

Kvartalsredovisning HSN

September 2025



Fokus för 2025

- Förberedelse inför Cybersäkerhetslagen
- Riktlinjer för incidenthantering
- Riktlinjer för kontinuitetshantering
- Informationsinsatser kring användning av AI med fokus på informationssäkerhet/cybersäkerhet
- Översyn av metoder för informationsklassning och riskanalyser.
- Utredning av förutsättningar för registerförteckning



Omvärldsbevakning

- I **Sverige** har vi inte sett rapporterade större cyberincidenter inom vårdsektorn under våren och sommaren 2025 (förutom tidigare DDoS 2024), vilket var goda nyheter – men beredskap och vaksamhet är fortfarande viktiga.
- **Globalt** har våren 2025 präglats av stora dataläckor och driftstörningar som påverkat miljontals patienter och kanske satt vårdsystemens tillgänglighet och datasekretess på prov.



Personuppgiftsincidenter/ informationssäkerhetsincidenter

- **Skolplattform:** Älvdalens kommun har stängt ner den kommunala skolplattformen på grund av en allvarlig säkerhetsbrist. Det handlar om att leverantören haft behörigheter de inte ska ha och därför kommit åt data som inte ska finnas tillgänglig
- **Nybro:** glömdes en väska kvar på tåget mellan Nybro och Kalmar. Väskan innehöll utskrivna handlingar från pågående ärenden där ett flertal personer förekommer. Trots att kommunen omedelbart kontaktade tågoperatören (Sodexo) och efterlyste väskan, har den tyvärr inte kunnat återfinnas. Känsliga uppgifter i det förlorade materialet berör ett flertal personer där bedömningen om risk för allvarlig skada bedöms som hög.



Miljödata AB

- Företagets system hanterar bland annat arbetsrättsliga ärenden, läkarintyg och hantering av arbetsskador och tillbud-Adato
- Novi används för disciplinäraärenden
- Ransomware- 23/8- 1,5 miljon uppgifter röjda varar 21000 Regionens
- Namn, personnummer kontaktuppgifter och antal sjukdagar



Miljödata AB

- AI algoritmer
- Samkörning av olika uppgifter med varandra
- Bedrägeri
- IT-stöld
- Nätfiske

svt

START

PROGRAM

KANALER

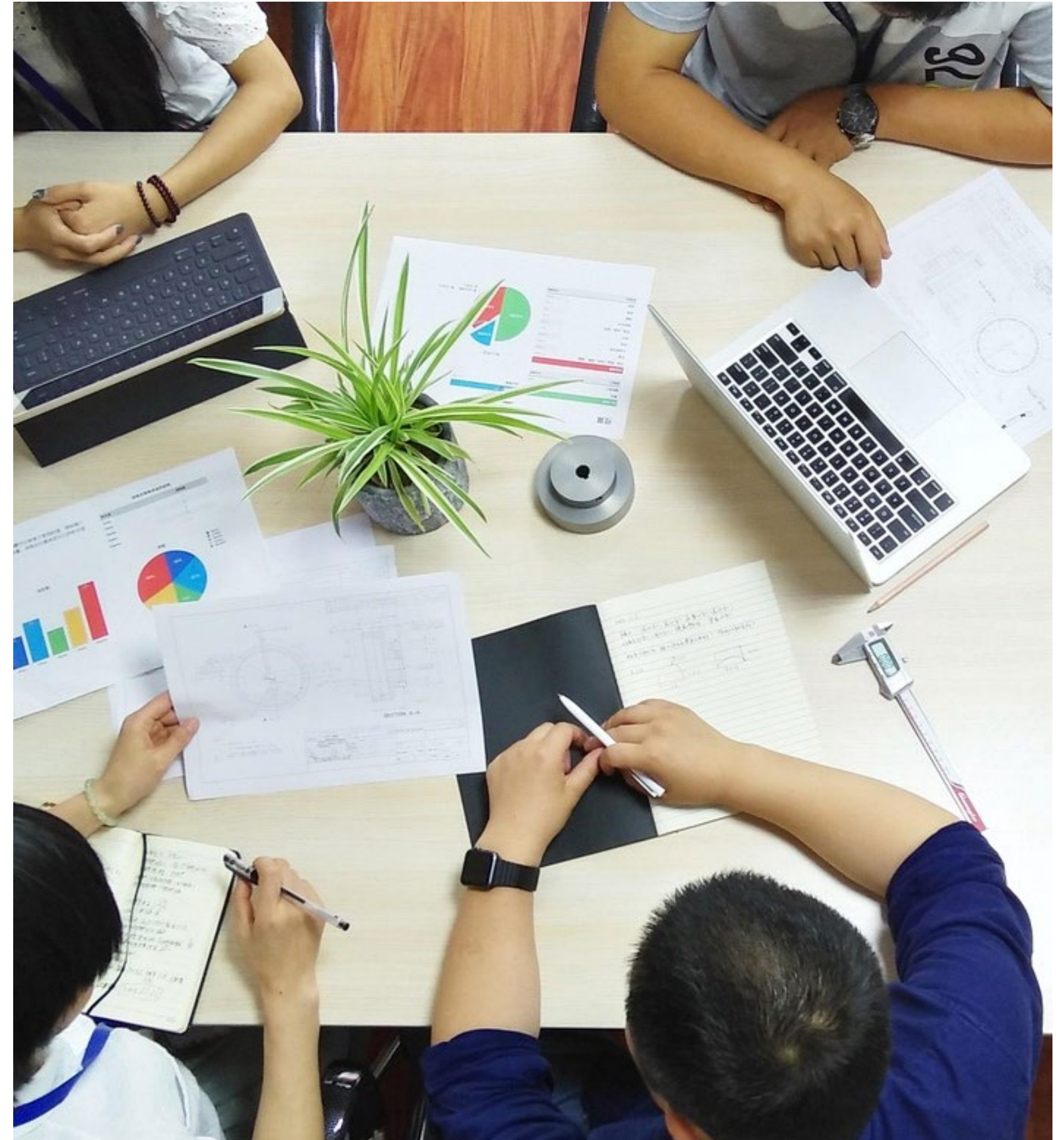
CYBERATTACKEN MOT MILJÖDATA

Så kan dina uppgifter användas för bedrägerier

Attacken mot Miljödatas system, ett företag som levererar HR-system till 80 procent av Sveriges kommuner, har drabbat över en miljon svenskar.

Utredning

- Analysgruppens arbete
- Frågan utreds och slutligt rapport med rekommendation kommer under oktober 2025



Ny lagstiftning på gång

- EU:s **NIS2-direktiv** ersätter det tidigare NIS-direktivet sedan januari 2023, och skulle varit genomfört i medlemsstaterna senast oktober 2024 .
- I Sverige pågår nu implementeringen genom en ny **cybersäkerhetslag**, grundad på utredningen **SOU 2024:18**. Regeringen skickade under **juni 2025** en lagrådsremiss, och målet är att lagen träder i kraft den **15 januari 2026** .
- Lagen innebär krav på systematiskt informationssäkerhetsarbete, riskhantering, incidentrapportering och tydligt ansvar för ledningen.



Nya riktlinjer under arbete

- Riktlinje för informationssäkerhet
- Incidenthantering
- Informationsklassning
- Riskhantering
- Personuppgiftsansvarig/biträde
- Personuppgiftsincidenter
- Registrerades rättigheter

Riktlinje för informationssäkerhet

- Allt på ett ställe, istället för många olika dokument samlar vi alla regler för området informationssäkerhet i ett gemensamt dokument.
- Syftet är att lättare hitta information man behöver.

Riktlinje för informationssäkerhet

Fyra olika block

- A: Informationssäkerhet för medarbetare
- B: Styrning av informationssäkerhet
- C: Informationssäkerhet i verksamhetsnära förvaltning
- D: Informationssäkerhet i IT-miljön

Riktlinjer för informationssäkerhet

Innehållsförteckning

Inledning	5
Omfattning	5
Struktur och läsanvisningar	5
Dispenser och avsteg	5
Introduktion till informationssäkerhet	5
Relevanta termer och definitioner	5
Del A: Informationssäkerhet för medarbetare	6
Inledning	6
Medarbetarens ansvar för informationssäkerhet	6
Informationsklasser	6
A.1 Lösenord	6
A.2 Mobila enheter	6
A.3 Skadlig kod	6
A.3.1 Spridning av skadlig kod	6
A.4 Internet och sociala medier	6
A.5 Digital kommunikation	6
A.6 Lagring och säkerhetskopiering	6
A.7 Spårbarhet och loggning	6
A.8 Säkert beteende	6
Del B: Styrning av informationssäkerhet	7
Inledning	7
B.1 Roller, ansvar och organisation	7
B.1.1 Grundprincip	7
B.1.2 Övergripande ansvar	7
B.1.3 Ansvar inom respektive verksamhet	7
B.1.4 Medarbetares ansvar	7
B.1.5 Personuppgiftsansvar	7
B.1.6 Regionarkivet	7
B.1.7 Objektägares ansvar	7
B.1.8 Ansvar i projekt	7
B.1.9 Informationsförsörjnings- och digitaliseringsavdelnings ansvar	7

B.1.10 Informationssäkerhetsfunktion (strateg, samordnare, ute på förvaltningarna-handläggare? DSO).....	7
B.1.11 Regionens revisorer	7
B.2 Dokumentstruktur	8
B.3 Informationsklassning	8
B.3.1 Region Västmanlands modell för informationsklassning	8
B.3.2 Konsekvensnivåer	8
B.3.3 Konsekvenskategorier	8
B.3.4 Vad ska klassificeras?	8
B.3.5 När klassning ska ske?	8
B.3.6 Användningsområden och målgrupper	8
B.4 Ledningssystem för informationssäkerhet	8
B.5 Personalsäkerhet	8
B.5.1 Före och i samband med anställning.....	8
B.5.2 Under anställning.....	8
B.5.3 Avslut eller ändring av anställning	8
B.6 Leverantörsrelationer	8
B.7 Efterlevnad och granskning	8
Del C: Informationssäkerhet i verksamhetsnära förvaltning	9
Inledning	9
Roller och ansvar	9
C.1 Dokumentation av informationssäkerhet.....	9
C.1.1 Systemsäkerhetsbeskrivningar	9
C.2 Informationsklassning och systemklassning.....	9
C.3 Behörigheter och logghantering	9
C.3.1 Logghantering.....	9
C.4 Ändringshantering.....	9
C.5 Användarinstruktioner	9
C.6 Riskanalyser	9
C.7 Incidenthantering.....	9
C.8 Kontinuitetshantering	9
C.9 Kontroll av IT-tjänst.....	9
Del D: Informationssäkerhet i IT-miljö.....	10
Inledning	10
Roller och ansvar flytta ihop?	10
D.1 Hantering av tillgångar	10

D.1.1 Identifiering av IT-resurser och tilldelning av ägare.....	10
D.1.2 Klassning av IT-resurser (flytta till klassning?).....	10
D.1.3 Användningsinstruktioner	10
D.2 Styrning av åtkomst.....	10
D.2.1 Identifiering och autentisering.....	10
D.2.2 Reglering av åtkomsträttigheter	10
D.2.3 Säkerhetsloggning	10
D.3 Kryptering.....	10
D.4 Fysisk och miljörelaterad säkerhet.....	10
D.4.1 Säkra utrymmen för IT-resurser	10
D.4.2 Godsmottagning och lastning	10
D.4.3 Underhåll, reparation och avveckling.....	10
D.4.4 Skydd av utrustning	10
D.4.5 Elförsörjning.....	10
D.5 Driftsäkerhet (Cybersäkerhetslagen?)	10
D.5.1 Driftsrutiner	10
D.5.2 Skydd mot skadlig kod	10
D.5.3 Säkerhetskopiering.....	10
D.5.4 Loggning och övervakning	10
D.5.5 Hantering av tekniska sårbarheter	10
D.6 Kommunikationssäkerhet	11
D.6.1 Nätverkssäkerhet	11
D.6.2 Informationsöverföring	11
D.7 Anskaffning och utveckling av IT-resurser	11
D.7.1 Säkerhetskrav på IT-resurser	11
D.7.2 Säkerhetskrav vid upphandling av IT-stöd	11
D.7.3 Säkerhet vid systemutveckling	11
D.7.4 Säkerhetskrav vid test.....	11
D.8 Informationssäkerhetsincidenter.....	11
D.8.1 Krigsorganisation och krisplan	11
D.9 IT-relaterad kontinuitetshantering	11
D.10 Granskning och kontroll	11

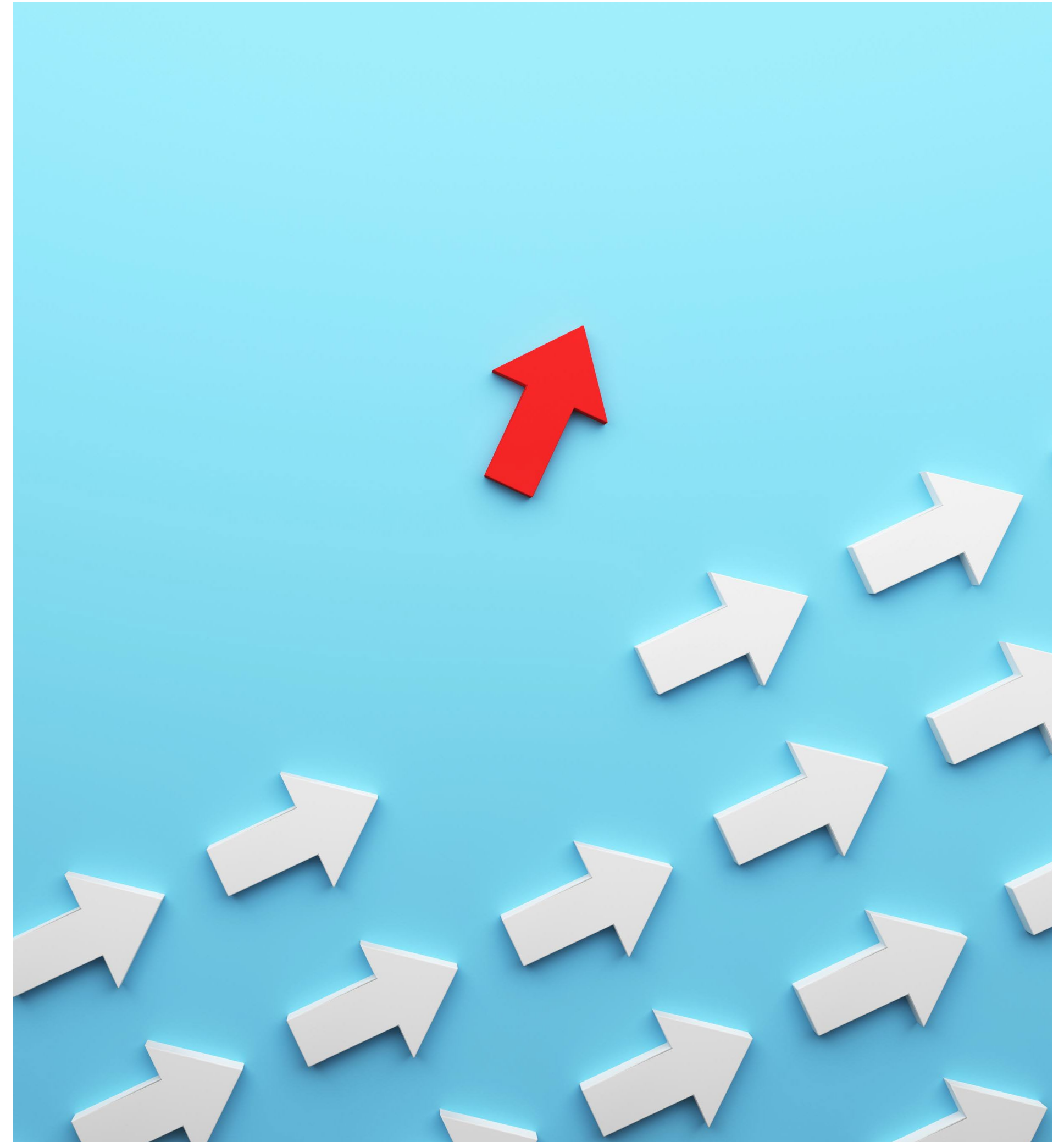
Metod för rapportering av incidenter

- Personuppgiftsincident:

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt

- Synergi

.



Utbildning- åtkomst till journalen

- Webbutbildning om när man får/inte får skaffa sig tillgång till journalinformation

Åtkomst till patientjournalen- grundutbildning

Cybersäkerhetskollen

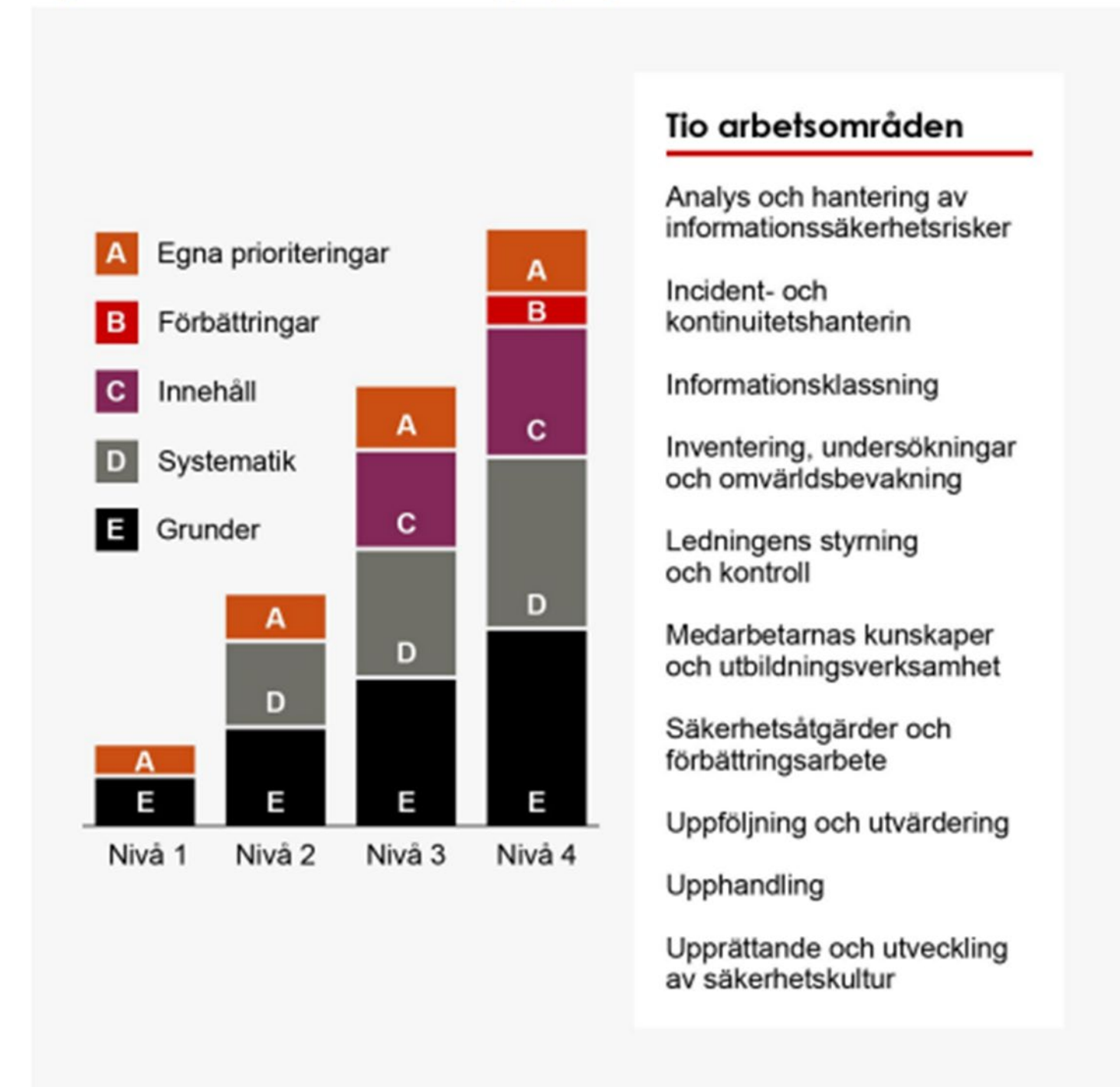
- Ett verktyg från Myndigheten för samhällsskydd och beredskap (MSB) för ökad motståndskraft och ett stärkt civilt försvar.
- MSB har utifrån tre regeringsuppdrag tagit fram en uppföljningsstruktur av det systematiska cybersäkerhetsarbetet samt säkra digitala leveranskedjor.



Cybersäkerhetskollen

- Med Cybersäkerhetskollen får regionen en bättre bild av vårt cybersäkerhetsarbete och förslag på utvecklingsområden, samt underlag för planering och prioritering.
- Senaste mätningen av Cybersäkerhetskollen påbörjades 23 april 2025.
- Sista inrapporteringsdatum var den 12 september 2025.

Figur 1. Infosäkkollens modell för uppföljning Illustration över

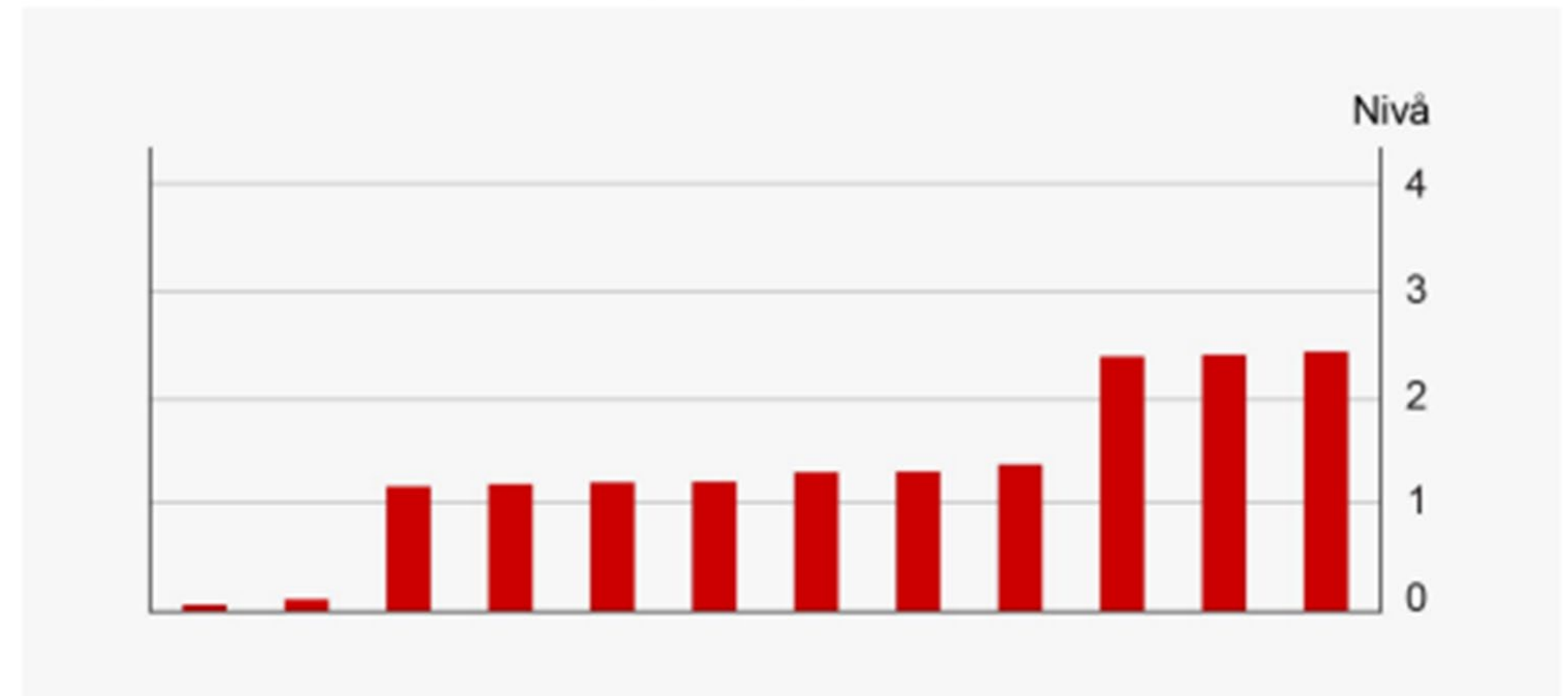


Närmare bakgrund till och beskrivning av den modell som ligger till grund för nivåindelning och resultatberäkning finns i *fördjupningsinformationen* som återfinns på Cybersäkerhetskollens webbsida.¹⁹

Cybersäkerhetskollen

- Vi kan också jämföra nivån på vår arbete med andra liknande organisationer.
- Cybersäkerhetskollen är både ett verktyg för att stötta den egna organisationen i uppföljningen av cybersäkerhetsarbetet och ett bic för att skapa en lägesbild över Sveriges förmåga inom cybersäkerhet.

Diagram 36. Resultattal för samtliga 12 regioner



83,3 procent av deltagande regioner uppnådde nivå 1 eller bättre, 25 procent uppnådde nivå 2. I likhet med 2023 uppnådde ingen region nivå 3 eller 4 i modellen.

Cybersäkerhetskollen

