Enheten för systematiskt informationssäkerhetsarbete

Bilaga – Framgångsfaktorer och exempel

Denna bilaga är resultatet av en förfrågan om att få tillgång till exempel på tillämpningar på de steg som beskrivs i Metodstödet och få ta del av de framgångsfaktorer som olika organisationer velat dela med sig av. Frågan ställdes till målgruppen kommuner, regioner och länsstyrelser. Alla inkomna exempel visas inte i sin helhet utan används för att illustrera hur en aktivitet i Metodstödet kan genomföras. Strukturen på denna bilaga efterföljer strukturen i ”Metodstöd för systematiskt informationssäkerhet – en översikt”. För varje aktivitet presenteras först framgångsfaktorer därefter exempel där någon av metodstödets rekommenderade aktiviteter genomförts.

3. Identifiera och analysera

Verksamhetsanalys

Framgångsfaktorer

- Kartlägg även intressenter och förutsättningar som kan ha stor informell påverkan. Det kan vara personer som har stort informellt inflytande i organisationen, eller personer som redan är engagerade i dessa frågor och som kan hjälpa till att driva frågorna. Ta reda på om det finns informella arbetssätt och beslutsvägar.
- Fokusera på de mest kritiska informationstillgångarna, men glöm inte att ha en helhetssyn så att viktiga informationstillgångar inte förbises.
- Glöm inte organisationens gemensamma infrastruktur men även stödsystem som kan vara kritiska eftersom verksamhetssystem kan vara beroende av sådana.
- Informationstillgångar är inte bara sådana som ”ägs” av organisationen. Externa informationstillgångar som organisationen är beroende av kan vara kritiska liksom informationstillgångar som är gemensamma, t.ex. med samarbetsparters eller systemleverantörer.

Exempel

Analys Verksamhet - Interna förutsättningar			Datum: Version:
Kategori	**Förutsättning**	**Beskrivning**	**Krav / Påverkan**
Policyer Mål Strategier	Vision för kommunen		Beskriv hur infosäkarbetet kan användas för att förverkliga visionen. Skulle kunna användas som hävstång för arbetet. Men sannolikt inte alltför effektivt.
Policyer Mål Strategier	Informationssäkerhetspolicy	Innehåller mål, ansvar och uppdrag på ett mycket övergripande plan	Styr det interna informationssäkerhetsarbetet
Policyer Mål Strategier	Internkontrollplan		Informationssäkerhet kan läggas in som en kontrollpunkt. Alltså ingen direkt påverkan på området utan snarare som ett sätt att implementera infosäkarbetet på ett strukturerat
Policyer Mål Strategier	Policy personuppgiftshantering	Beskrivning av hur kommunen lever upp till kraven i GDPR	Möjlighet att få in informationssäkerhetsarbetet i detta på ett bra sätt.
Policyer Mål Strategier	Nämndmål		Beskriv hur infosäkarbetet kan användas för att nå nämndmål. Handlar om att använda det som hävstång för att öka intresset och engagemanget för infosäkfrågorna.
Verksamhetsstyrning	Stratsys	Verksamhetssystem för måluppföljning	Kan användas för att integrera informationssäkerhetsarbetet i övriga processer och/eller få till en bra uppföljning av arbetet.
Verksamhetsstyrning	Avsaknad av förvaltningsmodell verksamhetssystem		Gör det svårare att fördela ansvar för informationssäkerhetsarbetet. Svårare att få ett löpande arbete och svårare att följa upp.
Verksamhetsstyrning	Verksamhetsplanering	Respektive verksamhets planering av året som kommer	Går det att få in aktiviteter kopplade till informationssäkerhet i dessa?
Verksamhetsstyrning	Informationssäkerhetsrutiner och -dokument	Hur personal ska agera vg hantering av information. Klassning av informationstillgångar.	Konkret styrning av informationssäkerhetsarbetet. Dels dokument på kommunövergripande nivå och dokument på verksamhetsnivå.
Verksamhetsstyrning	Rutiner för hantering av personuppgifter	Styrning för hur personal ska hantera personuppgifter för att följa GDPR	
Verksamhetsstyrning	Interna rutiner riktade mot personal	T.ex. för bokning av bilar, rutiner för agerande i sociala medier, för besvarande av mail mm. Finns väldigt många	Läs igenom för att se var man kan föra in informationssäkerhetsrelaterade krav
Verksamhetsstyrning	Kommunövergripande riktlinjer för vissa processer	T.ex. rutin för upphandling.	Läs igenom för att se var man kan föra in informationssäkerhetsrelaterade krav
Organisationskultur	*Behöver göras för respektive förvaltning?*	Till viss del liknande kultur i de olika verksamheterna. Men skiljer sig mycket mellan t.ex. skola, vård, kultur, kommunalteknisk infrastruktur	

Omvärldsanalys

Framgångsfaktorer

- Ta stöd av kollegor i branschen/sektorn, gemensamma förbund eller föreningar som har liknande förutsättningar i omvärlden. Viktigt att nätverka!
- Kommande rättsliga krav kan identifieras i exempelvis politiska uttalanden och i utredningar (t.ex. SOU).

Exempel

Analys Omvärld - Externa intressenter — Datum: — Version:

Kategori	Intressent	Roll	Krav / Påverkan
Styrning nationell nivå	Riksdag	Stiftar lagar	Stiftar lagar som styr informationssäkerhetsarbetet. T.ex. OSL, HSL,
Styrning nationell nivå	Statliga myndigheter	Utfärdar förordningar och allmänna råd som styr informationssäkerhetsarbetet. Övrig informell styrning genom metoder för genomförande av verksamhetsprocesser mm	Kravställare.
Styrning regional nivå	Länsstyrelsen Västra Götaland	Kan ge stöd i det övergripande arbetet med informationssäkerhet	Ingen större påverkan.
Ägare	Kommuninvånare		Förväntan att kommunen håller en tillräcklig standard för informationssäkerhet. Kan negativt påverkas vid bristfällig informationssäkerhet.
Mottagare	Kunder tjänsteköp kommunalteknisk infrastruktur	Exempel på personer som är mottagare av en viss kommunal tjänst/insats	Förväntan att deras uppgifter skyddas på ett tillräckligt bra sätt.
Mottagare	Brukare inom omsorg	Exempel på personer som är mottagare av en viss kommunal tjänst/insats	Förväntan att deras uppgifter skyddas på ett tillräckligt bra sätt.
Mottagare	Elever	Exempel på personer som är mottagare av en viss kommunal tjänst/insats	Förväntan att deras uppgifter skyddas på ett tillräckligt bra sätt.
Mottagare	*Övriga utöver ovan nämnda*		
Granskare	Media		Kan granska informationssäkerhetsarbetet. Medarbetare kan sprida information till media på grundlagsskyddat sätt som kan påverka informationssäkerhetsarbetet, påverka kommunens förtroende mm
Granskare	Revision	Reviderar kommunens arbete inom olika verksamhetsområden.	Kan granska informationssäkerhetsarbetet
Granskare	Tillsynsmyndigheter (beroende på verksamhet. Skolinspektionen, IVO, Livsmedelsverket mm. NIS-direktivets tillsynsmyndigheter. Datainspektionen.)	Granskar hur berörd verksamhet hanterar informationssäkerhetsrelaterade krav.	Granskar hur berörd verksamhet hanterar informationssäkerhetsrelaterade krav.

Riskanalys

Framgångsfaktorer

- Det är mycket viktigt att man bjuder in rätt deltagare till riskanalyser, och att dessa i god tid får information om vad som förväntas av dem. Deltagarna bör få i uppgift att innan själva riskanalysen förbereda sig genom att t.ex. kartlägga sitt område, t.ex. jurister – rättsliga krav, it-säkerhet – befintlig it-miljö och möjliga verktyg, verksamheten – vad syftet är och varför vill man göra det man vill.
- Använd aktuella beskrivningar av hotbild, exempelvis i trend- och årsrapporter (internationella, nationella och sektorspecifika).

Exempel

Exempel 1: *Tillvägagångssätt för riskanalys för att ta fram organisationens generella riskbild*

Omfattning
Riskanalysen var organisationsövergripande, men fokuserade på cybersäkerhetsrelaterade risker, dvs. risker som kan härledas till digital information och som direkt eller indirekt har koppling till internet, eftersom denna typ av risker ökar mest och är mest föränderliga.

Angreppssätt
Denna alternativa riskanalysmetod användes eftersom det på en övergripande nivå antogs vara omöjligt att identifiera alla risker i en stor och komplex organisation. Ett scenario, t.ex. att en medarbetares persondator försvinner, kan ha en mängd olika sannolikheter och konsekvenser beroende på omständigheter, t.ex. Var datorn krypterad? Vilken roll tillhörde datorn? Vad fanns för information på den? Var den säkerhetskopierad? Endast en sådan händelse kan alltså innebära en mängd risker med olika storlek.

Vidare gjordes riskanalysen med utgångspunkt i att organisationens hotbild inte är unik, utan delas till stora delar med andra organisationer. Därför analyserades både en generell hotbild och organisationens förhållanden och resulterade i en övergripande riskbild för organisationen. Riskbilden exemplifierades med några riskscenarier.

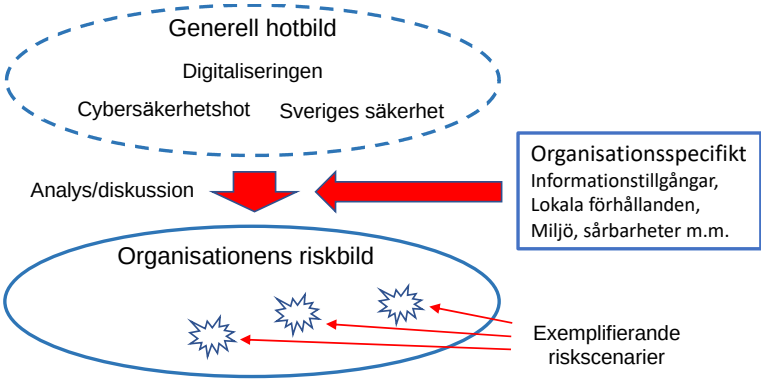
Arbetsordning
Riskanalysen bestod av tre steg:
1. Beskrivning av generell hotbild
2. Framtagning av organisationens riskbild
3. Framtagning av exempel på riskscenarier

Den generella hotbilden togs fram innan själva workshopen. Som underlag användes ett antal aktuella internationella och nationella rapporter, exempelvis Regeringens skrivelse *Nationell strategi för samhällets informations- och cybersäkerhet*, *Enisa Threat Landscape 2017*, *OWASP Top 10*, *2017*, *Säpos årsbok, 2017* och *FRA:s årsrapport 2017*. Den generella hotbilden kom att bestå av tre delar: samhällets digitalisering, generella cybersäkerhetshot och

det svenska säkerhetsperspektivet. Digitaliseringen är inget hot i sig, men utvecklingen kan medföra en ökad riskexponering och ökade sårbarheter.

Framtagning av organisationens riskbild gjordes också innan riskanalysen i workshopform och tog avstamp i den generella hotbilden. En analysgrupp diskuterade hur giltiga de generella hoten var för organisationen. För att hot ska utgöra risker mot organisationen ska det bedömas som möjligt att de riktas mot organisationen och att de i så fall ska kunna medföra skada. Här användes de tidigare analyserna av verksamhet och omvärld som grund, bl.a. för att bedöma de huvudsakliga värdena av informationstillgångar och befintliga och rättsliga krav.

Till sist valdes några exemplifierande specifika risker ur riskbilden i form av scenarier som värderades och placerades i en riskmatris. Arbetsordningen illustreras nedan.



Resultat
Den övergripande riskbilden kan sedan användas som underlag vid val av säkerhetsåtgärder och som viktigt ingångsvärde vid lokala, mer specifika risk-analyser av t.ex. processer, system och tjänster. Omvänt kan risker som identifieras på lokal nivå vara viktiga ingångsvärden för att efterhand revidera den övergripande riskbilden

Exempel 2: Riskanalys

Steg 1 - Identifiering av hot & sårbarheter					Steg 2 - Riskbedömning					Steg 3 - Riskhantering							
Skyddsvärt Skyddsvärda tillgångar relevanta för analysen		Hot Möjlig, oönskad händelse med negativa konsekvenser		Sårbarheter Problem/brister/orsaker som ligger till grund för hoten	Konsekvensbeskrivning Beskrivning av de troliga konsekvenserna om hotet inträffar.	Riskbedömning innan åtgärd			Fortsatt analys? Vilka risker som ska vidare till steg 3?	Åtgärdsförslag Vad kan göras för att eliminera, begränsa eller bevaka riskerna och dess sårbarheter?	Ansvarig för åtgärd Vem/vilka ansvarar för åtgärderna?	Ägare risk Vem äger risken och har övergripande ansvar för att åtgärderna genomförs?	Tidplan När ska åtgärden vara genomförd	Uppföljning Åtgärd genomförd?	Riskbedömning efter åtgärd		
						Konsekvens	Sannolikhet	Riskvärde							Konsekvens	Sannolikhet	Riskvärde
ID	*Tillgång*	*ID*	*Hot*	*Sårbarhet*	*Konsekvens*												
	Anmälan kränkande behandling	1	Obehörig får del av uppgifterna	Dokumentet läses/stjäls ur postfack för internpost	Integritetskänsliga uppgifter om elever och personal sprids. Kan orsaka psykisk skada, påverka skolgång, anställningsförhållanden mm.	2	1	2		Skicka inte med internpost. Ny rutin för hantering av denna typ av information.	Barn- och utbildningschef fattar beslut om reviderad blankett och regler. Rektorer implementerar			2018-08-31			
	Anmälan kränkande behandling	2	Obehörig får del av uppgifterna	Digitalt dokument skickas till fel e-postmottagare	Integritetskänsliga uppgifter om elever och personal sprids. Kan orsaka psykisk skada, påverka skolgång, anställningsförhållanden mm.	2	2	4		Uppmana till noggrannhet vid hantering av sekretessbelagd information	Rektor						
	Anmälan kränkande behandling	3	Obehörig får del av uppgifterna	Pärm med samlade anmälningar stjäls/läses. Kan ske i arbetslag, hos rektor eller KLK	Integritetskänsliga uppgifter om elever och personal sprids. Kan orsaka psykisk skada, påverka skolgång, anställningsförhållanden mm. Många personer drabbas av intrånget.	3	2	6		Förvara i låsta utrymmen. Gallra i pärmar när handlingarna inte längre behöver sparas där (långtidslagras i kommunarkiv). Se över dokumenthanteringsplan.	Rektor, arbetslag och kommunsekreterare						
	Anmälan kränkande behandling	4	Obehörig får del av uppgifterna	Personal/politiker för informationen vidare till obehörig (kollega, familj, vän)	Integritetskänsliga uppgifter om elever och personal sprids. Kan orsaka psykisk skada, påverka skolgång, anställningsförhållanden mm.	2	3	6		Tydliga och kända regler för hur hantera sekretessbelagd information. Verksamhetsanpassad utbildning till personal och politiker.	Barn- och utbildningschef samt rektorer						
	Anmälan kränkande behandling	5	Obehörig får del av uppgifterna	Någon läser dokumentet när det skickas med internposten	Integritetskänsliga uppgifter om elever och personal sprids. Kan orsaka psykisk skada, påverka skolgång, anställningsförhållanden mm.	2	1	2		Skicka inte med internpost. Ny rutin för hantering av denna typ av information.	Barn- och utbildningschef fattar beslut om reviderad blankett och regler. Rektorer implementerar			2018-08-31			
	Anmälan kränkande behandling	6	Obehörig får del av uppgifterna	Dokumentet levereras till fel person via internposten	Integritetskänsliga uppgifter om elever och personal sprids. Kan orsaka psykisk skada, påverka skolgång, anställningsförhållanden mm.	2	2	4		Skicka inte med internpost. Ny rutin för hantering av denna typ av information.	Barn- och utbildningschef fattar beslut om reviderad blankett och regler. Rektorer implementerar			2018-08-31			

Gapanalys

Framgångsfaktorer

- Inte lägga ned för mycket tid vid den övergripande gapanalysen på att välja/fastställa säkerhetsåtgärder. Ofta kan det vara bra att använda säkerhetsåtgärderna i Bilaga A rakt av + eventuellt ytterligare några man hittat genom riskanalysen när man genomför gapanalysen. Vid gapanalysen upptäcker man ofta om någon säkerhetsåtgärd är irrelevant.
- Tänk på att du kan behöva analysera djupare när du tar dig an ett område för att du ska förstå vilka säkerhetsåtgärder som verkligen saknas och som behöver tas fram som en del av att utforma åtgärdsplan.

4. Utforma

Organisation

Framgångsfaktorer

- Bättre att ta fram en enkel organisation till att börja med, roller kan utökas efter hand. Viktigast är att det är ett tydligt ansvar i de roller som utpekas och att det finns ett engagemang hos dessa.
- Bra att tänka igenom hur rollerna passar in i linjeorganisationen så att inte någon får ett ansvar som den inte har möjlighet att upprätthålla då den saknar mandat att agera.

Exempel

Befattning	Rollbeskrivning	Ansvarsprofil	Uppgifter	Namn
Informationssäkerhetschef	Exempel: Samordnar företagets arbete med informationssäkerhet. Har personalansvar för informationssäkerhetsgruppen	Referens eller länk till dokument.		
Kommunfullmäktige		Se informationssäkerhetspolicy	Beslutar om informationssäkerhetspolicy Fatta beslut om uppdatering av policy vid behov	
Kommunstyrelse		Se informationssäkerhetspolicy	Uppsiktsplikt över andra nämnder och styrelser. Personuppgiftsansvarig.	
Nämnd/styrelse		Se informationssäkerhetspolicy	Ansvar för informationssäkerhetsarbetet inom sitt ansvarsområde. Ska bedöma behov av särskilda rutiner inom sitt ansvarsområde Upprätta årlig rapport över informationssäkerhetsarbetet. Personupgiftsansvariga	
Kommunchef & ledningsgrupp		Se informationssäkerhetspolicy	Fattar beslut om styrdokument på lägre nivå (rutin)	
Förvaltningschef		Se informationssäkerhetspolicy	Operativt ansvar för informationssäkerhetsarbetet Ansvar för att informationsklassning genomförs Ansvarig för att systemsäkerhetsplan tas fram för vissa tillgångar. Se till att informationsklassning genomförs. Se till att systemsäkerhetsplaner tas fram vid behov.	
Medarbetare		Se informationssäkerhetspolicy samt rutin för informationssäkerhet	Känna till och följa styrning kring informationssäkerhet	
Dataskyddsombud		Se struktur för dataskyddsarbetet i MTG	Ge råd till verksamheter Kontaktpunkt för registrerade och tillsynsmyndighet Kontroll och granskning.	
Dataskyddssamordnare		Se struktur för dataskyddsarbetet i	Informationssäkerhetsrelaterade uppgifter inte beskrivna	

Informationssäkerhetsmål

Framgångsfaktorer

- Knyt målen till organisationens övriga mål, och visa hur informationssäkerheten stödjer eller möjliggör dessa. Detta är oftast lättast med de strategiska målen.
- Haka på frågor som för närvarande och framöver är eller förväntas vara viktiga för organisationen. Det kan exempelvis vara kvalitetsarbete eller digitalisering av hela eller delar av organisationen.

Exempel

Informationssäkerhetsmål - Exempel

Kortsiktiga informationssäkerhetsmål (1–2 år)

Färdigställande och implementering av LIS

- Alla funktioner med utpekat ansvar ska medvetandegöras om sitt ansvar
- Producera alla styrande dokument som behövs för att ett komplett LIS ska finnas
  - Informationsklassningsmetod. Inklusive säkerhetsåtgärder för respektive skyddsnivå
  - Metod för systemsäkerhetsanalys eller liknande
- Inför informationssäkerhetskrav i relevanta processer och styrdokument:
  - -Upphandling
  - Nyanställning, förändring, avslut av anställningar
  - Utbildning av/information till nya chefer. Chefshandbok och dylikt

Övriga mål

- Inventera informationstillgångar för alla verksamheter
- Påbörja informationsklassning för mest kritiska informationstillgångar
- Implementering av NIS-direktivet
- All personal ska få en grundläggande utbildning (redan gjort en gång i o m nanoloarning)
- Stöd för hur loggkontroll kan genomföras och dokumenteras
- Systemförvaltningsmodell behöver införas/inför informationssäkerhetsarbetet i den grundläggande metod som IT-avdelningen tar fram
- Bedömningar har gjorts av om verksamhetsspecifika styrdokument behöver tas fram

Prioriterade säkerhetsåtgärder

- Hantering av enheter
  - Vid uthämtning av dator och mobil, få läsa igenom dokument och skriva under. Hanteringsregler tyd.
  - MDM eller liknande. På kontroll över vilka telefoner som finns därute, hur de används, att de lämnas tillbaka.
- Tydligare rutiner för testning av back-up

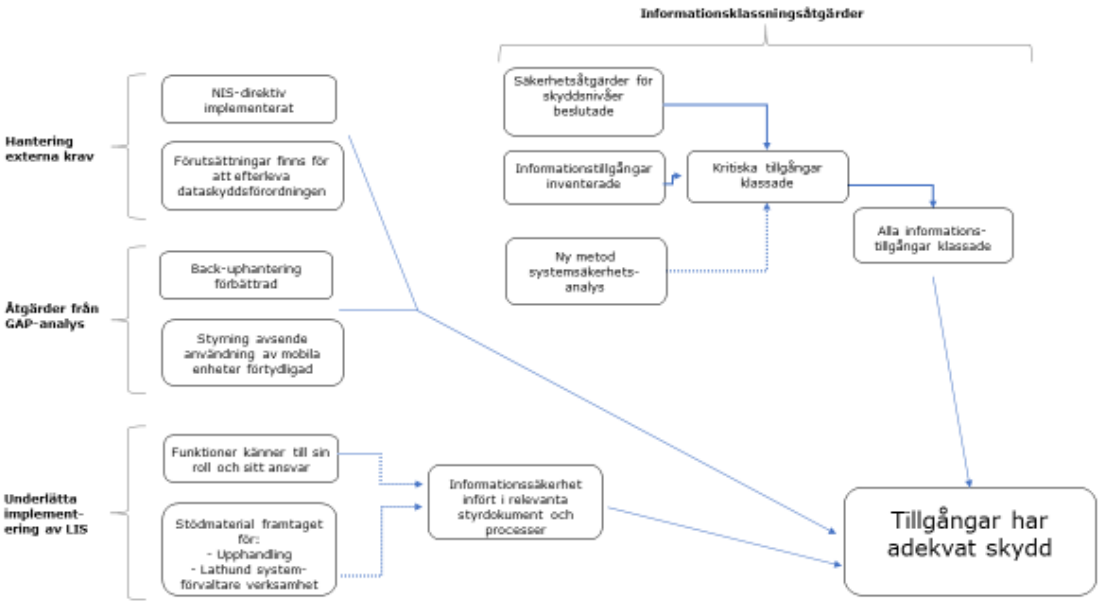
Strategiska informationssäkerhetsmål (3–5 år)

A. Alla kommunens informationstillgångar ska omfattas av en tillräcklig skyddsnivå med hänsyn till konfidentialitet, riktighet, tillgänglighet och spårbarhet. Rätt information ska finnas tillgänglig när den behövs för behörig person och på ett spårbart sätt.

B. Kommunens informationstillgångar ska klassificeras med hänsyn till krav på konfidentialitet, riktighet, spårbarhet och tillgänglighet. Därigenom kan lämpliga skyddskrav ställas upp för respektive informationstillgång. För de tillgångar som bedöms vara särskilt viktiga ska en informationsägare utses och riskanalyser upprättas.

C. För de verksamhetssystem som i informationsklassificeringen konstateras vara kritiska för verksamheten ska en systemsäkerhetsplan upprättas och hållas uppdaterad.

D. Informationsklassificering ska genomföras innan upphandling av nya verksamhetssystem i syfte att säkerställa relevant kravställning på systemet.



Styrdokument

Framgångsfaktorer

- Styrdokument som är underliggande till informationssäkerhetspolicyn, som anvisningar och instruktioner är ofta omfattande och riktar sig till olika målgrupper. De bör därför anpassas för dessa, exempelvis genom uppdelning i olika kapitel.
- Styrdokument måste vara tydliga, lätta att hitta i och att förstå. Ta gärna hjälp av kommunikatörer för arbetet med att utforma och kommunicera styrdokument.
- Håll nere antalet anvisningar och se om du kan föra in instruktioner gällande informationssäkerhet i målgruppernas befintliga dokumentation som beskriver hur de ska utföra olika arbetsuppgifter.

Klassningsmodell

Framgångsfaktorer

- Klassningsmodellen med tillhörande säkerhetsåtgärder kan gärna finnas med i styrdokument som anvisning, eventuellt med tillhörande instruktioner för hur man genomför klassning. Då kan de beslutas och kommuniceras samtidigt som övrigt regelverk.
- De flesta medarbetare behöver inte ”störas” med en hel klassningsmodell, utan det räcker att de har vetskapen om klassningsnivåer för aspekten konfidentialitet.
- Se över om riskbedömningsmodellens konsekvensnivåer är lämpliga att använda. Konkretisera utifrån vilka kriterier som bedömningen ska göras så att det går att förstå vad som är t.ex. ”allvarligt”, ”betydande” och ”måttligt/försumbart” i din organisation.

Exempel

Tabell 1 Informationssäkerhetsklassning

		Konfidentialitet	Riktighet	Tillgänglighet
4	Synnerligen allvarlig	K4 Röjande av informationen medför skada för rikets säkerhet som inte endast är ringa. Systemet behandlar information som omfattas av sekretess och rör rikets säkerhet (hemliga uppgifter) där röjande av information kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger. Informationen omfattas av t ex säkerhetsskyddslagstiftningen. (Skada för rikets säkerhet som inte endast är ringa.)	R4 Uppgifter som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför skada för rikets säkerhet som inte endast är ringa. Systemet behandlar information som omfattas av sekretess och rör rikets säkerhet (hemliga uppgifter) där felaktig information kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger. Informationen omfattas av t ex säkerhetsskyddslagstiftningen. (Skada för rikets säkerhet som inte endast är ringa.)	T3 Ett avbrott som medför skada för rikets säkerhet som inte endast är ringa. Systemet behandlar information som omfattas av sekretess och rör rikets säkerhet (hemliga uppgifter) där otillgänglighet kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger. Informationen omfattas av t ex säkerhetsskyddslagstiftningen. (Skada för rikets säkerhet som inte endast är ringa.)
3	Allvarlig Hög skyddsnivå	K3 Information där förlust av konfidentialitet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	R3 Information där förlust av riktighet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	T3 Information där förlust av tillgänglighet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ
2	Betydande Utökad skyddsnivå	K2 Information där förlust av konfidentialitet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	R2 Information där förlust av riktighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	T2 Information där förlust av tillgänglighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
1	Måttlig Grundläggande skyddsnivå	K1 Information där förlust av konfidentialitet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	R1 Information där förlust av riktighet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	T1 Information där förlust av tillgänglighet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
0	Ingen Ingen skyddsnivå	K0 Information där förlust av konfidentialitet inte medför någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ	R0 Information där förlust av riktighet inte medför någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	T0 Information där förlust av tillgänglighet inte medför någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.

Tabell 2 Konsekvenser

		Ekonomi	Förtroende	Verksamhet	Individ
4	Synnerligen allvarlig	-	-	Allvarliga konsekvenser för rikets säkerhet	-
3	Allvarlig Hög skyddsnivå	Allvarlig ekonomisk förlust innebär för organisationen en totalkostnad på mer än 2 miljoner kronor uppåt eller avvikelse på över 20 % av budget	Allvarlig förtroendeförlust innebär för Organisationen t.ex. ihållande drev i rikstäckande medier, eller av organiserade grupperingar i sociala medier. Ej endast enskilda personer pekas ut, utan även organisationens grundläggande kultur.	Allvarlig förlust av verksamhet innebär för organisationen Mycket stort produktions-bortfall Omfattande omprioriteringar av verksamheten Mycket höga återställningskostnader i tid och pengar	Allvarlig förlust av mänskliga fri och rättigheter, människors liv och hälsa innebär Svår personskada (fysisk eller psykisk) / dödsfall hos medborgare eller medarbetare (inkl. dennes familj)
2	Betydande Utökad skyddsnivå	Betydande ekonomisk förlust innebär för Organisationen en totalkostnad på mellan 500 000 kr och 2 miljoner kronor eller avvikelse på 10-20% av budget	Betydande förtroendeförlust innebär för Organisationen exempelvis nyheter i både riks- och lokalmedia och i organiserade grupperingar i sociala medier. Missnöjet är dock begränsat till enskilda händelser eller enskilda personers agerande.	Betydande förlust av verksamhet innebär för organisationen Stort produktions-bortfall Stora omprioriteringar av verksamheten Höga återställnings-kostnader i tid och pengar	Betydande förlust av mänskliga fri och rättigheter, människors liv och hälsa innebär Lindrig personskada (fysisk eller psykisk) hos medborgare eller medarbetare (inkl. dennes familj) Allvarliga hot och kränkningar
1	Måttlig Grundläggande skyddsnivå	Måttlig ekonomisk förlust innebär för Organisationen en totalkostnad på under 500 000 kr eller avvikelse på 5-10% av budget	Måttlig förtroendeförlust innebär för Organisationen exempelvis enstaka missnöjda kunder som uttalar sig i sociala medier, eller en mindre notis i lokalpress.	Måttlig förlust av verksamhet innebär för organisationen Måttligt produktions-bortfall Mindre omprioriteringar av verksamheten Måttliga återställningskostnader i tid och pengar	Måttlig förlust av mänskliga fri och rättigheter, människors liv och hälsa innebär Ingen personskada Lindriga hot och kränkningar
0	Ingen Ingen skyddsnivå	-	-	-	-

Handlingsplan

Framgångsfaktorer

- Håll en realistisk ambition i den årliga handlingsplanen som organisationen mäktar med.
- Undvik nyckelpersonsberoende när roller anges för olika aktiviteter som ansvariga och utförare.

Exempel

Exempel 1:

Mål	Aktivitet/säkerhetsåtgärd	Hur ska åtgärden göras?	Prioritet	Ansvarig	Startdatum	Slutdatum	Status
	Implementera NIS-direktiv VänerEnergi (plus stöd för bredare infosäkarbete)	Processledning i deras anpassning till direktivets krav (samma moment som för VA-avdelning). Processledning i ett bredare informationssäkerhetsarbete.	Välj	Välj			Välj
			Välj	Välj			Välj
			Välj	Välj			Välj
	Besluta om säkerhetsåtgärder till klassningsnivåer	Koppla säkerhetsåtgärder från ISO 27002 samt övriga eventuella åtgärder till klassningsnivåer. Söka samarbete med annan kommun?	Välj	Välj			Välj
	Inventera informationstillgångar	Gör klart. Använd för att sedan göra M&G.	Välj	Välj			Välj
	Klassa informationstillgångar	Ta fram en beskrivning för hur verksamheter själva ska kunna göra detta på ett någorlunda smidigt sätt. Stöd verksamheter i genomförande.					
	Metod för systemsäkerhetsanalys	Inventera andra organisationers metoder för systemsäkerhetsanalyser. Ta fram en så enkel metod som möjligt. Görs i samarbete med IT-avdelningen. Och med berörda i verksmheterna - hur säkerställs deras behov?	Välj	Välj			Välj
			Välj	Välj			Välj
			Välj	Välj			Välj
	Nya rutiner back-uphantering för IT-avdelningen.		Välj	Välj			Välj
	Ta fram rutiner för hantering av dator och mobiltelefon	IT-avdelningen bör ge kort info för användare som hämtar ut dator. Den som hämtar ut bör skriva under att man förstått och accepterar villkoren.	Välj	Välj			Välj
			Välj	Välj			Välj
	Förankra informationssäkerhetsarbetet i kommunledningarna	Be att få komma till respektive kommuns ledningsgrupp.	Välj	Välj			Välj

Exempel 2:

Handlingsplan för informationssäkerhet 2019

Datum: 2019-01-01

Organisation X

Version: 1.0

								Status			
ID	Mål	Aktivitet/säkerhetsåtgärd	Prioritet	Tid/kostnad	Ansvarig	Startdatum	Slutdatum	Kv 1	Kv 2	Kv 3	Kv 4
2019-01	Det ska finnas en beslutad informationssäkerhetspolicy	Ta fram förslag och remittera informationssäkerhetspolicy	Mycket hög	40 timmar	CISO	2019-02-01	2019-06-30	Klar 30-69%	Fastställd	Välj	Välj
2019-02	Det ska finnas beslutade riktlinjer för informationssäkerhet	Ta fram förslag och remittera riktlinjer för informationssäkerhet	Mycket hög	200 timmar	CISO	2019-01-01	2019-06-30	Klar 1-29%	Klar 70-100%	Välj	Välj
2019-03	Det ska finnas en organisations-övergripande klassningsmodell	Ingår i riktlinjerna	Mycket hög		CISO	2019-02-01	2019-06-30	Klar 30-69%	Klar 70-100%	Välj	Välj
2019-04	Det ska finnas vägledning för informationssäkerhet vid upphandling	Anpassad till olika typer av tjänster och produkter. Baserad på klassningsmodellen och riktlinjer för informationssäkerhet	Hög	80 timmar	Inköpschef	2019-05-01	2019-10-01	Ej påbörjad	Klar 1-29%	Välj	Välj
2019-05	Information om organisationens informationssäkerhet ska vara synligt på intranätet	Ta fram en sida på intranätet med styrdokument, informations-material och externa länkar	Hög	40 timmar	Kommunikation	2019-06-01	2019-09-01	Ej påbörjad	Klar 1-29%	Välj	Välj
2019-06	Projektledare och förvaltningsledare ska kunna genomföra riskanalyser	Uppdatera befintlig riskanalysmetod	Mellan	40 timmar	Säkerhetschef	2019-03-01	2019-04-01	Klar 30-69%	Fastställd	Välj	Välj
2019-07	Projektledare och förvaltningsledare ska kunna genomföra riskanalyser	Ta fram och genomför halvdagsutbildning för projekt-ledare och förvaltningsledare	Mellan	20 timmar	CISO	2019-04-01	2019-06-01	Klar 70-100%	Fastställd	Välj	Välj
2019-08	Alla medarbetare ska få utbildning i informationssäkerhet	Ta fram och genomför endags-utbildning för projektledare, förvaltningsledare, verksamhetsutvecklare och IT-personal	Hög	40 timmar	CISO	2019-05-01	2019-06-30	Klar 30-69%	Fastställd	Välj	Välj
2019-09	Alla medarbetare ska få utbildning i informationssäkerhet	Ta fram e-utbildning (genomförs under 2020) i samverkan med personalavdelningen	Hög	80 timmar	CISO	2019-09-01	2019-12-31	Ej påbörjad	Ej påbörjad	Välj	Välj

5. Använda

Exempel

Ett exempel för att hantera större händelser och förändringar som incidenter, upphandlingar, nya lagar, omorganisationer och ändrade hotbilder. Klassa, analysera risker och utforma skydd fortlöpande.

Hur har ni gått tillväga och vilka svårigheter har uppstått?

I ett exempel ska en verksamhet införskaffa ett it-system. Objektägaren, i detta fall den person som ställer krav på informationssäkerhet för den informationsmängd som ska behandlas i it-systemet, tar kontakt med CISO för att få stöd i att veta vilka informationssäkerhetskrav som ska uppfyllas. För att kunna ta fram informationssäkerhetskrav behöver informationsmängden och tillhörande it-system klassas, analyseras utifrån risker och skyddas med lämpliga säkerhetsåtgärder. För att genomföra klassning, riskanalys och utformning av skydd anordnar CISO två workshoppar med objektägaren och övriga roller. Syftet med att dela upp genomförande i två workshoppar är dels att deltagare ska orka bibehålla fokus vilket kan vara svårt om en workshop drar ut på tiden, dels att ge deltagarna möjlighet till reflektion och att lämna synpunkter på befintligt material emellan workshopparna.

Mål med första workshoppen är att analysera **vad** som ska skyddas (beskriva och definiera informationsmängden) och **varför** (klassa informationsmängdens skyddsvärde utifrån interna och externa krav)**.** Inför workshoppen får objektägaren i uppdrag att beskriva informationsmängden och tillhörande it-system samt syfte och mål med behandlingar. Resultatet från första workshoppen blir ingångsvärde till den andra workshoppen. **Mål med andra workshoppen** är att analysera **risker** och behov av **säkerhetsåtgärder**. När de båda workshopparna är genomförda har objektägaren förståelse för vilken informationsmängd som ska skyddas, varför informationsmängden ska skyddas, vilka risker informationsmängden utsätts för och med vilka säkerhetsåtgärder riskerna ska bemötas.

Vi har upplevt två utmaningar. Första utmaningen är att säkerställa att kontinuitet uppnås genom att samma person i de stödjande rollerna deltar i alla aktiviteterna. Den andra utmaningen är att fastställa vilken informationsmängd som ska analyseras: när objektägaren förstår vilka krav som ställs på behandlingen av information kan detta leda till att behandlingen förändras, vilket i sig leder till nya krav.

Vilka roller är viktiga att inkludera i denna typ av aktivitet?

Förutom objektägaren är det viktigt att få med stödjande roller som juridik, dataskydd, registratur och arkiv samt att objektägaren kanske har med ytterligare någon från verksamheten.

I den andra workshoppen kan någon med kunskap om säkerhetsåtgärder, gärna tekniska sådana vara med.

Vilket värde har ni sett av att genomföra denna typ av aktivitet?
Att nå en gemensam förståelse i verksamheten för vad som är skyddsvärt är i sig kunskapshöjande. Vi har upplevt att denna kunskap sprider sig vidare i objektägarens och de stödjande rollernas verksamheter.

Klassa informationen

Framgångsfaktorer

- Genomför en eller ett par piloter som leds av CISO (el. motsv.). Instruktioner för hur klassning ska genomföras kan sedan skapas utifrån erfarenheter från dessa.

Genomföra och efterleva

Framgångsfaktorer

- Som CISO är det viktigt att inte fastna i enskilda projekt.

Utbilda och kommunicera

Framgångsfaktorer

- Utbilda nyckelpersoner, t.ex. verksamhetsutvecklare eller förvaltningsledare, som kan leda riskanalyser och klassningar.

Exempel

Målgruppers kunskapsbehov

Målgrupp	Kunskapsbehov	Aktiviteter
Alla medarbetare	Kunskap för att undvika att de skapar problem för andra (t.ex. skadlig kod). Kunskap för att säkerställa skyddet för den information de själva har tillgång till. Kräver antingen att de själva har förmåga att analysera det alternativt att en inventering av tillgångar är gjord som ger lite övergripande riktlinjer.	Generell utbildningsinsats (typ nano-learning eller dylikt). Diskussion med kollegor om vad som är viktig information och hur den behandlas. Kan göras på APT eller andra forum.
Infosäksamordnare	Tillräckligt med kunskap för att kunna fungera effektivt i rollen.	Delta i/arrangera nätverksträffar. Genomgå utbildningar och annan kompetensutveckling. Omvärldsbevakning.
IT-säkerhetschef	Känna till IT-säkerhetskrav samt status i att leva upp till dessa.	Delta i genomförande av gap-analys.
IT-avdelning	Behöver tillräckligt med kunskap för att kunna rådge medarbetare i olika situationer. IT-support behöver kunskap om hur agera vid incidenter, hantering av lösenord, Alla bör som en lägstanivå hyffsat kunna riklinjer för informationssäkerhet.	Infosäksamordnare kan komma till APT för IT-avdelningen. Omvärldsbevakning och erfarenhetsutbyte med andra motsvarande funktioner i andra organisationer.
Avdelningschefer	Behöver tillräckligt med kunskap för att kunna vägleda sin personal. Behöver känna till sin egen roll och sitt eget ansvar.	Utbildas av informationssäkerhetssamordnare.
Verksamhetschef/förvaltningschef /sektorchef	Behöver känna till sin egen roll och ansvar i enlighet med styrdokument. Behöver förståelse för varför området är viktigt.	Bokas för personliga möten med informationssäkerhetssamordnare. Kan bl.a. innehålla genomgång av analyser, incidenter och liknande som gjorts inom deras område. Gå igenom styrdokument.
Förtroendevalda	Kunskap för att undvika att de skapar problem för andra (t.ex. skadlig kod). Kunskap för att säkerställa skyddet för den information de själva har tillgång till. Kräver antingen att de själva har förmåga att analysera det alternativt att en inventering av tillgångar är gjord som ger lite övergripande riktlinjer. Förståelse för sin roll och sitt ansvar, t.ex. personuppgiftsansvarig nämnd.	Utbildning för nya förtroendevalda i februari 2019.

6. Följa upp och förbättra

Utvärdera och följa upp

Framgångsfaktorer

- Utnyttja befintliga rutiner och verktyg för uppföljning.
- Att skapa goda relationer med internrevision kan vara mycket givande.

6.2 Ledningens genomgång av informationssäkerhetsläget

Framgångsfaktorer och exempel

Ledningens genomgång

Fastslå hur och när CISO ska rapportera till ledningen.

Hur har ni gått tillväga och vilka svårigheter har uppstått?
I ett förberedande samtal med organisationens ledning föreslogs hur vår organisation kan få ett systematiskt informationssäkerhetsarbete på plats. Syftet med *Ledningens genomgång* och vad den innehåller diskuterades också. Genom förmöte med hela ledningen, där innehållet och syftet med kommande *ledningens genomgång* beskrivs och diskuteras, får alla veta vilket resultat som kommer att presenteras och vilka åtgärder de förväntas vidta.

Ledningens genomgång hålls en gång per år. Förmötet inför detta kommer jag endast begära av den händelse att en större förändring väntas i ramen för det strategiska informationssäkerhetsarbetet. Förberedande möte med närmaste chef och representant i ledningsgruppen kommer däremot att genomföras inför varje ledningens genomgång.

Vilka roller är viktiga att inkludera i denna typ av aktivitet?
Eftersom informationssäkerhetsarbetet berör hela verksamheten och stor del av uppföljningsarbetet ligger hos avdelningsledningen, är det av stor vikt att alla känner till och förstår sitt ansvar och sin roll. Att alla i ledningen tar del av informationen och engageras i arbetet är avgörande för CISO:s förutsättningar i sitt arbete med verksamheter och medarbetare. Omfattande personalomsättning, nya chefer och nya nationella direktiv kan påverka kontinuiteten och förståelsen för informationssäkerhetsarbetet. När nya avdelningschefer tillsätts bör separat genomgång kring informationssäkerhetsarbetet genomföras för dem så de förstår sin roll och sitt ansvar.

Vilket värde har ni sett av att genomföra denna typ av aktivitet?
Ledningens genomgång är en klassisk del av LIS och kan avhandlas som ett möte med en fastslagen dagordning. Men det finns alla fördelar att lägga extra energi på just denna del. Ett visst förarbete kan öka kvalitén enormt. Att du som CISO samt övriga deltagarna vet vad som ska hända ökar förutsättningarna för att du får ett konkret underlag för ditt fortsatta arbete med dig från mötet. Ledningen får, genom ett förberedande möte, möjlighet att förbereda sig, och diskutera sina förväntningar och konkreta förslag till dig innan mötet. På så sätt kan du koncentrera dig på sakfrågor och innehåll eftersom alla i rummet är insatta i syftet och vad som förväntas av dem.

Att ha beredningsmöte med ytterst ansvarig ledning och förmöte med ledningsgrupp eller liknande ökar kvalitén på *ledningens genomgång* och rekommenderas varmt.

Ledningens kontinuerliga information

Rapportera status i informationssäkerhet till ledningen minst en gång per år.

Hur har ni gått tillväga och vilka svårigheter har uppstått?
För att kunna avgöra status för informationssäkerhetsarbetet behöver uppföljning bli en naturlig del av organisationens kvalitetsarbete och övriga ledningssystem. Därför bör statusavstämningar följa organisationens övriga intervall för avstämning av kvalité, ekonomi, arbetsmiljö osv. Det naturliga blir att uppföljningen faller samman med t.ex. internkontroller och blir en del av internrevisionen. Min rapportering till ledningen sker som informationspunkt under ordinarie ledningsmöte, en till två gånger per år. Underlag för informationspunkten skickas minst en vecka i förväg för att ge ledningen möjlighet att förbereda sig och om de bedömer hinner de hålla ett beredande möte inför ledningsmötet om så skulle önskas.

Vilka roller är viktiga att inkludera i denna typ av aktivitet?
Internrevisionen är bra att ha med sig. När statusuppföljning av informationssäkerhet genomförs kan denna kompletteras med en utvärdering i enkätform som riktas till verksamheten. Där kan du fånga upp mognadsgraden kring säkerhetskulturen, effekter av internutbildning samt efterlevnad av rutiner och strategiska mål i samma utvärdering. Verksamheterna involveras i uppföljningen och alla målgrupper som berörs kan lämna svar. Det ökar medvetenheten och när utvärderingen blir årligt återkommande kommer mognaden öka ytterligare. Ser medarbetarna att deras svar resulterar i åtgärder blir effekten ännu bättre.

Svårigheter kan uppstå när uppföljning av informationssäkerhet och övriga säkerhetsområden sker överlappande och i olika former. Uppföljning av säkerhetsfrågor bör sammanföras och samköras för att ge ledningen en helhetsbild av organisationens säkerhet samt undvika onödigt merarbete och förvirring i verksamheterna.

Vilket värde har ni sett av att genomföra denna typ av aktivitet?
Att återkommande rapportera status till ledningen stärker informationssäkerhetsarbetets status och normaliserar ämnet. Informationssäkerhet vävs in i det vardagliga arbetet, blir levande och ledningens engagemang ökar. Ledningens ökade medvetenhet om informationssäkerhet och förtroende för CISO, stärker CISO:s mandat och ökar dennas möjlighet till att utveckla arbetsformer och skapa starka nätverk i organisationen.