

KLASSA Användarforum #6

Zoom, 2024-11-28

Välkomna till det sjätte användarforumet!

Att tänka på under dagen

- Ingen sekretess
- Ljud och bild
- Frågor i chatten
- Speaker view/pin video
- Stanna kvar i mötet

Agenda

- 10:00 – Inledning – *Lotta Nordström*
- 10:10 – Vad har hänt sen sist? – *Jonas Nilsson*
- 11:00 – Paus – sträck på benen
- 11:10 – KLASSA 5.0 – *Thomas Nilsson*
- 12:00 – Lunch
- 13:00 – “Grupparbete”
- 14:45 – Summering – *Lotta, Jonas och Thomas*
- 15:00 – Avslut

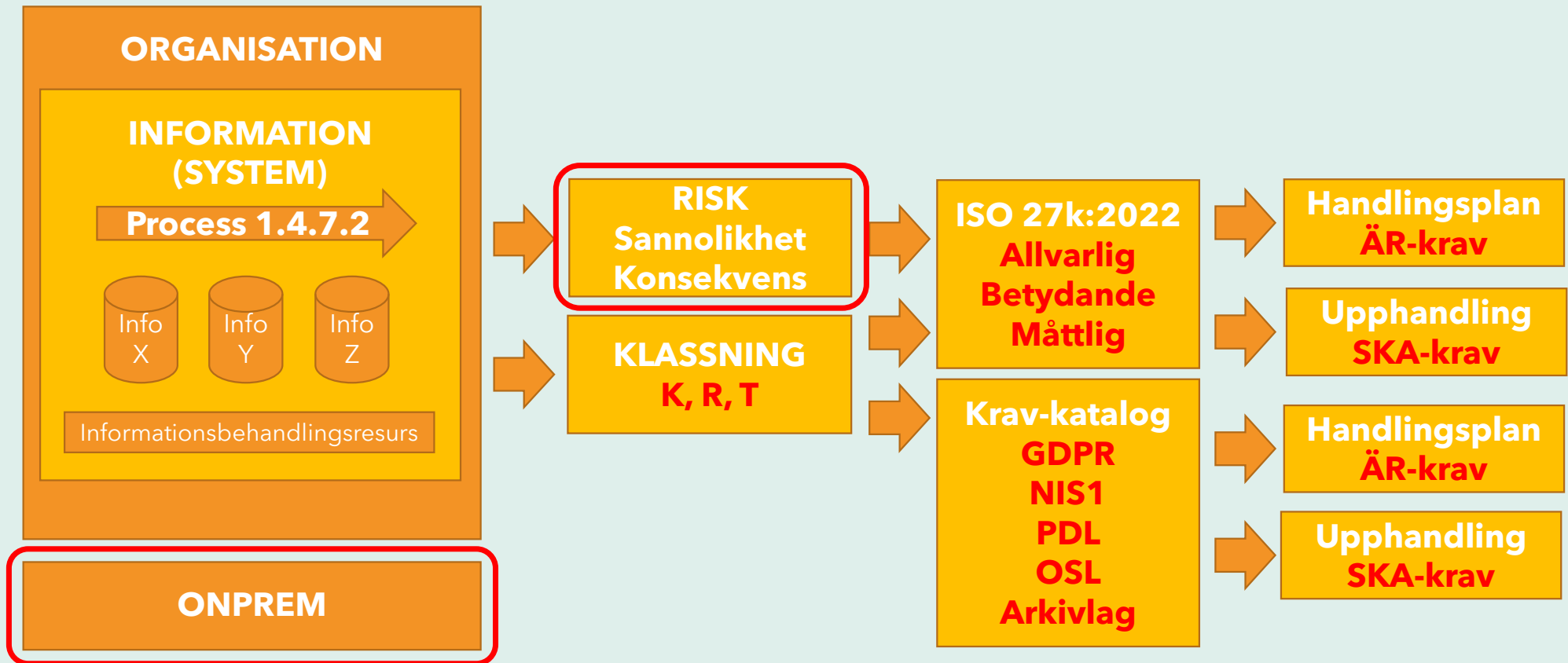
Inledning

Lotta Nordström

Vad har hänt sedan sist

Jonas Nilsson

KLASSA (v4), vad är på gång?



Forum

- **Expertgruppen** är begränsad till åtta (8) namngivna experter från betalande organisationer
 - KLASSA:s styrgrupp bestämmer vilka som utgör KLASSA:s expertgrupp
 - Ansvarar t.ex. för utformning av metodik och innehåll i kravkataloger
- **Användarforum** består av samtliga betalande medlemmar har en plats i KLASSA användarforum
 - Rådgivande för KLASSA:s utveckling
 - Prioritering och omfattning
- Källkoden utvecklas av upphandlade utvecklingsresurser

Användare av KLASSA 4.0

382 organisationer:

- Kommuner
- Regioner
- Kommunala bolag
- Statliga myndigheter
 - T.ex. IVO, Skatteverket och SJ
- Övriga organisationer
 - T.ex. SKR och Adda

4 322 användare!

Resultat från förra användarforum

- Börjat omhänderta resultatet med den nya utvecklingspartnern, men...

Användarträff 2024-06-13

- Är det rätt väg att gå, d.v.s. att ändra strukturen på kravkatalogen från ett ISO-perspektiv till ett regelverksperspektiv?
 - Ja = ca 63 %
 - Nej = ca 21 %

Användarträff 2024-06-13

- Vilken annan funktionalitet ser ni att KLASSA bör erbjuda?
 - Rapportmodul
 - Kontinuitetshanteringsplan, Registerförteckning
 - Statistik, visuell sammanställning för redovisning
 - Påminnelsefunktion
 - Ett chefsfönster, så chefer som är ansvariga kan kolla lite
 - Göra egna kravkataloger, för att öka flexibiliteten
 - Sökfunktion, konsekvensbedömning (GDPR)
 - Koppling till Infosäkkollen (MSB)

Användarträff 2024-06-13

- Vilken funktionalitet är mest prioriterade i KLASSA?
 1. Rapportmodul
 2. Processorienterad informationskartläggning (POIK)
 3. Mognadsmätning (Infosäkkollen)
 4. Incidenthanteringsmodul
 5. Stöd för kontinuitetsplanering
 6. Stöd för säkerhetskyddsanalys

Helt lika mellan de 4 sista!

Användarträff 2024-06-13

- Vilken funktionalitet, i KLASSA, vill ni ändra på?
 - Sökfunktion
 - Enklare behörighetsadministration

Användarträff 2024-06-13

- Vilka rapporter vill ni kunna generera från KLASSA?

Användarträff 2024-06-13

- Vilka integrationsmöjligheter önskar ni i KLASSA?
 - SSO
 - Integration med IdP
 - Länka in Infosäkkollen
 - Qlikview
 - QlikSense

Användarträff 2024-06-13

- Hur vill ni att användarträffarna arrangeras?
 - Digitalt = ca 90 %
 - Fysiskt = ca 10 %

Vad är nytt?

- Flera inrapporterade buggar har åtgärdats.
- Förbättringar av innehåll:
 - Utifrån era förbättringsförslag har vi uppdaterat flertalet texter kring upphandlingskrav.
 - Korrigeringar av referenser för GDPR-kraven.
- Stort fokus på riskmodulens funktionalitet

KLASSA - Riskmodulen

- Hur blir det?
- När blir det?



Jonastad

+ Skapa underorganisation

Användarlista

Informationstillgångar

Kravmallar

Papperskorgen

Riskanalyser

Inställningar

+ Skapa riskanalys



Nedan listas alla organisationens riskanalyser.

Riskanalyser (1st)



KLASSA Användarforum

Ansvarig: Jonas Nilsson

Visa



Skapa riskanalys

För att genomföra en riskanalys så behöver ni planera och vara väl förberedda. En mycket viktig faktor är att rätt deltagare finns med under processen.

Tänk på detta innan ni startar

1

Börja med att namnge och beskriva den aktivitet som skall riskanalyseras. Det kan vara t.ex. "Byte av personalsystem".

Namnge riskanalysen (*)

Beskriv aktiviteten

2

Ta med deltagare som har rätt kompetens. Fundera också på kring vilka områden som riskanalysen kan behöva expertbedömning.

Namn (*)

Roll (*)

+ Lägg till fler deltagare

3

Identificera vilka objekt som kan påverkas i samband med den här aktiviteten

+ Lägg till berört objekt

4

Välj en person som kommer att vara ansvarig för den här riskanalysen

Ange ansvarig

Starta riskanalys



KLASSA Användarforum

Denna riskanalys avser KLASSA Användarforum #6

Ansvarig: Jonas Nilsson

+ Skapa risk

👤 Hantera behörighet

📄 Exportera

⚙️ Redigera

🗑️ Ta bort

Risker

Det finns inga risker skapade för den här riskanalysen ännu

KLASSA-utbildning

Genomförda utbildningstillfällen:

- 11 september
- 1 oktober
- 6 november

För att anmäla sig:

<https://www.adda.se/larande-och-verksamhetsstod/utbildningar/smartautbildningar/effektiv-och-saker-informationsklassning-med-klassa-4.0/>

04 December	🕒 09:00 - 12:00	● Fullsatt ▲ Bokningsperioden är slut	
16 December	🕒 13:00 - 16:00	● Fullsatt ▲ Bokningsperioden är slut	
14 Januari	🕒 13:00 - 16:00	● 1 plats kvar	Anmäl nu
30 Januari	🕒 09:00 - 12:00	● Fullsatt	Väntelista
12 Februari	🕒 09:00 - 12:00	● 26 platser kvar	Anmäl nu
25 Februari	🕒 13:00 - 16:00	● 30 platser kvar	Anmäl nu

Vad kommer SKR att syssla med?

Tillsammans är vi starka!



Tillsammans är vi starka!

- Nätverk:
 - KIS
 - HoSIS
- Kompetensgemenskaper:
 - Informationssäkerhet
 - Cybersäkerhet
 - Informationshantering
 - Digitaliseringsjuridik
 - AI-rådet
 - Arkitekturrådet

Skapa de rätta förutsättningarna

- Systematiskt informationssäkerhetsarbete
 - Styrdokument
 - Ansvar och rättigheter
 - Utbildning
 - Kontinuitetshantering
 - Incidenthantering
- **Övning ger färdighet!**

Nivå 1 Om Metodstödet



Nivå 1: Informationssäkerhetsarbetets grunder

Nivå 1 handlar om att skapa en grund för informationssäkerhetsarbetet och ta fram styrning för området. För att genomföra nivå 1 behövs det resurser med kompetens inom informationssäkerhet samt ett engagemang från ledningen. Ett genomförande av nivå 1 innebär att organisationen har grunderna i informationssäkerhetsarbetet på plats.

I nivå 1 är det viktigt att samverka med olika delar av organisationen, exempel på lämpliga samverkanspartners är juridik, IT, internkontroll och arkiv.

Det är viktigt att anpassa nivå 1 utifrån organisationens tillgång till resurser och ambitionsnivå, de fiktiva exemplen i metodstödet är relativt ingående i sin fakta. Det är av stor vikt att organisationen påbörjar ett arbete **inom alla områden** än att ett område är implementerat fullt ut.

Genomförda aktiviteter i denna nivå 1 innebär att organisationen har grunderna i informationssäkerhetsarbetet på plats.

Cybersäkerhetskollen

MSB har utvecklat ett verktyg, cybersäkerhetskollen (tidigare infosäkkollen), som ska ge stöd till organisationer att följa upp och förbättra det systematiska informationssäkerhetsarbetet.

Med cybersäkerhetskollen kan organisationen själv undersöka vilken nivå arbetet befinner sig på och hur det kan utvecklas. Resultatet ger underlag för planering och prioritering, och med regelbundna uppföljningar kan utvecklingen följas över tid.

Efter genomförande av nedan checklistas aktiviteter kan det vara möjligt att nå nivå 1 i cybersäkerhetskollen.

Metodstödet innehåller fiktiva exempel

För varje aktivitet i checklistan innehåller varje steg ett fiktivt exempel hur aktiviteten kan genomföras. **Observera** att det fiktiva exemplet inte direkt kan kopieras och appliceras i den egna organisationen, utan en bearbetning måste ske för att anpassa underlaget till organisationens förutsättningar och befintliga processer, styrning med mera.

Metodstöd Informationssäkerhet

Här får du konkreta tips på och exempel om hur din kommun kan utveckla och förbättra organisationens systematiska- och riskbaserade informationssäkerhetsarbete. Metodstödet består av fyra nivåer och bygger på erfarenheter från olika verksamheter.

Detta metodstöd innehåller en checklista med aktiviteter i varje nivå. Varje aktivitet innehåller en kort beskrivning av aktiviteten samt ett fiktivt exempel hur aktiviteten kan genomföras i organisationen.



Utveckla informationssäkerheten (nytt fönster)

Målgrupp

Informationssäkerhetssamordnare, CISO, informationssäkerhetschef eller liknande. Metodstödet kan också användas av andra nyckelpersoner i organisationen som arbetar med informationssäkerhet.



Nivå 1: Informationssäkerhetsarbetets grunder

Nivå 1 handlar om att skapa en grund för informationssäkerhetsarbetet och ta fram styrning för området. För att genomföra nivå 1 behövs det resurser med kompetens inom informationssäkerhet samt ett engagemang från ledningen. Ett genomförande av nivå 1 innebär att organisationen har grunderna i informationssäkerhetsarbetet på plats.

I nivå 1 är det viktigt att samverka med olika delar av organisationen, exempel på lämpliga samverkanspartners är juridik, IT, internkontroll och arkiv.

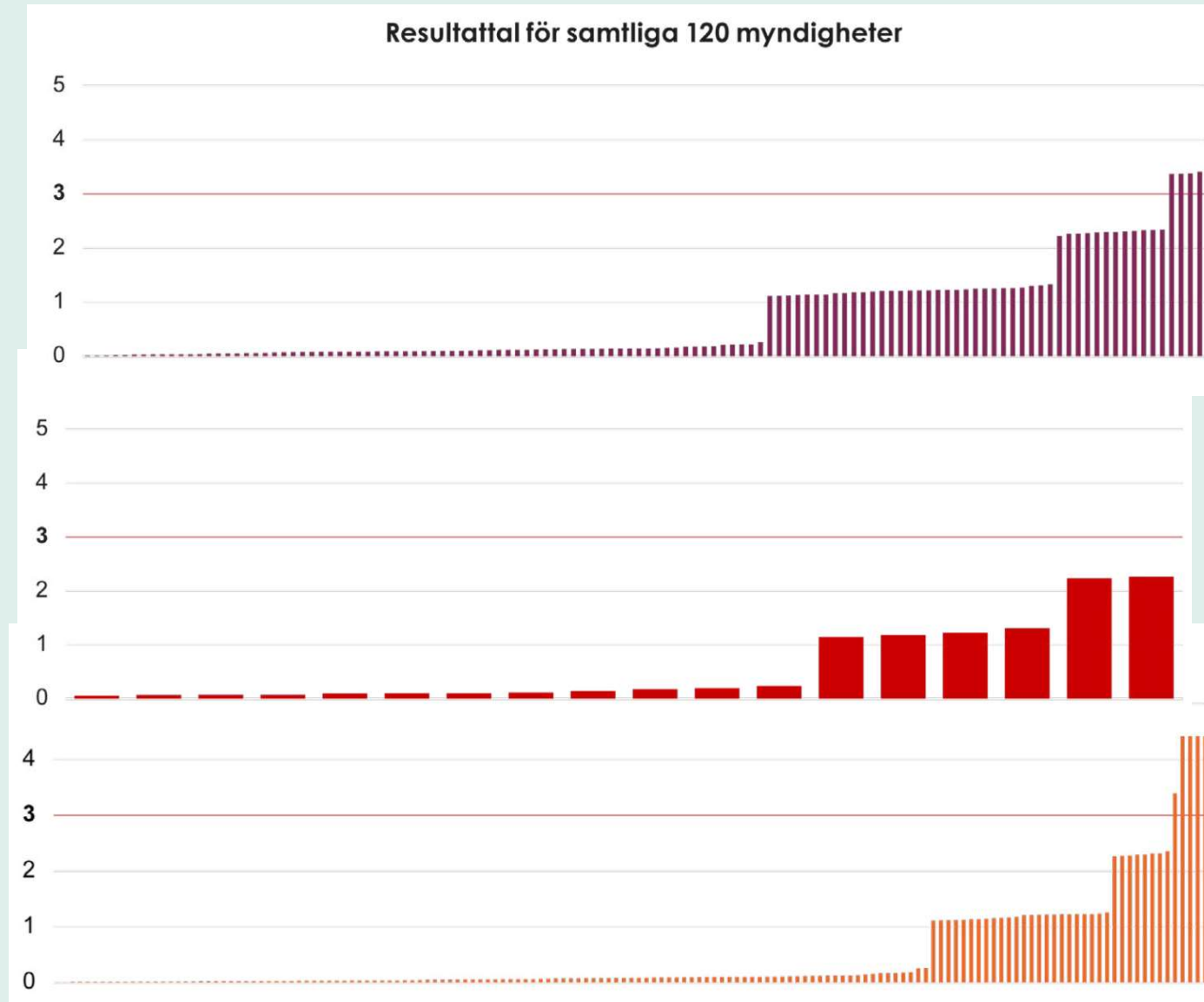
Det är viktigt att anpassa nivå 1 utifrån organisationens tillgång till resurser och ambitionsnivå, de fiktiva exemplen i metodstödet är relativt ingående i sin fakta. Det är av stor vikt att organisationen påbörjar ett arbete **inom alla områden** än att ett område är implementerat fullt ut.

Varför satsar SKR på KLASSA?

Utgångsläget

- Kommunerna
- Regionerna
- Myndigheterna

Resultattal för samtliga 120 myndigheter



NIS2

- Krav på ledningens deltagande i cybersäkerhetsarbetet
- Riskhantering
- Incidenthantering
- Driftskontinuitet
- Säkerhet i leveranskedjor
- Förmåga att bedöma effektiviteten i vidtagna åtgärder



Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster

t.o.m. SFS 2022:521

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

t.o.m. SFS 2022:508

Myndigheten för samhällsskydd och beredskaps författningssamling



Utgivare: Anna Asp, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

**MSBFS
2021:9**
Utkom från trycket
den 9 december 2021

Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster;

beslutade den 7 december 2021.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 3, 4 och 16 §§ förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Denna författning innehåller bestämmelser om anmälan enligt 23 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster samt bestämmelser om identifiering av leverantörer av samhällsviktiga tjänster enligt 3 § 1 st. 1 p. samma lag.

2 § 13-9 kap. finns en förteckning över samhällsviktiga tjänster där en incident skulle medföra en betydande störning enligt 3 § 1 st. 1 p. lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

informationssäkerhet
2018 om
direktiv (EU)
säkerhet i nätverks- och
tjänstleverans

ark och

Vad gäller nu?

- När kommer lagen?
- När kommer förordningen?
- När kommer föreskrifterna?



Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster

t.o.m. SFS 2022:521

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

t.o.m. SFS 2022:508

Myndigheten för samhällsskydd och beredskaps författningssamling



Utgivare: Anna Asp, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

**MSBFS
2021:9**
Utkom från trycket
den 9 december 2021

Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster;

beslutade den 7 december 2021.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 3, 4 och 16 §§ förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Denna författning innehåller bestämmelser om anmälan enligt 23 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster samt bestämmelser om identifiering av leverantörer av samhällsviktiga tjänster enligt 3 § 1 st. 1 p. samma lag.

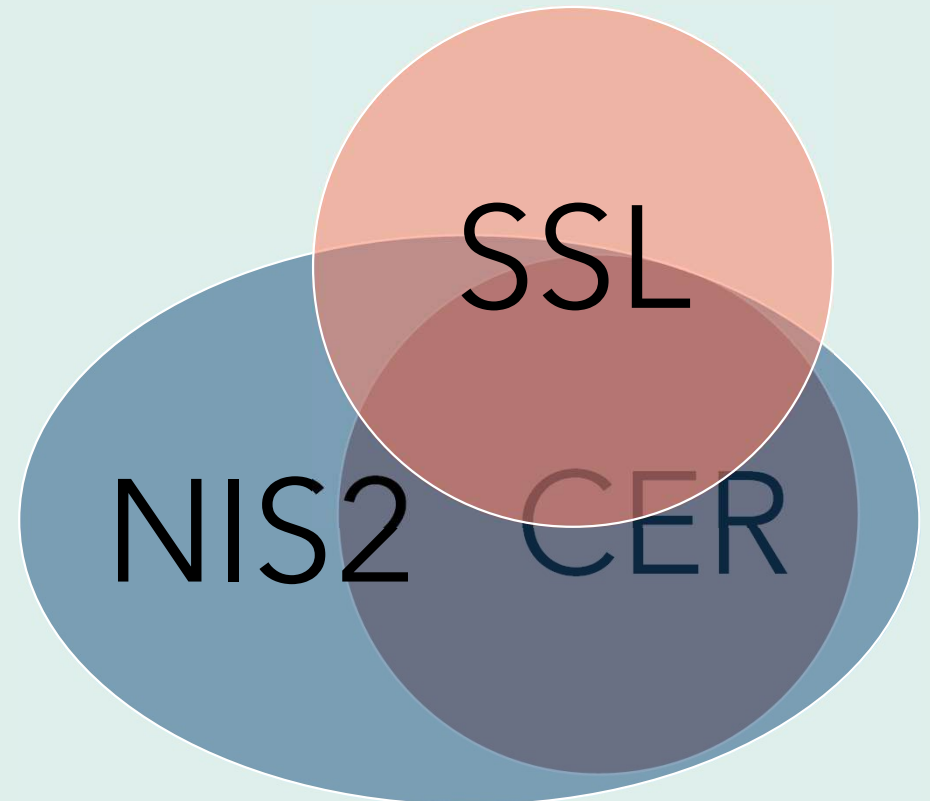
2 § 13-9 kap. finns en förteckning över samhällsviktiga tjänster där en incident skulle medföra en betydande störning enligt 3 § 1 st. 1 p. lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

informationssäkerhet
2018 om
företag (EU)
säkerhet i nätverks- och
tjänstleverans

ark och

Vad gäller sen?

- Regelöverlapp



Paus till 11:10

KLASSA 5.0

Thomas Nilsson

Med stöd från

VINNOVA
Sveriges innovationsmyndighet

 **Energimyndigheten**

FORMAS 

Strategiska
innovations-
program

Syftet och målet med KLASSA

- KLASSA ska höja mognadsgraden i det systematiska informations- och cybersäkerhetsarbetet
- KLASSA ska vara lätt att använda och vända sig till breda målgrupper för att kontinuerligt förbättra organisationens informations- och cybersäkerhet
- KLASSA ska utvecklas kontinuerligt för att följa en föränderlig omvärld med nya lagkrav, nya risker och nya sätt att behandla information

Effekterna av ett gemensamt metodstöd

- Drygt 10 år med KLASSA visar på:
 - Ökad mognad inom informations- och cybersäkerhet
 - Likartad normerande kravställning avseende säkerhetskrav
 - Minskat gap i organisationen mellan olika professioner

Det är skillnad på då och nu

- Idén till KLASSA föddes 2010 i kölvattnet av de [16 principerna för samverkan](#)
 - En princip var att klassificera och värdera information på ett likartad sätt
 - Det var då oklart hur resultatet skulle omsättas i faktiska säkerhetskrav
- En kravmatris som tillämpades på systemnivån togs fram 2012 vilket var fröet till KLASSA som lanserades av SKR 2014
 - Utgångspunkten var en gemensam konsekvensskala från SiS/MSB
- Målgruppen för KLASSA var ursprungligen systemförvaltaren eller motsvarande
- Ingen större reglering med avseende på informations- och cybersäkerhet

KLASSA 4.0 - Idag



Bedömningen av konfidentialitet, riktighet och tillgänglighet leder fram till förslag på säkerhetsåtgärder som kravställs eller följs upp.

KLASSA 4.0 - Ett praktiskt exempel

VÄGLEDNING

GDPR känslig personuppgift
K=Allvarlig, R=Allvarlig

GDPR personuppgift
K=Betydande, R=Betydande

KLASSNING
K, R, T

ISO 27k:2022
Allvarlig
Betydande
Måttlig

Krav-katalog
GDPR
NIS1
PDL
OSL
Arkivlag

Exempel på
autentiseringskrav:

- Autentisering K/R=A(3)
tillitsnivå 3
- Autentisering K/R=B(2)
tillitsnivå 2

KLASSA 4.0 - Ett praktiskt exempel

VÄGLEDNING

GDPR känslig personuppgift
K=Allvarlig, R=Allvarlig

GDPR personuppgift
K=Betydande, R=Betydande

KLASSNING
K, R, T

ISO 27k:2022
Allvarlig
Betydande
Måttlig

Krav-katalog
GDPR
NIS1
PDL
OSL
Arkivlag

Exempel på
autentiseringskrav:

- Autentisering K/R=A(3)
tillitsnivå 3
- Autentisering K/R=B(2)
tillitsnivå 2

Säkerhetsåtgärder som
inte täcks av grundkraven
adderas till kravbilden

KLASSA 4.0 - Ett praktiskt exempel

VÄGLEDNING

GDPR känslig personuppgift
K=Allvarlig, R=Allvarlig

GDPR personuppgift
K=Betydande, R=Betydande

NIS1 samhällsviktig process
K=Allvarlig, R=Allvarlig

KLASSNING
K, R, T

ISO 27k:2022
Allvarlig
Betydande
Måttlig

Krav-katalog
GDPR
NIS1
PDL
OSL
Arkivlag

Exempel på
autentiseringskrav:

- Autentisering K/R=A(3)
tillitsnivå 3
- Autentisering K/R=B(2)
tillitsnivå 2

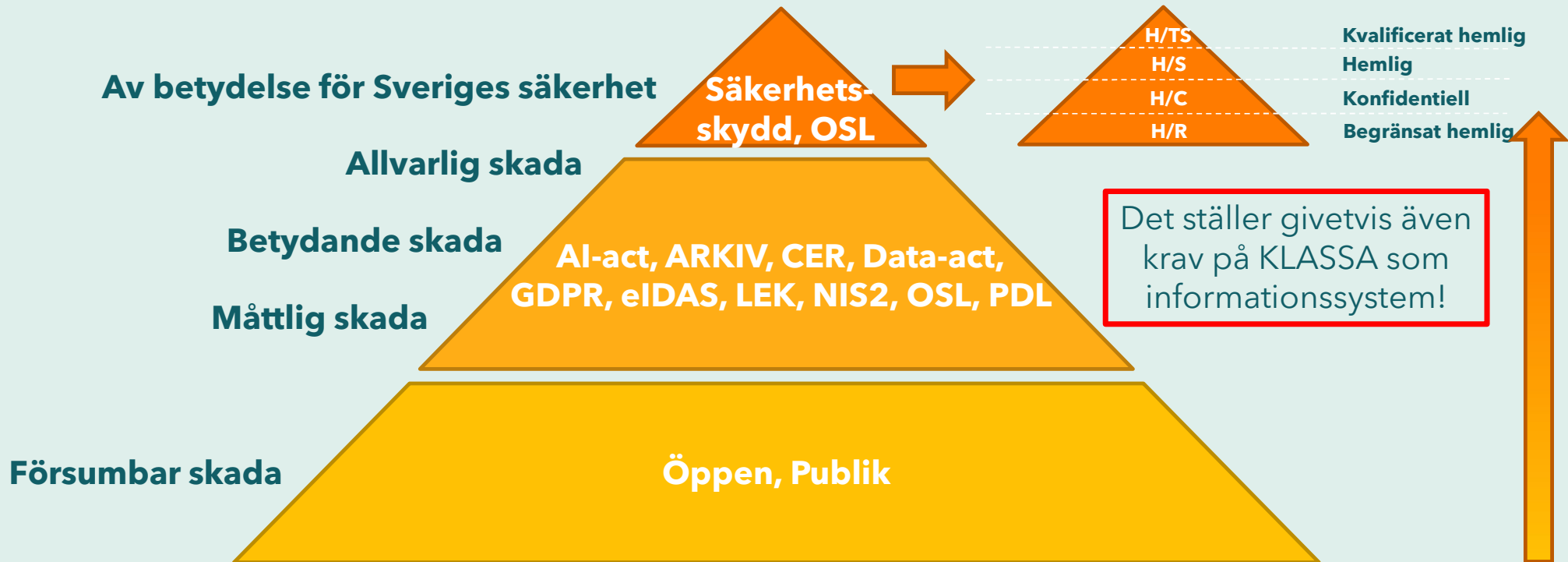
Säkerhetsåtgärder som
inte täcks av grundkraven
adderas till kravbilden

KLASSA 5.0 anpassas till ökad reglering

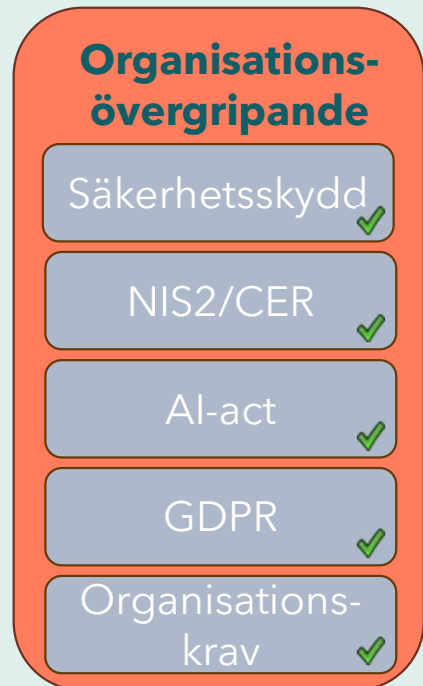
- För att undvika att varje reglering hanteras som en silo arbetas det med ett uppdaterat metodstöd.
 - En stor mängd reglering på området
 - Det kräver en mer ledstångsliknande approach
 - Gränsöverskridande riskhantering
 - Olika fokusområden som kan samordnas
- Målbilden är att rätt tekniska och organisatoriska säkerhetsåtgärder påförs och att det är hållbart över tid oavsett reglering



Behov av metodstöd även för säkerhetsskydd?



Samordnat regulatoriskt metodstöd i KLASSA 5.0



Stöd i det övergripande
arbetet i organisationen



Stöd i analysen av
verksamhetsprocessen

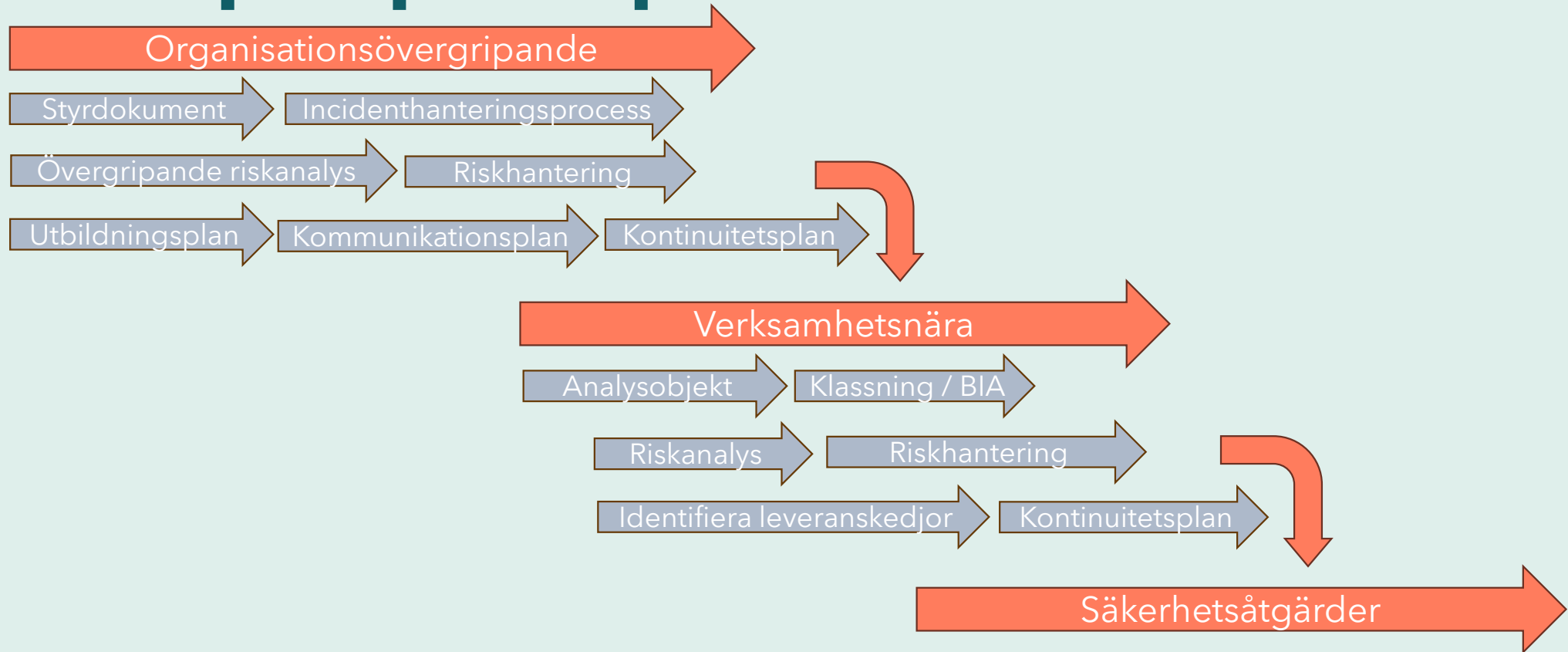


Handlingsplan och
kravunderlag

Grundkatalog med
riskhanteringsåtgärder
enligt NIS2 art 21

Stöd att addera
sektors-specifika
krav ex IoT
Stöd att addera egna
mer detaljerade krav

Exemplet på ett processflöde



Fler lagrum?

- I det strategiska projektet har AI-akten, GDPR, NIS2 och Säkerhetsskydd använts som exempel hur ett modernare metodstöd kan stötta på en organisationsövergripande och en verksamhetsnära nivå.
- Behoven är fler. Exempelvis:
 - EU:s dataakt som trädde i kraft den 11 januari 2024 och som kommer att börja tillämpas fullt ut den 12 september 2025. Regleringen ställer bland annat krav på datadelning, särskilt för tjänster och produkter inom Internet of Things (IoT).
- Vilka lagrum vill ni se? Vilka vill ni inte se?

Säkerhetsåtgärder enl. strukturen NIS2 art 21

- Riskhantering
- Systemsäkerhet
- Incidenthantering
- Driftskontinuitet
- Säkerhet i leveranskedjor
- Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem
- Förmåga att bedöma effektiviteten i vidtagna åtgärder
- Cyberhygien och utbildning i cybersäkerhet
- Användning av kryptografi och krypto
- Personalsäkerhet, åtkomstkontroll och tillgångsförvaltning
- Användning av lösningar för multifaktorautentisering

Säkerhetsåtgärder enl. strukturen NIS2 art 21

- Riskhantering
- Systemsäkerhet
- Incidenthantering
 - **Ansvar, rutiner, kontaktvägar och kommunikationsplaner vid informationssäkerhetsincidenter finns dokumenterat och är kommunicerat.**
(Ref ISO 27k 5.24, ref NIST osv...)
- Driftskontinuitet
- Säkerhet i leveranskedjan
- Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem
- Förmåga att bedöma effektiviteten i vidtagna åtgärder
- Cyberhygien och utbildning i cybersäkerhet
- Användning av kryptografi och krypto
- Personalsäkerhet, åtkomstkontroll och tillgångsförvaltning
- Användning av lösningar för multifaktorautentisering

Vinnova - "Gemensamma kravkataloger"

- Ett Vinnovafinansierat projekt i fyra faser (hösten 2023 - våren 2025)
 - Fas 1 - Beskriva nuläget och ge förslag på väg fram med en tydlig målbild
 - Lagrum, klassning, konsekvensnivåer, kravkataloger, samverkan, avgränsningar mm
 - Fas 2 - Realisera de föreslagna vägen fram för att nå målbilden
 - Metodik, djup/bredd på kravkataloger, samverkan, avgränsningar mm
 - Fas 3 - Vidareutveckla KLASSA 5.0 för att möta den nya målbilden
 - Fas 4 - Med Fas 2 och Fas 3 i ryggen genomföra piloter



Leveranser i *Gemensamma kravkataloger för informations- och cybersäkerhet så långt 1(2)*

- Kartläggning av kravkataloglandskapet
- Metodik för ett modernare metodstöd i syfte att leda verksamhetsutövarna till rätt tekniska och organisatoriska säkerhetsåtgärder och för att bättre stötta i lagstiftarens viljeriktning.
- Exempel kopplade till den framtagna metodiken med AI-akten, GDPR, NIS2 och Säkerhetsskydd som grund
- Synergierna mellan lagstiftning som exemplifieras med AI-akten och GDPR.
- Genomgång av svensk GDPR-praxis
- Fördjupade juridiska analyser av de processuella delarna för GDPR och NIS2.
- Förslag på ett flexibelt it-baserat process- och beslutsstöd för dynamisk implementation av de regulatoriska processerna som implementeras i KLASSA 5.0

Leveranser i *Gemensamma kravkataloger för informations- och cybersäkerhet så långt 2(2)*

- Förslag till grund för en ny gemensam kravkatalog med NIS2 art 21.2 som grund.
- Förslag till federativt stöd.
- Förslag på hur SSNF kommande riktlinjer baserad på CSL kan implementeras i metodstödet.
- Uppdatering av befintliga kravkataloger i KLASSA som sedermera ska migreras till resultatet av det strategiska projektet.
- Konkret stöd till VGR:s IoT-plattformsupphandling.
- Framtagande och implementation av helt ny riskmodul till KLASSA, inklusive SSNF "hotkatalog", som är central i det nya metodstödet
- Dialog med SKR:s medlemmar, bland annat genom KLASSA användarforum och genom SKR:s kompetens-gemenskaper för informations- och cybersäkerhet.

Lunchpaus till 13:00

Gruppdiskussion

Mentikod: 67 00 92 0

Menti-fråga

- Är det rätt väg att gå, d.v.s. att ändra strukturen på kravkatalogen från ett ISO-perspektiv till ett regelverksperspektiv?
 - Fritext

Menti-fråga

- Vilken annan funktionalitet ser ni att KLASSA bör erbjuda?
 - Fritext

Menti-fråga

- Vilka funktionaliteter är mest prioriterade i KLASSA?
 - Incidenthanteringsmodul (likt riskmodul)
 - Mognadsmätning ("infosäkkollen")
 - Processorienterad informationskartläggning (POIK)
 - Rapportmodul
 - Stöd för kontinuitetsplanering
 - Stöd för säkerhetskyddsanalys

Menti-fråga

- Vilken funktionalitet, i KLASSA 4.0, vill ni ändra på?
 - Exempel:
 - Vill kunna ändra namn på en informationstillgång
 - Vill kunna ta bort en skapad informationstillgång

Menti-fråga

- Tänker vi rätt kring "nya" riskhanteringsmodulen?
 - Fritext

Menti-fråga

- Vilka rapporter vill ni kunna generera från KLASSA?

Menti-fråga

- Vilka integrationsmöjligheter önskar ni i KLASSA?

Menti-fråga

- Vilka roller vill ni se i KLASSA 5.0?
 - Fritext

Menti-fråga

- Vilka andra lagrum ser ni behov av att få systematisk vägledning kring?
 - Dataakten

Menti-fråga

- Ska AI-akten och säkerhetsskydd fördjupas och implementeras i KLASSA 5.0?
 - Fritext

Menti-fråga

- Vilka övriga standarder eller motsvarande vill ni att kraven i KLASSA har referens till?
 - Fritext

Menti-fråga

- Hur vill ni att användarträffarna arrangeras?
 - Fysiskt
 - Digitalt

Menti-fråga

- Vilken är den upplevda nyttan med metodstödet i er organisation idag och skulle den bli större med de förändringar vi föreslår?

Summering

Jonas Nilsson och Thomas Nilsson

Användarforum #7

Informationssäkerhet behöver inte vara svårt

KLASSA är verktyget som hjälper organisationer att systematiskt arbeta med informationssäkerhet.

[Kom igång](#)

[Så fungerar Klassa](#)



Till verktyget

För dig som redan är registrerad



Lär dig klassa

Utforska vårt stödmaterial



Nyheter

Detta händer runt Klassa

Tack!

klassa@skr.se