

NIS2/Cybersäkerhetslagen

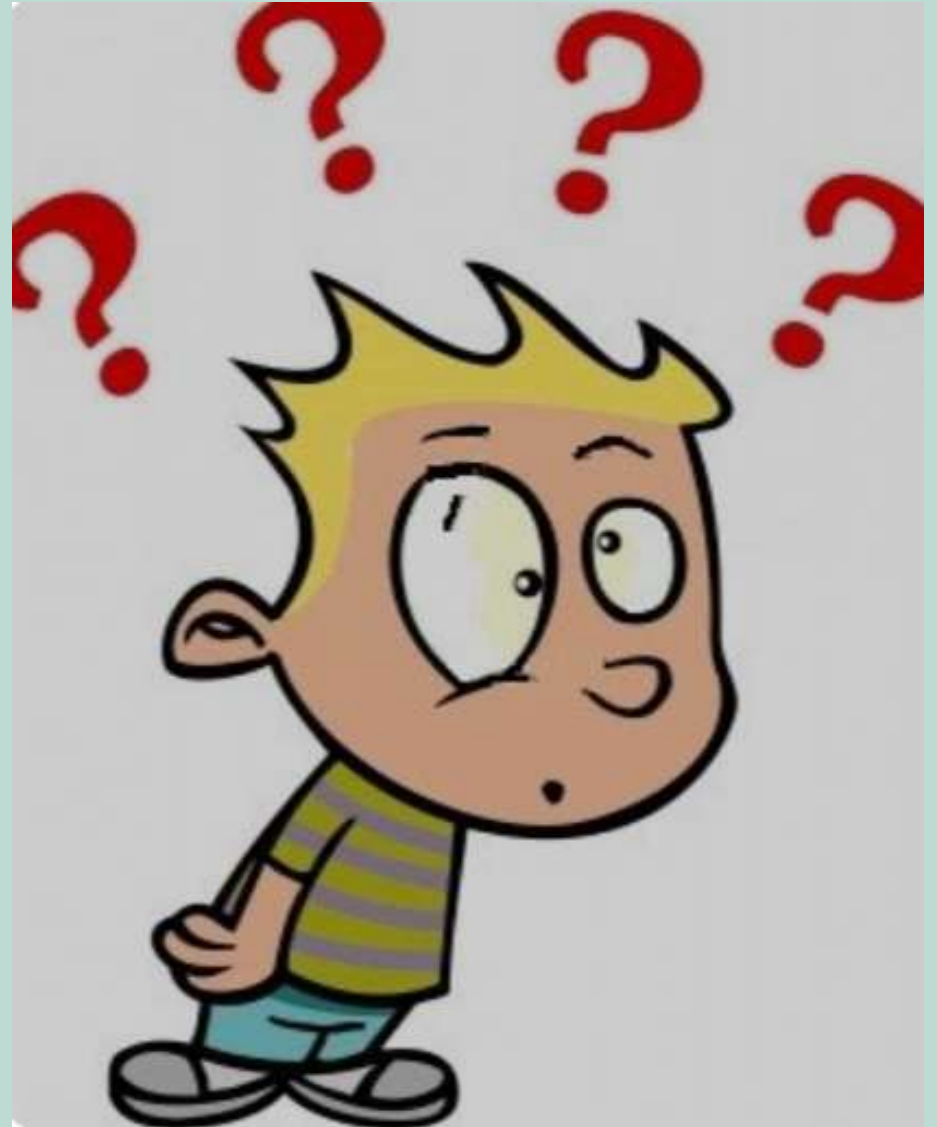
2025-10-13

Agenda

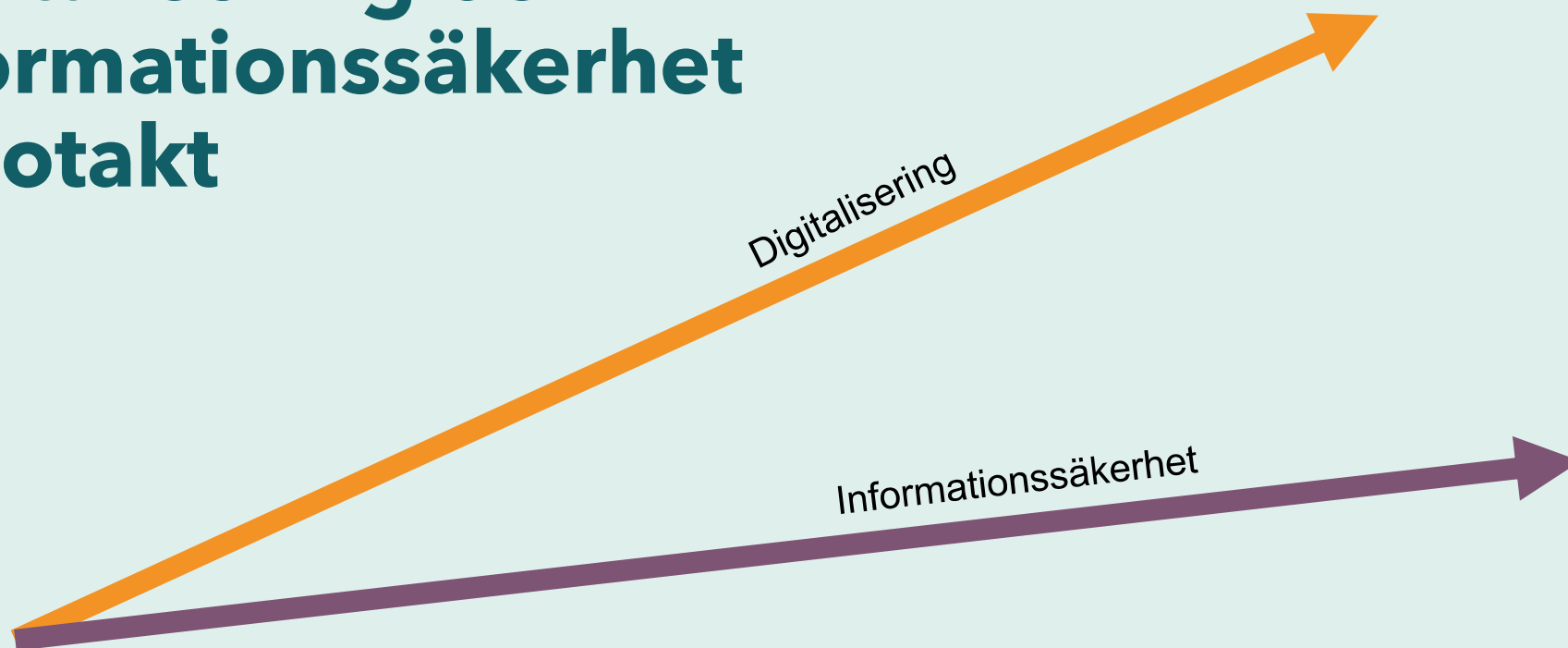
- Varför?
- Vem omfattas?
- Vad innebär det?
- Vad gör vi?



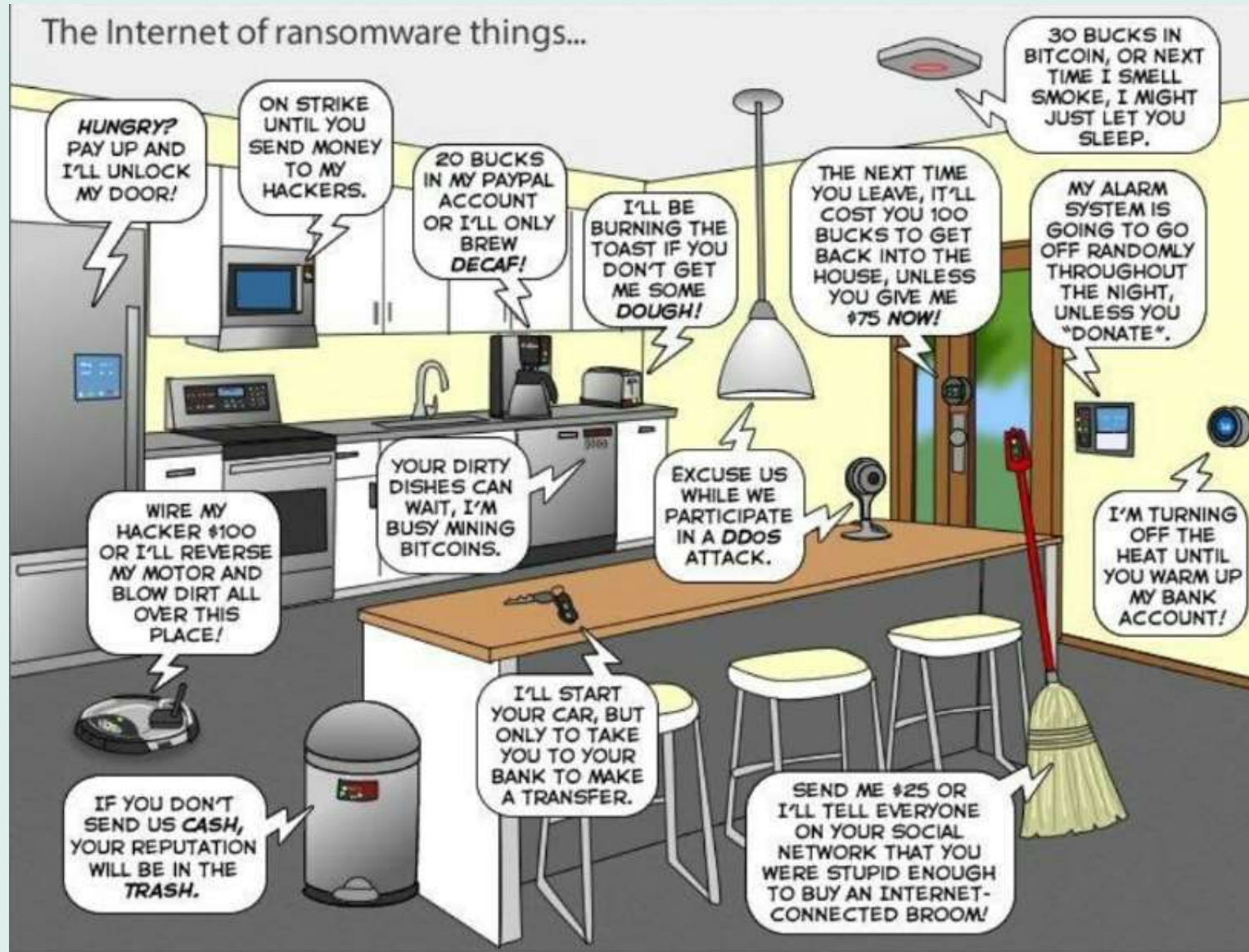
Varför?



Digitalisering och informationssäkerhet är i otakt



The Internet of ransomware things...



Vad händer i vår omvärld?

EKONOMI

Coops it-problem forts många butiker fortsatt

UPPDATERAD 2021-07-04 PUBLICERAD 2021-07-04



Dagens Samhälle

Cyberattack mot Härjedalen: "Vi betalar inte"

Publicerad: 28 december 2023, 14:27

IT-attacken kommun får

Information från 24/1 kl. 15.30

TietoErvys datacenter för en kund hos TietoErvy har drabbats av en IT-attack. Omfattningen av skadorna har inte varit helt utrett av TietoErvy

Rysk hackergrupp hotar Bjuvs kommun

UPPDATERAD 2 APRIL 2024 PUBLICERAD 27 FEBRUARI 2024

Bjuvs kommun hotas av den ryska hackergruppen Akira – som nyligen utfört flera cyberattacker mot svenska myndigheter och företag. Hotet handlar om att offentliggöra känsligt material men enligt kommunledningen har det inte riktats några krav från hackergruppen. Vellinge kommun var inte målet för attacken. Omfattningen av skadorna har inte varit helt utrett av TietoErvy



Härjedalens kommun är drabbad av en IT-attack

Kommunens e-tjänster och system har stannat igen. Övriga IT-system rullar igång allt eftersom och arbetet återgår successivt till det normala.

Läs mer



Cyberattack mot sjukhus

DAGENS NYHETER.

Nyheter Sverige Världen Ekonomi Kultur Sport Klimatet DN Direkt Politik Kriget i Ukraina Fakta i frågan Vetenskap Tipsa DN E-DN ARKIVET KORSORD KUND QUIZ ERBJUD

Senaste nyheterna i korthet

2024-02-28 10:11 Uppdaterad 2024-03-01 06:21

Region Stockholm i stabsläge efter cyberattack mot sjukhus

Region Stockholm beslutade på tisdagskvällen att gå upp i stabsläge efter cyberangreppet mot sjukhuset Sophiahemmet i Stockholm. Närmare bestämt är det den regionala särskilda sjukvårdsledningen som är aktiverad i stabsläge.

Hackargrupper hotar att läcka svenska data

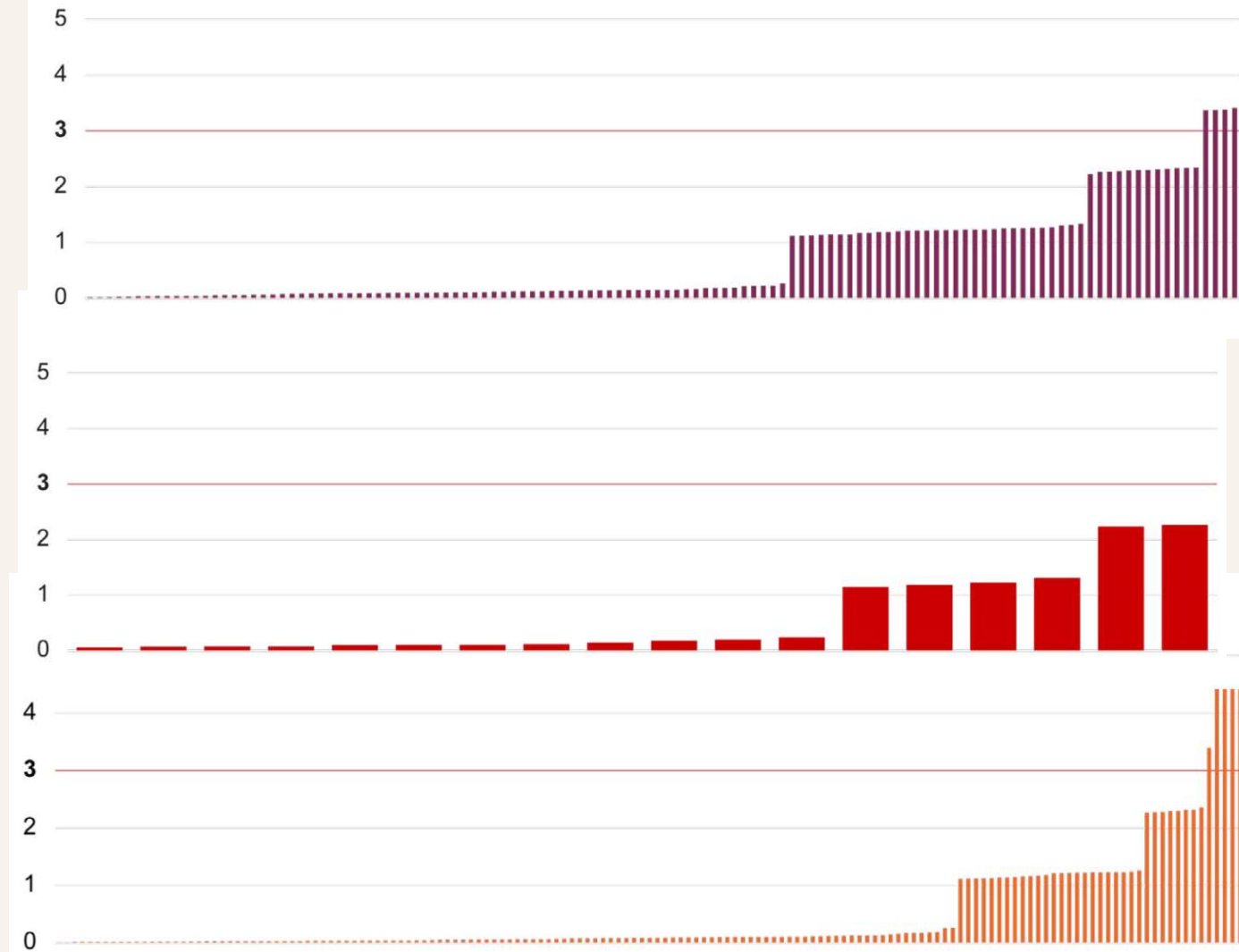
Uppdaterad 2024-02-27 Publicerad 2024-02-26



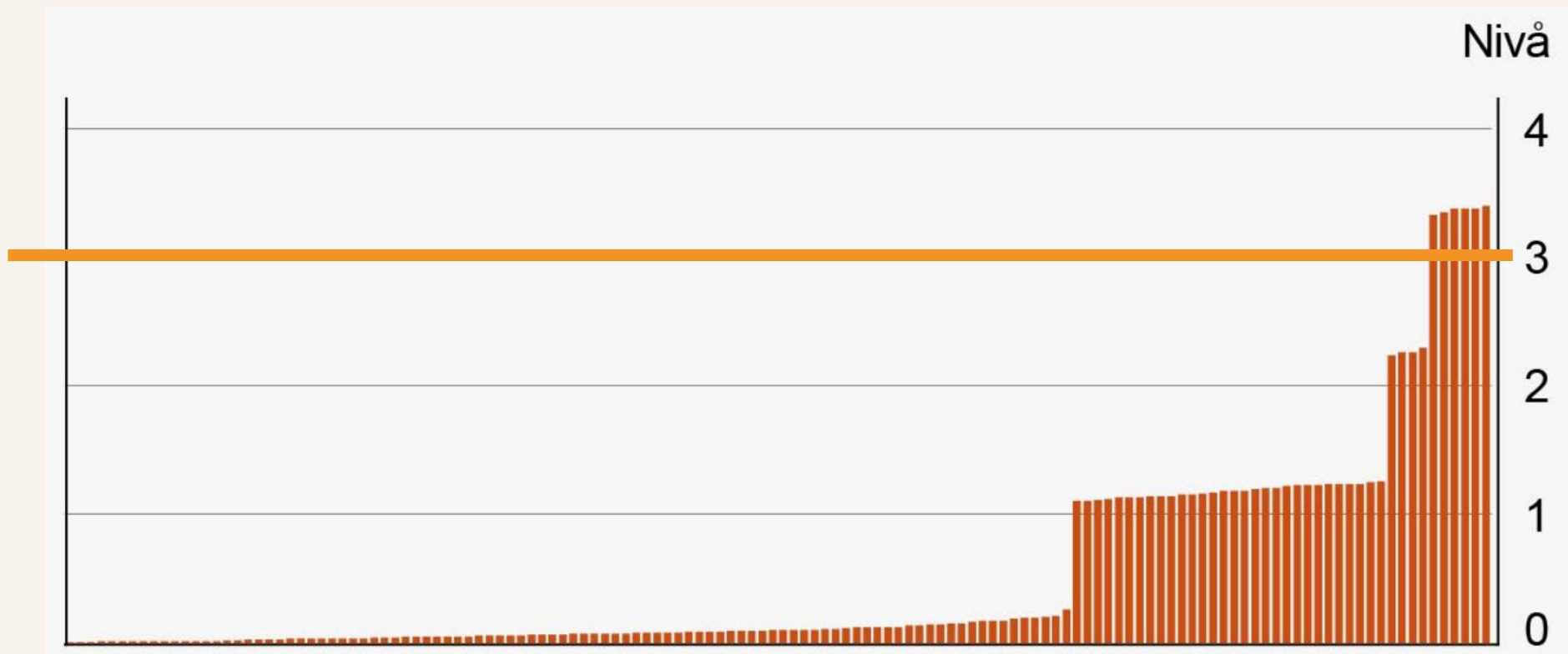
Utgångsläget

- Kommunerna
- Regionerna
- Statliga myndigheter

Resultattal för samtliga 120 myndigheter



Utgångsläget



* Svar från 136 kommuner

Vi måste bli bättre!

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

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**



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.

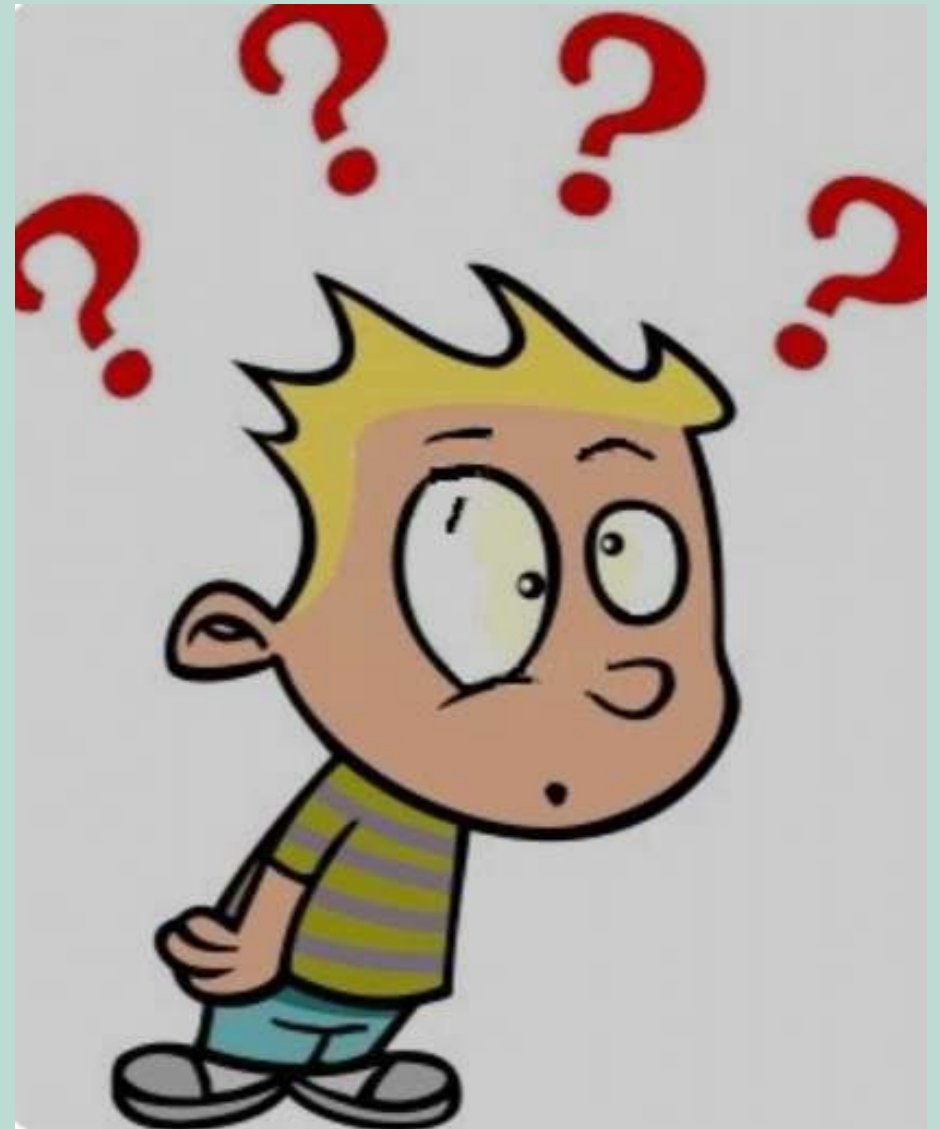
2 § I 3-9 kap. finns en förteckning över samhällsviktiga tjänster där en incident skulle medföra en betydande störning enligt 3 § 1 st. 1 p. lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

informationssäkerhet

2018 om
direktiv (EU)
rhet i nätverks- och
ficering av de

ark och

Vem omfattas?



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

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

Cybersäkerhetslagens inverkan på kommuner och regioner

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



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.

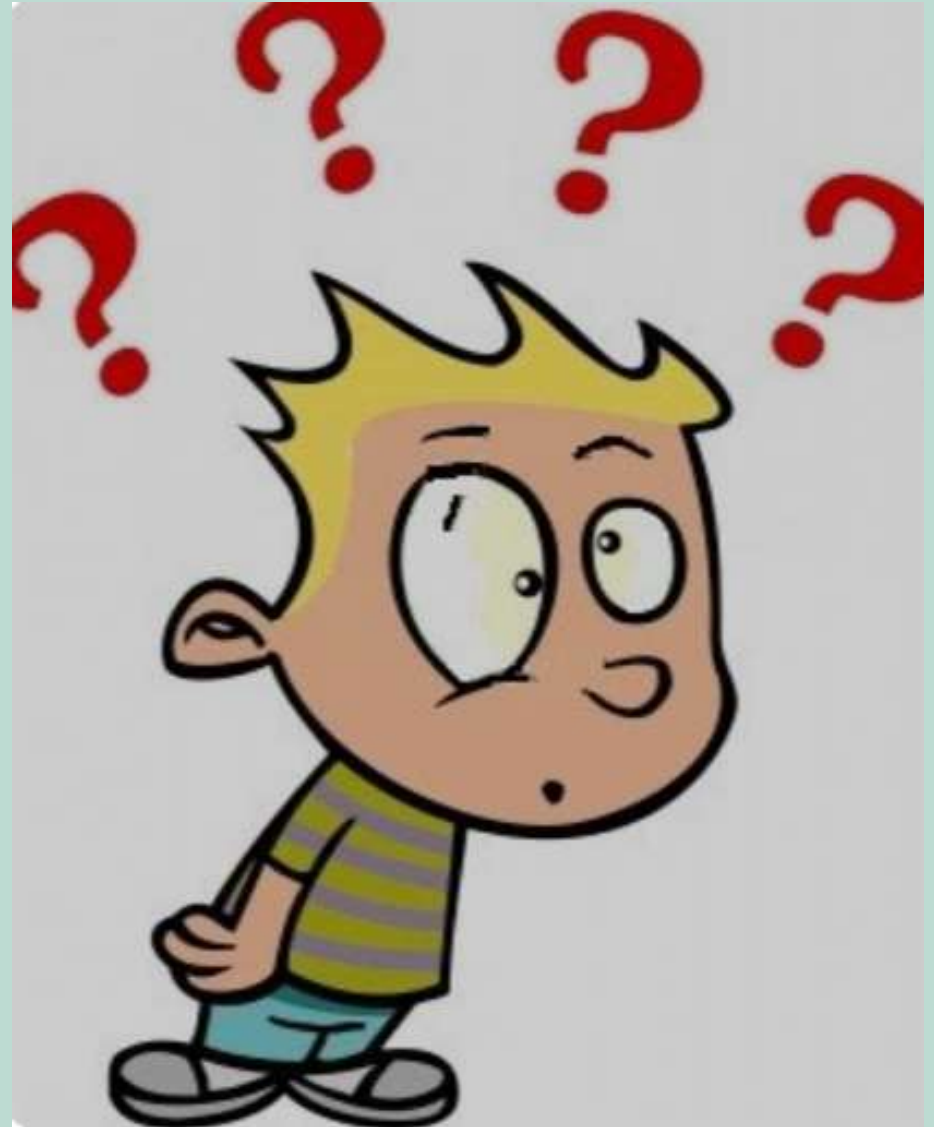
2 § I 3-9 kap. finns en förteckning över samhällsviktiga tjänster där en incident skulle medföra en betydande störning enligt 3 § 1 st. 1 p. lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

informationssäkerhet

2018 om
direktiv (EU)
rhet i nätverks- och
ficering av de

ark och

Vad innebär det?



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.



Utbildning

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



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.



Tillsyn

Tillsyn sker genom:

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



Ingripande

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



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.

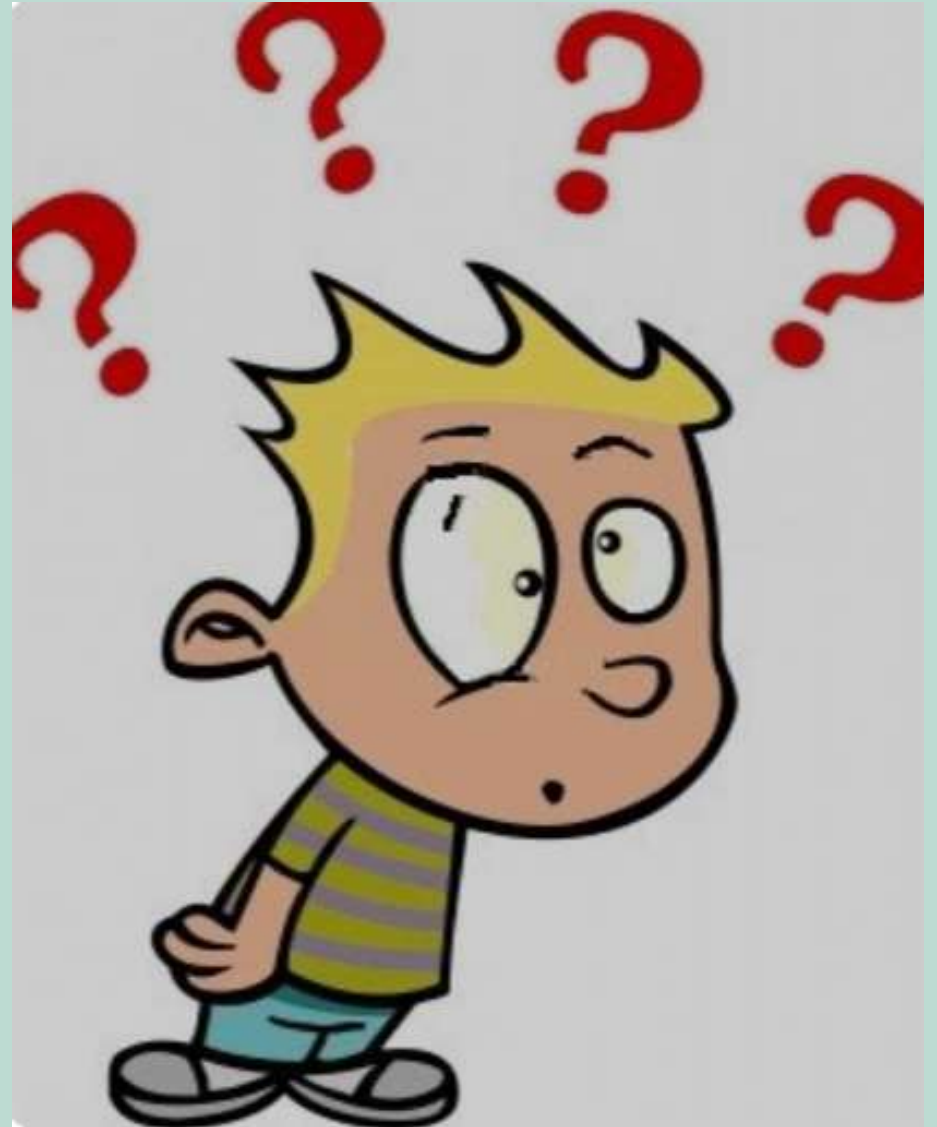
För kommuner och regioner är sanktionsavgiften lägst 5 000 kr och högst 10 000 000 kr.

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



Vad gör vi?



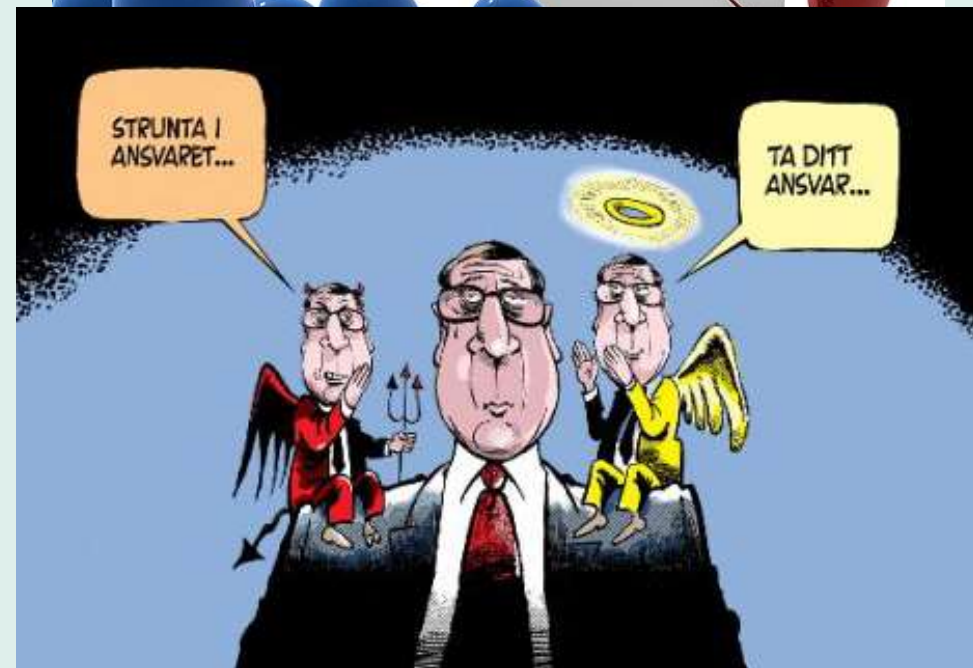
Systematiskt och riskbaserat informationssäkerhetsarbete

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

Systematiskt informationssäkerhets- arbete

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

Policy



Systematiskt informationssäkerhets- arbete

- Tillämpa
 - Analysera
 - Undersök
 - Beslut

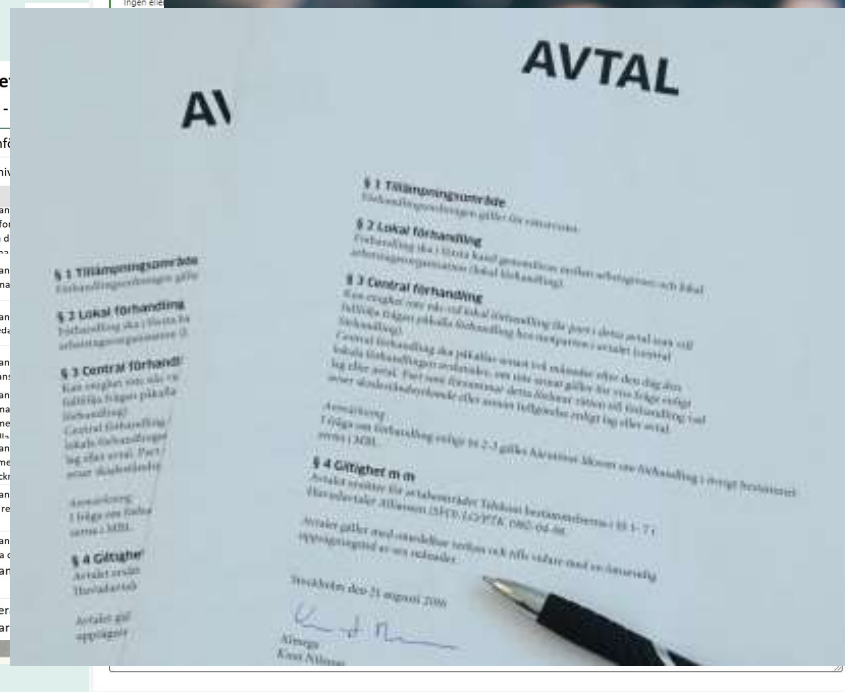
KLASSA - Krav på säkerhe

Namn: Inför upphan

Säkerhetsnivåer: Konfid

Säkerhetsnivå

#	Krav	#	Krav
6001	Leverantören ska för informationssäkerhet	6001	Leverantören ska för informationssäkerhet
6002	Leverantören ska ha informationssäkerhet	6002	Leverantören ska ha informationssäkerhet
6003	Leverantören ska ha kan leda till missbruk	6003	Leverantören ska ha kan leda till missbruk
6005	Leverantören ska ha leveransen.	6005	Leverantören ska ha leveransen.
6007	Leverantören ska bed informationssäkerhet informera en utpekad	6007	Leverantören ska bed informationssäkerhet informera en utpekad
6009	Leverantören ska för dokumenterad förteckning	6009	Leverantören ska för dokumenterad förteckning
6010	Leverantören ska ha av de resurser som ingår i leveran	6010	Leverantören ska ha av de resurser som ingår i leveran
6011	Leverantören ska ha dokument	6011	Leverantören ska ha dokument



Fastställ

Konfid

- att inform

Välj nivå:

Ingen ele

Hur

Hur

1

1

1

1

1

1

1

1

1

Systematiskt informationssäkerhets- arbete

- Följa upp
 - Handlingsplan

Fastställt säkerhetsnivåer 3 uppgifter ▼

Konfidentialitet ⓘ

- att informationen kan åtkomstbegränsas

Välj nivå:

Nivå 0
Ingen eller försumbar skada

Nivå 1
Måttlig skada

Nivå 2
Betydande skada

Nivå 3
Allvarig skada

Nivå 4
Av betydelse för Sveriges säkerhet

Beskriv valet av nivå

Riktighet ⓘ



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 tor de delar av verksamheten som berörs i leveransen ha ett ledningssystem för informationssäkerhet (IS) 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, exempelvis Årsvärda 3 och om behövande bedrivare eller	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	

Konfidentialitet



Dina svar

Uppfyller helt: 61
Uppfyller delvis: 16
Uppfyller inte alls: 6
Vet ej: 2
Ej relevant: 2

Riktighet



Dina svar

Uppfyller helt: 40
Uppfyller delvis: 10
Uppfyller inte alls: 6
Vet ej: 1
Ej relevant: 2

Tillgänglighet



Dina svar

Uppfyller helt: 19
Uppfyller delvis: 8
Uppfyller inte alls: 2
Vet ej: 1
Ej relevant: 1

Lagrum



Dina svar

Uppfyller helt: 73
Uppfyller delvis: 8
Uppfyller inte alls: 2
Vet ej: 0
Ej relevant: 0

Riskbaserat arbetssätt

- Förmåga att bedöma effektiviteten i vidtagna åtgärder



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

Vad är en risk?

- En ögonblicksbild!



Hur hanteras en risk?

Riskhantering

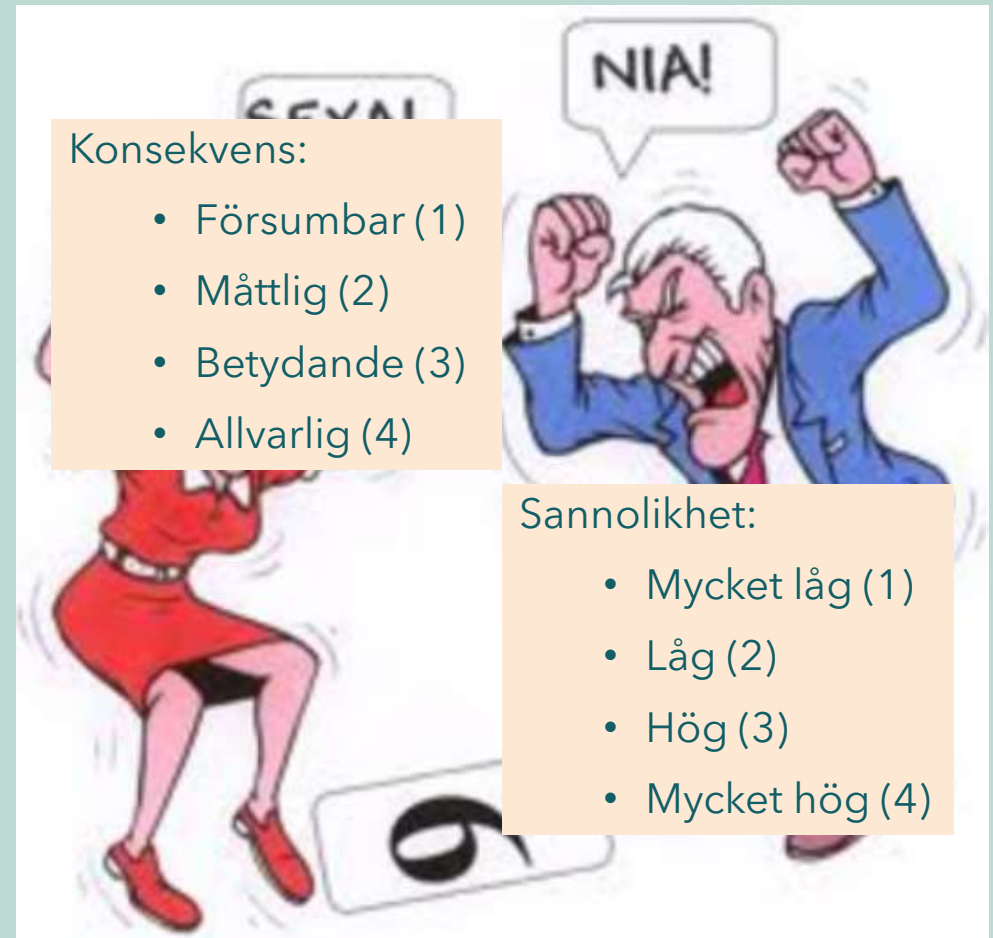
- **Identifiering**
- *Värdering*
- *Behandling*
- *Uppföljning*



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

Riskhantering

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



Konsekvens * Sannolikhet = **Riskvärde**

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)	Hög (3)	Mycket hög (4)
Mycket hög (4)	Mellan	Hög	Mycket hög	Mycket hög
Hög (3)	Mellan	Hög	Mycket hög	Mycket hög
Låg (2)	Låg	Medel	Medel	Mycket hög
Mycket låg (1)	Låg	Låg	Medel	Medel

Tekniska säkerhetsåtgärder

Personella säkerhetsåtgärder

Administrativa säkerhetsåtgärder

Organisatoriska säkerhetsåtgärder

Riskhantering

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



Vem äger risken?

- Jag äger risken!



Eskalering!



Vad gör SKR?



Tillsammans är vi starka!



Metodstöd Informationssäkerhet

- Skapa de rätta förutsättningarna för ett systematiskt informationssäkerhetsarbete

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.

Metodstöd informationssäkerhet

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



The diagram shows a horizontal sequence of 11 steps, each represented by a yellow circle with a number inside, connected by a dotted line. Below each circle is a label in Swedish. Step 1 is highlighted with a yellow background.

1	2	3	4	5	6	7	8	9	10	11
Analys	Policy	Ansvar	Utbilda	KLASSA	Risk	Incident	Kontinuitet	Bevaka	Utvärdera	Ledning

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

Metodstöd informationssäkerhet

- Kliva ut i organisationen!
- ...fler analyser
- ...t.ex. upphandling



Informationsklassning - KLASSA

Här får du ta del av fiktiva exempel på informationsklassning i nivå 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).

Metodstöd informationssäkerhet

- Lära sig!
- ...göra om
- ...och göra "rätt"



Utbildning

Organisationens personal och relevanta intressenter bör få lämplig utbildning och övning för ökad medvetenhet om informationssäkerhet. De ska också erbjudas regelbundna uppdateringar om organisationens informationssäkerhetspolicy och ämnesspecifika styrdokument utifrån vad som är relevant för deras arbetsuppgifter.

Fiktivt exempel - Utbildning nivå 3 Mittköping

” Detta avsnitt ger exempel på hur en organisation kan genomföra kunskapstester hos medarbetare samt revidera en utbildning.

 Arbetsmaterial: Fiktivt exempel Utbildning nivå 3 (WORD)

Genomför kunskapstester hos medarbetare

Innan den årliga uppreningen av utbildningen ska göras genomför medarbetaren ett kunskapstest. I kunskapstestet finns olika scenarier beskrivet med svarsalternativ.

- Resultatet av kunskapstestet styr vilka delar av utbildningen som behöver upprepas.
- Resultatet används även för att undersöka om utbildningen har rätt effekt och om kunskapen även finns kvar efter en viss tid.

Här anges ett exempel. I arbetsmaterialet finns det fler exempel på ett innehåll för att genomföra ett kunskapstest.

Fråga	Svarsalternativ

Metodstöd informationssäkerhet

- ...lite av ett självspelande piano...



Metodstöd informationssäkerhet

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

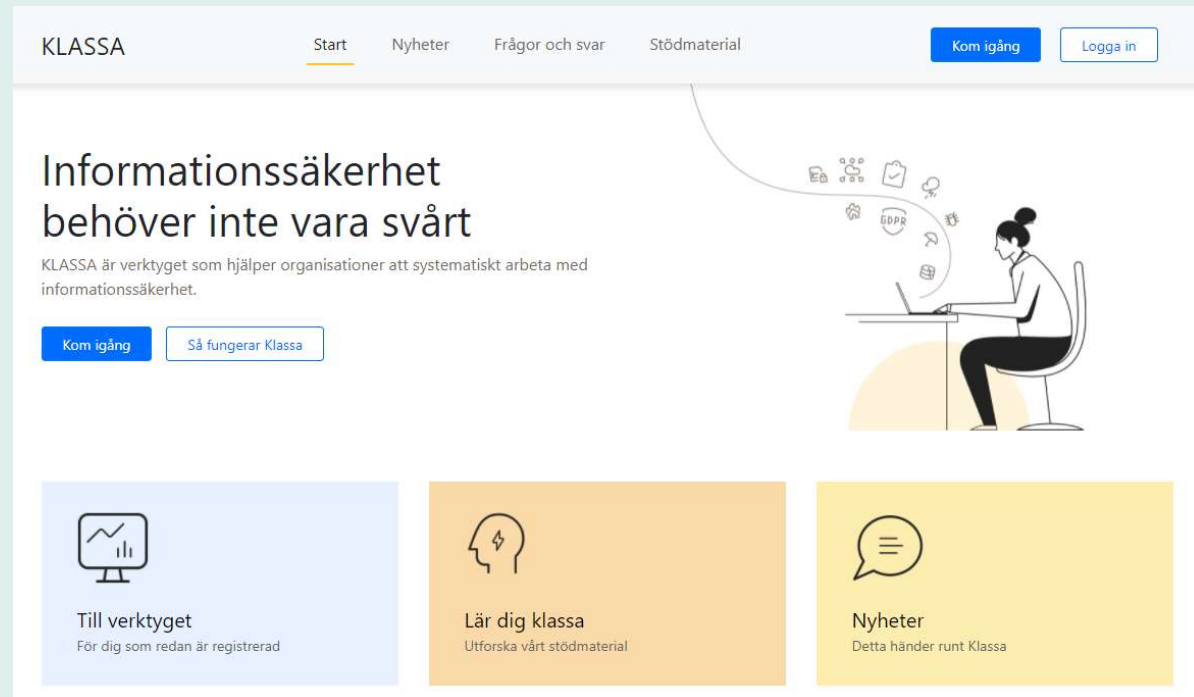
Nivå 2 kännetecknas av att viss medvetenhet och viss systematik börjar etableras.

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.

Vad ingår i KLASSA?

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



The screenshot shows the KLASSA website homepage. At the top is a navigation bar with the KLASSA logo, links for Start, Nyheter, Frågor och svar, and Stödmaterial, along with buttons for 'Kom igång' and 'Logga in'. The main heading reads 'Informationssäkerhet behöver inte vara svårt'. Below this is a subtext: 'KLASSA är verktyget som hjälper organisationer att systematiskt arbeta med informationssäkerhet.' There are two buttons: 'Kom igång' and 'Så fungerar Klassa'. To the right is an illustration of a person sitting at a desk with a laptop, with various icons (lock, key, document, etc.) floating around. Below the main content are three colored boxes: a light blue box with a monitor icon titled 'Till verktyget' (För dig som redan är registrerad), an orange box with a head icon titled 'Lär dig klassa' (Utforska vårt stödmaterial), and a yellow box with a speech bubble icon titled 'Nyheter' (Detta händer runt Klassa).

klassa@skr.se

Utbildning

- Grundläggande utbildning
 - Effektiv och säker informationsklassning med KLASSA

28 okt	🕒 13:00 - 16:00	● Platser kvar	Anmäl nu
06 nov	🕒 09:00 - 12:00	● Platser kvar	Anmäl nu
13 nov	🕒 09:00 - 12:00	● Platser kvar	Anmäl nu
01 dec	🕒 13:00 - 16:00	● Platser kvar	Anmäl nu
17 dec	🕒 09:00 - 12:00	● Platser kvar	Anmäl nu

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

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

Tack!

