Administrationsvägledning KLASSA 5

Att identifiera alla de informationsmängder som finns inom en verksamhet kan vara svårt. Men genom att utgå från t.ex. de informationstillgångar eller system som en organisation använder (eller planerar att införa) kan man strukturera upp informationsmängderna och lättare hantera eventuella risker och hot.

KLASSA är ett självskattningsverktyg som fungerar som en länk mellan verksamhetens behov av skydd och tekniken som kan säkerställa detta skydd. Skydden kan vara såväl tekniska som organisatoriska och benämns ofta säkerhetsåtgärder (se ex. NIS2 och Cybersäkerhetslagen) eller skyddsåtgärder (se ex. GDPR/Dataskyddsförordningen).

Med hjälp av KLASSA:s kravkataloger och automatiserade flöden underlättas arbetet med att värdera de informationsmängder som en verksamhet har. Därmed blir det också enklare att skapa handlingsplaner med de identifierade säkerhetsåtgärder som behöver vidtas för att hålla verksamheten trygg, samt säkerställa relevant regelefterlevnad. Genom att använda KLASSA kan verksamheten också sammanställa behovet av säkerhet avseende sina informationsmängder, inför upphandlingar av nya system eller verktyg.

KLASSA har utvecklats från föregående versioner för att vara bättre anpassat efter den ökade reglering som skett inom området informations- och cybersäkerhet. Vad det innebär i praktiken är att olika regulatoriska krav (som t.ex. hantering av personuppgifter, behov av riskanalyser, incidenthantering, m.m.) bättre kan samordnas i KLASSA, vilket även underlättar en gränsöverskridande riskhantering.

KLASSA är också mer flexibelt än tidigare, då det finns möjligheter för användaren att själv lägga till olika kravkataloger, anpassa användarflöden efter mer övergripande organisatoriska krav men också efter krav som är mer verksamhets- och informationsnära. Sammantaget bör detta bidra det till att ev. påförda säkerhetsåtgärder är mer hållbara över tid, oavsett hur den relevanta regleringen förändras inom den närmsta framtiden.

Sveriges Kommuner och Regioner
info@skr.se, www.skr.se
Post: 118 82 Stockholm *Besök:* Hornsgatan 20
Tfn: 08-452 70 00 *Org nr:* 222000-0315

Innehåll

Administrationsvägledning KLASSA 5 1
Innehåll 2
Vägledning för administratörer i KLASSA 5 3
Komma igång 3
Förberedelser 3
Att logga in i systemet 3
Startvy när du loggat in 4
Roller 5
Organisationsövergripande roller 5
Underorganisationsroller 7
Tilldela behörigheter och roller 8
Organisationsträdet 9
Kravkataloger 10
Grundläggande information 10
Kategorier 11
Skapa ny kravkatalog 11
Flöden 13
Grundläggande information 13
Skapa nytt flöde 16
Kravöverskrivning 22
Grundläggande information 22
Ett exempel på väg fram 23
Skapa organisation 23
Välj flöden 24
Koppla flöden till organisatorisk enhet 26

Vägledning för administratörer i KLASSA 5

Komma igång

Förberedelser

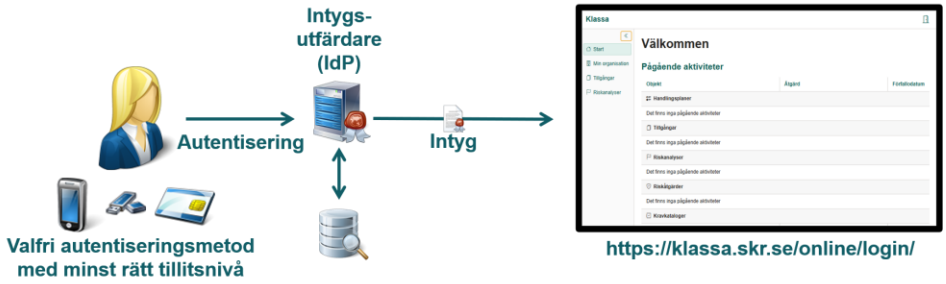
För att er organisation ska kunna börja använda KLASSA, behöver ni fylla i ett beställningsformulär för licens. Läs mer här.

Utöver uppgifter om er organisation och vilken typ av licens ni önskar, så behöver ni också utse någon som ska administrera systemet för er organisations räkning. Lämplig roll för det uppdraget kan vara er informationssäkerhetssamordnare, DSO, CISO eller liknande roll.

När ni har fyllt i de nödvändiga uppgifterna skickas normalt sett ett avtalsförslag till er inom en arbetsvecka. Anslutning till KLASSA sker vanligtvis några veckor efter signerat avtal.

Åtkomst till KLASSA

KLASSA har en auktorisationsförmåga som förlitar sig helt på att autentisering sker utanför KLASSA. Beslut om åtkomst grundas på elektroniska intyg och attribut inom ramen för de federationer eller relationer som KLASSA är en del i.



För åtkomst till KLASSA finns en separat vägledning som beskriver detta mer i detalj. Se https://KLASSA.skr.se/sidor/stodmaterial/a-KLASSA-5-vagledning.

Att logga in i systemet

Första steget är att anropa https://KLASSA.skr.se/online/login eller den URL som är aktuell för er organisation. För den som använder KLASSA on-prem bestämmer organisationen själv vad som är sökvägen (URL) för åtkomst till KLASSA.

Inloggning i KLASSA ser olika ut och är beroende på vilken typ av inloggningstjänst (IdP) som din organisation använder. Klicka på det alternativ som passar bäst för dig, och följ instruktionerna i inloggningstjänsten.

Din organisation har rollen som informationsägare av innehållet i KLASSA när ni använder verktyget. Därmed är det också din organisation som bestämmer kraven för lägsta tillitsnivå vid inloggning i KLASSA för den egna organisationen.

Första gången

Första gången en vanlig användare ansluter till KLASSA finns inte denne inlagd i systemet ännu. Ett konto skapas med automatik i samband med inloggningen och sedan visas en knapp för användaren för att generera en engångskod (”Invite ID”). Den används för att koppla ihop användarens konto med organisationen.

Denna engångskod ska användaren skicka till organisationens KLASSA-administratör. Administratören kan sedan med hjälp av engångskoden koppla användaren till en organisationsenhet i organisationen. När detta är gjort kan användaren sedan logga in till sin organisationsgren i KLASSA.

Den allra första gången är det Adda/KLASSA som kopplar ihop organisationens KLASSA-organisationsadministratör till er organisation i KLASSA enligt en given process. Engångskoden (”Invite ID”) skickas därför vid det första tillfället till klassa@skr.se. Efterföljande tillfällen skickas det till organisationens organisationsadministratör(er).

Startvy när du loggat in

Startvyn när du loggat in i KLASSA visar en överblick över alla dina pågående aktiviteter, och en huvudmeny till vänster. Som administratör har du fler behörigheter än en vanlig användare varför du också ser mer i startvyn.



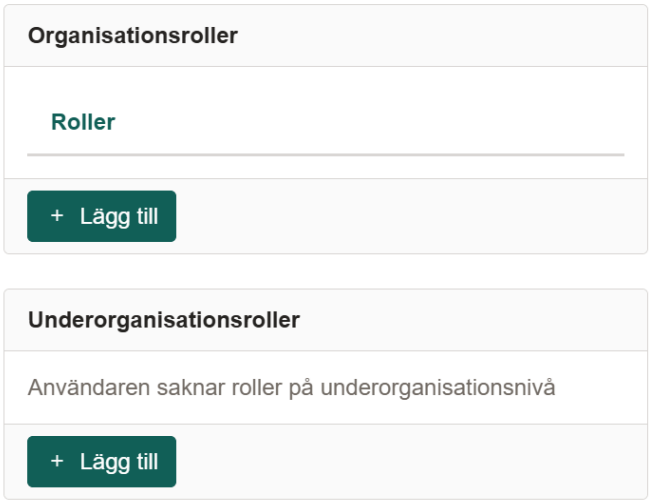
Objekt visar namnet på, och en direktlänk till, din pågående aktivitet.

Åtgärd visar vad du behöver göra för att bli klar med din pågående aktivitet.

Förfallodatum visar det datum som angivits då åtgärden för din pågående aktivitet ska vara klar. Om datumet har överskridits kommer texten att vara röd.

Roller

Behörighetssystemet i KLASSA är rollbaserat. Det innebär att varje roll ger en rad behörigheter som beskrivs nedan. Därutöver kan den som blir tilldelad en tillgång eller en riskanalys också få behörigheten att se den. Den som har ägandeskapet för en tillgång eller en riskanalys får även behörigheten att redigera och ta bort den. I övrigt är behörigheterna rollbaserade.



Rollerna kan tilldelas övergripande för organisationen eller per underorganisation. En roll på en underorganisation gäller dock bara den underorganisationen, inte under- eller överliggande organisationer. Undantaget är läsbehörigheter, de ärvs ner i organisationen.

Har en person flera roller får hen summan av behörigheterna.

Organisationsövergripande roller

De roller som är organisationsövergripande innebär att behörigheten som följer av en viss roll omfattar alla delar inom organisationen. De här behörigheterna kan inte begränsas till en viss underorganisation.

Underorganisationsroller beskrivs i nästa avsnitt.

Organisationsadministratör

Den som har rollen *organisationsadministratör* har alla behörigheter inom den egna organisationen i KLASSA. Det är den enda rollen som kan:

- hantera användare och roller
- acceptera inbjudningar
- hantera underorganisationer
- välja vilka flöden underorganisationerna använder
- återställa från karantänen

Därutöver har organisationsadministratören alla behörigheter nedan.

Administratör

Organisationens *administratör* kan skapa, se och ta bort:

- Tillgångar
- Flöden
- Kataloger
- Riskanalyser
- Rapporter

Flödesadministratör

Rollen *flödesadministratör* kan skapa se och ta bort:

- Flöden
- Kravkataloger
- Kravöverskrivningar
- Hotkataloger

Flödesadministratören kan inte bestämma vilka underorganisationer som använder vilka flöden.

Riskägare

Den som har rollen *riskägare* förväntas vara med när riskanalyser genomförs. Det är *riskägaren* som föreslår vilka säkerhetsåtgärder organisationen bör ta, för att den förmodade risken ska minska. I arbetet med att föreslå mitigerande säkerhetsåtgärder är det också *riskägaren* som ansvarar för att bedöma förväntat utfall av dessa (vilket sedan är upp till rollen *informationsägare/systemägare* att besluta om).

Informationsägare/Systemägare

Din organisation har många informationstillgångar. I KLASSA omnämns dessa helt enkelt som ”tillgångar”. Den som är ägare av en informationstillgång är den inom organisationen som ansvarar för att en klassning av just den tillgången är korrekt. Det är också rollen *informationsägare/systemägare* som ansvarar för att fatta beslut om föreslagna säkerhetsåtgärder (vilka föreslås från rollen *riskägare*) vid riskanalyser, samt bedömer förväntat nytt riskvärde för tillgången efter att åtgärderna implementeras. Föreslagna säkerhetsåtgärder kan också uppstå i arbetet med handlingsplaner, och även där är det rollen *informationsägare/systemägare* som förväntas säkerställa att de föreslagna säkerhetsåtgärderna implementeras i organisationen.

Användare

Alla andra inom organisationen som ska arbeta i KLASSA har som minst rollen *användare*. Den som har rollen *användare* men ingen annan roll, förväntas dokumentera arbetet som sker i KLASSA. Det kan innebära allt från att lägga upp de tillgångar som ska klassificeras, påbörja klassificeringar, dokumentera status

för pågående aktiviteter, m.m. Det finns ett antal roller i KLASSA som förväntas vara de som fattar beslut som driver processerna framåt, men *användarens* roll är främst att vara den som dokumenterar arbetet.

Revisor

Många organisationer har externa revisorer som kontrollerar arbetet som görs inom informationssäkerhet. Den här rollen är till för dem, och har inget ansvar i KLASSA utöver att kunna läsa och se arbetet som skett i systemet.

En revisor har behörighet att läsa allt i organisationen, men kan inte ändra något.

”Ingen”

Rollen ”Ingen” ger ingen behörighet. Den rollen används för att stänga av en användare från systemet utan att ta bort kontot.

Underorganisationsroller

Begreppet underorganisationsroller avser en viss del av organisationen i KLASSA. Det kan vara en viss avdelning eller en viss sektion. Därför är organisationsstrukturen en väsentlig del när det kommer till begränsning av behörigheter för en specifik roll.

Rollerna som nämns nedan har samma typ av behörighet som på den organisationsövergripande nivån, men att den bara ger behörighet till de utpekade underorganisationerna.

Riskägare

Den som har rollen *riskägare* förväntas vara med när riskanalyser genomförs. Det är *riskägaren* som föreslår vilka säkerhetsåtgärder organisationen bör ta, för att den förmodade risken ska minska. I arbetet med att föreslå mitigerande säkerhetsåtgärder är det också *riskägaren* som ansvarar för att bedöma förväntat utfall av dessa (vilket sedan är upp till rollen *informationsägare/systemägare* att besluta om).

Informationsägare/systemägare

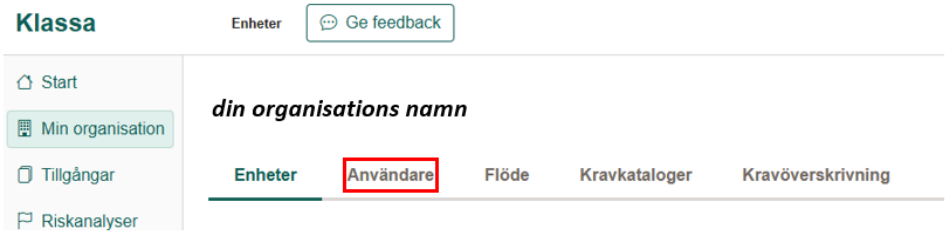
Din organisation har många informationstillgångar. I KLASSA omnämns dessa helt enkelt som ”tillgångar”. Den som är ägare för en informationstillgång är den inom organisationen som ansvarar för att en klassning av just den tillgången är korrekt. Det är också rollen *informationsägare/systemägare* som ansvarar för att fatta beslut om föreslagna säkerhetsåtgärder (vilka föreslås från rollen *riskägare*) vid riskanalyser, samt bedömer förväntat nytt riskvärde för tillgången efter att åtgärderna implementeras. Föreslagna säkerhetsåtgärder kan också uppstå i arbetet med handlingsplaner, och även där är det rollen *informationsägare/systemägare* som förväntas säkerställa att de föreslagna säkerhetsåtgärderna implementeras i organisationen.

Användare

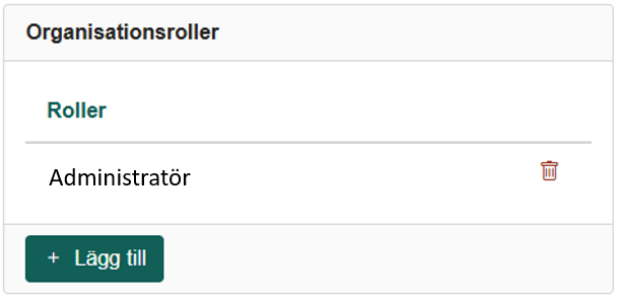
Alla andra inom organisationen som ska arbeta i KLASSA har som minst rollen *användare*. Den som har rollen *användare* men ingen annan roll, förväntas dokumentera arbetet som sker i KLASSA. Det kan innebära allt från att lägga upp de tillgångar som ska klassificeras, påbörja klassificeringar, dokumentera status för pågående aktiviteter, m.m. Det finns ett antal roller i KLASSA som förväntas vara de som fattar beslut som driver processerna framåt, men *användarens* roll är främst att vara den som dokumenterar arbetet.

Tilldela behörigheter och roller

Tilldelning av behörigheter och roller görs under fliken **Användare**:



Klicka på en användare för att tilldela eller ta bort roller för den användaren. Tilldelade roller tas bort med hjälp av soptunnan och nya roller tilldelas med knappen *”+ Lägg till”*.



Organisationsträdet

Roller, tillgångar och flöden kopplas till en organisatorisk enhet. För att din organisation ska kunna börja arbeta i KLASSA, behöver du skapa ett organisationsträd. Det gör du under fliken ”*Organisationsträd*”.



Längst ner på sidan finns knappen 

Klicka på den för att påbörja ditt organisationsträd. Skapade organisationsdelar kan flyttas eller tas bort genom att klicka på enheten i trädet och sedan välja soptunnan för att ta bort enheten, eller klicka på ”*Överliggande underorganisation*” för att välja en annan del av organisationsträdet.

Beroende på hur din organisation ser ut kan du bygga upp enheter som har informationstillgångar som behöver hanteras.

Här nedan följer en exempelbild på hur ditt organisationsträd kan se ut när du börjat bygga upp det med de enheter som din organisation består av.



Utöver tillgångar, kan du också bestämma vilka flöden som ska kopplas till vilken enhet. Detta görs under respektive flöde vilket beskrivs närmare under det avsnittet.

Kravkataloger

Grundläggande information

De krav som ställs på din organisation sammanställs i kravkataloger. I en kravkatalog definieras varje enskilt krav eller åtgärd som gäller för respektive område, samt vilken parameter det är i flödet, exempelvis klassningen, som genererar respektive krav eller åtgärd. Alla krav eller åtgärder som ska ingå vid exempelvis en klassning kan antingen samlas i en kravkatalog, eller fördelas på ämnesspecifika kravkataloger.



Som organisationsadministratör kan du inte ändra en existerande global kravkatalog, men du kan skapa egna lokala kravkataloger för din organisation.

Globala kravkataloger

De finns ett antal globala kravkatalogerna som följer med KLASSA och som administreras centralt.

- *MCFFS 2026:11* – En kravkatalogen som är direkt kopplad till MCF:s föreskrifter
- *Klassa5-kravkatalog* - Baskrav gällande verksamhetens informations-säkerhet. En kravkatalog som inspirerats av NIS2 genomförande-förordningen och utformats likt kravkatalogen i Klassa 4.
- *AI* – Åtgärder relaterade till AI-förordningen
- *GDPR5* - Åtgärder relaterade till GDPR-förordningen
- *NIS2-5* - Åtgärder relaterade till NIS2-direktivet/CSL
- *GDPR4* – En kvarleva från KLASSA 4 för den som vill hantera GDPR som en kravsamling. Vi rekommenderar den uppdaterade personuppgifts-hanteringen i KLASSA 5
- *ssnf* – Riktlinjer för säkerhet i telenät och teletjänster, version 1.1-1.5

Ovanstående kravkataloger förvaltas av SKR med undantag för *ssnf* som förvaltas av Stadsnätsföreningen (SSNF)

Det går att använda flera kravkataloger parallellt. För verksamheten kan det vara aktuellt att ha en kravkatalog med baskrav och en kompletterande katalog för just

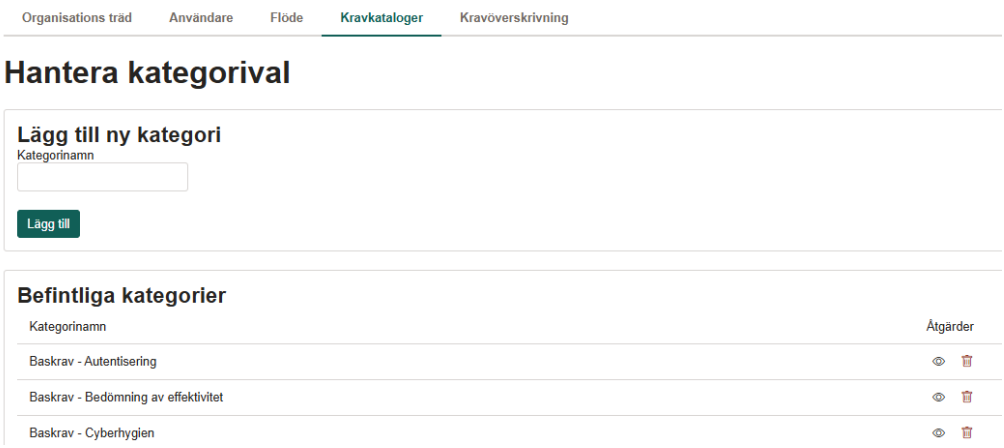
egna kompletteringar och för överskrivningar av de globala kravkatalogerna. Exempelvis om man vill precisera krav.

Kraven kan filtreras genom att flöden anpassas för olika ändamål. Se vidare i avsnittet om flöden.

Kategorier

Kraven i en kravkatalog struktureras i kategorier. Dessa definieras i förväg under menyn ”*Hantera kategorival*” i ovanstående bild. Med de globala kravkatalogerna följer det ett par grupper med fördefinierade kategorier.

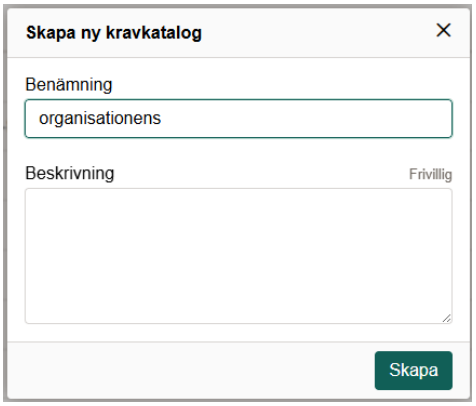
Om organisationen skapar egna kravkataloger bör även nya kategorier skapas för dessa. Skriv ett nytt namn i fältet ”*Kategorinamn*” och klicka på ”*Lägg till*” för att skapa en ny kategori.



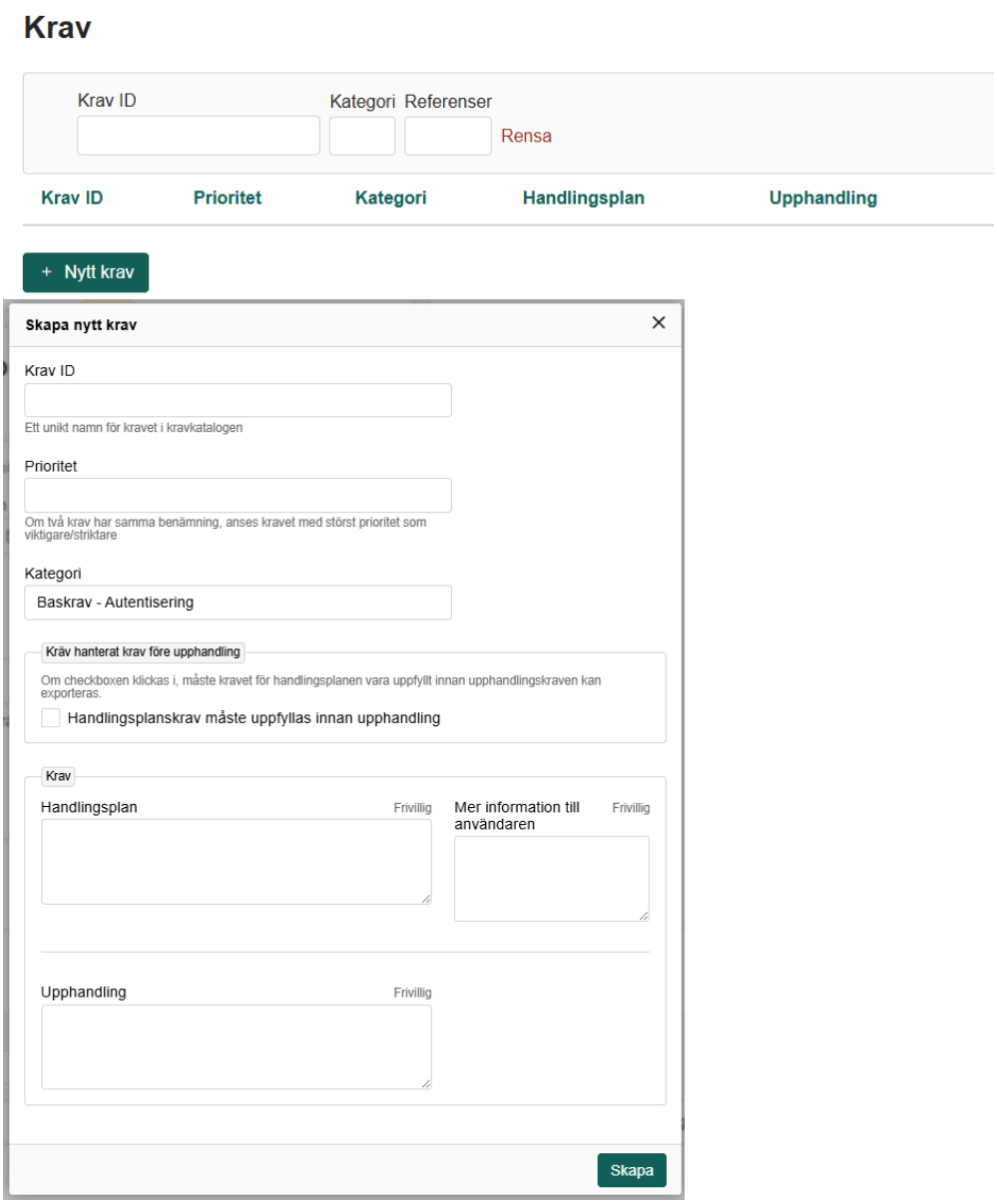
Exemplen är hämtade från kategorierna i *Klassa5-kravkatalog* som bygger på genomförandeförordningens kategorier.

Skapa ny kravkatalog

För att skapa en ny kravkatalog, klicka på *”+ Ny kravkatalog”* längst ned på sidan med kravkataloger och namnge den nya kravkatalogen.



Skapa ett nytt krav med hjälp av knappen *”+ Nytt krav”*.



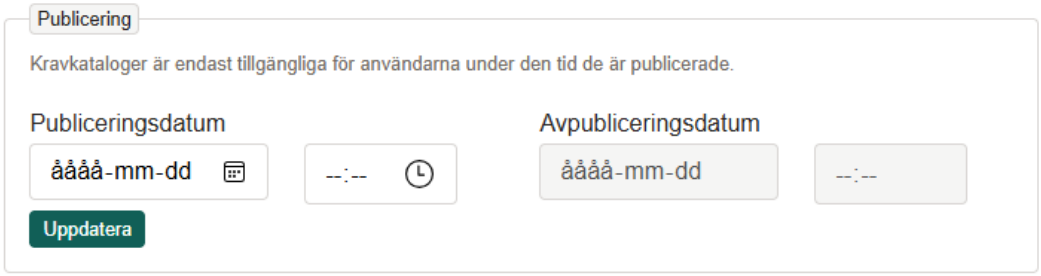
Följande information ska anges:

- ”*Krav ID*” – Ett unikt namn för detta krav
- ”*Prioritet*” – Om varje krav har mer än en prioritetsnivå anges den här. Om kravet är av typen ”on/off”, utan flera nivåer, anges värdet ”1”.
- ”*Kategori*” – Välj något av de fördefinierade alternativen.
- ”*Handlingsplan*” – Här definieras själva kravtexten.
- ”*Mer information till användaren*” – Detta är informationstexten som kan tas fram vid klassningstillfället.
- ”*Upphandling*” – Här anges de krav som gäller vid upphandling.

Klicka på ”*Skapa*” och välj eventuella referenser och klicka *”+ Lägg till”*. Fortsätt sedan med nästa krav.

Publicering av kravkatalogen

För att en kravkatalog ska kunna användas av organisationen måste den vara publicerad. Ange publiceringsdatum och tidpunkt på kravkatalogens sida och klicka sedan på ”*Uppdatera*”. Eventuell tidigare version av kravkatalogen kommer då att avpubliceras samtidigt som den nya versionen publiceras.



Flöden

Grundläggande information

Flöden används för att definiera hur exempelvis hur en klassning ska gå till, vilka parametrar som ska användas inklusive ordningsföljden, samt vilka kravkataloger som är aktuella.

Varje flöde kan kopplas till hela organisationen eller till en eller flera valda enheter. Vid klassning av en tillgång så aktiveras samtliga flöden kopplade till den organisatoriska enhet som den aktuella tillgången är kopplad till.



För att bestämma koppling mellan existerande flöden och enheter i din organisation, klicka på det flöde som är aktuellt och sedan på knappen ”*Organisation*”. Välj sedan om hela organisationen eller endast delar av den (enheter) ska använda flödet.



Som organisationsadministratör kan du inte ändra ett existerande, globalt flöde, men du kan skapa egna lokala flöden för din organisation. Dessa lokala flöden kan använda både globala kravkataloger, samt din organisations egna lokala kravkataloger.

Globala flöden

De globala flöden som följer med KLASSA är följande:

- *Informationsklassning och verksamhetskrav* – Ett flöde som påminner om KLASSA 4, men som har utformats med genomförandeförordningen för NIS2 som utgångspunkt. Referenser finns även till andra regler och standarder. Svaren på konfidentialitet, riktighet och tillgänglighet väljer ut lämpliga säkerhetsåtgärder. I slutet av flödet fångas också uppgifter kopplade till en kontinuitetsanalys.
    - Detta flöde är kopplat till *klassa5-kravkatalog*.

- *Ledning – Informationsklassning och verksamhetskrav* – Detta flöde är ett filtrerat flöde av *Informationsklassning och verksamhetskrav* som väljer säkerhetsåtgärder som riktar sig till själva organisationen.
    - Detta flöde är kopplat till en delmängd av *klassa5-kravkatalog*.

- *Verksamhet – Informationsklassning och verksamhetskrav* – Detta flöde är ett filtrerat flöde av *Informationsklassning och verksamhetskrav* som väljer säkerhetsåtgärder som riktar sig till verksamheten och de delar av organisationen som arbetar informations- och/eller systemnära.
    - Detta flöde är kopplat till en delmängd av *klassa5-kravkatalog*.

- *MCFFS2026-11* – Ett flöde som har en direkt relation till *föreskriften och allmänna råden MCFFS 2026:11 om säkerhetsåtgärder och ledningens utbildning* kan tillämpas likt flödet *Informationsklassning och verksamhetskrav* där svaren på konfidentialitet, riktighet och tillgänglighet väljer ut lämpliga säkerhetsåtgärder.
    - Detta flöde är kopplat till kravkatalogen *mcffs2026-11.*

- *AI* – Ett flöde som har en direkt relation till AI-förordningen och vägleder vid användningen av AI. Åtgärderna som flödet leder till är relaterade till AI-förordningen. Detta flöde är att betrakta som ett verksamhetsnära flöde och flödet inleds med frågan om AI används. Vid ett nekande svar passeras flödet utan åtgärd.
    - Detta flöde är kopplat till åtgärder som finns i kravkatalogen *AI*

- *Personuppgifter 5* – Ett flöde som har en direkt relation till GDPR och vägleder vid personuppgiftsbehandling. Åtgärderna som flödet leder till är relaterade till Dataskyddsförordningen. Det innebär också att informationen som samlas in i flödet är de uppgifter som förväntas i ett register över behandlingar av personuppgifter i enlighet med kravet i artikel 30 i Dataskyddsförordningen. Detta flöde är att betrakta som ett verksamhetsnära flöde och flödet inleds med frågan om personuppgifter behandlas. Vid ett nekande svar passeras flödet utan åtgärd.
    - Detta flöde är kopplat till åtgärder som finns i kravkatalogen *GDPR5.*

- *Cybersäkerhet* – Ett flöde som är uppbyggt som ett självskattnings-formulär för hur er organisation i nuläget efterlever kraven som ställs gällande den organisatoriska delen av regleringen. På grund av Cybersäkerhetslagens omfattning ska denna självskattning inte ses som ett facit på regelefterlevnad, utan en indikation om nuläget. Detta flöde riktar sig till organisationens ledning.
    - Detta flöde är kopplat till åtgärder som finns i kravkatalogen *NIS2-5.*

- *Personuppgifter 4* – Ett enklare flöde för behandling av personuppgifter som följer med från KLASSA 4. Vi rekommenderar den uppdaterade personuppgiftshanteringen i flödet *Personuppgifter 5.*
    - Detta flöde är kopplat till åtgärderna som finns i kravkatalogen *GDPR4*.

- *ssnf* – Utgår från Stadsnätsföreningens riktlinjer för säkerhet i telenät och teletjänster, version 1.1-1.5.
    - Detta flöde är kopplat till kraven som finns i kravkatalogen *ssnf.*

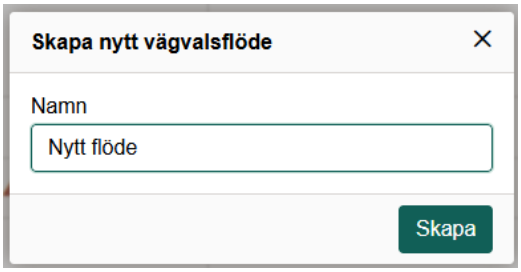
Ovanstående flöden förvaltas av SKR med undantag för *ssnf* som förvaltas av Stadsnätsföreningen (SSNF)

Det går att använda flera flöden parallellt. För verksamheten kan det vara aktuellt att ha ett flöde med baskrav för informations- och cybersäkerhet som filtreras för

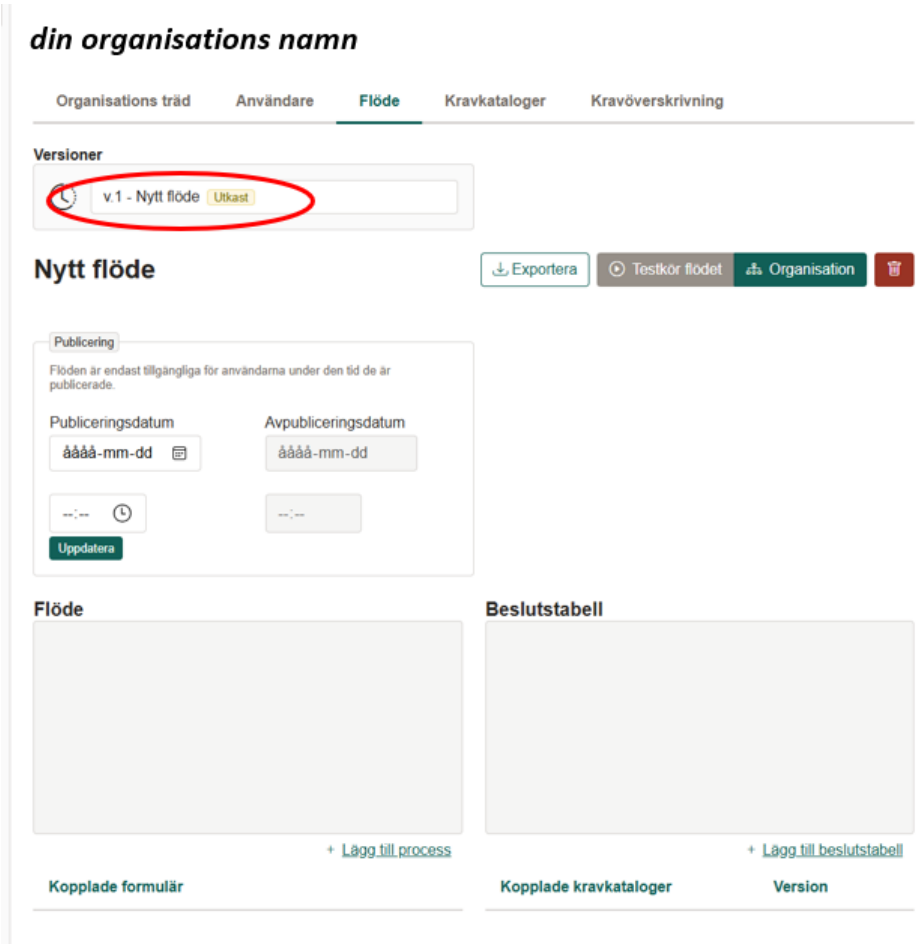
informations- och verksamhetsnära användning och sedan komplettera det med exempelvis flöden för AI och personuppgiftsbehandling. Dessa exempel på flödena inleds med information om flödet och om det är aktuellt med AI och om det är aktuellt att behandla personuppgifter.

Skapa nytt flöde

För att skapa ett nytt flöde, klicka på *”+ Skapa nytt vägvalsflöde”* längst ned på sidan med flöden och namnge det nya flödet.



Du har nu skapat ett nytt flöde, som än så länge enbart finns som ett tomt utkast.



Formulär

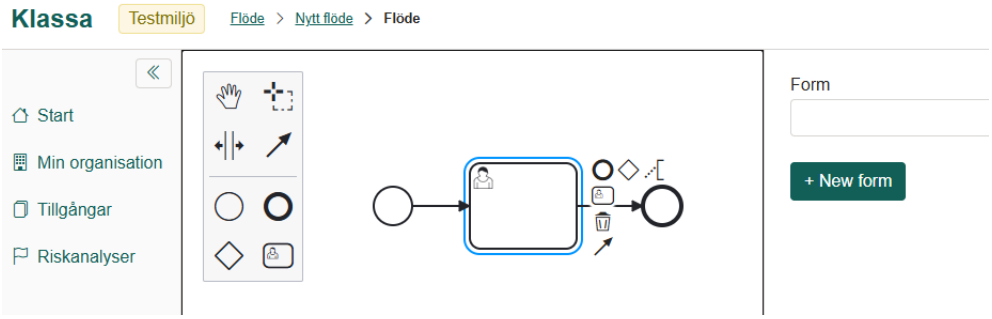
Nästa steg i designen av ett flöde är att bestämma själva processen med hjälp av ett eller flera formulär. Frågorna som systemet ställer vid exempelvis informationsklassning definieras nämligen med hjälp av formulär i respektive flöde.

I formulären skapas den information och dialog som ska ske med användaren under klassningen av information. Varje parameter som ska bedömas definieras med hjälp av dessa formulär.

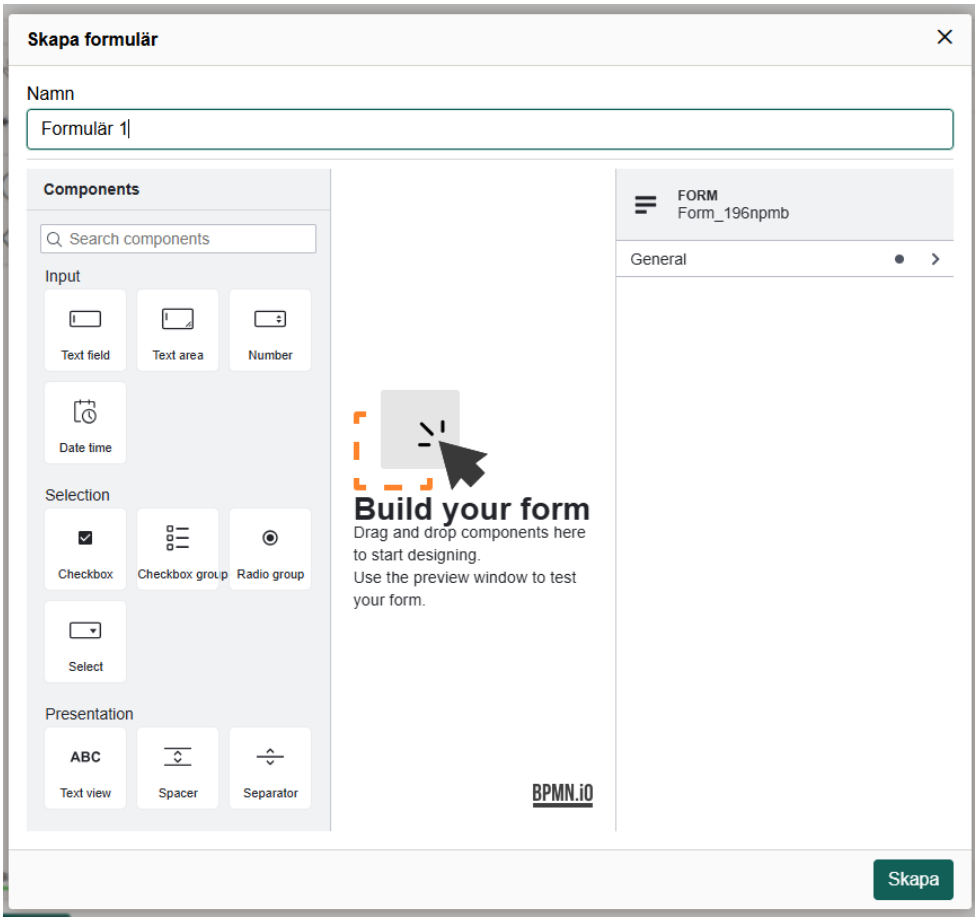
Du som din organisations administratör kan bygga egna formulär för att generera de variabler som sedan används av en *beslutstabell* (mer om dessa längre fram). Beslutstabellen är den funktion i systemet som avgör vilka krav som är relevanta, och hur dessa ska prioriteras.

För att påbörja bygget av ditt organisationsspecifika flöde, klicka på *”+ Lägg till process”* under den grå flödesrutan (se bild ovan).

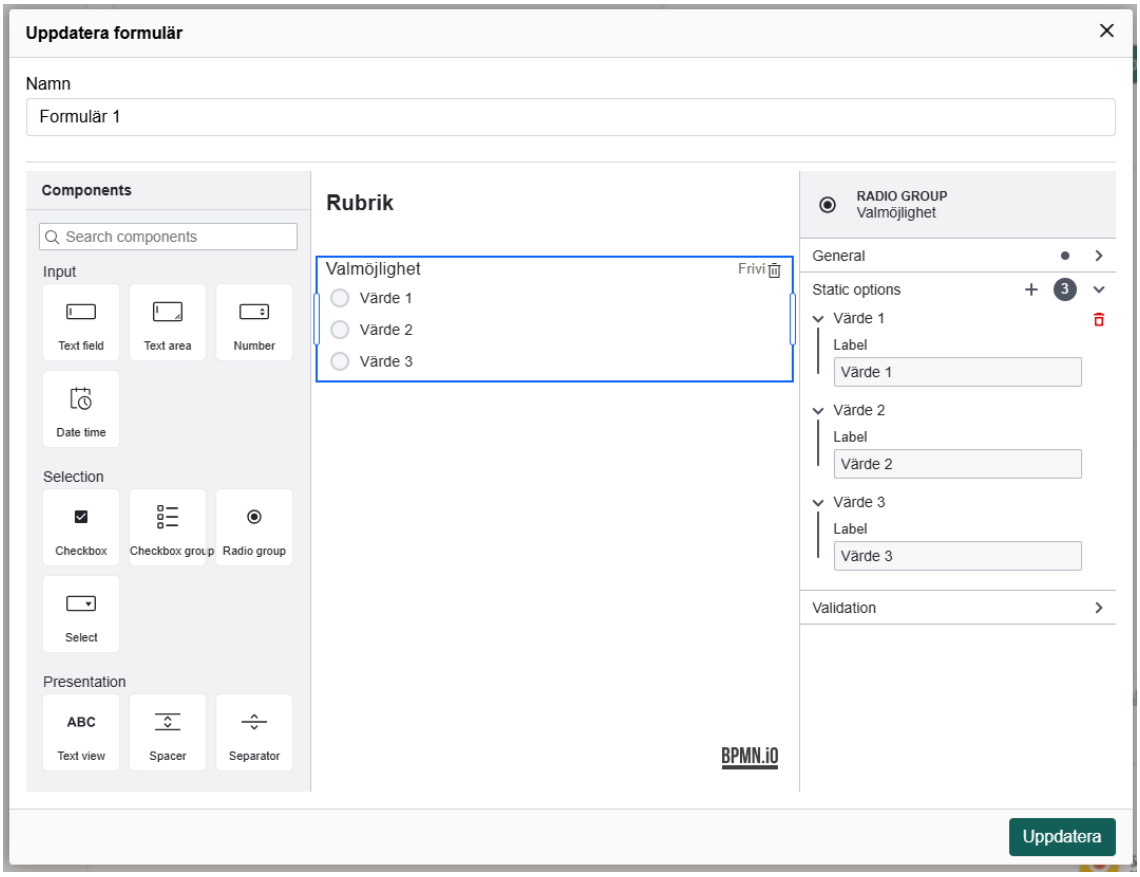
Skapa det önskade processflödet, där varje rektangel motsvarar ett formulär. Formulären kommer att visas i den ordning de anges i flödet. Varje formulär kan bestå av mer eller mindre information till användaren, samt frågan efter en eller flera variabler som ska användas för val av rader i beslutstabellen.



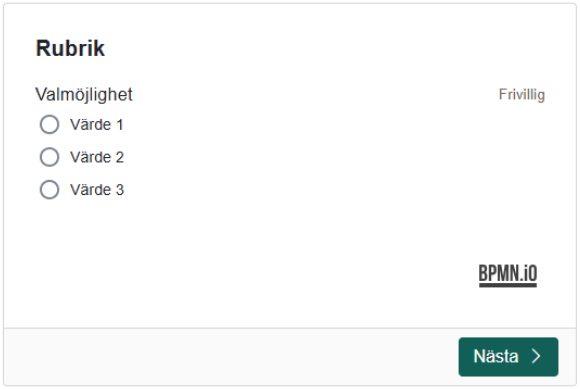
Klicka på *”+ New form”* för att skapa det nya formuläret.



Namnge det nya formuläret och bygg strukturen med hjälp av komponenterna i vänstra spalten. Det gör du genom att klicka på en komponent och sedan dra den till mittenspalten. Nödvändig information för respektive komponent anges sedan i högra spalten.



Ovanstående exempel på ett formulär kommer att generera nedanstående dialogruta vid klassning av information:

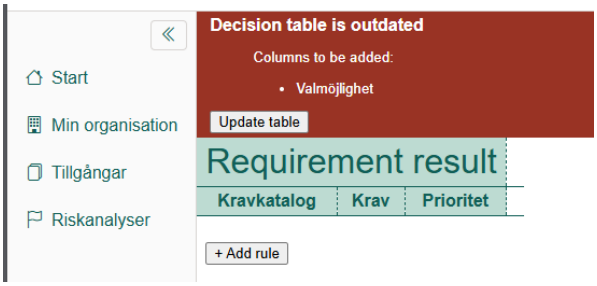


Beslutstabell

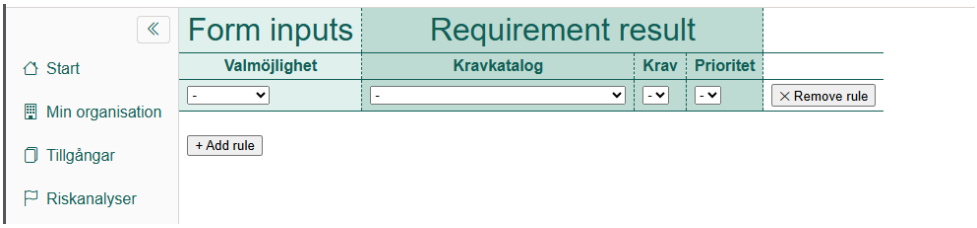
När det finns ett formulär enligt ovanstående beskrivning, så ska man också ha definierat de parametrar som behövs för att en beslutstabell ska kunna byggas. Beslutstabellen är sedan den faktor som avgör om och vilka krav från kravkatalogen som ska ingå i de den handlingsplan som skapas i samband med att en tillgång exempelvis klassificeras.



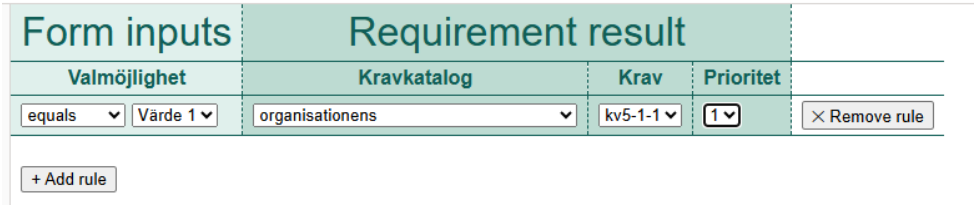
Skapa en ny beslutstabell genom att klicka på *"+ Lägg till beslutstabell"*. När en beslutstabell skapas, eller om förutsättningarna från formulär och/eller kravkatalog har ändrats, behöver systemet uppdatera informationen. När detta sker, klicka på *"Update table"*.



Klicka på *"+ Add rule"* för att lägga till en ny regel.



Kolumnen *"Form inputs"* kommer nu innehålla samtliga variabler som definierats i formulären. Ange villkoren för första kravet, vilken kravkatalog som ska användas, vilket krav det gäller, samt prioritet. Sätt värde "1" på prioriteten om det inte finns några prioritetsnivåer, utan kravet är av typen "on/off".
Gå sedan vidare med nästa krav.



Spara beslutstabellen för att återgå till vyn för flödet.

Publicering av flöde

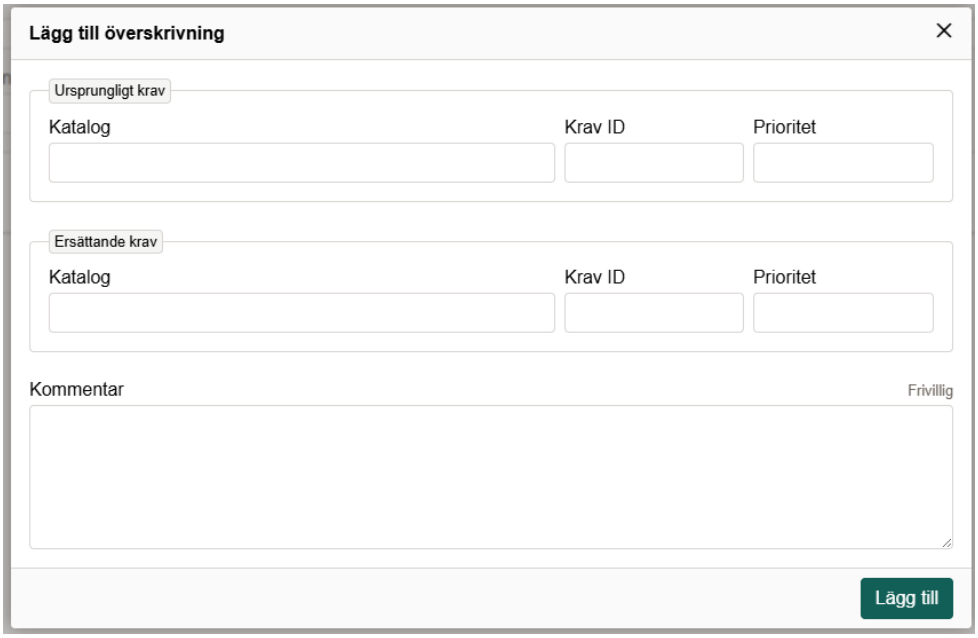
För att ett flöde ska kunna användas av organisationen måste det vara publicerat. Säkerställ att flödet är kopplat till organisationen enligt inledningen på detta kapitel. Ange publiceringsdatum och tidpunkt i flödet och klicka på ”*Uppdatera*”. Eventuell tidigare version av flödet kommer då att avpubliceras samtidigt som den nya versionen publiceras.



Kravöverskrivning

Grundläggande information

I vissa fall finns det behov av att låta ett krav överrida ett annat krav. Det kan exempelvis vara så att de båda kraven avser samma område, men är definierade i olika kravkataloger. Administratören kan styra detta med hjälp av funktionen kravöverskrivning, där hen definierar vilket krav som ska överrida det andra.



Om båda de angivna kraven skulle vara aktuella enligt beslutstabellerna, kommer enbart det ersättande kravet att visas i handlingsplanen.

Ett exempel på väg fram

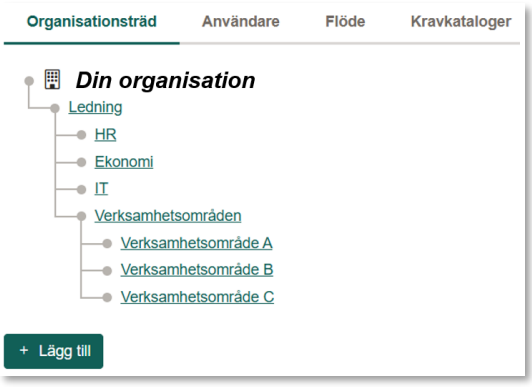
Skapa organisation

Till att börja med så finns ingen organisationsstruktur skapad i KLASSA. Som organisationens administratör behöver du skapa de organisatoriska enheter som ska användas.

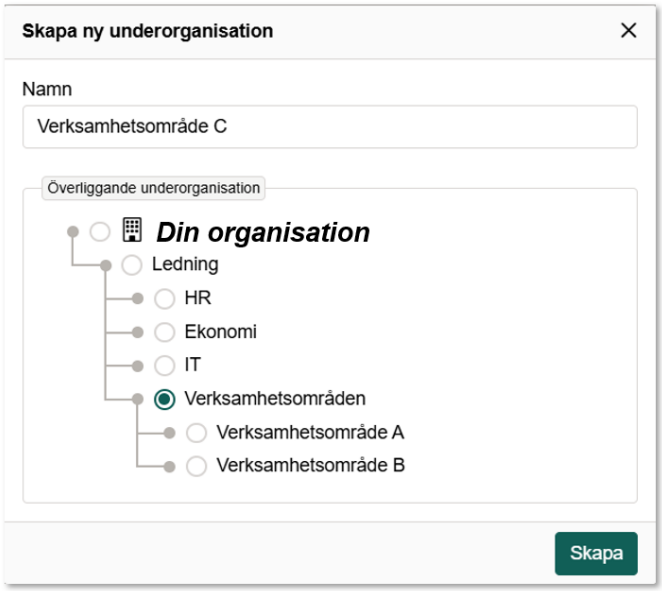


Strukturen i KLASSA kan mycket väl motsvara den verkliga organisationen, men tänk på att val av flöden med tillhörande kravkatalog kopplas till organisatoriska enheter som tillgångarna tillhör. Om det är tänkt att använda olika flöden för tillgångar som hör till samma fysiska organisationsdel, behöver enheten delas upp på flera enheter i KLASSA. Alla tillgångar som är kopplade till en viss enhet kommer att hanteras enligt samma flöde(n) i KLASSA.

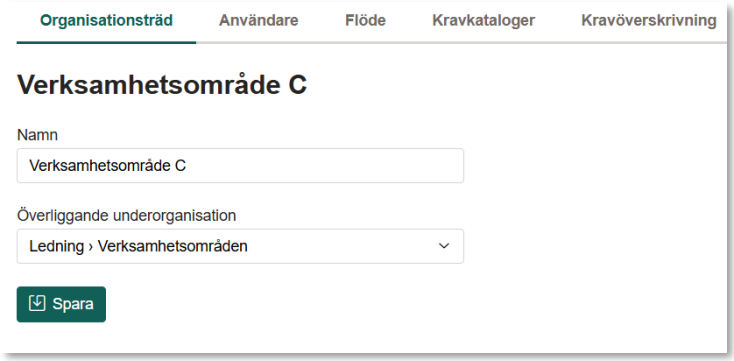
Ett exempel på hur en organisation kan sättas upp visas nedan.



Skapa nya organisationsdelar genom att klicka på knappen *”+ Lägg till”*.



Ange namnet på den nya enheten och markera även vilken enhet som är överordnad. Klicka sedan på skapa.



Kontrollera namn och överliggande underorganisation. Tryck sedan på *”Spara”*.

Klicka sedan på menyvalet *”Organisationsträd”* för att se resultatet.

Välj flöden

I KLASSA finns flera fördefinierade, globala, flöden. Dessa flöden använder sig av globala kravkataloger och kan kopplas till hela eller delar av den egna organisationen för att därefter användas vid exempelvis klassning av organisationens tillgångar. Flera flöden kan kopplas till varje del av organisationen.

Ett exempel på flöden som kan kopplas till verksamhets- eller informationsnära delar i organisationen är:

- *Verksamhet – Informationsklassning och verksamhetskrav* – Detta flöde är ett filtrerat flöde av *Informationsklassning och verksamhetskrav* som väljer säkerhetsåtgärder som riktar sig till verksamheten och de delar av organisationen som arbetar informations- och/eller systemnära.

- *Personuppgifter 5* – Ett flöde som har en direkt relation till GDPR och vägleder vid personuppgiftsbehandling. Åtgärderna som flödet leder till är relaterade till Dataskyddsförordningen. Det innebär också att informationen som samlas in i flödet är de uppgifter som förväntas i ett register över behandlingar av personuppgifter i enlighet med kravet i artikel 30 i Dataskyddsförordningen.

- *AI* – Ett flöde som har en direkt relation till AI-förordningen och vägleder vid användningen av AI. Åtgärderna som flödet leder till är relaterade till AI-förordningen.

Därutöver kan följande flöden användas för en mer organisationsövergripande del av verksamheten:

- *Ledning – Informationsklassning och verksamhetskrav* – Detta flöde är ett filtrerat flöde av *Informationsklassning och verksamhetskrav* som väljer säkerhetsåtgärder som riktar sig till själva organisationen

- *Cybersäkerhet* – Ett flöde som är uppbyggt som ett självskattnings-formulär för hur er organisation i nuläget efterlever kraven som ställs gällande den organisatoriska delen av regleringen. På grund av Cybersäkerhetslagens omfattning ska denna självskattning inte ses som ett facit på regelefterlevnad, utan en indikation om nuläget.

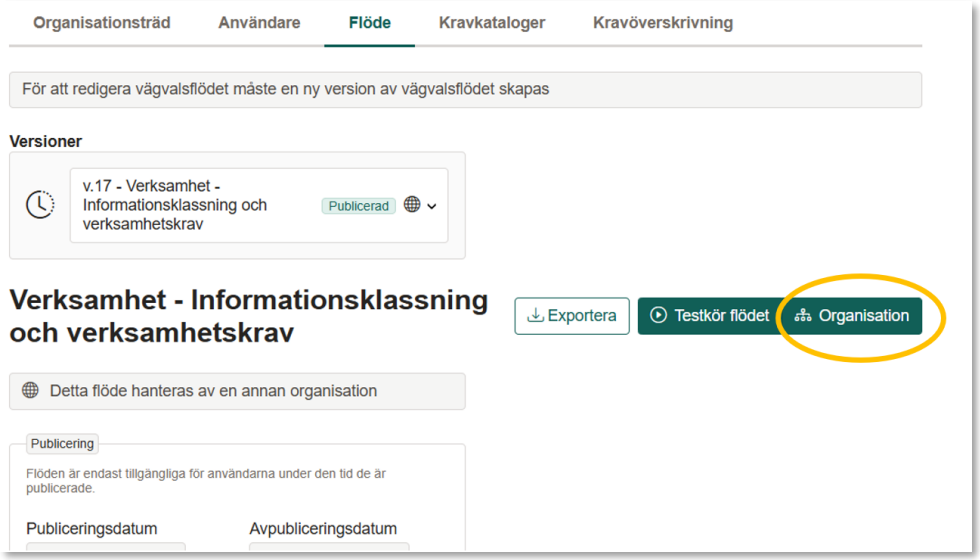
För den som helt vill utgå från Myndigheten för civilt försvars *föreskrift och allmänna råden MCFFS 2026:11 om säkerhetsåtgärder och ledningens utbildning* kan flödet *MCFFS2026-11* tillämpas likt flödet *Informationsklassning och verksamhetskrav* där svaren på konfidentialitet, riktighet och tillgänglighet väljer ut lämpliga säkerhetsåtgärder.

De globala flödena beskrivs mer i detalj i tidigare avsnitt.

Koppla flöden till organisatorisk enhet

Alla tillgångar som hör till en organisatorisk enhet kommer att använda de flöden som är kopplade till aktuell enhet.

För att koppla ett flöde till en enhet – gå in på aktuellt flöde och klicka på knappen *”Organisation”*.

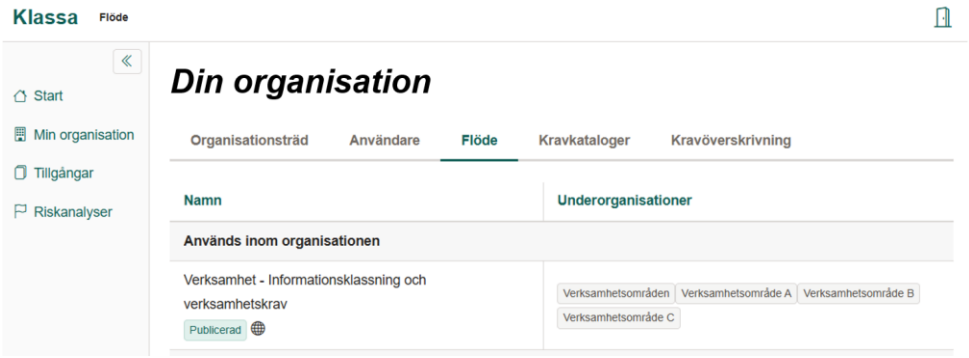


Välj om flödet ska kopplas till hela organisationen, eller enbart en eller flera enheter inom organisationen.



Klicka på *”Lägg till”*. På sidan *Flöde* visas nu att flödet nu är kopplat till organisationen, samt vilka enheter inom organisationen som är berörda.

I vårt exempel kopplades flödet till enheterna *Verksamhetsområden, Verksamhetsområde A, Verksamhetsområde B* samt *Verksamhetsområde C.*



Fortsätt sedan med att koppla alla relevanta flöden till aktuella organisatoriska enheter. När sedan tillgångar skapas och kopplas till en enhet, kommer de flöden som är kopplade till just den enheten att användas för exempelvis informationsklassning av aktuell tillgång.