassning innebär också att det kommer att ställas högre säkerhetskrav för att säkra informationen.	6
	Vår modell för skyddsklassning av information baseras på en bedömning av informationens skyddsvärde. Skyddsvärdet är en bedömning av den värsta tänkbara skadan som kan inträffa om informationen sprids till obehöriga. Baserat på skyddsvärdet klassas informationen, vilket innebär inplacering i någon av de fastställda skyddsvärdesnivåerna.	5
	Det är att bedöma hur information skall ordnas. Exempelvis i öppen (tillgänglig för alla), personskyddad (skydda individers uppgifter), hemlig (sekretessbedömd till en begränsad krets behöriga att se och använda informationen). Denna klassning är helt oberoende av media.	3
	Att enligt fördefinierat system identifiera en skyddsnivå.	3
	Att vara medveten om de olika nivåerna gällande hantering av information, så som fri data vs. sekretess kring personuppgifter, etc. Även genom att ha kontroll över hur informationen ska användas kan man även veta hur man ska ta hand om den.	0

Risk	Risk beskriver i vilken grad information, fysiska objekt, personal och omgivning kan råka ut för olika hot, som på något sätt skadar, förändrar eller förstör objektet.	9
	Om ett hot, t.ex. strömavbrott, inträffar så innebär det konsekvenser. Konsekvenser och sannolikheten att ett hot kommer att inträffa är de två delar som tillsammans ger ett riskvärde. Sannolikhet x Konsekvens = RISK.	7
	Risk är en del i konsekvens- och riskanalysen vid en informationsklassning där risk får ett värde (klassning x konsekvens = riskvärde).	7
	En risk är en omständighet som kan utgöra ett hot mot möjligheten att fullgöra ansvaret för verksamheten, d.v.s. när en omständighet riskerar medföra att myndigheten inte fullgör sina uppgifter, når sina mål eller utför sina uppdrag på avsett vis. Risker kan innefatta både nu uppkomna som framtida omständigheter.	5
	Bedömning av vilken risk information kan utsättas för om den kommer i orätta händer eller kommer på villovägar. Mycket allvarlig (katastrofal) till ingen skada har uppstått.	3
	Möjlig negativ konsekvens av en oplanerad händelse	3
	Att vara medveten om riskerna för att undvika intrång. Riskanalys.	0

Säkerhetsteknik, panel T:1

Begrepp	*Definitioner*	*Poäng*
Informations-säkerhet	Informationssäkerhet är den övergripande säkerheten som omfattar både tekniskt (IT-säkerhet) och administrativt (regler och rutiner) skydd och syftar till att informationen alltid skall vara korrekt, tillgänglig som avsett och skyddad från obehörigt tillträde.	15
	Övergripande begrepp för att beskriva informations tillgänglighet, riktighet, spårbarhet och i förekommande fall, sekretess.	12
	Informationssäkerhet handlar om att skydda organisationens information så • att den alltid finns när vi behöver den (tillgänglighet) • att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet) • att endast behöriga personer får ta del av den (konfidentialitet/sekretess) • att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet).	12

	Tillstånd som innebär skydd med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet hos information.	4
	Kvalitet. Utan ett fungerade informationssäkerhetsarbete så är det svårt att säkerställa hög kvalitet i verksamheten. Information är centralt och kan man inte lita på den eller ta del av den så är det svårt att upprätthålla kvaliteten.	3
	Skyddande av information mot obehörig åtkomst, spridning och förvanskning.	2
	Att information är tillförlitlig, aktuell, relevant och nåbar för relevant personal, icke nåbar för andra.	0
Ansvar	Ansvar tilldelas en person eller roll och innebär att denne är ålagd att tillse att arbetet sker enligt de regler som har fastställts och innebär att personen/rollen också har mandat att fatta beslut och leda arbetet inom ansvarsområdet.	18
	Ansvar innebär att det finns åtagande och skyldigheter som man måste efterleva. Detta är styrt i policy och riktlinjer och är en grundsten för att få policy och riktlinjer att fungera.	12
	En tydlighet i fördelning av arbetsuppgifter och att relevanta resurser finns till förfogande för att ansvaret skall kunna tas och inte minst, eventuella påföljder om de ålagda uppgifterna utförs så att de bryter mot givna instruktioner eller regler/förordningar. Ansvar avseende information omfattar dess tillgänglighet, korrekthet, spårbarhet och skydd mot obehörig åtkomst.	9
	Ansvar för att ta del av och säkerställa förståelse för formella regelverk, samt att hantera de privilegier som tilldelas i syfte att utföra arbetsuppgiften i enlighet med organisationens behov av säkerhetskultur.	5
	Man behöver tänka på, i varje situation, hur man hanterar den information man har tillgång till.	2
	Ägandeskap av information och åtgärder för dess skydd.	2
	Tänk efter vad som kan hända och låt det påverkar ditt agerande.	0
Tillgänglighet	Tillgänglighet innebär att informationen är nå- och användningsbar på den tid och på det sätt som har beslutats för den/de som skall använda den.	18
	Möjlighet att kunna använda information i förväntad utsträckning och inom önskad tid.	14
	Möjligheten att nå efterfrågad information eller andra resurser inom rimlig (utlovad) tid, att den är tillförlitlig.	6

	Att information är tillgänglig när man behöver den.	4
	Informationstillgång utifrån behov.	3
	Lätt tillgänglig för de som ska ha tillgång, inte tillgänglig för de som inte ska ha tillgång, rätt språklig nivå, tydligt.	2
	Kontroll av åtkomst till information.	1
Informations-klassning	Informationsklassning är en process som syftar till att bedöma informationens värde och skyddsbehov så att rätt åtgärder kan vidtas för att informationen skall få rätt hantering och skydd.	20
	Att genom konsekvensanalys identifiera skyddsbehovet med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet för en viss informationsmängd.	12
	Att värdera och klassificera information med avseende på betydelse för arbetet eller organisationen, regler rörande hur den får bevaras, överföras eller hanteras, eventuellt säkerhets- och sekretessklassning och utifrån detta avgöra hur den skall förvaras och skyddas. I värderingen ingår eventuella skadeverkningar om sekretessbelagd information kommer på avvägar, allmänt om information förvanskas eller förstörs.	8
	Metod för att avgöra hur information i organisationen värderas utifrån att upprätthålla att informationen är tillgänglig, riktig och att rätt personer kommer åt den. Klassning innebär att du som medarbetare vet hur pass viktig informationen är och att du vet hur man skall agera utifrån hur viktig informationen är.	6
	Känslighetsbedömning av information. Skyddsvärde.	2
	Märkning utifrån lagar, förordningar och verksamhetens krav så att den som ska hantera informationen åt ägaren har rätt förutsättningar.	0
Risk	Kombination av sannolikheten för att en incident(oönskad händelse) ska inträffa och konsekvenserna av en sådan händelse.	16
	En risk är en sårbarhet i kombination med sannolikheten för att den infaller.	12
	Sammanvägning av sannolikheten för att en händelse skall inträffa och skadeverkningarna (ekonomiska, goodwill etc) om den skulle inträffa.	11
	Utifrån informationssäkerhet så är det en händelse som påverkar informationssäkerheten negativt. Risken värderas utifrån hur allvarligt det är om det inträffar samt vilken sannolikhet det är att det inträffar.	8

	Något som kan störa informationstillgången.	1
	Värdera risk, arbetsinsats, relevans. Värdera, stäm av med ansvariga.	0
	Bedömning av skyddsvärde och konsekvenser vid bristande informationssäkerhet.	0

Bilaga 2: Jämförelse av de aktuella definitionerna i HB550 och SIS-TR 50:2015 med ISO:s internationella definitioner.

Begrepp	**HB550**	**SIS-TR 50:2015**	**ISO/IEC 27000: 2014**
Informations-säkerhet *Information security*	säkerhet för **informationstillgångar** avseende förmågan att upprätthålla önskad **konfidentialitet**, **riktighet** och **tillgänglighet** (även **ansvarighet** och **oavvislighet**)	bevarande av **konfidentialitet, riktighet** och **tillgänglighet** hos **information**	preservation of *confidentiality*, *integrity* and *availability* of information

Här ser vi att SIS-TR 50:2015:s definition mest stämmer överens med ISO:s definition – den är lika kort och i det närmaste direkt översatt.

Begrepp	**HB550**	**SIS-TR 50:2015**	**ISO/IEC 27000: 2014**
Ansvar *Liability*	- -	- -	- -

Begrepp	**HB550**	**SIS-TR 50:2015**	**ISO/IEC 27000: 2014**
Tillgänglighet *Availability*	Skyddsmål där **informationstillgångar** skall kunna utnyttjas i förväntad utsträckning och inom önskad tid	**åtkomst** för behörig person vid rätt tillfälle	property of being accessible and usable upon demand by an authorized entity

Här ser vi att SIS-TR 50:2015:s definition mest stämmer överens med ISO:s definition och där det betonas att åtkomsten gäller för behörig (authorized) person.

Begrepp	**HB550**	**SIS-TR 50:2015**	**ISO/IEC 27000: 2014**
Informationsklassning *Information asset classification*	- -	- -	- -

Begrepp	**HB550**	**SIS-TR 50:2015**	**ISO/IEC 27000: 2014**
Risk *Risk*	Kombination av sannolikheten för att ett givet **hot** realiseras och därmed uppkommande **skadekostnad**	Osäkerhetens effekt på **mål**	Effect of uncertainty on objectives

Här ser vi att SIS-TR 50:2015:s definition mest stämmer överens med ISO:s definition och där kopplingen görs till mål (objectives).

Bilaga 3: Panelernas definitioner och överensstämmelse med HB550 och SIS-TR 50:2015

Ett kryss i ruta HB550 och/eller SIS-TR 50:2015 betyder att centrala begrepp från dessa definitioner har lyfts fram i den egna definitionen. Då begreppen ansvar och informationsklassning ej finns definierade i dokumenten så skriver vi bara n/a (not applicable) avseende jämförelsen.

Informationsförvaltning och dokumenthantering, panel I:1

Begrepp	*Definition*	*HB550*	*SIS-TR 50:2015*
Informations-säkerhet	Med detta menas hur vi tar hand om och skyddar den information vi hanterar inom myndigheten. Detta med utifrån informationens tillgänglighet, riktighet, konfidentialitet och spårbarhet. Tillgänglighet innebär att informationen ska vara nåbar när vi behöver den. Riktighet att innehållet i informationen är korrekt och autentisk och inte förvanskad. Konfidentialitet att informationen bara kan nås av eller delges den eller de personer som har behörighet att ta del av den. Spårbarheten är viktig för att säkerställa att informationen inte ändrats, eftersökts eller lämnats ut till någon som inte har behörighet att ta del av den.	X	X
Ansvar	Den som ansvarar för en verksamhet ansvarar också för informationssäkerheten för den information som hanteras i verksamheten.	n/a	n/a
Tillgänglighet (2 med samma poäng)	"Att informationen finns att tillgå i förväntad utsträckning och inom önskad tid."	X	-
	"Tillgång till informationstillgång(ar) för behöriga användare i förväntad utsträckning och inom önskad tidsrymd."	X	X
Informations-klassning	Att bestämma vilka säkerhetskrav som ska gälla för en informationstillgång, utifrån vilka konsekvenser som kan uppstå om informationen inte hålls tillgänglig, riktig och konfidentiell.	n/a	n/a
Risk	"En sammanvägning av sannolikheten för att en händelse ska inträffa och de	X	-

	konsekvenser händelsen kan leda till.”		

Informationsförvaltning och dokumenthantering, panel I:2

Begrepp	*Definition*	*HB550*	*SIS-TR 50:2015*
Informations-säkerhet	Systematisk planering för att information ska skyddas mot obehörig åtkomst (både intrång av extern part och behörighetsstyrning inom organisationen) samt mot förvanskning (d.v.s. informationens autenticitet garanteras).	-	-
Ansvar	Person eller funktion inom organisationen som har en roll att genomföra vissa specifika aktiviteter eller att följa upp att vissa specifika aktiviteter blir genomförda.	n/a	n/a
Tillgänglighet	Information går att återsöka och ta del av för personer med rätt behörighet, med bibehållen kvalitet och autenticitet.	-	X
Informations-klassning	För mig är informationsklassning två begrepp: 1. Klassning efter ämne t.ex. i en diarieplan eller kontoplan, 2. Säkerhetsklassning, dvs. vem som ska tillgång till vilken information och hänger samman med sekretessregler.	n/a	n/a
Risk	Risk innebär en kalkylerad sårbarhet som organisationen måste planera för och ha en plan för att möta konsekvenserna som risken kan innebära.	X	-

Juridik och regelverk, panel J:1

Begrepp	*Definition*	*HB550*	*SIS-TR 50:2015*
Informations-säkerhet	Information är uttryck för din, min och organisationens kunskap. Säkerhet för information är att säkerställa att kunskapen är A) tillgänglig B) endast känd av behöriga C) riktig.	X	X

Ansvar	En uppgift som är definierad för en person och att det blir påföljd om man inte följer den.	n/a	n/a
Tillgänglighet	Tillgänglighet är att beskriva i vilken grad användarna kan nå önskad information vid ett givet tillfälle eller tidpunkt	X	-
Informations-klassning	En process för att ge informationen rätt behandling i avseende sekretess, spårbarhet, riktighet och tillgänglighet.	n/a	n/a
Risk	Risk är bedömning av sannolikhet att en given händelse inträffar och dess konsekvenser.	X	-

Juridik och regelverk, panel J:2

Begrepp	*Definition*	*HB550*	*SIS-TR 50:2015*
Informations-säkerhet	Med informationssäkerhet avses att upprätthålla: • Konfidentialitet, informationstillgångar är tillgängliga endast för behöriga • Riktighet, informationstillgångar förändras eller påverkas inte oönskat eller utom kontroll • Tillgänglighet, informationstillgångar kan nyttjas efter behov i förväntad utsträckning och inom önskad tid Med informationstillgångar avses all information och informationshanterande resurser såsom manuella och IT-baserade informationssystem.	X	X
Ansvar	Ansvaret för informationssäkerheten följer verksamhetsansvaret. Är man ansvarig för en verksamhet är man också ytterst ansvarig för säkerställandet av verksamhetens information. Som medarbetare har hen ett ansvar att inom sitt ansvarsområde informera sig om och följa gällande lagar, förordningar, styrdokument etc. samt aktivt arbeta för ökad säkerhet och rapportera brister och svagheter.	n/a	n/a

Tillgänglighet	Med tillgänglighet menas att informationstillgångar kan nyttjas efter behov i förväntad utsträckning och inom önskad tid (med informationstillgångar avses all information och informationshanterande resurser såsom manuella och IT-baserade informationssystem).	X	**-**
Informations-klassning	Innebär att man bedömer informationens betydelse för verksamheten samt de krav (såväl interna som externa) som finns på informationen för att på så sätt tydliggöra skyddsbehovet för informationen.	n/a	n/a
Risk	Risk är sannolikheten för att en oönskad händelse inträffar och konsekvenserna som detta i så fall skulle innebära.	X	-

Ledning och samordning, panel L:1

Begrepp	*Definition*	*HB550*	*SIS-TR 50:2015*
Informations-säkerhet	Informationssäkerhet handlar om hur vi på ett förtroendefullt och säkert sätt kan hantera den information inom vår verksamhet och som vi har i såväl pappersdokument som i våra digitala system.	-	-
Ansvar	Skyldighet att se till att något utförs på angivet sätt inom ett avgränsat område. Till ansvaret hör befogenheter och beslutsmandat samt att stå till svars för om något inte utförts på angivet sätt.	n/a	n/a
Tillgänglighet	Att informationstillgångar är tillgängliga i förväntad utsträckning och inom önskad tid för behöriga användare.	X	X
Informations-klassning	Att klassa information utifrån de konsekvenser som kan uppkomma vid brister eller förlust av konfidentialitet, riktighet och tillgänglighet hos information.	n/a	n/a

Risk	Tänkbar och oönskad händelse som, om den inträffar, bedöms hindra eller försvåra att mål nås. En risk uttrycks ofta som en kombination av sannolikheten att händelsen inträffar och de konsekvenser den bedöms kunna medföra.	X	-

Ledning och samordning, panel L:2

Begrepp	*Definition*	*HB550*	*SIS-TR 50:2015*
Informations-säkerhet	Samtliga tekniska och regelmässiga åtgärder som skyddar organisationens information.	-	-
Ansvar	Tydligt ägande och innehavande av processens, inom tilldelade områden, förutsättningar, händelser och effekter.	n/a	n/a
Tillgänglighet	Att informationen är tillgänglig för den som har behov och rätt till åtkomst till den när den behövs.	X	X
Informations-klassning	En metod för att kategorisera en informationsmängd utifrån dess behov av skydd avseende tillgänglighet, riktighet och konfidentialitet. Till varje klass knyter man en uppsättning skyddsåtgärder.	n/a	n/a
Risk	En sammanvägning av sannolikheten för att en oönskad händelse ska inträffa och konsekvensen av den.	X	-

Ledning och samordning, panel L:3

Begrepp	*Definition*	*HB550*	*SIS-TR 50:2015*
Informations-säkerhet	Informationssäkerhet är ytterst en kvalitetsfråga och inbegriper alla delar av myndighetens verksamhet. Oavsett vilken form informationen har, eller på vilket sätt den överförs eller lagras, måste den få ett tillräckligt skydd avseende korrekthet och fullständighet, tillgänglighet, skydd mot obehörig åtkomst, tillgrepp, skada och förstörelse och kunna spåras och återskapas.	X	X
Ansvar	Oavsett roll i organisationen så har man som medarbetare ansvar för den verksamhet man arbetar med avseende informationssäkerhet. Ansvaret finns innan, under och efter anställning. Personalansvarig chef ansvarar för att informera om vad som specifikt gäller för dina arbetsuppgifter vad gäller avseende skyddet och ansvaret för informationen avseende dina arbetsuppgifter.	n/a	n/a
Tillgänglighet	Att använda informationen ska kunna motiveras ur arbetssynpunkt, d v s bara för att man har behörighet så har man inte automatiskt rätt att tillgängliggöra sig den. Med andra ord så ska informationen vara tillgänglig och användas enkom av dem som är behöriga att ta del av den samt när behovet finns för att lösa arbetsuppgiften.	X	X
Informations-klassning	Informationsklassning är ett sätt att säkerställa att information erhåller en lämplig skyddsnivå med hänsyn tagen till informationens värde och de risker som omger den. Information klassas i termer av rättsliga krav, värde, verksamhetsbetydelse och känslighet för obehörigt röjande eller modifiering. Som hjälp används kriterierna konfidentialitet, riktighet, spårbarhet och tillgänglighet. Med konfidentialitet avses att informationen inte får göras tillgänglig eller avslöjas för obehöriga. Med riktighet avses att informationen inte ska kunna förändras	n/a	n/a

	och förvanskas av misstag eller av någon obehörig. Med tillgänglighet avses att informationen ska finnas till hands för behöriga användare då den behövs. Resultatet från de olika klassificeringarna skall utgöra det samlade kravet på nivån för skyddet av den aktuella informationen eller IT-systemet.		
Risk	Säkerhetsarbetet är riskbaserat. Det innebär att skyddsåtgärder regelbundet ska bedömas och anpassas utifrån hur verksamheten förändras eller när det uppstår ändrade förutsättningar i omvärlden (både internt som externt) som har eller kan ha påverkan.	X	-

Ledning och samordning, panel L:4

Begrepp	*Definition*	*HB550*	*SIS-TR 50:2015*
Informations-säkerhet	Informationssäkerhet är de åtgärder som vidtas för att förhindra att information: görs tillgänglig för eller i övrigt kommer obehöriga till del (konfidentialitet), förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning (riktighet), och information ska kunna utnyttjas i förväntad utsträckning och inom önskad tid (tillgänglighet).	X	X
Ansvar	Ansvar och styrning ur ett informationsperspektiv behövs för att säkerställa att informationen är anpassad till samtliga intressenters behov samt till gällande regler och riktlinjer.	n/a	n/a
Tillgänglighet (2 med samma poäng)	I informationssäkerhetssammanhang avses möjlighet att komma åt information när och där den behövs.	X	-
	Att information finns då när den behövs. Den brukar handla om tre företeelser: - vardagsrobusthet - krav på tillgång till information i dagligt arbete; - återställning av information efter förlust - krav på att få	X	-

	tillbaka information efter en incident eller katastrof, det brukar handla om krav på backupper; - tillgång till information i framtiden - krav på arkivering.		
Informations-klassning	Att genom konsekvensanalys värdera sin information utifrån aspekterna konfidentialitet, riktighet och tillgänglighet.	n/a	n/a
Risk	Sannolikheten och konsekvensen av att ett hot/en händelse inträffar.	X	-

Systemutveckling och förvaltning, panel S:1

Begrepp	*Definition*	*HB550*	*SIS-TR 50:2015*
Informations-säkerhet	Information är en grundläggande byggsten i vår organisation. Informationssäkerhet omfattar både administrativa rutiner med policys och riktlinjer samt tekniskt skydd med bland annat brandväggar och kryptering. Det handlar om att ta ett helhetsgrepp och skapa en fungerande långsiktig process för att ge organisationens kritiska information det skydd den förtjänar. Informationssäkerhet syftar till att upprätthålla önskad nivå av konfidentialitet, riktighet och tillgänglighet för våra informationstillgångar.	X	X
Ansvar	Detta är de skyldigheter och uppgifter en person har att fullgöra. Ett ansvar kan aldrig delegeras, däremot uppgifter kopplade till ansvaret.	n/a	n/a
Tillgänglighet	Information som behövs ska vara åtkomlig på ett enkelt men ändå kontrollerat sätt. Information ska vara åtkomlig utan onödig fördröjning.	X	-
Informations-klassning	Informationsklassning är en hjälp för informationssäkerhetsansvariga och informationsägare att vidta skyddsåtgärder för att uppnå rätt nivå av informationssäkerhet.	n/a	n/a

	Informationsklassning mäts enligt: konfidentialitet, tillgänglighet, riktighet och spårbarhet.		
Risk	Risk beskriver i vilken grad information, fysiska objekt, personal och omgivning kan råka ut för olika hot, som på något sätt skadar, förändrar eller förstör objektet.	-	-

Säkerhetsteknik, panel T:1

Begrepp	*Definition*	*HB550*	*SIS-TR 50:2015*
Informations-säkerhet	Informationssäkerhet är den övergripande säkerheten som omfattar både tekniskt (IT-säkerhet) och administrativt (regler och rutiner) skydd och syftar till att informationen alltid skall vara korrekt, tillgänglig som avsett och skyddad från obehörigt tillträde.	-	-
Ansvar	Ansvar tilldelas en person eller roll och innebär att denne är ålagd att tillse att arbetet sker enligt de regler som har fastställts och innebär att personen/rollen också har mandat att fatta beslut och leda arbetet inom ansvarsområdet.	n/a	n/a
Tillgänglighet	Tillgänglighet innebär att informationen är nå- och användningsbar på den tid och på det sätt som har beslutats för den/de som skall använda den.	X	-
Informations-klassning	Informationsklassning är en process som syftar till att bedöma informationens värde och skyddsbehov så att rätt åtgärder kan vidtas för att informationen skall få rätt hantering och skydd.	n/a	n/a
Risk	Kombination av sannolikheten för att en incident(oönskad händelse) ska inträffa och konsekvenserna av en sådan händelse.	X	-

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB976 - februari 2016 ISBN 978-91-7383-644-9