Sveriges Kommuner och Regioner

# NIS2/Cybersäkerhetslagen

2025-10-13

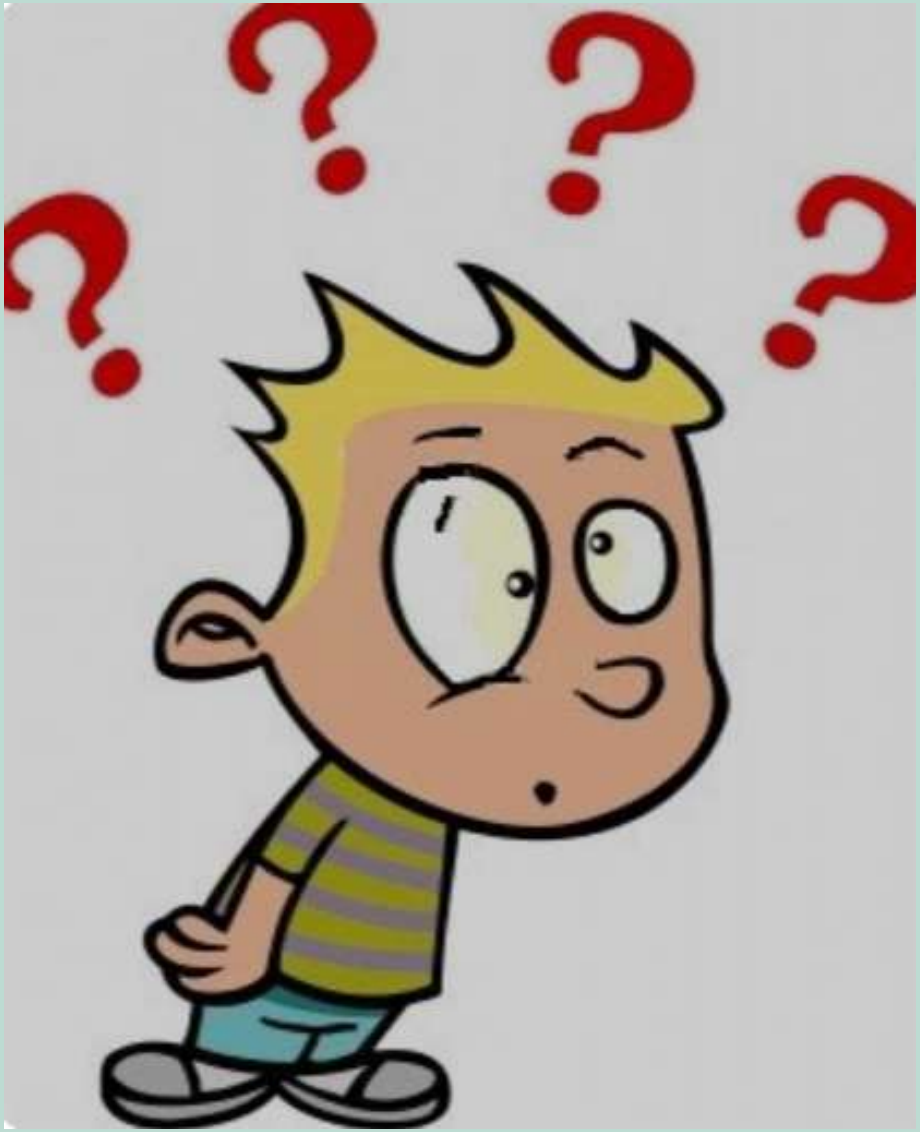
Sveriges Kommuner och Regioner

# Agenda

- Varför?
- Vem omfattas?
- Vad innebär det?
- Vad gör vi?

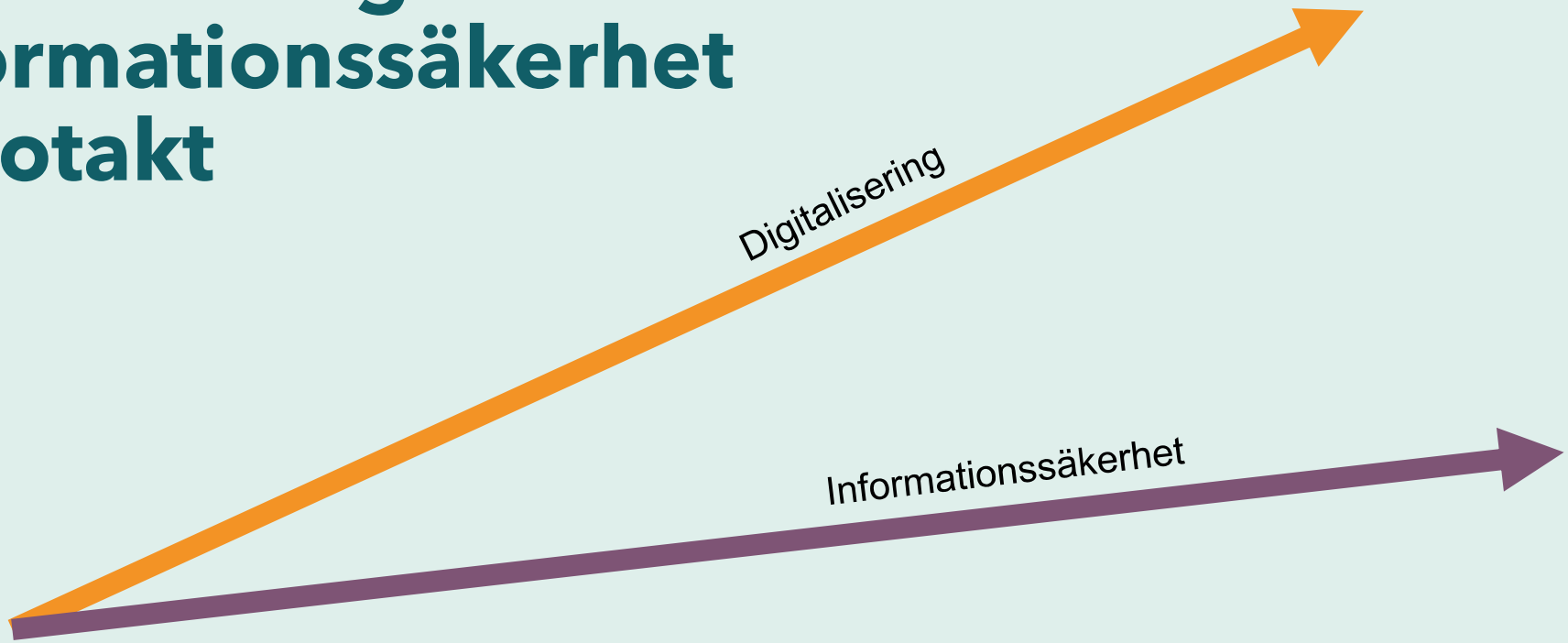
Sveriges Kommuner och Regioner

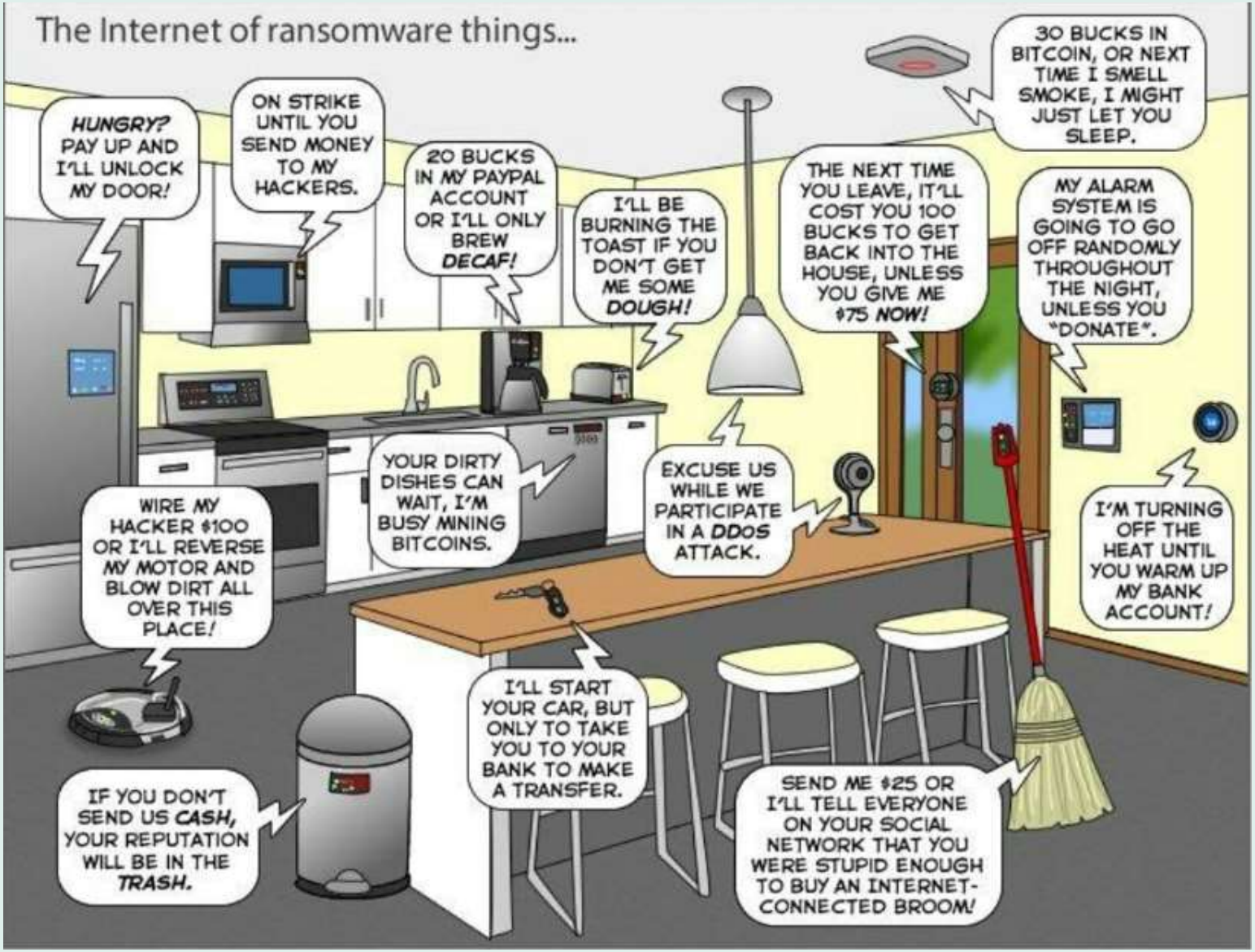
# Varför?



Sveriges Kommuner och Regioner

# Digitalisering och informationssäkerhet är i otakt




The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

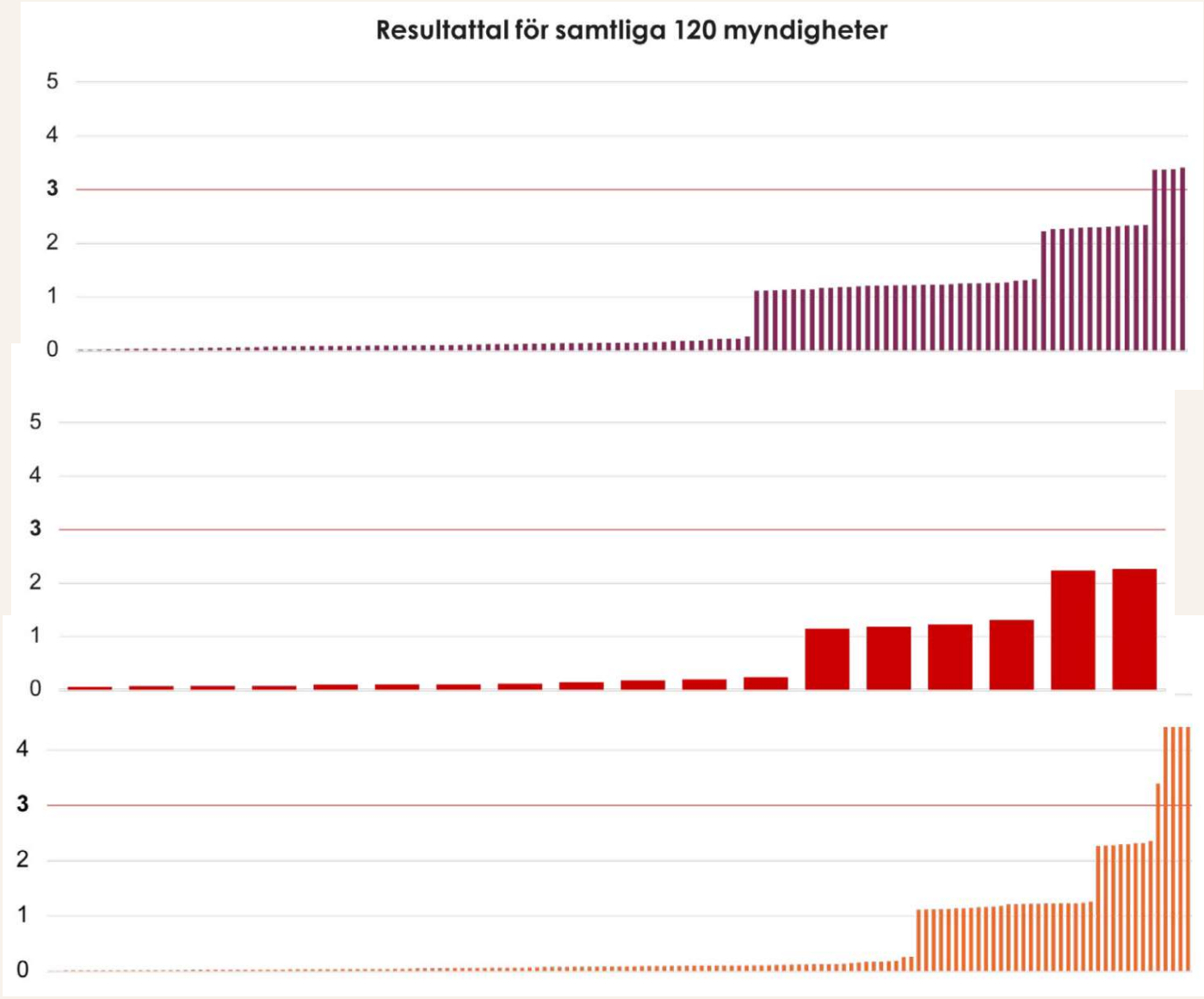
Sveriges Kommuner och Regioner

# Vad händer i vår omvärld?

Sveriges Kommuner och Regioner

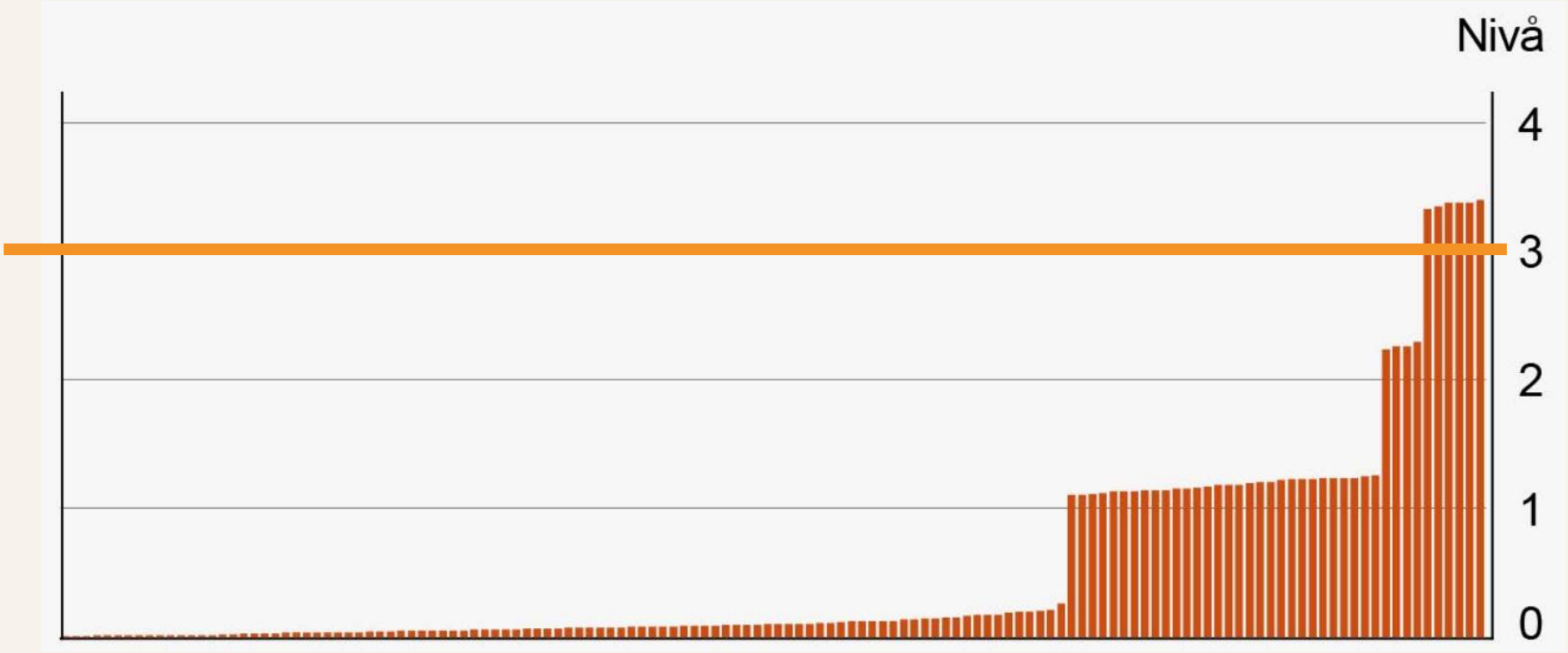
# Utgångsläget

- Kommunerna
- Regionerna
- Statliga myndigheter



Sveriges Kommuner och Regioner

# Utgångsläget




* Svar från 136 kommuner

Sveriges Kommuner och Regioner

# Vi måste bli bättre!

Sveriges Kommuner och Regioner

# NIS blir NIS2!

1. EU direktiv till syfte att höja och harmonisera cybersäkerhetsnivån för samhällsviktig verksamhet i Europa
2. Föreslås bli svensk lag 15/1 2026
    - Cybersäkerhetslagen
    - Cybersäkerhetsförordningen
3. Föreskrifter från myndigheter
    - MSB
    - PTS

Sveriges Kommuner och Regioner

# Cybersäkerhetslagen

- 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

Myndigheten för samhällsskydd och beredskap

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**

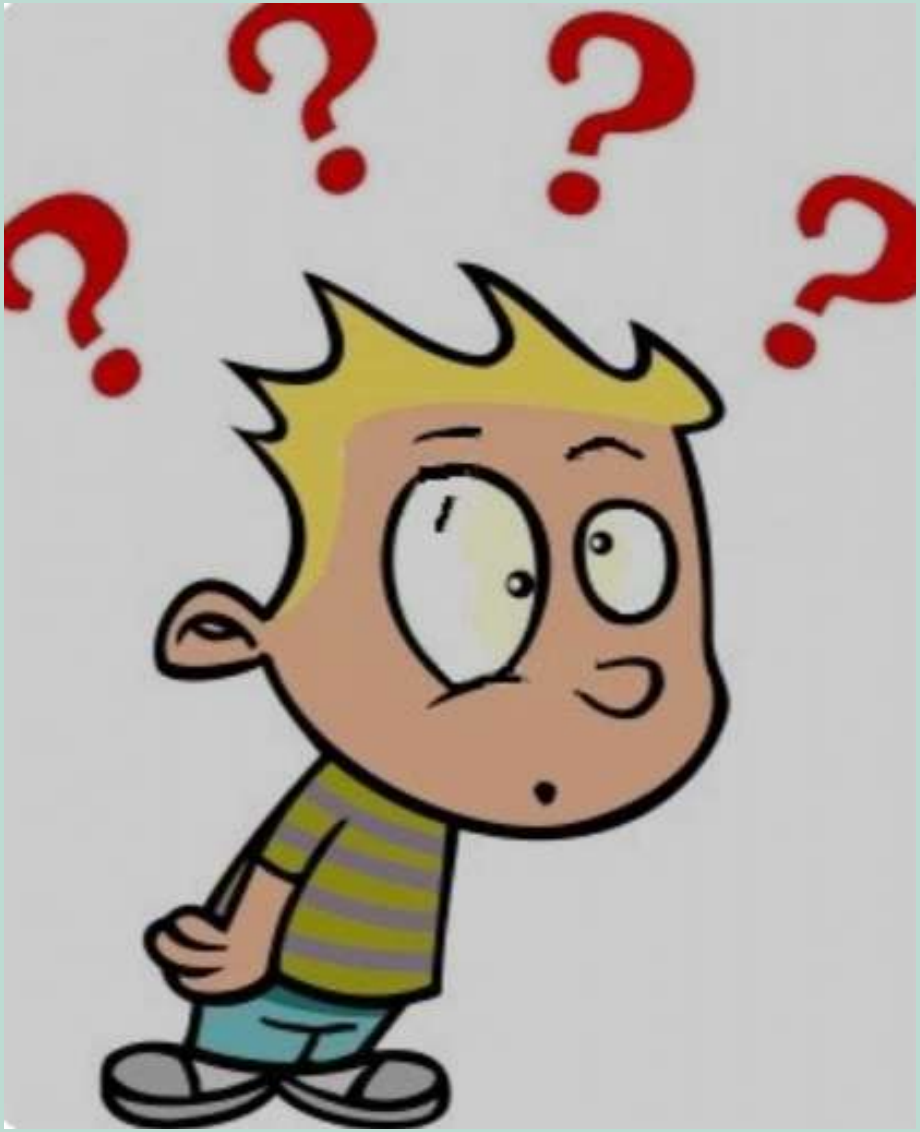
**Tillämpningsområde**

**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 §** I 3-9 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.

Sveriges Kommuner och Regioner

# Vem omfattas?



Sveriges Kommuner och Regioner

# Väsentliga verksamhetsutövare

Röd text = Nya sektorer

- Avloppsvatten
- Bankverksamhet
- Digital infrastruktur
- Dricksvatten
- Energi
  - elektricitet
  - fjärrvärme eller fjärrkyla
  - olja
  - gas
  - vätgas
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn
- Offentlig förvaltning
- Rymden
- Transport
  - lufttransport
  - järnvägstransport
  - sjöfart
  - vägtransport

Sveriges Kommuner och Regioner

# Viktiga verksamhetsutövare

Röd text = Nya sektorer

- Avfallshantering
- Digitala leverantörer
- Post- och budtjänster
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning, produktion och distribution av kemikalier
- Tillverkning av
  - medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik
  - datorer, elektronikvaror och optik
  - elapparatur
  - övriga maskiner
  - motorfordon, släpfordon och påhängsvagnar
  - andra transportmedel

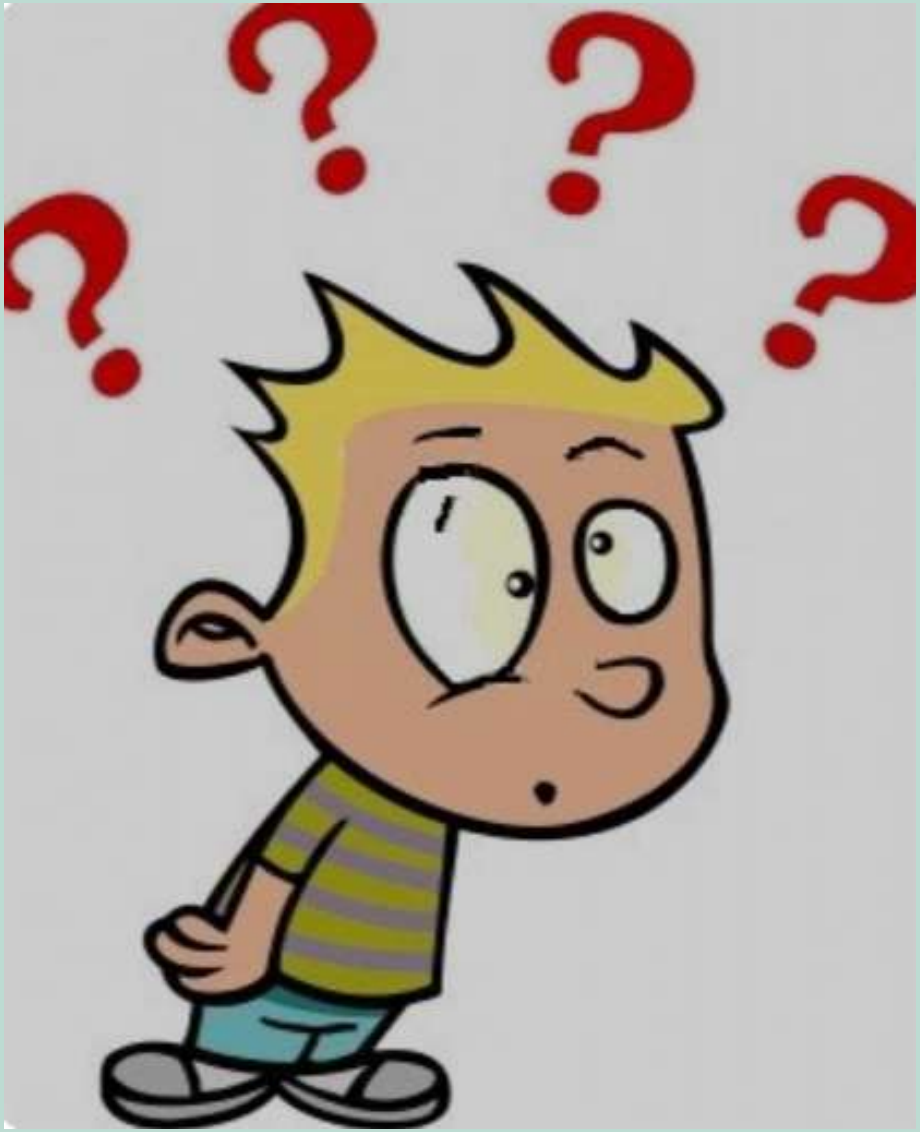
Sveriges Kommuner och Regioner

# Cybersäkerhetslagens inverkan på kommuner och regioner

- Avloppsvatten
- Dricksvatten
- Energi
- Avfallshantering
- Produktion, bearbetning och distribution av livsmedel
- Hälso- och sjukvård
- Transport
- Offentlig förvaltning

Sveriges Kommuner och Regioner

# Vad innebär det?



Sveriges Kommuner och Regioner

# MSB har föreskrift ute på remiss

## Anmälningsskyldighet

- Verksamhetsutövare ska göra anmälan till tillsynsmyndigheten
  - Identitet
  - Kontaktuppgift
  - IP-adressintervall
  - Verksamhet
  - Uppgift om i vilka länder verksamheten bedrivs
- Ändras uppgifterna ska verksamhetsutövaren anmäla förändringen inom 14 dagar.

Sveriges Kommuner och Regioner

# Utbildning

- Ledningen ska genomgå utbildning om riskhanteringsåtgärder och anställda ska erbjudas sådan utbildning.
  - Det är RS och KS som ska genomgå utbildning.

Sveriges Kommuner och Regioner

# Incidentanmälan

Verksamhetsutövaren ska:

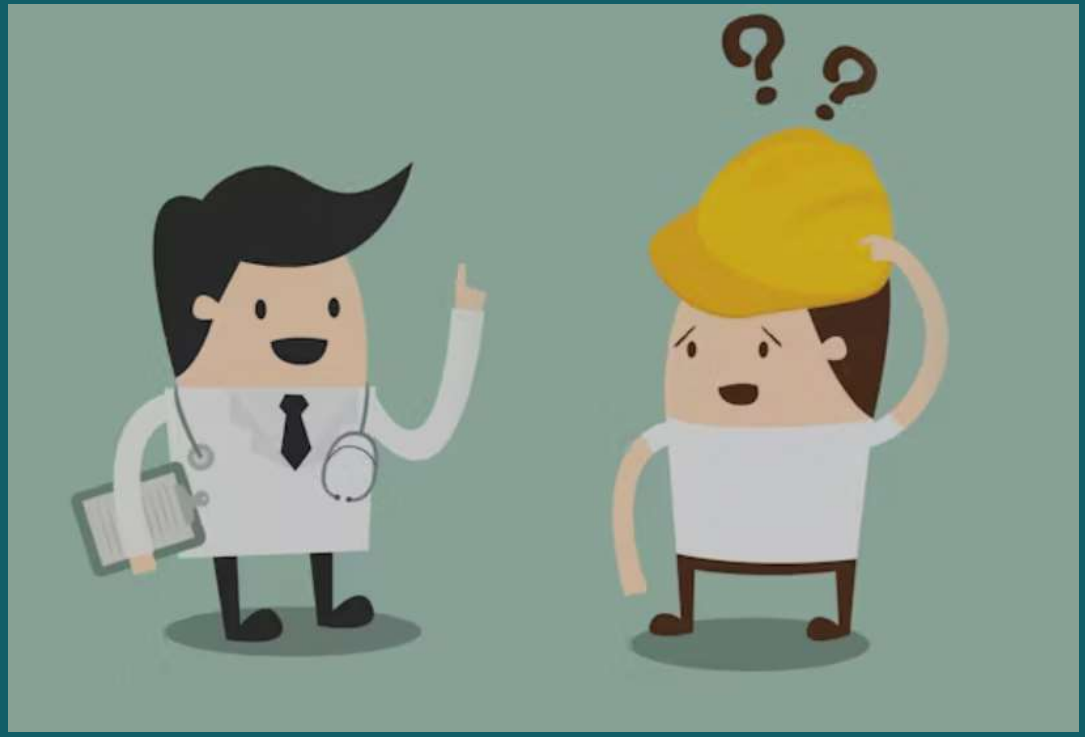
- inom 24 timmar från tidpunkten från kännedom ska som en varning underrätta till CSIRT-enheten om betydande incidenter.
- inom 72 timmar från tidpunkten från kännedom göra en incidentanmälan till CSIRT-enheten om betydande incidenter.
- inom en månad från incidentanmälan lämna en slutrapport till CSIRT-enheten.

Sveriges Kommuner och Regioner

# Tillsyn

Tillsyn sker genom:

1. Information
2. Tillträde till lokaler
3. Säkerhetsrevision
4. Säkerhetsskanning



Sveriges Kommuner och Regioner

# Ingripande

- Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter.
- Ingripanden sker genom…

Sveriges Kommuner och Regioner

# Sanktionsavgift

För kommunala bolag är sanktionsavgiften lägst 5 000 kr och högst det högsta av:

Väsentliga verksamhetsutövare:

1. 2 procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

Viktiga verksamhetsutövare

1. 1,4 procent av den viktiga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 7 000 000 euro.

För kommuner och regioner är sanktionsavgiften lägst 5 000 kr och högst 10 000 000 kr.

Sveriges Kommuner och Regioner

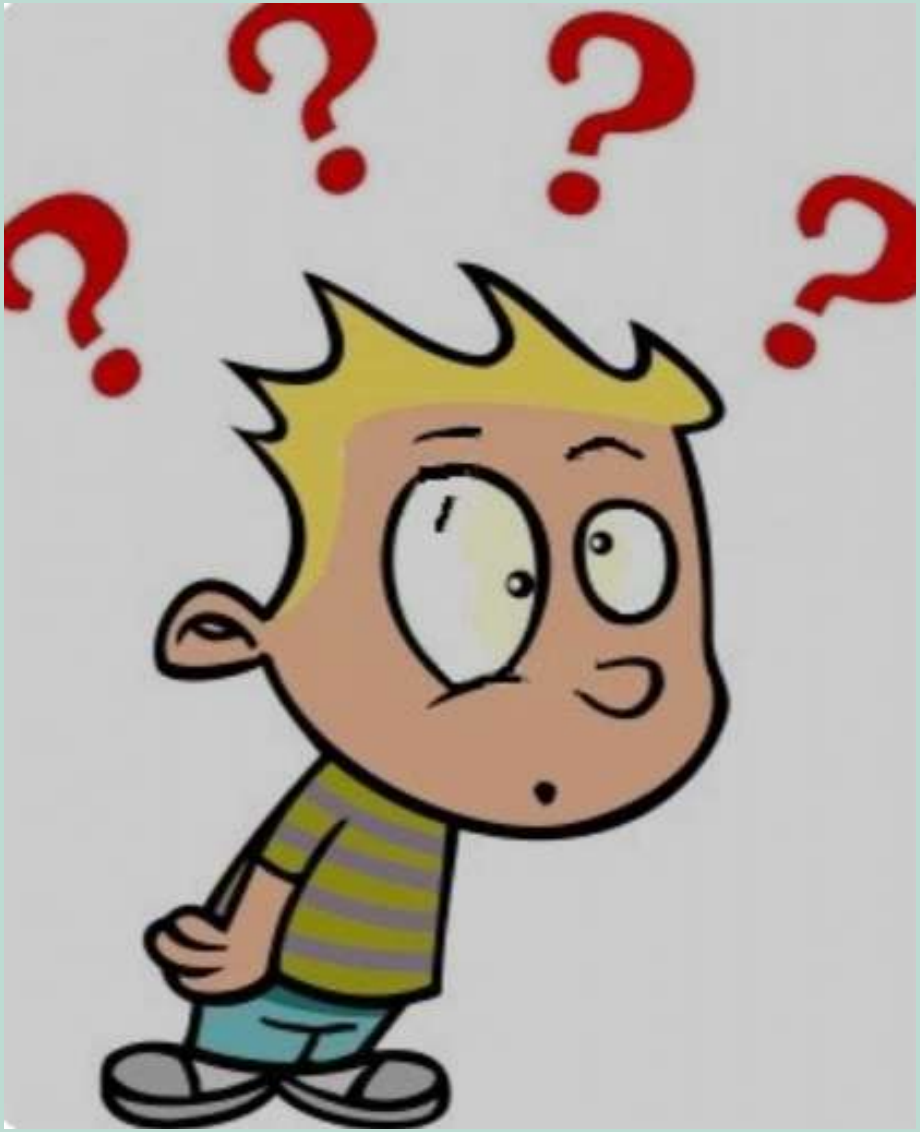
# Förbud att utöva ledningsfunktion

- Föreläggande inte följts
- Ansökan domstol
- Allvarlig, uppsåt eller grov oaktsamhet
- Tidsbegränsat 1-3 år
- Ska upphävas omedelbart om inte längre förutsättningar

- Gäller **inte** offentliga verksamhetsutövare

Sveriges Kommuner och Regioner

# Vad gör vi?



Sveriges Kommuner och Regioner

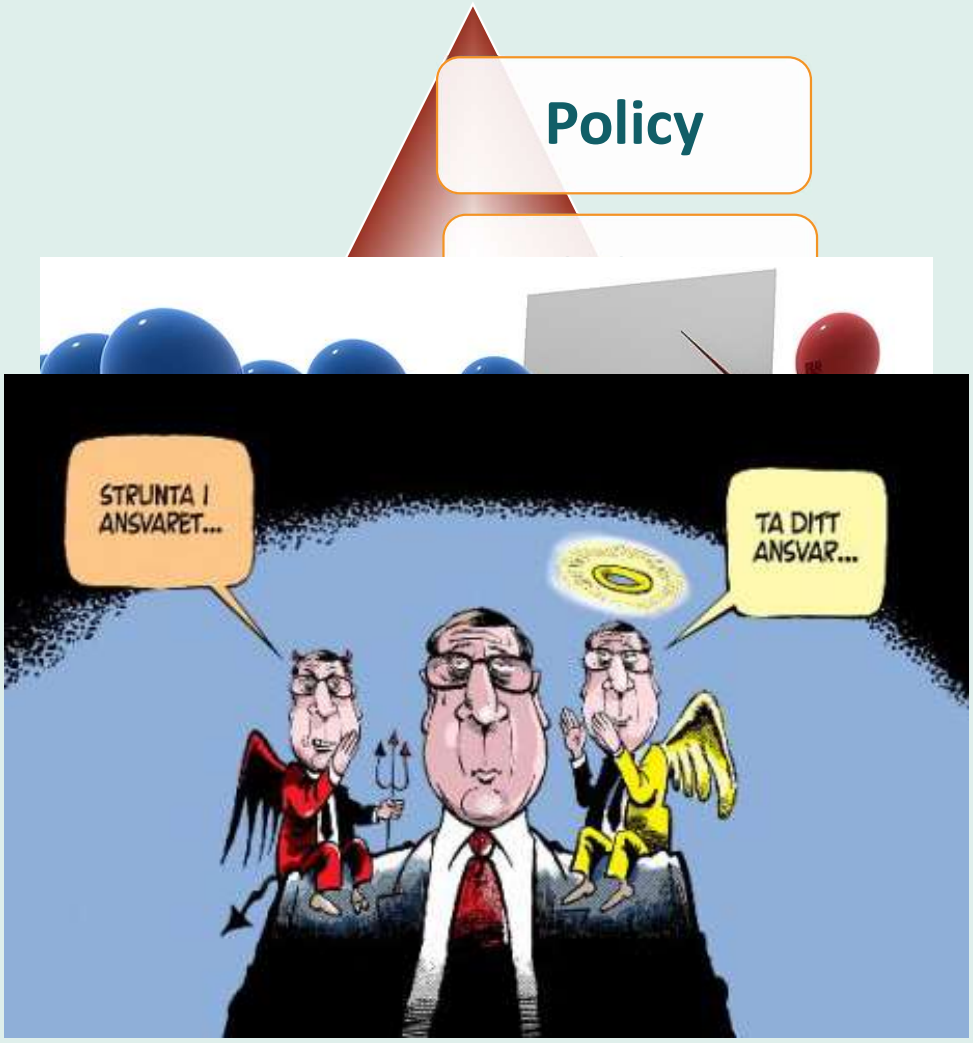
# Systematiskt och riskbaserat informationssäkerhetsarbete

- SDK ställer krav på ett…
- Digital post ställer krav på ett…

Sveriges Kommuner och Regioner

# Systematiskt informationssäkerhets-arbete

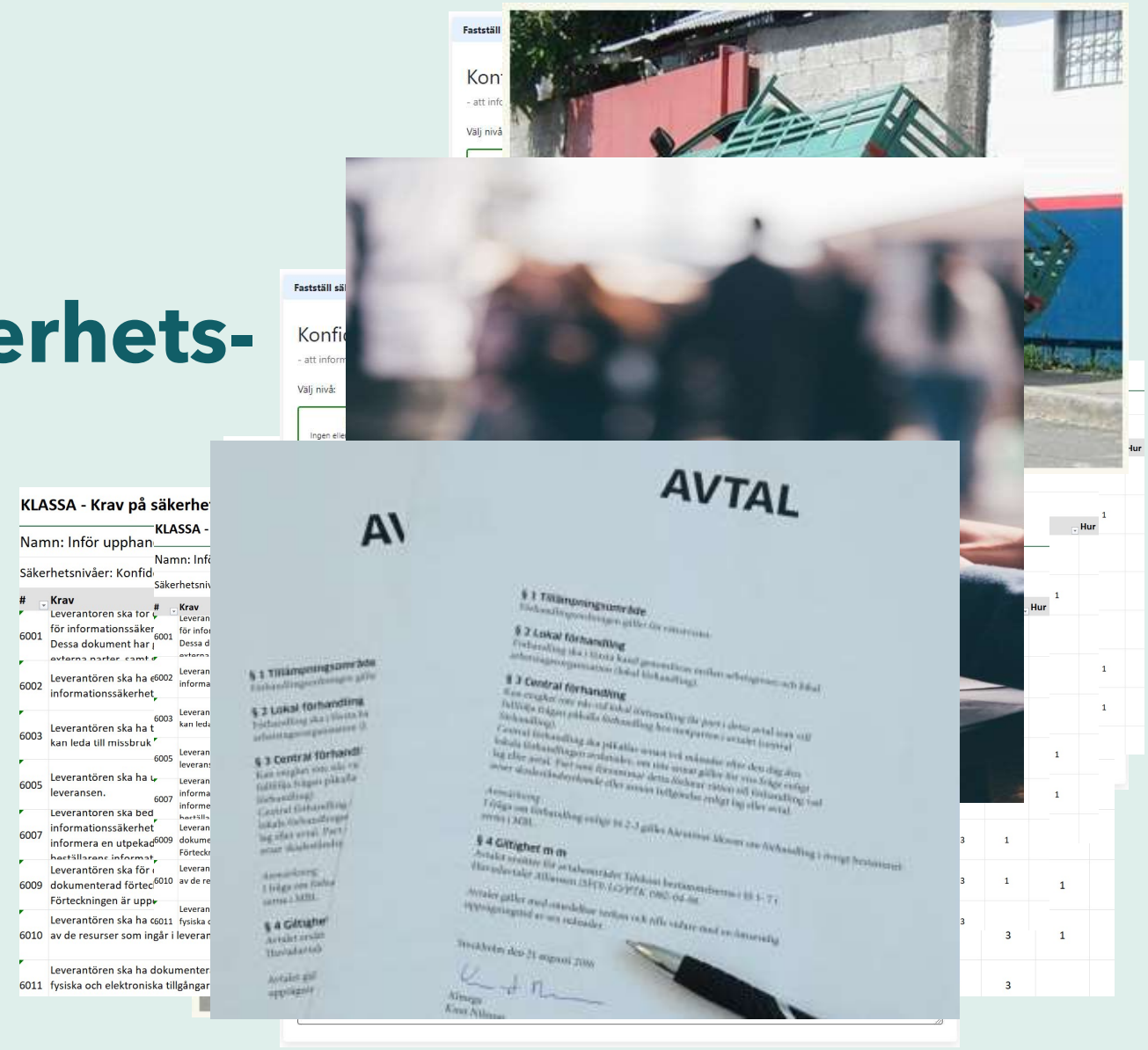
- Skapa de rätta förutsättningarna
  - Styrdokument
  - Utbildning och information
  - Ansvar



Sveriges Kommuner och Regioner

# Systematiskt informationssäkerhets-arbete

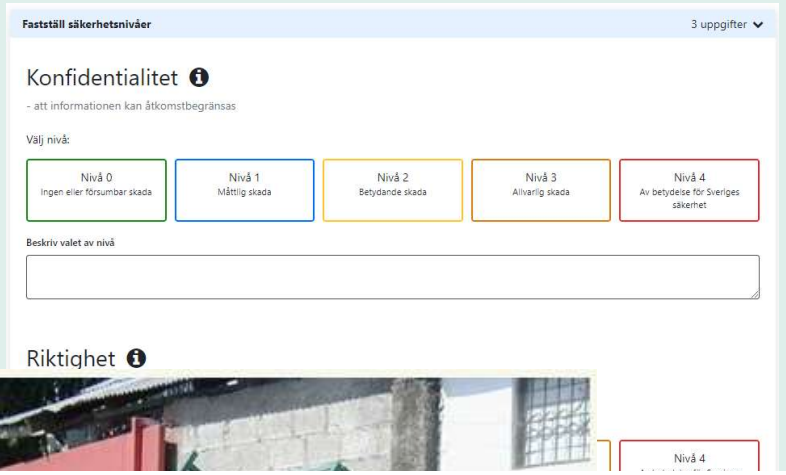
- Tillämpa
  - Analysera
  - Undersök
  - Beslut



Sveriges Kommuner och Regioner

# Systematiskt informationssäkerhets-arbete

- Följa upp
  - Handlingsplan

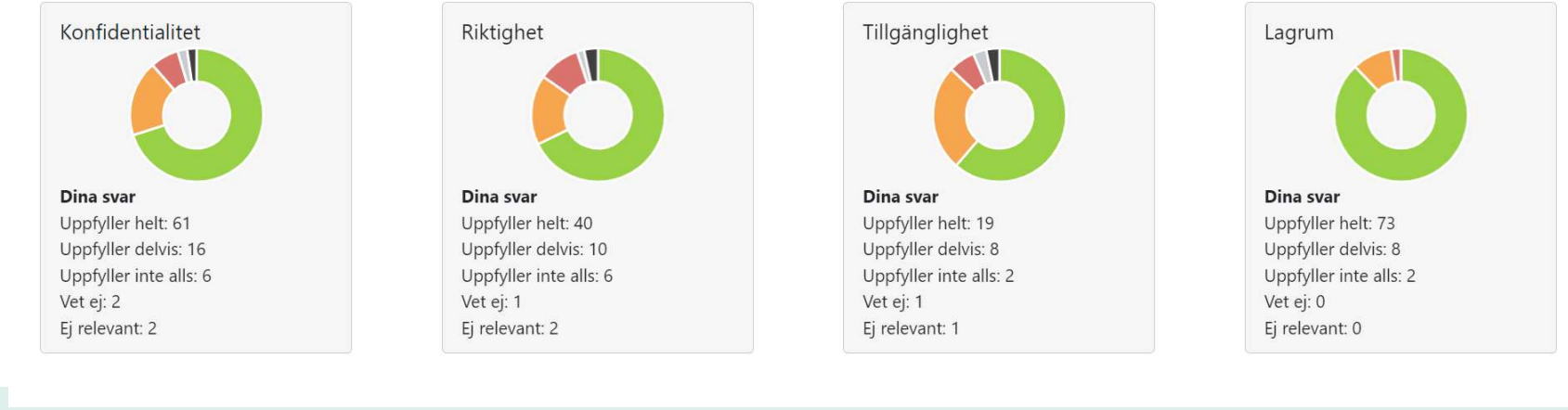



**KLASSA - Krav på säkerhetsåtgärder till leverantör**

Namn: Inför upphandling | Informationstillgång: System A | Senast ändrad: 2024-11-06 10:26

Säkerhetsnivåer: Konfidentialitet - Nivå 2, Riktighet - Nivå 3, Tillgänglighet - Nivå 1

| # | Krav | ISO kapitel | ISO kravområde | Kon. | Rik. | Til. | Hur |
|---|---|---|---|---|---|---|---|
| 6001 | Leverantören ska för de delar av verksamheten som berörs i leveransen ha ett ledningssystem för informationssäkerhet (LIS) som baseras på SS-EN ISO/IEC 27001:2022 eller motsvarande. Dessa dokument har godkänts och har kommunicerats till berörd personal och relevanta externa parter, samt ses över varje år och om betydande ändringar sker. | 5.1 | Policyer för informationssäkerhet | | 3 | | |
| 6002 | Leverantören ska ha en dokumenterad organisation där roller och ansvar avseende | 5.2 | Roller och ansvar för informationssäkerhet | 2 | 3 | 1 | |



Sveriges Kommuner och Regioner

# Riskbaserat arbetssätt

- Förmåga att bedöma effektiviteten i vidtagna åtgärder


Foto: https://projektledning.se/riskhantering/

Sveriges Kommuner och Regioner

# Vad är en risk?

- En ögonblicksbild!

Sveriges Kommuner och Regioner

# Hur hanteras en risk?

Sveriges Kommuner och Regioner

# Riskhantering

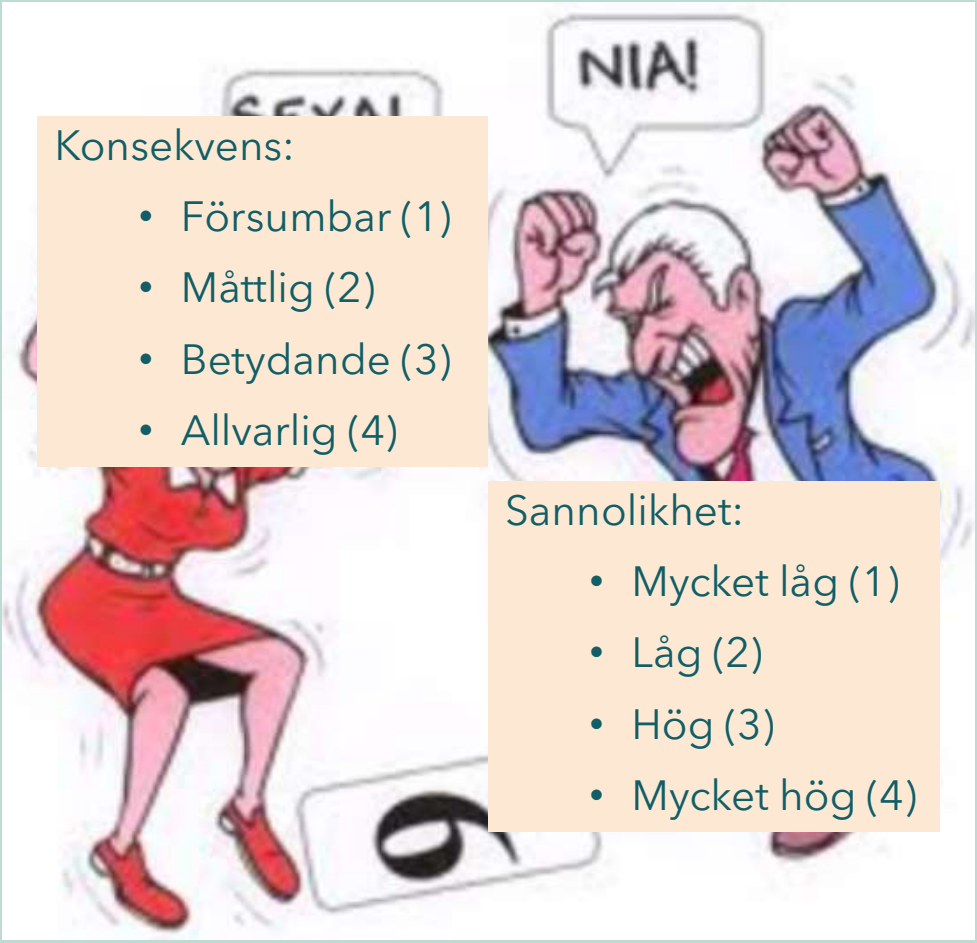
- **Identifiering**
- *Värdering*
- *Behandling*
- *Uppföljning*

Risk för **[hot]** mot **[tillgång]** som leder till **[konsekvens]**

Sveriges Kommuner och Regioner

# Riskhantering

- *Identifiering*
- **Värdering**
- *Behandling*
- *Uppföljning*




Konsekvens * Sannolikhet = **Riskvärde**

Sveriges Kommuner och Regioner

# Riskhantering

- *Identifiering*
- *Värdering*
- **Behandling**
- *Uppföljning*

…att vidta alla lämpliga och proportionella åtgärder för att hantera riskerna för sina tjänster…


| Konsekvens / Sannolikhet | Försumbar (1) | Måttlig (2) | (3) | (4) |
|---|---|---|---|---|
| Mycket hög (4) | Mellan | | Hög | Mycket |
| Hög (3) | Mellan | | Hög | |
| Låg (2) | Låg | Mede | Medel | |
| Mycket låg (1) | Låg | Låg | Medel | Mede |

Sveriges Kommuner och Regioner

# Riskhantering

- *Identifiering*
- *Värdering*
- *Behandling*
- **Uppföljning**

Sveriges Kommuner och Regioner

# Vem äger risken?

- Jag äger risken!

Sveriges Kommuner och Regioner

# Eskalering!

Sveriges Kommuner och Regioner

# Vad gör SKR?

Sveriges Kommuner och Regioner

# Tillsammans är vi starka!

Sveriges Kommuner och Regioner

# Metodstöd Informationssäkerhet

- Skapa de rätta förutsättningarna för ett systematiskt informationssäkerhetsarbete


https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/cyberochinformationssakerhet/informationssakerhet/metodstodinformationssakerhet.83648.html

Sveriges Kommuner och Regioner

# Metodstöd informationssäkerhet

- Lägga grunden!
- …de första stapplande stegen mot ett systematiskt informationssäkerhetsarbete

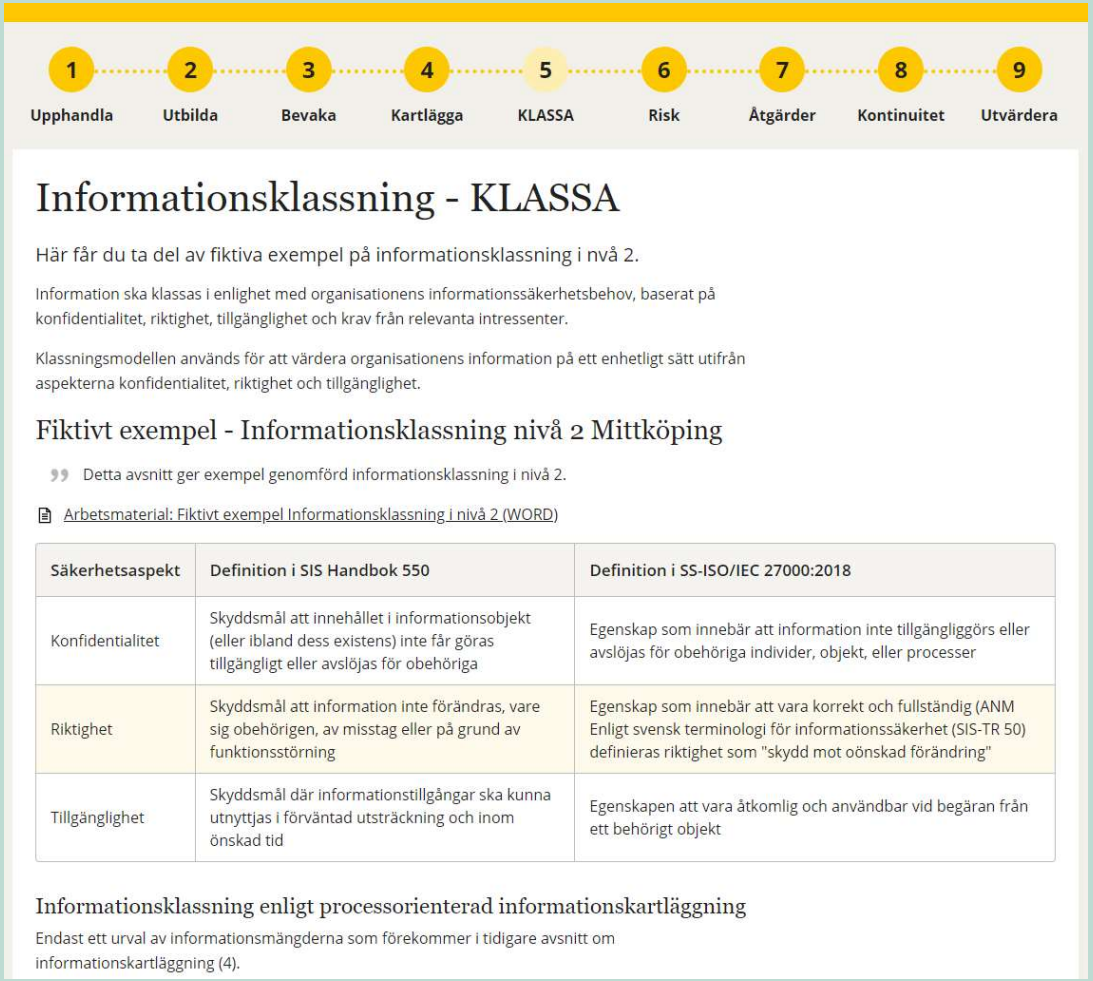

https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/cyberochinformationssakerhet/informationssakerhet/metodstodinformationssakerhet.83648.html

Sveriges Kommuner och Regioner

# Metodstöd informationssäkerhet

- Kliva ut i organisationen!

- …fler analyser
- …t.ex. upphandling



1 Upphandla · 2 Utbilda · 3 Bevaka · 4 Kartlägga · 5 KLASSA · 6 Risk · 7 Åtgärder · 8 Kontinuitet · 9 Utvärdera

## Informationsklassning - KLASSA

Här får du ta del av fiktiva exempel på informationsklassning i nvå 2.

Information ska klassas i enlighet med organisationens informationssäkerhetsbehov, baserat på konfidentialitet, riktighet, tillgänglighet och krav från relevanta intressenter.

Klassningsmodellen används för att värdera organisationens information på ett enhetligt sätt utifrån aspekterna konfidentialitet, riktighet och tillgänglighet.

### Fiktivt exempel - Informationsklassning nivå 2 Mittköping

Detta avsnitt ger exempel genomförd informationsklassning i nivå 2.

Arbetsmaterial: Fiktivt exempel Informationsklassning i nivå 2 (WORD)

| Säkerhetsaspekt | Definition i SIS Handbok 550 | Definition i SS-ISO/IEC 27000:2018 |
|---|---|---|
| Konfidentialitet | Skyddsmål att innehållet i informationsobjekt (eller ibland dess existens) inte får göras tillgängligt eller avslöjas för obehöriga | Egenskap som innebär att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt, eller processer |
| Riktighet | Skyddsmål att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning | Egenskap som innebär att vara korrekt och fullständig (ANM Enligt svensk terminologi för informationssäkerhet (SIS-TR 50) definieras riktighet som "skydd mot oönskad förändring" |
| Tillgänglighet | Skyddsmål där informationstillgångar ska kunna utnyttjas i förväntad utsträckning och inom önskad tid | Egenskapen att vara åtkomlig och användbar vid begäran från ett behörigt objekt |

### Informationsklassning enligt processorienterad informationskartläggning

Endast ett urval av informationsmängderna som förekommer i tidigare avsnitt om informationskartläggning (4).

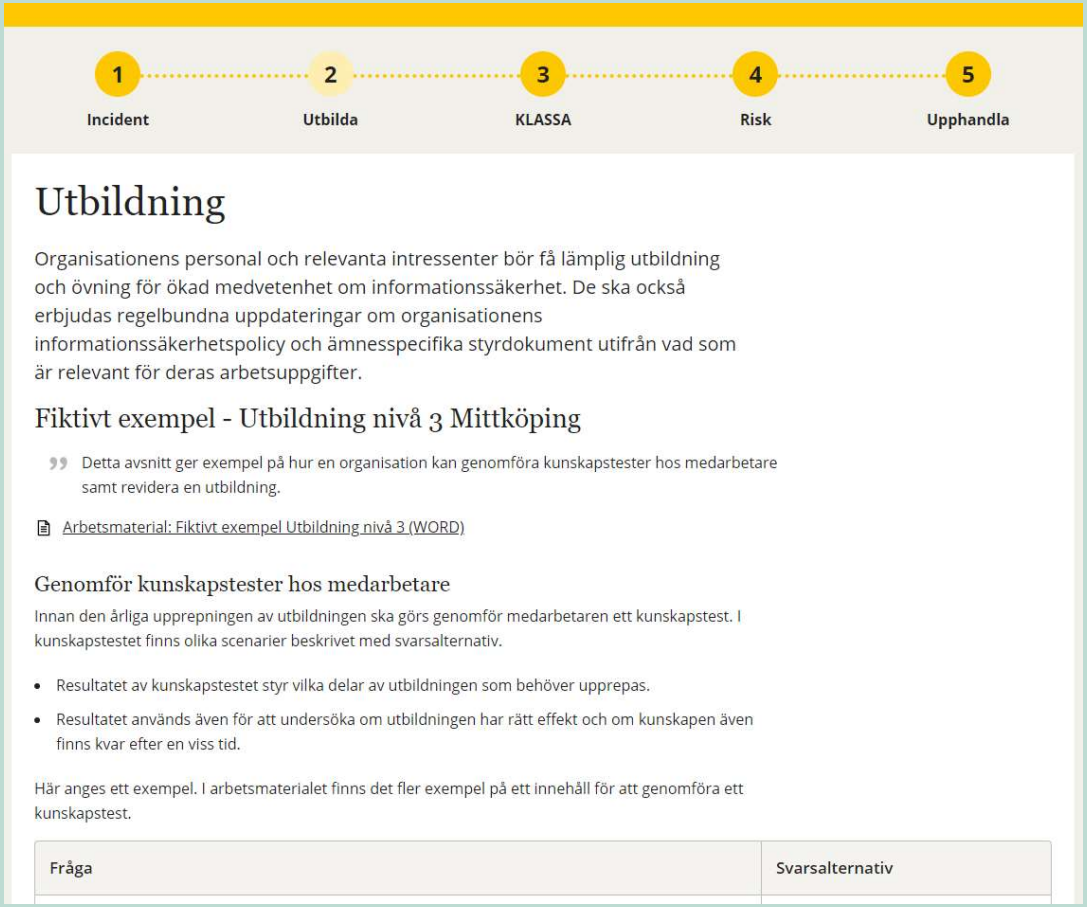
https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/cyberochinformationssakerhet/informationssakerhet/metodstodinformationssakerhet.83648.html

Sveriges Kommuner och Regioner

# Metodstöd informationssäkerhet

- Lära sig!

- …göra om
- …och göra ”rätt”




https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/cyberochinformationssakerhet/informationssakerhet/metodstodinformationssakerhet.83648.html

Sveriges Kommuner och Regioner

# Metodstöd informationssäkerhet

- …lite av ett självspelande piano…


https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/cyberochinformationssakerhet/informationssakerhet/metodstodinformationssakerhet.83648.html

Sveriges Kommuner och Regioner

# Metodstöd informationssäkerhet

**Nivå 1** kännetecknas av låg medvetenhet och avgörande brister i arbetssätt och systematik. Kan ha påbörjat arbetet, men det är inte etablerat.

**Nivå 2** kännetecknas av att viss medvetenhet och viss systematik börjar etableras.

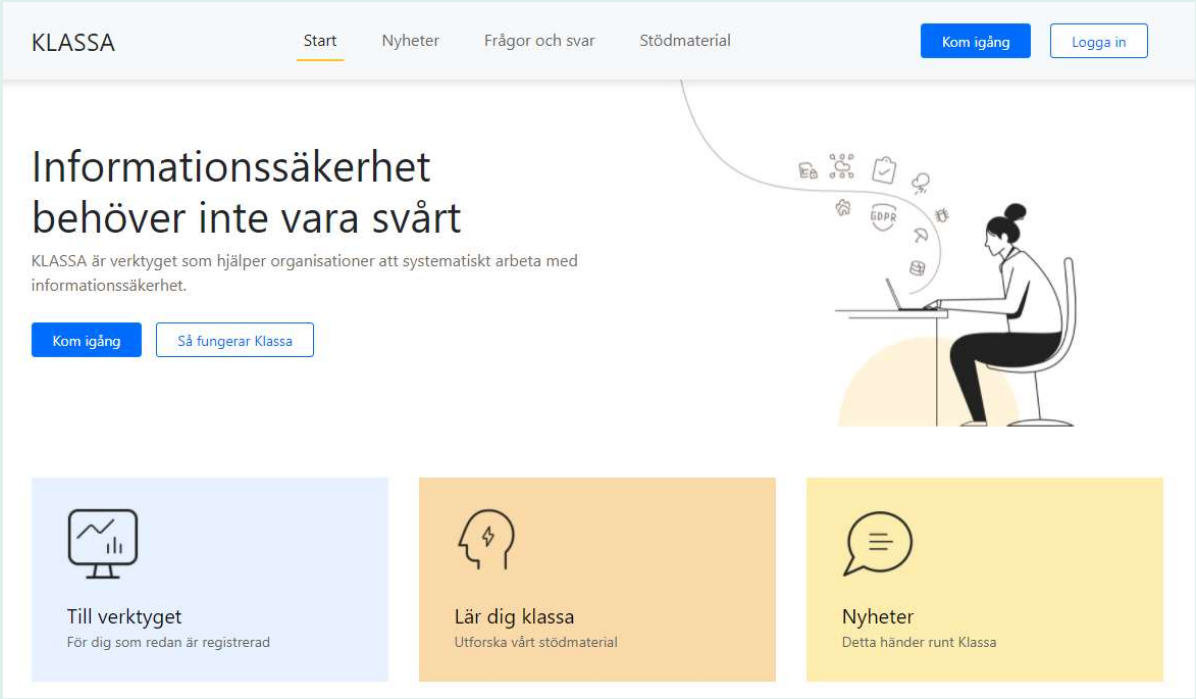
**Nivå 3** kännetecknas av hög medvetenhet, systematik och ständiga förbättringar.

**Nivå 4** kännetecknas av hög medvetenhet, proaktivitet och enastående resultat – den här nivån uppnås av mycket få organisationer.

Sveriges Kommuner och Regioner

# Vad ingår i KLASSA?

- Organisationsstruktur
- Registrera ett system/informationstillgång
- Klassning av ett system
- Riskhantering
- Upphandlingskrav
- Handlingsplan (och självvärdering)
- Kravmallar

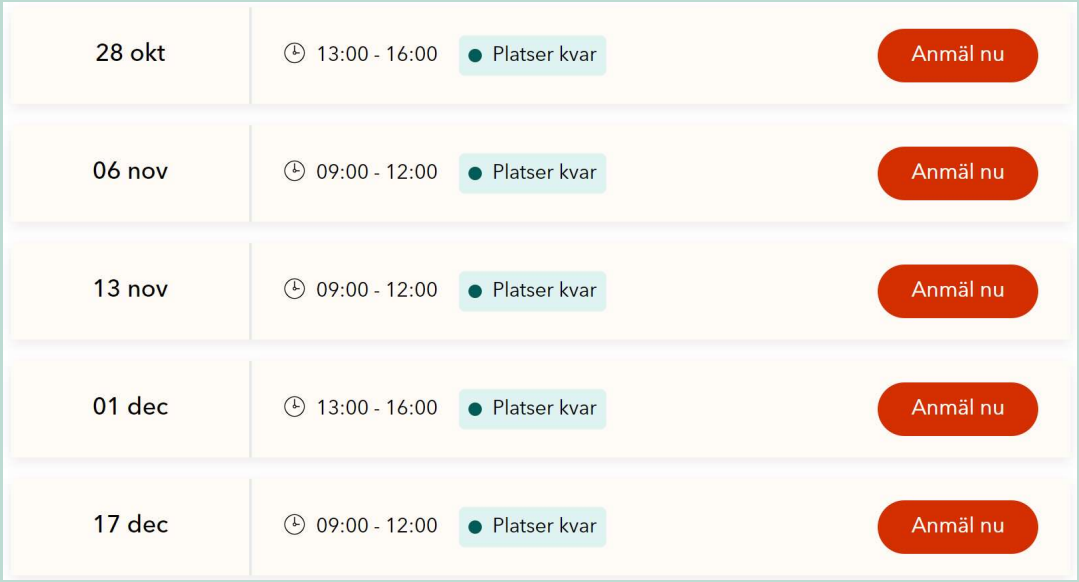



klassa@skr.se

Sveriges Kommuner och Regioner

# Utbildning

- Grundläggande utbildning
  - Effektiv och säker informationsklassning med KLASSA




https://www.adda.se/utbildningar/utbildningskatalog/effektiv-och-saker-informationsklassning-med-klassa/

Sveriges Kommuner och Regioner

# Utbildning

En timmes utbildning, anpassat för kommun- och regionstyrelsen.
Varje organisation kan anpassa materialet

- Om hotbilden
- Viktiga begrepp
- Relevanta lagar
- Arbetssätt
- Ansvar och uppföljning
- Vem gör vad inom staten

En timmes workshop där workshopledarna hjälper deltagarna att diskutera, utifrån deras perspektiv

Sveriges Kommuner och Regioner

# Tack!