Klassningsmodell

I denna vägledning får du stöd med arbetet att skapa en organisationsgemensam modell för klassning av informationstillgångar. Genom att använda en gemensam klassningsmodell kan organisationens informationstillgångar skyddas på ett enhetligt sätt utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

Om klassningsmodeller

Informationsklassning innebär att man värderar organisationens informationstillgångar utifrån de interna och externa krav på konfidentialitet, riktighet och tillgänglighet som kommit fram i analysfasen. Kraven konkretiseras genom gradering av informationstillgångarna i olika nivåer, ofta kallade konsekvensnivåer. Kraven på skydd verkställs sedan genom att man kopplar adekvata säkerhetsåtgärder till varje konsekvensnivå. Genom att man kopplar säkerhetsåtgärder till organisationens konsekvensnivåer får man så kallade skyddsnivåer. När man kopplar säkerhetsåtgärder till konsekvensnivåerna är det viktigt att inte bara se till informationens värde och de oönskade konsekvenserna. Man behöver också väga in en riskbedömning. Hur stor är sannolikheten att information i en viss klass exponeras för en risk som innebär att den oönskade konsekvensen inträffar? Vilka säkerhetsåtgärder krävs för att minska just den risken?

Konsekvensnivåerna och skyddsnivåerna ska anpassas och konkretiseras på ett sätt som gör modellen funktionell och användbar i just er verksamhet. I arbetet med att ta fram en klassningsmodell ska ni också väga in huruvida ni behöver anpassa modellen till externa aktörers modeller för att underlätta informationshanteringen organisationerna emellan.

Ingångsvärden

Resultaten från samtliga analyser som gjorts i analysfasen och organisationens riskanalysmodell är ingångsvärden till er klassningsmodell och de nivåer ni beslutar er för att använda. Nivåerna förs in i verktygets klassningsmatris. Ett centralt ingångsvärde för många verksamheter är de rättsliga krav på skydd av information som framkommit i omvärldsanalysen (se Identifiera & Analysera Omvärld). Om ni, genom er säkerhetsskyddsanalys, kommit fram till att ni omfattas av

säkerhetsskyddslagen behöver ni se till att er modell och era arbetssätt gällande informationsklassning kan hantera detta.

Särskilt om klassning och säkerhetsskyddslagen

Den 1 april 2019 trädde Säkerhetsskyddslag (SFS 2018:585) i kraft. Lagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige internationellt åtagande om säkerhetsskydd, i lagtexten benämnda som säkerhetskänslig verksamhet. Lagen ställer krav på att den som bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd och göra en säkerhetsskyddsanalys. Verksamhetsutövare som lyder under säkerhetsskyddslagen ska klassificera information i enlighet de fastställda nivåerna i säkerhetsskyddslagens andra kapitel, 5 §.

Mer information om säkerhetsskyddslagen och aktuella föreskrifter och vägledningar finner du på Försvarsmaktens och Säkerhetspolisens hemsidor.

I praktiken kan man behöva hantera och skydda både organisationsspecifik information och säkerhetsskyddsklassificerad information i det systematiska informationssäkerhetsarbetet. En organisation som berörs av säkerhetsskyddslag-stiftningen behöver göra en bedömning av hur den klassificeringen ska hanteras i relation till den organisationsanpassade klassningsmodellen. Ofta kräver säkerhetsskydd särskild hantering. Längre fram i vägledningen finner du exempel på en klassningsmatris i vilket detta framgår.

Klassningsmodellens funktion och syfte

Klassningsmodellen används för att värdera information och skapa en organisationsgemensam bedömningsgrund för hur information ska hanteras. Genom att värdera information med hjälp av en klassningsmodell kan ni identifiera vilka konsekvenser otillräckliga säkerhetsåtgärder skulle orsaka och utifrån det säkerställa att rätt åtgärder vidtas.

Klassning syftar till att värdera informationstillgångar och ge dem rätt skydd. Klassningen hjälper oss också att undvika att informationstillgångarna överskyddas, vilket kan bli både kostsamt och göra hanteringen onödigt krånglig.

Den klassningsmodell som organisationen tar fram används i första hand till roller som verksamhetsansvariga, objektägare (information och system) och projektägare som ansvarar för att sina informationstillgångar är klassade och skyddade på rätt sätt. De krav på skydd som framkommer vid klassningen kan användas som underlag i kontakter med externa aktörer vid behov av utkontraktering av organisationens informationshantering.

Utformning av klassningsmodellen

Klassningsmodellens innehåll

En klassningsmodell bör minst innefatta följande delar:

- **En matris** med ett antal konsekvensnivåer till exempelmåttlig, betydande och allvarlig (rader) och aspekterna konfidentialitet, riktighet och tillgänglighet (kolumner) samt beskrivningar av konsekvensnivåerna under respektive aspekt (celler).
- **Definitioner av konsekvensnivåernas innebörd,** det vill säga vad till exempel*måttliga*, *betydande* och *allvarliga* konsekvenser innebär i er organisation.
- **Koppling mellan konsekvensnivåer och skyddsnivåer med säkerhetsåtgärder,** det vill säga att det finns tydligt beskrivet hur information i en viss konsekvensnivå ska skyddas i praktiken.
- **Stödmaterial** som hjälper organisationen att använda klassningsmodellen och genomföra klassning av informationstillgångar.

Bild Process Utforma Klassningsmodell.

För dig som ska arbeta med att ta fram organisationens klassningsmodell beskriver vi arbetet i sex steg.

Börja med en workshop

Om organisationen saknar en riskanalysmodell med fastställda konsekvensnivåer behöver ni ta fram och besluta konsekvensnivåer till klassningsmodellen. Detta bör ni göra i workshopform med deltagare som tillsammans kan identifiera och värdera olika typer av konsekvenser som brister eller förlust av konfidentialitet, riktighet och tillgänglighet kan medföra. Representanter från organisationens viktigaste **verksamheter** bör delta för att olika typer av konsekvenser ska kunna identifieras och värderas.

Workshoppen kan lämpligen ledas av dig som är **CISO.**

Det kan vara klokt att inleda workshopen med att gå igenom vad informationsklassning är, vad en klassningmodell innehåller och vad den fyller för funktion och vad som är dess syfte Presentera gärna metoden som beskrivs i vägledningen nedan men begränsa workshopen till att fokusera på att specificera skyddsvärd information och att definiera konsekvensnivåerna. När ni ska koppla

säkerhetsåtgärder till konsekvensnivåerna behövs annan kompetens och detta sker lämpligast i en separat workshop. Förbered gärna diskussionsfrågor, till exempel ”vad innebär *betydande konsekvenser* för oss, i form av ekonomiska termer eller minskat förtroende?”.

Utgå från informationen

Det är själva informationen i sig som ska klassas. Resurser som hanterar information, exempelvis it-system, it-infrastruktur och fysiska tillgångar ska sedan utformas så att de möter de krav som klassningen av informationen medför. När ni tar fram er klassningsmodell är det bra att specificera vilka olika typer av information som hanteras i verksamheten, exempelvis personuppgifter, kunduppgifter, ekonomisk data, journaler eller olika typer av rapporter.

Fastställ krav

Som vi nämnde i inledningen så är resultaten från de analyser som gjorts i metodsteget **Analysera**, ingångsvärden till klassningsmatrisen. Här ska ni särskilt se över de rättsliga krav som framkommit i **Omvärldsanalysen** (och i en eventuell säkerhetsskyddsanalys). Om er verksamhet behöver kunna dela klassad information med andra verksamheter och ändå bibehålla rätt skyddsnivå behöver ni utforma klassningsmatrisen på ett sätt som säkerställer detta.

I **Verksamhetsanalysen** kan ni hämta uppgifter om vilka informationstillgångar som ska skyddas, vad verksamheten har definierat som kritiska informationstillgångar och vilka krav verksamheten har på informationen.

Använd aspekterna konfidentialitet, tillgänglighet och riktighet.

Klassning görs för att ge informationen rätt skydd utifrån aspekterna **konfidentialitet, riktighet och tillgänglighet**, ofta gemensamt förkortat **KRT**. Information behöver skyddas så att endast behöriga får ta del av informationen (krav på konfidentialitet), att vi kan lita på att den inte manipulerad eller förstörd (krav på riktighet) och att den finns när behörig efterfrågar den (krav på tillgänglighet).

Säkerhetsåtgärder är olika typer av skydd som avser upprätthålla eller öka informationssäkerheten genom att uppnå eller upprätthålla en viss nivå av konfidentialitet, riktighet eller tillgänglighet.

I standarden SS-EN ISO/IEC 2700:2017 definieras dessa begrepp såhär:

- *Konfidentialitet:* egenskapen att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.
- *Riktighet*: egenskapen att vara korrekt eller fullständig.
- *Tillgänglighet:* egenskapen att vara åtkomlig och användbar på begäran av ett behörigt objekt.

Aspekterna är den första byggstenen i klassningsmatrisen och kommer att utgöra dess kolumner.

Konfidentialitet	Riktighet	Tillgänglighet

Definiera konsekvens- och skyddsnivåer

Er organisationsanpassade klassningmodell ska innehålla ett lämpligt antal konsekvensnivåer. Ni ska också beskriva vad det innebär att konsekvenser är till exempel*måttliga*, *betydande* och *allvarliga* i organisationen. Har organisationen en riskmodell som beskriver konsekvenser i nivåer så använd den. Konsekvensnivåerna i klassningsmodellen bör kunna relateras till konsekvensnivåerna i den riskmatris som används i den övergripande riskanalysen (**Identifiera och analysera Risk**). De behöver inte vara exakt likalydande eller samma till antalet men bör kunna relatera till varandra på ett entydigt sätt.

Konsekvensnivåerna kommer ni att använda när ni bygger vidare på er klassningsmatris. De utgör raderna i matrisen.

	Konfidentialitet	Riktighet	Tillgänglighet
4 Ex. Allvarlig			
3 Ex. Betydande			
2 Ex. Måttlig			
1 Ex. Försumbar			

För att underlätta arbetet med att definiera konsekvensnivåer kan det vara bra att utgå från vilka olika kategorier av konsekvenser som otillräckligt skydd skulle kunna orsaka för just er verksamhet. Nedan finner du några exempel på sådana konsekvenskategorier:

- Ekonomisk förlust (orsaker till exempelminskade intäkter, ökade kostnader, skada på tillgångar)
- Negativ påverkan på, eller avbrott i den operativa verksamheten
- Överträdelse/bristande efterlevnad av rättsliga krav
- Skadat varumärke/minskat förtroende
- Skada på annan organisation/omgivande samhället
- Personskada

- Miljöskada
- ...

Kategorierna ovan ska ses som exempel och inte en fullödig lista. Konsekvenskategorierna kan också ha samband, till exempel minskat förtroende kan leda till minskade intäkter och därmed ekonomisk förlust. Det går att skapa kategorier på olika sätt, det viktigaste är att de känns relevanta för den egna organisationen och att de är konkreta. Nedan visas ett exempel på hur konsekvensnivåer kan konkretiseras gällande ekonomisk förlust i absoluta tal, eller som andelar av något nyckeltal. Men detta kan likaväl konkretiseras i andra former, till exempel hur länge ett system är nere i timmar och minuter, antalet negativa artiklar i media inom en viss tidsram eller antalet drabbade kunder.

Här kan man med fördel använda samma matris som användes som stöd vid riskanalysen. Gör en tabell med valda kategorier, så som exemplet visar.

Konsekvens	Ekonomisk förlust	Minskat förtroende	Avbrott i verksamheten
Allvarlig	2 miljoner kronor och uppåt eller avvikelse på över 20% av budget	Ihållande drev i rikstäckande medier, eller av organiserade grupperingar i sociala medier. Ej endast enskilda personer pekas ut, utan även organisationens grundläggande kultur.	Avbrott i en eller flera kritiska verksamheter som är längre än godtagbart. Omfattande omprioriteringar av verksamheten.
Betydande	500 000 – 2 miljoner kronor eller avvikelse på 10-20% av budget	Nyheter i både riks- och lokalmedia och i organiserade grupperingar i sociala medier. Missnöjet är dock begränsat till enskilda händelser eller enskilda personers agerande.	Avbrott i en kritisk verksamhet som är längre än godtagbart. Stora omprioriteringar av verksamheten.
Måttlig	1 – 500 000 kronor eller avvikelse på 5-10% av budget	Enstaka missnöjda individer som uttalar sig i sociala medier, eller en mindre notis i lokalpress.	Avbrott i en eller flera verksamheter som inte är kritiska och som är längre än godtagbart. Mindre omprioriteringar av verksamheten.
Försumbar	Ingen förlust	Liten negativ uppmärksamhet	Försumbara avbrott i verksamheten och/eller inga omprioriteringar av verksamheten.

När klassningsmodellen sedan ska användas vid klassning av informationstillgångar, så kommer de olika typerna av konsekvenser att tjäna som stöd. De olika typerna av konsekvenser bör dock inte skrivas in i själva matrisen, utan hellre i anslutning till den för att inte fylla den med för mycket information och göra den svåröverskådlig.

Skapa en klassningsmatris

När ni utifrån aspekterna konfidentialitet, riktighet och tillgänglighet har bestämt och definierat era konsekvensnivåer ställer ni upp dessa i en matris. Er anpassade klassningsmatris kan skapas i **Verktyget Utforma Klassningsmodell**. Eftersom

klassningsmodellerna kan utformas på olika sätt, bland annat i förhållande till säkerhetsskydd har vi tagit fram flera olika exempel som presenteras nedan.

Det är viktigt att se dessa matriser som just exempel. Ni ska alltid utforma er egen matris utifrån de interna och externa krav som finns på er organisations information och se till att den byggs på ett sätt som gör den funktionell i er verksamhet.

Klassningsmatris A – Tre nivåer, förutsätter att man inte hanterar säkerhetsskyddsklassificerade uppgifter.

Denna klassningsmatris kan användas när man genom en säkerhetsskyddsanalys har konstaterat att man inte hanterar sekretesskyddade uppgifter. Matrisen passar organisationer som hanterar flera olika typer av information vars värde behöver graderas och differentieras i flera nivåer. Här hanteras öppen information utanför matrisen. Konsekvenser av ringa eller obetydlig karaktär hanteras inte heller i matrisen. Detta passar organisationer vars minst skyddsvärda information är av sådan art att felhantering skulle passera obemärkt förbi och därför inte heller behöver klassas.

		Konfidentialitet	**Riktighet**	**Tillgänglighet**
3	**Allvarlig konsekvens**	**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 konsekvens**	**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 konsekvens**	**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.

Klassningsmatris B – två nivåer, förutsätter att man inte hanterar säkerhetsskyddsklassificerade uppgifter.

	Konfidentialitet	**Riktighet**	**Tillgänglighet**
Hög (2)	K2	R2	T2
Normal (1)	K1	R1	T1
Ingen (0) s	K0	Ej tillämpligt	Ej tillämpligt

Även denna matris kräver att man genom en säkerhetsskyddsanalys har konstaterat att man inte hanterar sekretesskyddade uppgifter.

I vissa verksamheter kan klassning av information upplevas som svårt. Det kan bero på att man använder för avancerade modeller i relation till den information som hanteras. Detta kan leda till att det blir svårt att förankra modellen och uppnå effekt i organisationen. I dessa organisationer skiljer sig inte kraven på olika typer av informations så mycket åt och kan med fördel delas in i endast två klasser. Klassningsmodeller med flera nivåer blir svåra att kommunicera, implementera och efterleva i dessa organisationer. Det kan i slutändan leda till sämre informationssäkerhet. Om man stött på dessa utmaningar kan man prova denna matris som är enklare att förstå och använda.

I detta exempel har angivits ”Ej tillämpligt” på den lägsta nivån för riktighet och tillgänglighet. Det är ovanligt att organisationer inte har några krav alls på dessa aspekter – i så fall har informationen knappast något värde och behöver inte klassas. Avseende konfidentialitet kan det dock vara till nytta för att tydliggöra vilken information som är öppen.

Klassningsmatris C – Fem nivåer, med säkerhetsskydd lagt ovanpå för särskild hantering.

	Konfidentialitet	Riktighet	Tillgänglighet
Sveriges säkerhet **Säkerhetsskydd**	**K5** Information som omfattas av Säkerhetsskyddslagen. Särskild hantering.		
Allvarlig **konsekvens**	**K4** Information som vid obehörig spridning kan leda till allvarlig skada för organisationen, tredje person eller enskild individ.	**R4** Konsekvensen av obehörig förändring av informationen är allvarlig.	**T4** Informationen kan tillåtas vara icke tillgänglig under högst xx timmar. Ingen information får gå förlorad.
Betydande **konsekvens**	**K3** Information som vid obehörig spridning kan leda till betydande skada för organisationen, tredje person eller enskild individ.	**R3** Konsekvensen av obehörig förändring av informationen är betydande.	**T3** Informationen kan tillåtas vara icke tillgänglig under högst x antal arbetsdag. Information från högst xx timmar får gå förlorad.
Måttlig **konsekvens**	**K2** Information som vid obehörig spridning kan leda till måttlig skada för organisationen, tredje person eller enskild individ.	**R2** Konsekvensen av obehörig förändring av informationen är måttlig.	**T2** Informationen kan tillåtas vara icke tillgänglig under högst x antal arbetsdag. Information från högst xx timmar får gå förlorad.
Ringa **konsekvens**	**K1** Information som vid obehörig spridning kan leda till ringa skada/obehag för organisationen, tredje person eller enskild individ.	**R1** Konsekvensen av obehörig förändring av informationen är ringa.	**T1** Informationen kan tillåtas vara icke tillgänglig under högst x antal arbetsdagar. Information från högst xx arbetsdagar får gå förlorad.

I klassningsmatris C ovan visar vi på hur en organisation som hanterar både säkerhetsskyddade uppgifter och annan information kan utforma sin klassningsmatris. Detta exempel förutsätter att det finns en organisation och rutiner för särskild hantering av säkerhetsskyddade uppgifter. Här klassificeras säkerhetsskyddade uppgifter i enlighet de fastställda nivåerna i säkerhetsskyddslagens andra kapitel, 5 §, av en särskild verksamhet i organisationen, medan övriga verksamheter bara behöver känna till att sådan information kan förekomma och att den i så fall ska klassas av den verksamhet som hanterar säkerhetsskydd.

Övrig information som organisationen hanterar klassas i denna matris enligt en femgradig skala. Detta passar organisationer som hanterar många olika typer av information och aggregerade informationsmängder vars värde behöver graderas och differentieras i flera nivåer. Denna matris används med fördel i organisationen som

kan behöva göra skillnad på konsekvens och/eller skydd även beträffande den minst skyddsvärda informationen, på måttlig eller ringa nivå.

Nivån med den särskilda hanteringen som vi lagt ovanpå denna matris kan naturligtvis adderas till vilken annan matris som helst.

Koppla säkerhetsåtgärder till klassningsmodellen

För att nå syftet med klassningen, nämligen att informationstillgångar ges rätt skydd, ska ni koppla säkerhetsåtgärder till modellen.

Konsekvensnivåerna ska omvandlas till skyddsnivåer, vilka innehåller säkerhetsåtgärder. Utgångspunkten är de säkerhetsåtgärder som organisationen tidigare valt (**Identifiera och analysera – Val av säkerhetsåtgärder**). Saknas åtgärder, eller har åtgärder identifierats som bristande, behöver de införas eller förbättras.

Detta är viktigt att den klassningsmodell ni tar fram innehåller kopplade säkerhetsåtgärder och att dessa sedan appliceras på respektive klass. Du behöver uppdatera handlingsplanen med aktiviteter som säkerställer att skyddsåtgärden finns på plats.

Vissa säkerhetsåtgärder bör användas generellt, medan andra kan varieras beroende på skyddsnivå. Vissa säkerhetsåtgärder går inte att indela i olika nivåer (läs ordet ”nivå” som ”styrka”). Ett exempel är att organisationen ska ha en informationssäkerhetspolicy; antingen finns den eller så finns den inte. Andra säkerhetsåtgärder går att ha i olika nivåer till exempel autentisering (enbart användarnamn och lösenord jämfört med flerfaktorsautentisering), hur kryptonycklar ska hanteras och lagras samt vilka uppgifter som ska samlas in till loggsystemet.

Ny workshop

Precis som vid framtagningen av klassningsmodellen, så bör ni ha en workshop när det är dags att ta fram skyddsnivåer och koppla utvalda säkerhetsåtgärder till konsekvensnivåerna i klassningsmodellen. Här är det dock en annan typ av kompetens som behövs jämfört med när ni formulerar konsekvensnivåerna. Nu behövs kompetenser som kan avgöra vilket skydd säkerhetsåtgärder ger, och kan konkretisera dess nytta. Det är därför snarare stödverksamheter som ska bidra med

kunskap än verksamhetsrepresentanter. Det kan vara CISO, it-säkerhetschef, säkerhetschef, annan säkerhetspersonal och specialister inom it, fastighet, personal, upphandling och juridik.

Utgå från Gapanalys och valda säkerhetsåtgärder SoA (Statement of Applicability)

För att nå syftet med klassningen, nämligen att ge informationstillgångar rätt skydd, ska ni koppla säkerhetsåtgärder till modellen. Utgångspunkten är de säkerhetsåtgärder som organisationen valt (**Identifiera och analysera – Val av säkerhetsåtgärder**).

I första hand ska ni koppla existerande säkerhetsåtgärder till modellen. Saknas åtgärder, eller har åtgärder identifierats som bristande, behöver de införas respektive förbättras.

Det är inte så att alla säkerhetsåtgärder ni valt i organisationen måste ”skiktas” och finnas med i olika nivåer. Erfarenheten visar att de flesta säkerhetsåtgärder i de flesta verksamheter bör gälla för samtliga klasser, och att det är ett fåtal som bör gälla för en enbart en klass.

Koppla säkerhetsåtgärder till konsekvensnivåer och aspekterna.

Vissa säkerhetsåtgärder bör användas generellt, medan andra kan varieras beroende på konsekvensnivå. Exempelvis autentisering (enbart användarnamn och lösenord jämfört med flerfaktorsautentisering), hur kryptonycklar ska hanteras och lagras samt vilka uppgifter som ska samlas in till loggsystemet. Vissa säkerhetsåtgärder kan kopplas till alla tre aspekter (konfidentialitet, riktighet och tillgänglighet) medan andra åtgärder tar sikte på en eller två av aspekterna.

I Verktyget i **Verktyget Utforma Klassningsmodell** under fliken **Guide variation säkerhetsåtgärder** ser du vilka aspekter respektive säkerhetsåtgärd har effekt på samt vilka säkerhetsåtgärder som kan varieras beroende på nivå och vilka som är generella och inte bör varieras.

Gå igenom de säkerhetsåtgärder ni har fastställt i **Identifiera och Analysera Val av säkerhetsåtgärder (SoA).**

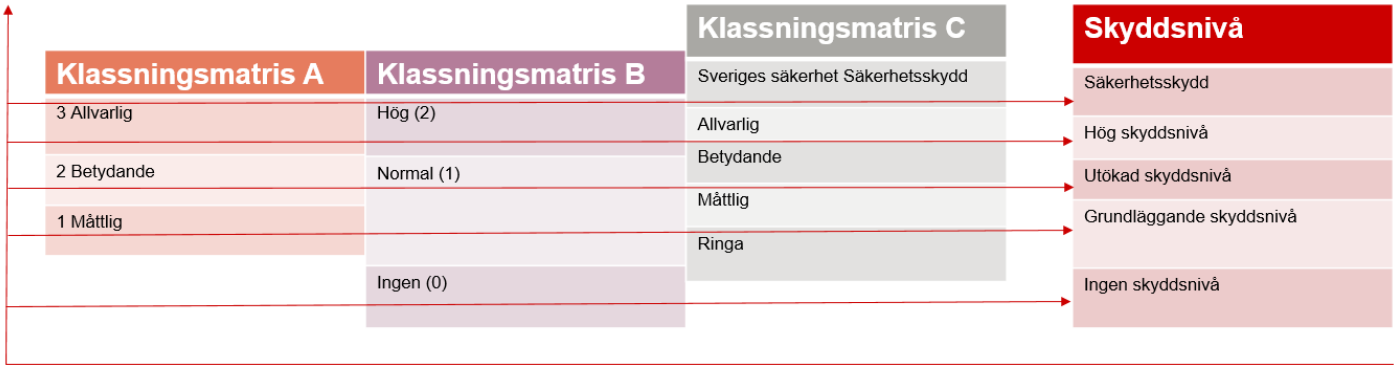
För varje säkerhetsåtgärd, bedöm om den:

i. Skyddar mot konfidentialitet, riktighet och/eller tillgänglighet
ii. Ska gälla för de konsekvensnivåer ni beslutar om att använda och hur skyddsåtgärden eventuellt ska varieras mellan olika konsekvensnivåer.

I Verktyget i **Verktyget Utforma Klassningsmodell** under fliken **Kopplade säkerhetsåtgärder** kan ni skriva in vilka säkerhetsåtgärder som ska gälla för respektive nivå. I kolumnen **ID Säk.åtg**. kan en referens skapas till aktuell/a säkerhetsåtgärd/er i **Identifiera och Analysera Val av säkerhetsåtgärder (SoA)**.

Klassningsmatrisernas förhållande till skyddsåtgärder

Bilden nedan beskriver på ett övergripande plan de olika klassningsmatrisernas konsekvensnivåer i förhållande till skyddsnivåer. Självklart behöver både konsekvensnivåerna och skyddsnivåerna definieras utifrån den egna organisationens förutsättningar. En uppställning liknande denna nedan kan vara till hjälp när man ska jämföra olika matriser eller för att tydliggöra klassningsmatrisens innebörd.



Utforma stödmaterial

När klassningsmodellen för organisationen är fastställd och lämpliga säkerhetsåtgärder är kopplade till de olika nivåerna är modellen klar att användas i verksamheten. För att organisationens informationstillgångar ska få rätt skydd är det avgörande att den klassas och hanteras i enlighet med dess skyddsnivå. I metodsteget **Använda** finns ett avsnitt som vi kallar **Använda klassningsmodell**. Det stödmaterial som du som CISO tar fram underlättar för organisationens verksamheter och medarbetare att använda den framtagna klassningsmodellen och klassa informationstillgångar.

Underlätta med hjälp av informationstyper och organisationsövergripande klassning

För att underlätta utformningen av stöddokument och det löpande arbetet med klassning rekommenderas att viss förberedande klassning genomförs.

1. Gruppera organisationsgemensam information i informationstyper. På så vis får ni fram kategorier av information som kan bedömas enhetligt avseende krav på konfidentialitet, riktighet, tillgänglighet.

2. Klassa organisationsgemensamma tillgångar på central nivå**.** Ni kan förenkla arbetet med klassning genom att klassa informationstyper och organisationsgemensamma informationsresurser baserat på vilken information den innehåller.

Detta gör det enkelt för användarna genom att de kan kontrollera om den information de hanterar passar in i en informationskategori eller en viss informationsresurs som redan är klassad.

Anpassa stödmaterialet

När du tar fram stödmaterialet för klassning bör du, precis som i arbetet med att utforma styrdokument, ta fram material som fungerar för din organisation.

Att information ska klassas enligt fastställd klassningmodell förs till exempellämpligast in i *informationssäkerhetspolicyn*. Exempelvis kan ett mål i informationssäkerhetspolicyn vara att ”Alla kritiska informationstillgångar ska vara klassade i enlighet med organisationens gemensamma klassningsmodell”.

Vem som ansvarar för att klassning sker ska till exempelframgå av *riktlinjer* och dokumentation som tagits fram kring utformningen av *organisationen*.

Hur och när klassning ska genomföras sammanställs lämpligen i stödjande instruktioner.

Exempel på innehåll i stödmaterial

Stödmaterial ska hjälpa och underlätta genomförandet av klassning i praktiken. Läsaren behöver förstå *vad* klassning innebär, *varför* klassning ska genomföras, *vem* som ska genomföra den och *hur* den ska genomföras. Om det stödjande materialet ger information om detta blir det lättillgängligt och pedagogiskt.

Exempel på innehåll i stödmaterial:

- Information om vad, varför, vem och hur enligt ovan.
- Organisationens klassningsmatris
- Beskrivningar av innebörden av konsekvensnivåerna
- Beskrivning av skyddsnivåer och kopplade säkerhetsåtgärder
- Instruktioner om klassningsprocess
- Sammanställningar av informationstyper och organisationsgemensamma tillgångar, dess klassning och motivering till klassningen.
- Mallar och vägledning för märkning av klassad information

(Observera att även stödmaterialet i sig kan behöva klassas)

Dokumentation och beslut

Den organisationsövergripande klassningsmodellen har en central roll i det systematiska informationssäkerhetsarbetet och bör därför beslutas av ledningen. Klassningsmodellen kan med fördel finnas med i styrande dokument som till exempel organisationsövergripande riktlinjer för informationssäkerhet (se **Utforma Styrdokument**). Då riktas den till de målgrupper som ska använda klassningsmodellen, såsom informationsägare och systemägare. Klassningsmodellen, inklusive specifikation av konsekvensnivåer och skyddsnivåer kan skapas och dokumenteras i **Verktyg Utforma Klassningsmodell.**

Referens till standarder i 27000-serien:

SS-EN ISO/IEC 27002:2017: avsnitt 8.2 Informationsklassning.