Myndigheten för samhällsskydd och beredskap

Exempel klassningsmatris B

Det här är ett fiktivt exempel på en klassning av informationstillgångar i en kommunal verksamhet. Exemplet hör till MSB:s Metodstöd för systematiskt informationssäkerhetsarbete.

Bakgrund

Som ett led i att införa ett systematiskt informationssäkerhetsarbete i en mellanstor kommun påbörjades arbetet med klassning av informationstillgångar. En modell och ett arbetssätt för klassning togs fram och prövades i en pilotverksamhet. Därefter beslutades modellen och arbetssättet i styrdokument för informationssäkerhet. Det är den klassningsmodell och det arbetssätt som tillämpades i pilotverksamheten som beskrivs här.

Klassningsmodellen bestod av en klassningsmatris med konsekvensbeskrivningar för de olika nivåerna. Efter pilotverksamheten skulle de olika konsekvensnivåerna definieras tydligare, till exempel i form av ekonomisk förlust, och förtroendeförlust.

Vid framtagningen av klassningsmodellen gjordes bedömningen att det skulle räcka med en enkel klassningsmatris med endast tre nivåer där konsekvenserna bedöms och organisationen fastställer krav på behov av skydd. Eventuella säkerhetsskyddsklassificerade uppgifter i kommunen skulle inte omfattas av denna klassningsmatris utan sådana uppgifter skulle hanteras separat.

Klassningsmatrisen som användes i pilotverksamheten

Kravnivå	Konfidentialitet	Riktighet	Tillgänglighet
2. Höga skyddskrav	**K2** Känslig information som, om den sprids till obehöriga, kan medföra allvarliga konsekvenser för organisationen, externa aktörer eller individer.	**R2** Information som, om den ej är riktig och fullständig, kan medföra allvarliga konsekvenser för organisationen, externa aktörer eller individer.	**T2** Information som, om den ej är tillgänglig, kan medföra allvarliga konsekvenser för organisationen, externa aktörer eller individer.
1. Normala skyddskrav	**K1** Intern information som, om den sprids till obehöriga, kan medföra måttlig negativ påverkan på organisationen, externa aktörer eller individer.	**R1** Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverkan på organisationen, externa aktörer eller individer.	**T1** Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan på organisationen, externa aktörer eller individer.
0. Inga skyddskrav	**K0** Öppen information som kan spridas fritt inom och utom organisationen.	**R0** Nivån används inte då krav alltid finns på att information ska vara riktig.	**T0** Nivån används inte då krav alltid finns på att information ska vara tillgänglig.

Inledningsvis söktes en lämplig verksamhet som kunde fungera som en pilot för den framtagna klassningsmatrisen och arbetssättet. Valet föll på kommunens överförmyndarkansli. Verksamhetschefen visade intresse och det syntes vara en väl avgränsad och förhållandevis liten verksamhet och innehöll kritisk och känslig information.

Klassningsobjektet

Överförmyndarkansliet ansvarar för tillsyn över förmyndares, förvaltares och gode mäns uppdrag enligt föräldrabalken. Ansvarig politisk nämnd är Överförmyndarnämnden.

Överförmyndarkansliet är en liten verksamhet (cirka 12 medarbetare) som har ett specifikt uppdrag och är lokaliserade på ett (1) kontor.

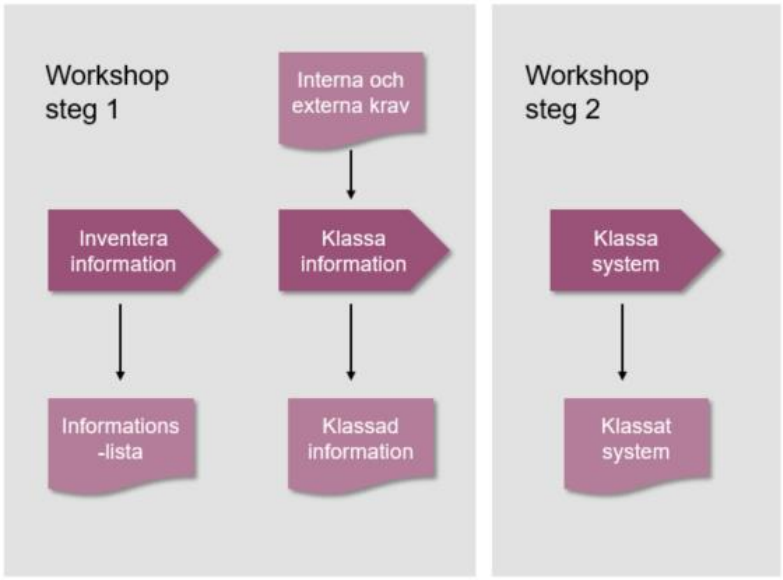
Överförmyndarkansliet har ett it-system som stödjer handläggarnas arbete med huvudmän och ställföreträdare (förmyndare, förvaltare och gode män). Det finns även ett system som används av ställföreträdarna, detta ingick dock inte i piloten.

Överförmyndarens chef och personal använder även kommunens persondatorer, e-post med mera samt några av kommunens centrala stödsystem, som exempelvis personalsystem, diariesystem och ekonomisystem. Dessa omfattades inte heller av piloten.

Arbetssätt

Arbetet genomfördes i workshopform. Deltagare vara kommunens CISO (workshopledare), överförmyndarkansliets chef, en handläggare som var väl insatt i verksamheten och dess stödsystem samt en konsult som var anlitad för att utveckla stödsystemet.

Workshopen inleddes med en kort presentation av CISO om informationssäkerhet, om klassningsmodellen och hur arbetet var tänkt att gå till. Därefter skedde workshopen i två steg (se Figur 2).



Figur 1: Workshopens två steg.

Inventering av information

Chefen för överförmyndarkansliet och handläggaren hade tillsammans goda kunskaper om vilken information som fanns i verksamheten. Inventeringen visade att det var två huvudsakliga informationsmängder som hanterades: Akt huvudman och Akt ställföreträdare. Dessa båda innehöll ett antal informationstyper som tillsammans bildade en sammanhållen informationsmängd som aldrig delades upp under hanteringen. Det kändes därför lämpligt att betrakta akterna som två informationsmängder även om innehållet i dem inventerades och bedömdes under klassningen. Utöver akterna fanns det två filer som innehöll arvode och fakturaunderlag. Även dessa betraktades som två informationsmängder även om de innehöll flera informationstyper. De totalt fyra informationsmängderna listas i Tabell 1.

Klassning av information

Grunder för bedömning hur varje informationsmängd skulle klassas var interna och externa krav, och hur allvarlig konsekvensen bedömdes vara för den egna verksamheten, kommunen i stort och huvudmän och ställföreträdare vid försämringar av konfidentialitet, riktighet och tillgänglighet. Klassningsmodellen var utformad så att normala skyddskrav (1) är ”defaultvärde”, det vill säga finns inte argument för en högre klass i respektive aspekt så ska informationstillgångar klassas på den nivån.

Under klassningen skulle alltså informationsmängderna klassas utifrån konsekvens och ges ett skyddskrav, och inte varje ingående informationstyp. Däremot var varje

informationstyp tvungen att gås igenom och bedömas, för att se om förekomsten av minst en informationstyp kunde motivera en viss nivå för informationsmängden.

Både Akt huvudman och Akt ställföreträdare bedömdes ha höga skyddskrav gällande konfidentialitet och riktighet (se Tabell 1). Skälet till detta var främst att akter ofta innehåller känsliga personuppgifter och även kan innehålla skyddade identiteter. Akt huvudman klassades dessutom i den högsta nivån avseende tillgänglighet, då på grund av höga krav på bevarande. Båda informationsmängderna i filerna klassades på den normala nivån i alla tre aspekter.

Tabell 1: Inventerad information och dessas klassning.

Informationsmängd	Informationstyper	K-R-T	Anm.
Akt huvudman	Namn, personnr, adress, namn och adress på stf, stöd, beslut, omfattning på beslut, handläggare, startdatum, tingsrätt, tidigare stf, till o från tingsrätt (offentligt), pengar som förvaltas, bankkonton, ev. skyddade identiteter	2-2-2	1) Tillgänglighet i huvudsak *bevarande* som motiverar tvåan 2) Finns även som pappersakt (2-2-2)
Akt ställföreträdare	Ställföreträdare (gode män, förvaltare), Namn, personnr, adresser, kontroller (polisens belastningsregister, k-fogden (ej innehåll)), noteringar (t.ex. att klagomål, utredning,), bedömning, skyddade identiteter	2-2-1	1) Finns även som pappersakt (2-2-1)
Arvode	Uppgifter om ställföreträdaren: anställningsnummer, belopp, sociala avgifter, namn, kontoslag, för vilken huvudman m.m. Personnummer är maskat	1-1-1	
Fakturaunderlag	Underlag till redovisningsenheten med uppgifter på huvudmannen som ska betala fakturan: belopp, namn, adress m.m.	1-1-1	

Systemklassning

När informationen var inventerad och klassad gick workshopen in i steg 2, att klassa it-systemet som stödjer handläggarnas arbete med huvudmän och ställföreträdare. Samtliga fyra informationsmängder som ingår i klassningsobjektet hanterades i it-systemet. Akterna för huvudmän och ställföreträdare finns också som pappersakter.

Eftersom informationsmängderna i systemet hade höga skyddskrav (2) i samtliga aspekter var det ingen tvekan för workshopsdeltagarna att ge systemet klassningsprofilen K2-R2-T2. Själva systemklassningen gick därför snabbt, men ett visst arbete gick åt att kartlägga systemet och dess integrationer, samt att dokumentera detta (se nedan).

Dokumentation

Under workshopen användes Excel för att dokumentera klassningen av informationen och systemet. Informationen fördes senare över till en rapport i Word som kunde diarieföras i kommunen och kommuniceras vidare till berörda parter (se nedan Användning av resultatet). Rapporten innehöll förutom en del beskrivande text Tabell 1 ovan för informationsklassningen och Tabell 2 nedan för klassning av systemet och annan systemdokumentation.

Tabell 2: Dokumentation över systemstöd och dess klassning.

Klassningsobjekt/system	**[Namn]**
Klassning genomförd	[Datum]
Klassning genomförd av	[Namn] och roller på deltagare
Klassningsresultat	Konfidentialitet: 2 – Riktighet 2 – Tillgänglighet 2
Systembeskrivning	System för hantering av akter för huvudmän och ställföreträdare…
Systemleverantör	[Leverantör]
Nämnd/personuppgiftsansvarig	Överförmyndarnämnden
Systemägare	[Namn] Chef Överförmyndarkansliet
Förvaltningsledare	Tillsvidare systemägaren
Förvaltningsledare IT	[Namn] [Befattning]
Interna användare	Handläggare Överförmyndarkansliet
Andra användare i kommunen	Ekonomer, It-administratörer, Statistiker (utdataanalytiker)
Externa användare	-
Systemdrift	It-avdelningen
Systemsupport	It-avdelningen, [Leverantör]
Input	Integrationer, inmatning tangentbord,
Bearbetning	Sammanställningar m.m. presentationer, underlag till arvoden och fakturering
Output	Skärm, rapporter (MS Word), statistik, utskrifter, brev
Integrationer	HR-system (arvoden), Ekonomisystem (fakturor) m.m.
Lagringsytor	S-mapp (Konfidentiell), P-mapp
Manuella rutiner	Pappersakt huvudman, Pappersakt ställföreträdare. Handlingar kan komma till [Systemet] genom e-post, fax eller brev och skannas in.

Användning av resultatet

Parallellt med pilotverksamheten togs nya styrdokument för informationssäkerhet fram i kommunen. Resultatet från pilotverksamheten gav viktig input till detta arbete. Informationssäkerhetspolicyn kom att innehålla texter på övergripande nivå om klassning – att klassning ska ske i kommunen och att en enhetlig modell ska användas. I riktlinjer för informationssäkerhet beskrevs och reglerades klassningen på en mer detaljerad nivå – vad klassning innebär, hur det går till, roller och ansvar med mera. Själva klassningsmodellen ingick också i riktlinjerna.

Riktlinjerna innehöll också säkerhetsåtgärder som i stort baserades på standarden SS-EN ISO/IEC 27002. De flesta säkerhetsåtgärder gällde generellt, oavsett vilka

informationstillgångar som hanterades, och var likställda med nivå 1 ”Normala skyddskrav” i klassningsmodellen. I riktlinjerna var ett antal säkerhetsåtgärder markerade som gällande om informationstillgångar var klassade på nivå 2 ”Höga skyddskrav”.

I och med att säkerhetsåtgärder för normala och höga skyddskrav var uttryckta i riktlinjerna behövde inte verksamheten själv komma fram till vilka säkerhetsåtgärder som behöver användas och vilka krav som skulle ställas mot olika aktörer, utan dessa genererades så att säga ”automatiskt”. Eftersom systemet fick klassningsprofilen K2 – R2 – T2 så ställdes höga krav på säkerhetsåtgärder.

Riktlinjerna var strukturerade utifrån fyra målgrupper 1) Alla medarbetare 2) Styrning av informationssäkerhet 3) Objektägare och 4) It-verksamhet. Främst var det regler som riktade sig till alla medarbetare och it-verksamheten som innehöll säkerhetsåtgärder kopplade till höga skyddskrav. Detta innebar att regler skärptes för medarbetare i pilotverksamheten eftersom de hanterade informationstillgångar med höga skyddskrav.

Kommunikation inleddes med it-avdelningen där rapporten från klassningen fungerade som ett bra underlag. De olika kraven diskuterades och hur arbetet skulle ske för att uppnå dessa. Vissa säkerhetsåtgärder behövde införas som var specifika för just detta system, medan andra handlade om förbättringar av kommunens generella it-miljö.

Krav på externa leverantörer

Klassningsresultatet användes som grund för kravställning på leverantören av it-systemet. Detta sammanföll i tid med att ett nytt personuppgiftsbiträdesavtal skulle upprättas i samband med den nya dataskyddsförordningen. Avtalet innehöll ett antal säkerhetsåtgärder som var hämtade ur riktlinjerna för informationssäkerhet, och särskilt viktiga var de säkerhetsåtgärder som gällde för informationsmängderna med höga skyddskrav.

Säkerhetsmedvetande

Deltagarna fick en ökad medvetenhet om vikten av att skydda informationen i verksamheten. När information klassades utifrån konsekvensbedömning blev det mycket tydligt för verksamhetschefen och handläggaren vilka allvarliga följder det skulle bli om information skulle röjas till obehöriga, förvanskas eller vara otillgänglig.

Piloten var lyckad. Flera andra verksamheter i kommunen som hörde talas om arbetet visade intresse för att påbörja ett arbete med klassning.

Reflektioner

Klassningsmodellen och arbetssättet fungerade bra. Den enkla klassningsmodellen upplevdes av verksamheten som lätt att använda och logisk.

Att välja en liten och inte för komplex verksamhet var bra för en pilot.
Det viktigaste var att verksamheten var intresserad och ställde upp med ett stort engagemang.

Informationen i systemet var i stort sett likställd med informationen i verksamheten, vilket gjorde att informationsklassningen och systemklassningen kunde genomföras i en gemensam workshop. Om systemet hade innehållit olika slags information, med olika informationsägare och personuppgiftsansvariga, så hade arbetet blivit mer omfattande och systemet hade kunnat klassas först efter att ett antal workshops med olika verksamheter hade genomförts.

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240
Fax: 010-240 56 00
registrator@msb.se
www.msb.se
Org.nr: 202100-5984