NIS2 och nya cybersäkerhetslagen – så uppfylls kraven med ISO/IEC 27001

Hej och välkomna, ha gärna bild & ljud avstängt fram till vi börjar kl 11.30

sis.se

Agenda

01. Välkomna

02. Presentation: Anna Andersson

03. Samtal & intervju kring NIS2 och cybersäkerhetslagen

04. Inspiration till fortsatt lärande

05. Frågor

Senior konsult och utbildningsledare

- Deltar i utvecklingen av ISO 27000-serien såväl i Sverige som nationellt
- Deltagit i utvecklingen av ISO/IEC 27002:2022 under flera år
- Informationssäkerhetskonsult med bland annat införanden av LIS, riskhantering, informationsklassningar, mätningar gentemot ISO-standarder men även mot ex. NIS-direktivet
- Kundgrupper inom offentlig och privat sektor
- Utbildningsledare inom SIS informationssäkerhetsakademi

Anna Andersson

ISO/IEC 27001 som stöd för NIS2 och cybersäkerhetslagen

03.

Cybersäkerhet och informationssäkerhet

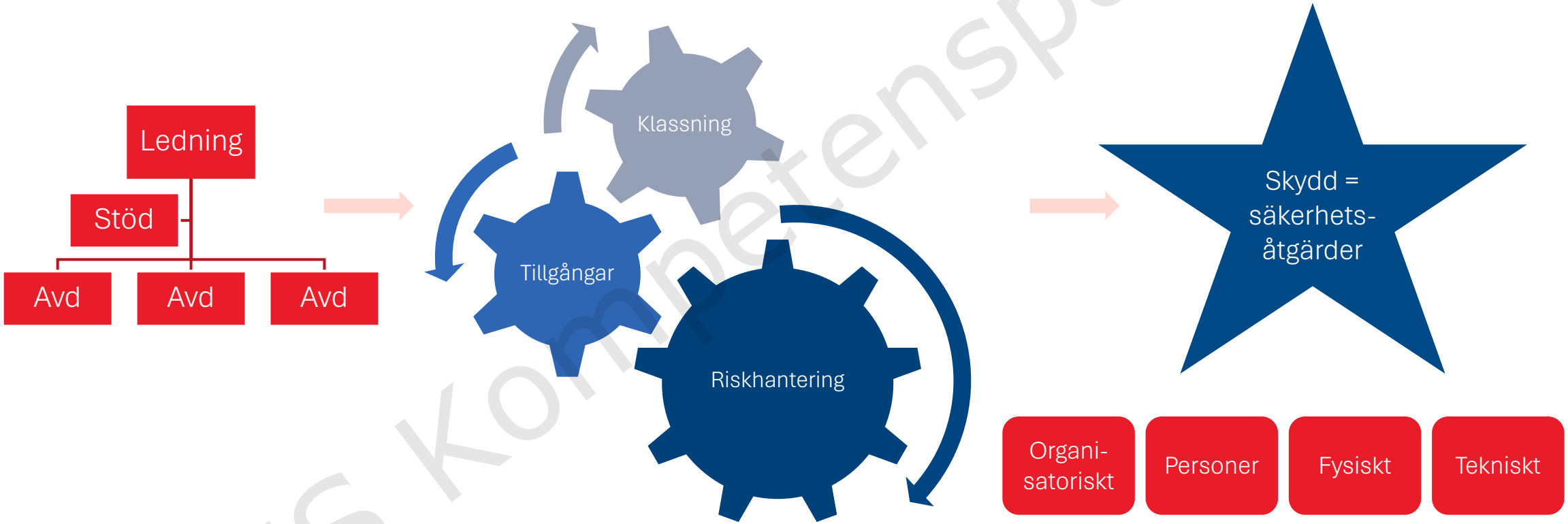
- Informationssäkerhet: bevarande av konfidentialitet, riktighet och tillgänglighet hos informationstillgångar
- Cybersäkerhet: skyddande av människor, samhälle, organisationer och nationer från cyberrisker

Cybersäkerhet fokuserar på att skydda nätverk och informationssystem, användare av dessa system och andra tjänster i cyberrymden från cyberhot som skadlig kod, hackning och nätfiske. Cybersäkerhet inkluderas i organisationens ledningssystem för informationssäkerhet. Det innebär att regelverk utformat för att skydda information utifrån ett allriskperspektiv även inkluderar åtgärder för skydd av informationstillgångar och arbetssätt i cybermiljön.

https://termbanken.informationssakerhet.se/

Informationssäkerhet på en bild

- Informationssäkerhet: bevarande av konfidentialitet, riktighet och tillgänglighet hos informationstillgångar



sis

27001:

- Styrprocesser för informations-säkerhet
- Riskbaserat arbetssätt
- Systematiskt arbete och ska leda till ständiga förbättringar
- Fokus på ledningens ansvar

Krav = ”ska”
(krav för certifiering)


SVENSK STANDARD
SS-ISO/IEC 27001:2022

Informationssäkerhet- Cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav (ISO/IEC 27001:2022, IDT)

Information technology – Cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022, IDT)

Bilaga A
(normativ)

Hänvisning till informationssäkerhetsåtgärder

Informationssäkerhetsåtgärderna i tabell A.1 är direkt härledda från och samordnade med informationssäkerhetsåtgärderna i ISO/IEC 27002:2022[1], avsnitt 5–8, och ska användas i samband med 6.1.3.

Tabell A.1 – Informationssäkerhetsåtgärder

5	Organisatoriska säkerhetsåtgärder	
5.1	Policyer för informationssäkerhet	Säkerhetsåtgärd Informationssäkerhetspolicy och ämnesspecifika policyer ska fastställas, godkännas av ledningen, publiceras, kommuniceras till och accepteras av berörd personal och berörda intressenter, samt ses över vid planerade intervall och om betydande ändringar sker. Svensk nationell anmärkning: Termen ämnesspecifik policy är ovanlig i svenskt ordbruk. I dokumentet avses ett regeldokument hierarkiskt underliggande informationssäkerhetspolicyn, såsom en riktlinje, en instruktion, en rutin, eller liknande.
5.2	Roller och ansvar för informationssäkerhet	Säkerhetsåtgärd Roller och ansvar för informationssäkerhet ska fastställas och tilldelas utifrån organisationens behov.
5.3	Uppdelning av arbetsuppgifter och ansvar	Säkerhetsåtgärd Arbetsuppgifter och ansvarsområden som står i konflikt med varandra ska åtskiljas.
5.4	Ledningens ansvar	Säkerhetsåtgärd Ledningen ska ställa krav på att informationssäkerhet ska tillämpas av

Vägledning = ”bör”


SVENSK STANDARD
SS-EN ISO/IEC 27002:2022

Informationssäkerhet – cybersäkerhet och integritetsskydd - Informationssäkerhetsåtgärder (ISO/IEC 27002:2022)

Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022)

SIS Svenska Institutet för Standarder

Väljs utifrån riskbilden – även andra referensverk kan användas

Bilaga A/27002:

- 93 säkerhets-åtgärder
  - Organisa-toriska
  - Person-relaterade
  - Fysiska
  - Tekniska

Många lagar stöds av ISO/IEC 27001

Många lagar ställer krav på informationssäkerhet i olika former

- Vissa gällande systematiskt informationssäkerhetsarbete
- Vissa gällande skydd av konfidentialitet, riktighet och tillgänglighet av information
- Vissa på direkta säkerhetsåtgärder

- Exempel: säkerhetsskyddslagen, GDPR (dataskyddsförordningen), lagen om offentlig upphandling, bokföringslagen, lagen om skydd av företagshemligheter, arkivlagen…

En analys måste genomföras och underhållas – så man vet i vilka processer och system vilka krav ska efterlevas.

Tips! Suboptimera inte, dvs. starta inte ett nytt område för varje ny lagstiftning. Tänk helhet i organisationen!

NIS2-direktivet

- Utökning av “NIS1” som syftade till säkerhet i nätverk och informationssystem för samhällsviktiga tjänster
- CSL gäller från 15 januari 2026
- Stark koppling till ISO 27001 och 27002
- För IT-leverantörer har det kommit ut ett förtydligande till direktivet – en ”genomförandeförordning” – som gäller **direkt**
- Övriga väntar på MCF:s föreskrifter om säkerhetsåtgärder som förtydligar lagkraven

Följande sektorer omfattas

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning (flera olika)
- Digitala leverantörer
- Forskning

sis

Vad måste göras?

- Verksamhetsutövare ska anmäla sig till tillsynsmyndighet
- Genomföra **riskbaserat** säkerhetsarbete för att skydda nätverk och informationssystem mot incidenter
- Krav på ett **systematiskt och riskbaserat arbete**
- Riskhanteringsåtgärder (säkerhetsåtgärder) ska skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter – tekniska, driftsrelaterade och organisatoriska. Åtgärder ska vara proportionella i förhållande till risken.
- Ledning ska genomgå utbildning
- Betydande incidenter ska förvarnas om till MCF inom 24 timmar från vetskap, incidentrapport inom 72 timmar, med slutrapport inom en månad
- Tillsynsmyndighet kommer att dela in verksamheterna i väsentliga eller viktiga
- Gränsöverskridande verksamhetsutövare registreras särskilt med särskilda regler

Riskhantering – och systematiskt arbete

- Vid bedömning av riskhantering ska hänsyn tas till riskexponering, verksamhetens storlek och sannolikheten för att incidenter inträffar, samt hur allvarliga incidenterna skulle kunna bli för *samhället* och ekonomiskt
- Riskhanteringsåtgärder ska vara såväl förebyggande som hanterande – dvs. även att minska konsekvenserna av inträffade incidenter

Gott stöd för detta finns i ISO/IEC 27001 men även 27005!

Riskhanteringsåtgärdernas koppling till ISO/IEC 27002

Krav i NIS2*
Incidenthantering
Kontinuitetshantering
Säkerhet i leveranskedjan
Säkerhet vid upphandling och utveckling…
Kryptografi
Personalsäkerhet
Åtkomstkontroll och tillgångsförvaltning
Säker kommunikation
Lösningar för autentisering

Notera! Tillsynsmyndigheternas föreskrifter förväntas ställa specifika krav – men om man följer 27002 är man på god väg!!!

*Artikel 21

MCF:s föreskrifter har varit ute på remiss…

2 kap. Organisatoriska säkerhetsåtgärder

Systematiskt och riskbaserat arbete

1 § Verksamhetsutövarens arbete med cybersäkerhet ska vara systematiskt, riskbaserat och integrerat med befintliga sätt att leda och styra organisationen. Verksamhetsutövaren ska identifiera och hantera behovet av att använda relevanta standarder i arbetet.

Allmänna råd

Som stöd för arbetet bör följande eller motsvarande standarder användas:

1. Svensk standard SS-ISO/IEC 27001:2022 Informationssäkerhet - cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav, och
2. Svensk standard SS-EN ISO/IEC 27002:2022 Informationssäkerhet – cybersäkerhet och integritetsskydd- Informationssäkerhetsåtgärder.

MCF:s föreskrifter sätter specifika krav utöver standardernas

sis

Slutsats:

Om organisationen har ett LIS som bygger på ISO/IEC 27001 och 27002 så behöver en inventering göras på tilläggsregler från CSL/föreskrifter

Inspiration till fortsatt lärande

04.

Utbildningsdatum för våren ligger uppe på sis.se

Kvalitet
ISO 9001

Miljö och Energi
ISO 14001 och ISO 50001

Arbetsmiljö
ISO 45001

Intern revision
ISO 19011

Informationssäkerhet - Cybersäkerhet
ISO 27001

Medicinteknik
ISO 14971 och MDR - IVDR

Maskinsäkerhet och CE-märkning
Nya maskinförordningen

Hållbarhet
Cirkulär ekonomi, CSRD och biologisk mångfald

Innovation
ISO 56001

Bygg
Ritningar, Area och BIM enligt ISO 19650

AI - Artificiell intelligens
ISO/IEC 42001

Laboratorier
Provning och Kompetens

Risk och Kontinuitetshantering
Verksamhetsutveckling med ISO standarder

Standardisering
Utveckla och skriva standard

Företagsanpassade utbildningar
Vi kommer till dig!

Grundutbildning

UTBILDNING
Informationssäkerhet och cybersäkerhet - steg 1 enligt ISO 27000
Vi tar bland annat upp certifiering mot SS-ISO/IEC 27001, juridiska aspekter av informationssäkerhet såsom NIS2-direktivet...
Pris: 24900 kr
Boka

UTBILDNING
Informationssäkerhet och cybersäkerhet - steg 2 enligt ISO 27000
Vi tar bland annat upp förbättringsarbete, incidenthantering, åtkomstkontroll, säkerhet i IT-system och nätverk, fysisk sä...
Pris: 24900 kr
Boka

UTBILDNING
Systematiskt cyber- och informationssäkerhetsarbete för styrelse- och ledningsmedlemmar - med stöd av ISO 27000-serien
Kategori: utbildningar inom informationssäkerhet – cybersäkerhet ISO 27001 Vad önskar högsta ledningen få ut av organisa...
Pris: 10500 kr
Boka

Expertutbildning

UTBILDNING
Att hantera informationssäkerhetsrisker, inklusive incidenthantering och kontinuitet
Kategori: utbildningar inom informationssäkerhet – cybersäkerhet ISO 27001 För dig som berörs av NIS2-direktivet (svenska...
Pris: 24900 kr
Boka

sis

Frågestund

05.

Svenska Institutet för Standarder

Tack för att ni har lyssnat!

Kontaktuppgifter

utbildning@sis.se
08-555 522 00

Utbildningsrådgivare

nannie.krantz@sis.se
sofia.roberg@sis.se

En samlande kraft för ett konkurrenskraftigt Sverige