NIS2 och cybersäkerhetslagen – en uppdatering

Björn Sjöholm

bear@unidot.se

NIS2 och cybersäkerhetslagen – en uppdatering

” NIS2-direktivet för kritiska verksamheter i EU har trätt i kraft och kommer genomföras i svensk lagstiftning med en kommande cybersäkerhetslag. Lagstiftningen kommer bland annat gälla lärosäten och offentlig förvaltning. Här presenteras en uppdatering om vad NIS2 och cybersäkerhetslagen innebär för lärosäten och hur man kan arbeta med efterlevnad av lagarna.”

Björn Sjöholm

Cyber Security Entrepreneur

bear@unidot.se

Business leader, Advisor, Auditor, Trainer
Cyber Security, IT-Security, Information Security

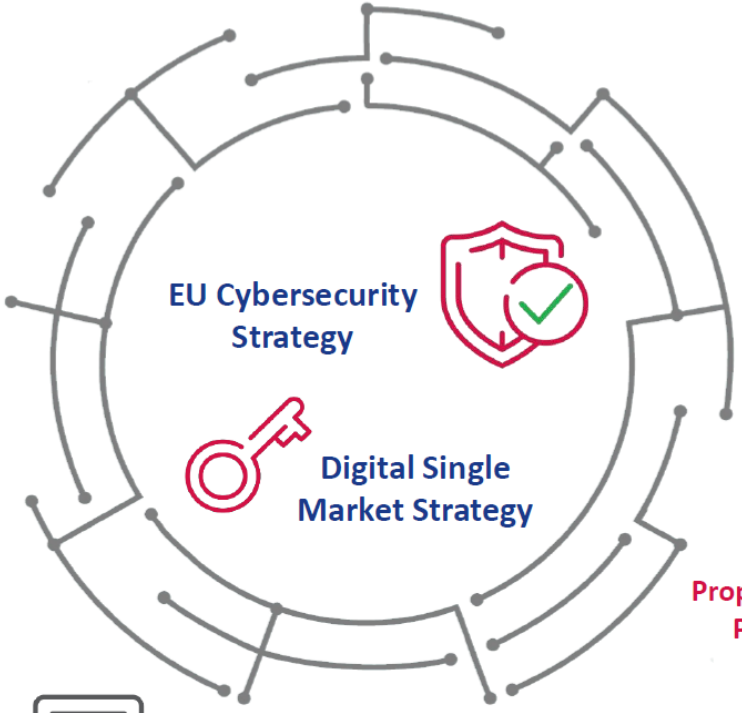
M.Sc. Comp.Sci.
CISA, CISM, CRISC, CGEIT, CDPSE, CISSP
ISO 27001 Lead Auditor, Kantara Accredited Assessor

Linkedin: linkedin.com/in/bjornsjoholm

unidot

seadot
CYBERSECURITY

EU Cybersecurity legislation



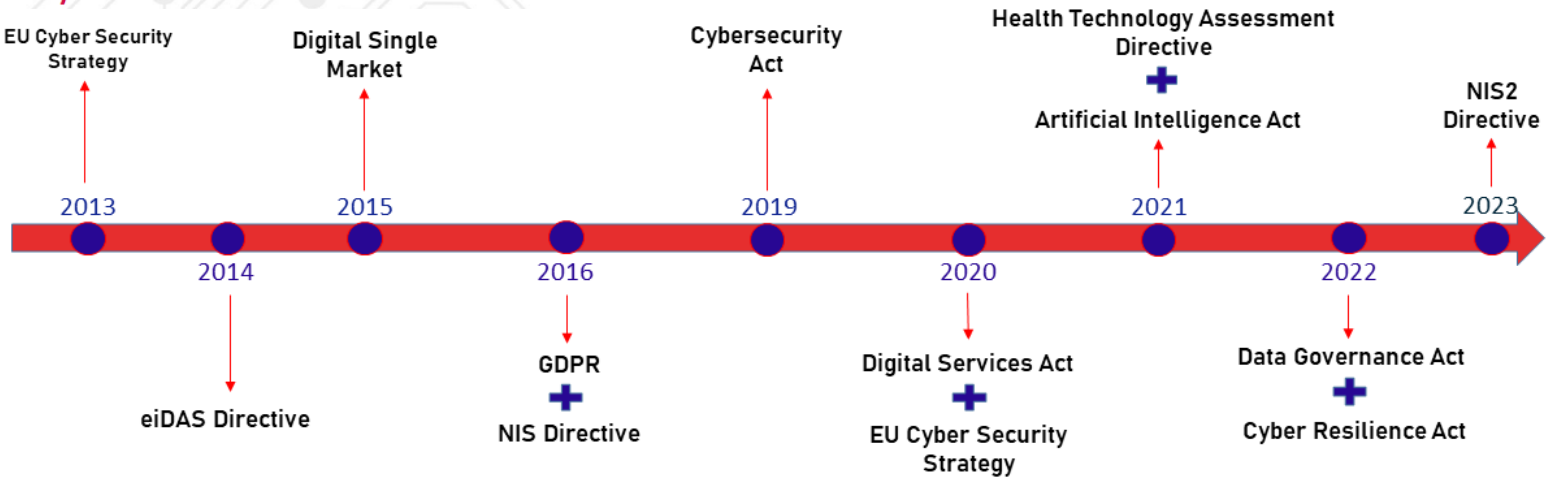
Network and Information Security Directive

eIDAS Regulation

Payment Services Directive 2

General Data Protection Regulation

Proposal for a Regulation on Privacy and Electronic Communications



Agenda

- Vem / Vad berörs?
- Ansvar / Sanktion
- Vad är kraven?
- När gäller lagstiftningen?
- Hur efterlever en organisation?

- Bonus:
  - Angränsande lagstiftningar
  - Vad är regelefterlevnad / compliance egentligen?

Vem / Vad berörs

Vem / Vad berörs – NIS2

Vilka organisationer berörs:

- Högkritiska sektorer:
  - energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster, offentlig förvaltning, rymden.
- Kritiska sektorer
  - post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, digitala leverantörer och forskning, samt lärosäte med examenstillstånd.
- Myndigheter och regioner
- Om verksamheten träffas av CER

- Vad berörs:
- Cybersäkerhet för att skydda nätverks- och informationssystem.

Storlekskrav:

- Fler än 50 anställda eller omsättning över 10 M €

Undantag från NIS2

Om annan författning gäller, som t.ex.

- Säkerhetskänslig verksamhet
- Brottsbekämpande verksamhet
- DORA-förordningen (finansiell verksamhet)

Leveranskedjan

NIS2

- Säkerhet i leveranskedjan är ett minimikrav.
- Leveranskedjan, inbegripande säkerhetsaspekter mellan verksamhetsutövare och dess direkta leverantörer eller tjänsteleverantörer.

Ansvar / Sanktion

Ansvar / Sanktion

NIS2

- Sanktionsavgift: (förslag)
- För väsentiga verksamhetsutövare:
  - Lägst 5 000 SEK
  - Max det högsta av: 10 M €, eller
  - 2% av global årsomsättning, eller
- För viktiga verksamhetsutövare:
  - Lägst 5 000 SEK
  - Max det högsta av: 7 M €, eller
  - 1,4% av global årsomsättning, eller
- För offentliga verksamhetsutövare:
  - lägst 5 000 SEK eller högst 10 MSEK
- Personligt ansvar för ledningsorgan

Vad är kraven?

Mål

Skydda nätverks- och informationssystem

Skydda systemens fysiska miljö

Vad är kraven – NIS2

- Verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.
  - Kräver inte specifikt exempelvis ISO 27001.
  - Föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete kan komma.
- Åtgärder ska vara proportionella
- Föreskriftsrätt per sektor
- Inga kravställda baskrav inom exempelvis IT-säkerhet i Sverige

Artikel 21, …. åtgärder … ska minst inbegripa:

a) strategier för riskanalys och informationssystemens säkerhet,

b) incidenthantering,

c) driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering,

d) säkerhet i leveranskedjan, …

e) säkerhet vid förvärv, utveckling och underhåll …, inbegripet hantering av sårbarheter och sårbarhetsinformation,

f) strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna …

g) grundläggande praxis för cyberhygien och utbildning i cybersäkerhet

h) strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering,

i) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,

j) användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering … och säkrade nödkommunikationssystem….

Cybersäkerhetslagen (3 kap 1 §)

- Krav på riskhantering genom:
  1. incidenthantering,
  2. kontinuitetshantering
  3. säkerhet i leveranskedjan,
  4. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation,
  5. strategier och förfaranden för användning av kryptografi och kryptering,
  6. personalsäkerhet,
  7. strategier för åtkomstkontroll och tillgångsförvaltning,
  8. säkrade lösningar för kommunikation,
  9. lösningar för autentisering.

Incidentrapportering

Rapporteringsskyldighet vid betydande incident

Orsakat eller kan orsaka allvarlig störning

Påverkat eller kan påverka betydande materiell eller immateriell skada

När gäller lagstiftningen

När gäller lagstiftningen

NIS2

- Medlemsländerna ska anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. Bestämmelserna ska tillämpas från den 18 oktober 2024.
- Inga övergångsbestämmelser finns i direktivet
- Genomförandeförordning för NIS2 gäller från 7e november

Cybersäkerhetslagen (förslag)

- Den svenska genomförandelagen
- (förslag) Cybersäkerhetslagen och cybersäkerhetsförordningen, antas tidigast under våren 2025
- (förslag) Ändringarna i lag (2006:24) om nationella toppdomäner, antas tidigast under våren 2025

Tillsynsmyndigheter

- Statens energimyndighet (Energimyndigheten)
  - Energi
  - Transportstyrelsen
  - Transporter
  - Tillverkning av motorfordon, släpfordon, påhängsvagnar och andra transportmedel
- Finansinspektionen
  - Bankverksamhet
  - Finansmarknadsinfrastruktur
- Inspektionen för vård och omsorg (IVO)
  - Vårdgivare inom hälso- och sjukvårdssektorn
- Läkemedelsverket
  - Hälso- och sjukvårdssektorn, med undantag för vårdgivare
  - Tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik
- Livsmedelsverket
  - Avloppsvatten
  - Dricksvatten
  - Produktion, bearbetning och distribution av livsmedel
- Post- och telestyrelsen (PTS)
  - Digital infrastruktur
  - Digitala leverantörer
  - Förvaltning av IKT-tjänster
  - Post- och budtjänster
  - Rymden
- Länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län
  - Avfallshantering
  - Forskning
  - **Lärosäten med examenstillstånd**
  - Offentligförvaltning
  - Tillverkning, produktion och distribution av kemikalier
  - Tillverkning av datorer, elektronikvarorochoptik
  - Tillverkning av elapparatur
  - Tillverkning av övriga maskiner

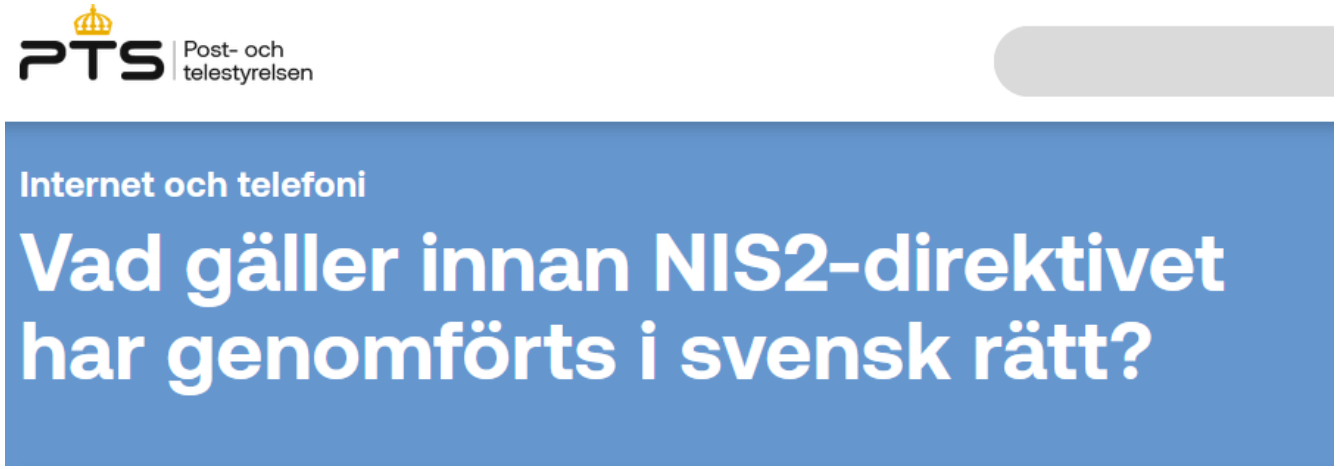
Utmaningar NIS2 – Svenskt perspektiv

- Tillsyn och sektorsspecifika föreskrifter från flera tillsynsmyndigheter
  - Komplicerat om man har verksamhet i olika sektorer
- Gränsdragning mot säkerhetsskyddslagen
- Egen bedömning om vilken verksamhet som berörs

- Cybersäkerhetslagen inte beslutad av Riksdagen ännu

NIS - Vad gäller just nu?

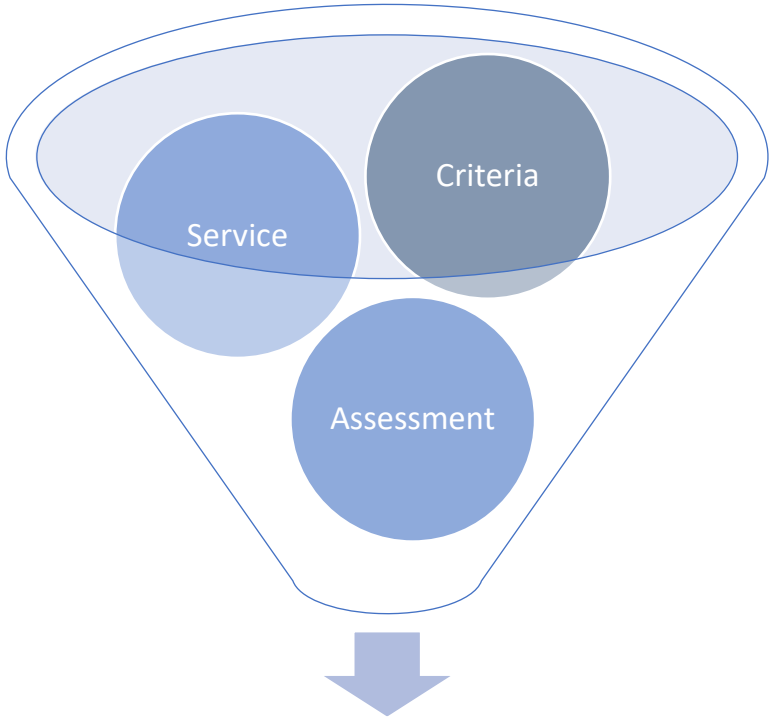
- EU-kommissionens genomförandeförordning för NIS2 gäller från 7e november 2024.
  - Gäller riskhanteringsåtgärder och incidentrapporteringskrav.
- Verksamhetsutövare som omfattas NIS (1):
  - måste uppfylla motsvarande skyldigheter i NIS2 och NIS2 genomförandeförordning
- Verksamhetsutövare som inte omfattas av NIS, men av NIS2:
  - Omfattas inte av NIS2 till dess cybersäkerhetslagen träder i kraft



Vad är compliance?

… eller regulatorisk efterlevnad

Compliance & Trust



Trusted Service

Compliance is handling another party's risk

Adhering to requirements or set of controls in a standard, contract or regulation

Hur efterlever en organisation?

NIS2 och angränsande regelverk

Ledningssystem för informationssäkerhet

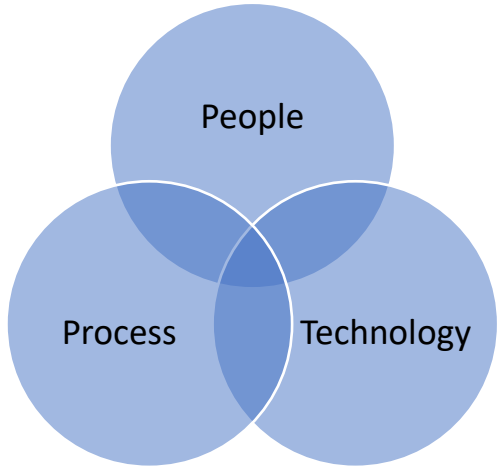
Fokus i regelverk som NIS2 och CRA, CER, etc

- Fokus på säkerhet (före funktion)
- Regulatorisk risk
- Incidenthantering
- Riskhantering
- Leverantörskedjan

Utmaningar för NIS2

- Förståelse för konsekvenserna för organisationen
  - Regelefterlevnad
  - Risker för verksamheten och regulatorisk risk
  - Säkerhet
- Incidenthantering
- Leverantörskedjan

Compliance management



Your Compliance Activities

Scope

- Critical services
- Covered by other legislation

Maturity analysis

- How do we comply today?
- Starting point for due diligence

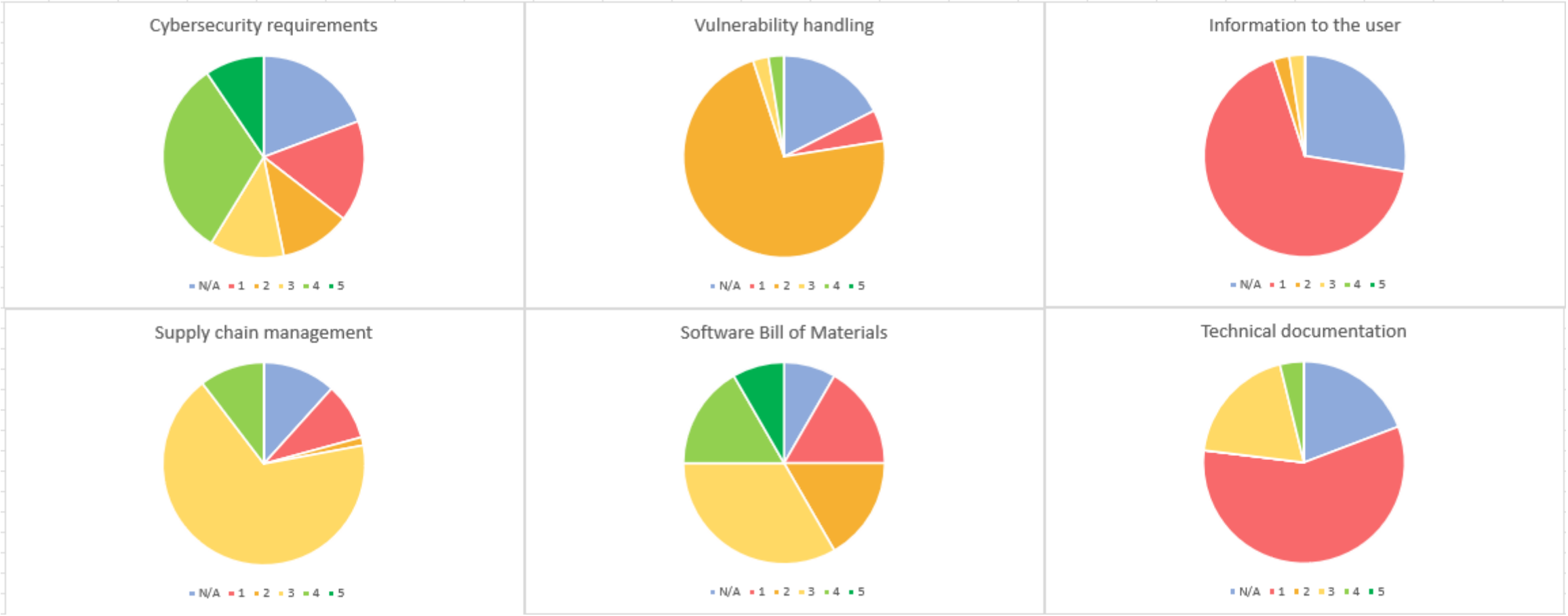
Compliance project

- Management support, Risk Management
- Incident management
- Third party and Supply chain management. Technical documentation
- Information to users

Maintenance

- Management system implementation and integration

Example gap/maturity assessment



ISO 27001

LIS – Ledningssystem för informationssäkerhet

ISO 27001

ISO 27001 includes mandatory requirements covering:

- Context of organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

ISO 27001 (appendix A) also includes 93 controls in the areas:

- Organizational controls
- People controls
- Physical controls
- Technological controls

ISO 27002 could be used to better understand the controls in appendix A of ISO 27001

Implementera 27001

- 11 Clauses (actually 7)
- 93 Security Controls
- + Contractual obligations
- + Regulatory requirements

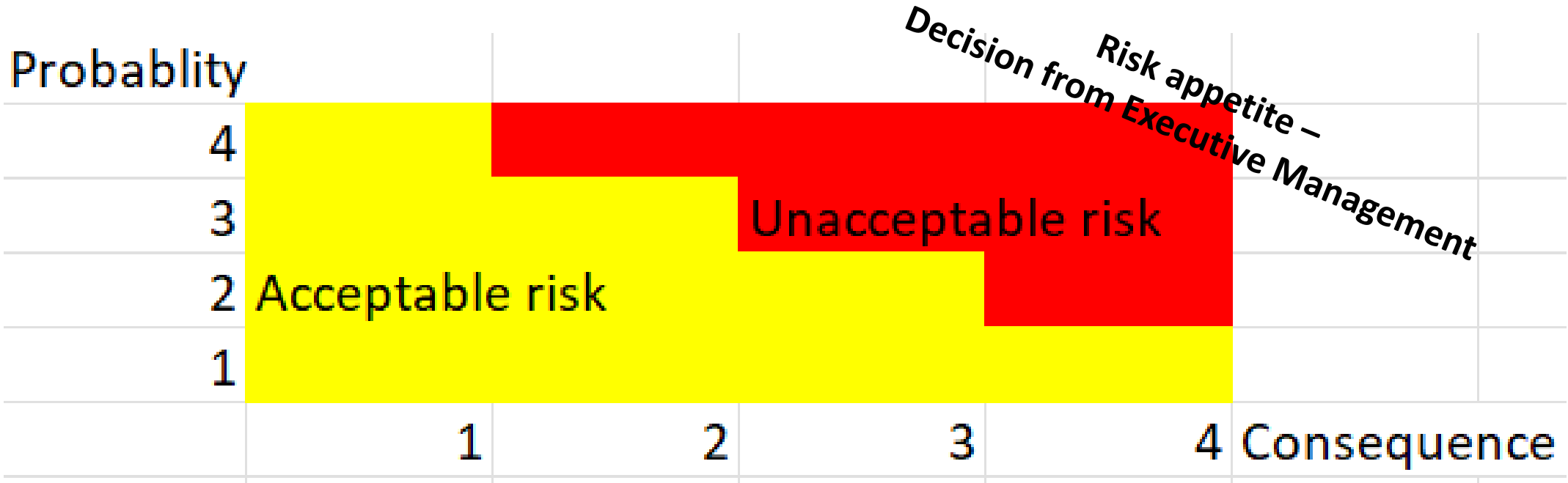
SOA

Risk Management

Risk treatment:

- Risk mitigation
- Risk transfer
- Risk acceptance
- Risk avoidance

Risk appetite and Risk acceptance



Frågor?

NIS2 och cybersäkerhetslagen – en uppdatering

Björn Sjöholm

bear@unidot.se