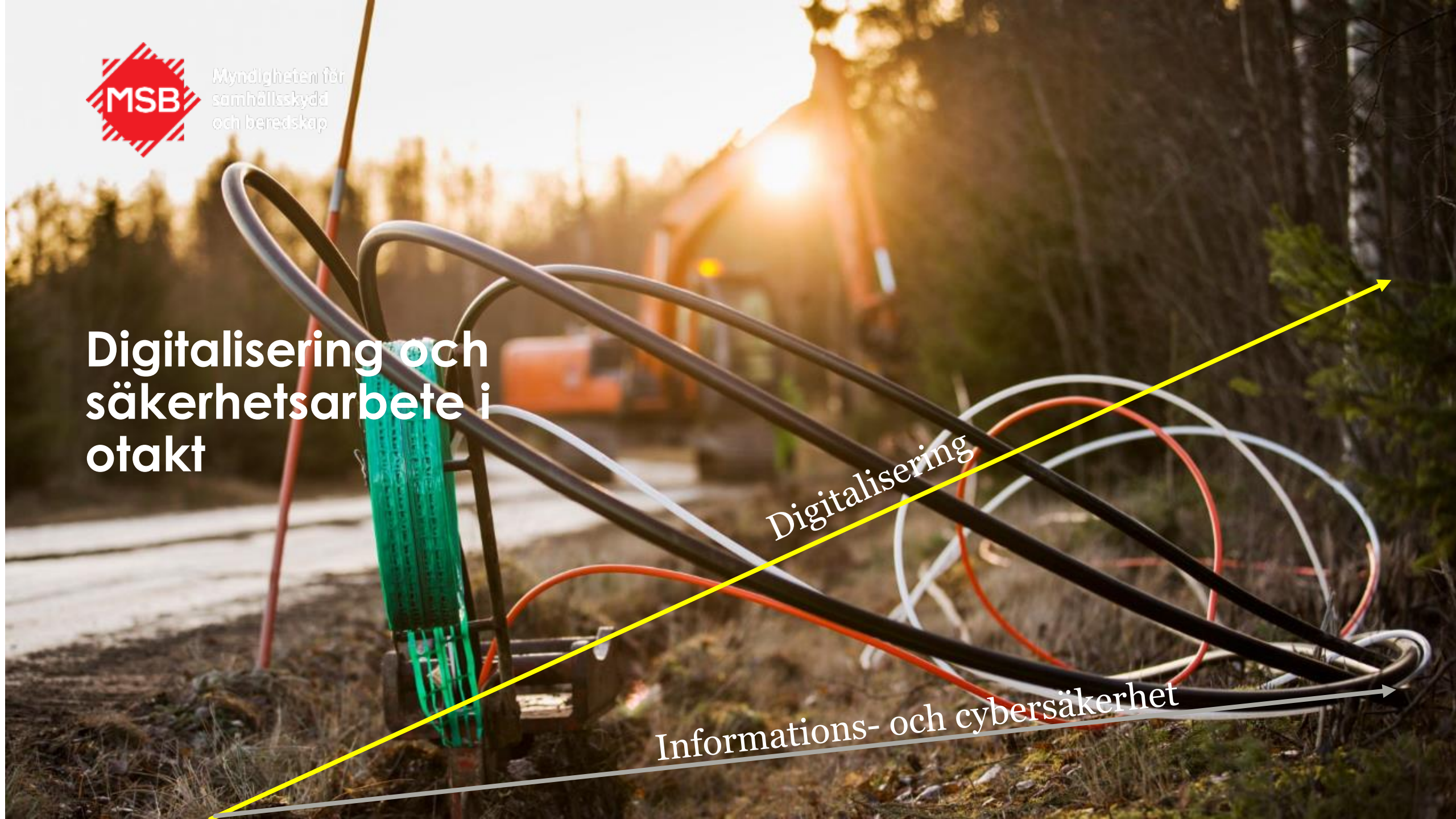
NIS-reglering

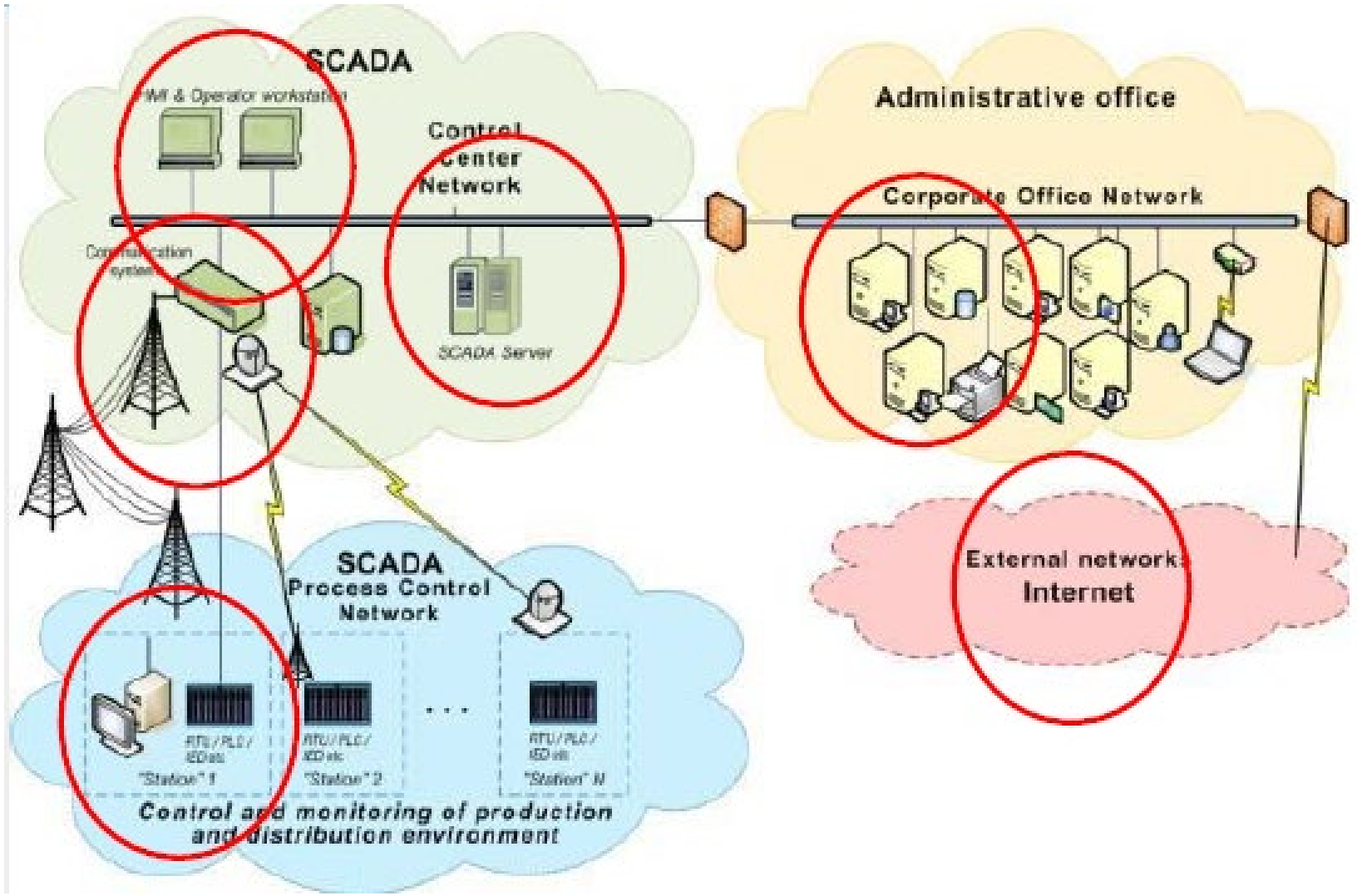
Jan-Olof.Olsson@msb.se

Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap

Digitalisering och säkerhetsarbete i otakt




SCADA
HMI & Operator workstation
Control Center Network
Communication system
SCADA Server
Administrative office
Corporate Office Network
External networks
Internet
SCADA
Process Control Network
RTU / PLC / IED etc.
"Station" 1
"Station" 2
"Station" N
Control and monitoring of production and distribution environment

Övergripande syftet med NIS-direktivet

Nätverks- och informationssystem spelar en viktig roll i samhället. Deras tillförlitlighet och säkerhet är grundläggande för ekonomisk och samhällelig verksamhet och i synnerhet för den inre marknadens funktion.

Krav på medlemsstaterna

Anta en nationell strategi

Nationell strategi för säkerhet i nätverk och informationssystem

- Handlingsplan framtagen av MSB och SAMFI-myndigheterna

Hantera incidenter

Inrätta en organisation för hantering av incidenter, CSIRT

Samarbeta inom EU

- Utse nationell kontaktpunkt för gränsöverskridande samarbete
- Delta i operativt och strategiskt samarbete
- Informera om gränsöverskridande incidenter

Redovisa till EU

- En förteckning över samhällsviktiga tjänster och antalet leverantörer
- En årlig rapport över inrapporterade incidenter

Rapportering

NUMBER OF OPERATORS AND INDICATION OF THEIR IMPORTANCE 5.7 (C)		
Sector*	Name/Title of the Essential Service	April 2019
Energy - Electricity	Energy - Electricity TSO	0
Energy - Electricity	Energy - Electricity DSO	44
Energy - Electricity	Energy - Electricity Production	5
Energy - Electricity	Energy - Electricity sale	2
Energy - Gas	Energy - Gas TSO	1
Energy - Gas	Energy - Gas DSO	3
Energy - Gas	Energy - Gas sale	5

Myndigheten för samhällsskydd och beredskap

Två kategorier av tjänster

Samhällsviktiga tjänster

- Energi
- Transporter
- Bankverksamhet
- Finansmarknads-infrastruktur
- Hälso- och sjukvård
- Leverans och distri-bution av dricksvatten
- Digital infrastruktur

Digitala tjänster

- Internetbaserad marknadsplats
- Molntjänst
- Internetbaserad sökmotor

Lag, förordning och föreskrifter

Lagen om informationssäkerhet i samhällsviktiga och digitala tjänster (SFS 2018:1174)

Förordning om informationssäkerhet i samhällsviktiga och digitala tjänster (SFS 2018:1175)

MSB:s föreskrifter om

- identifiering leverantörer av samhällsviktiga tjänster
- Informationssäkerhet
- incidentrapportering

Tillsynsmyndigheterna och Socialstyrelsen får meddela sektorsspecifika föreskrifter om säkerhetsåtgärder

Tillsynsmyndigheter

Sektor	Tillsynsmyndighet
Energi	Statens energimyndighet
Transport	Transportstyrelsen
Bankverksamhet	Finansinspektionen
Finansmarknadsinfrastruktur	Finansinspektionen
Hälso- och sjukvårdssektorn	Inspektionen för vård och omsorg
Leverans och distribution av dricksvatten	Livsmedelsverket
Digital infrastruktur	Post- och telestyrelsen

För digitala tjänster är Post- och telestyrelsen tillsynsmyndighet.

5. Bilaga 1, Checklista

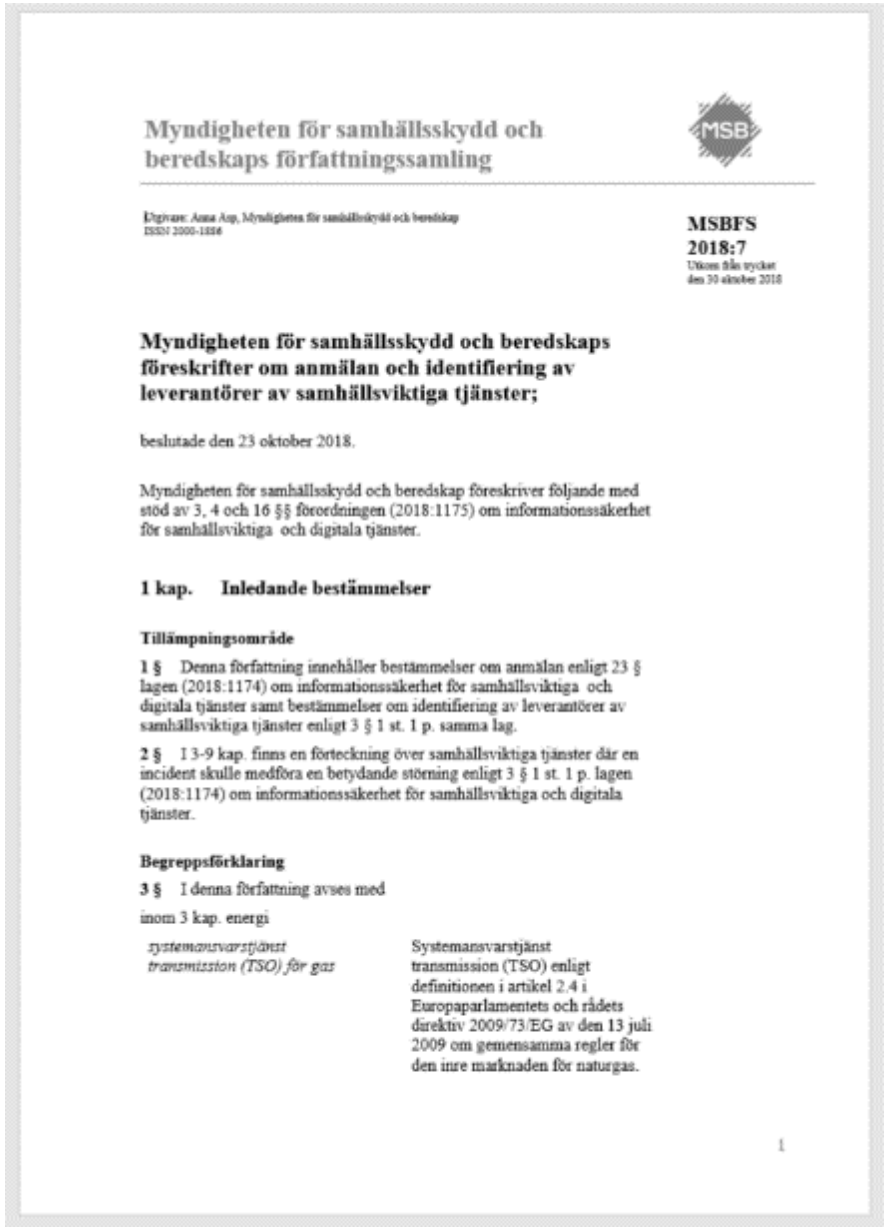
Här följer en checklista för om en leverantör berörs av NIS-regleringen eller inte. Besvaras punkterna 1-5 med ja berörs leverantören av NIS regleringen. Ett nej innebär att leverantören inte berörs av NIS regleringen. Hänvisningar till kapitel i denna vägledning med mer information.

1. Är etablerad i Sverige enligt 2.2.1.
2. Verksam inom sektor enligt kap 2.2.2.
3. Levererar tjänst(er) beskriven i kap 3.
4. Är beroende av nätverk och informationssystem för att leverera tjänsten enligt kap 2.2.4.
5. En incident i nätverk och informationssystem skulle medföra en betydande störning vid tillhandahållandet av tjänsten enligt kap 2.2.5.

Om leverantören svarar ja på punkterna 1-5 ska leverantören:

6. Utreda om någon, och i så fall vilka, delar av den samhällsviktiga tjänsten som omfattas av säkerhetsskydd.
7. Anmäla enligt kap 2.3 att organisationen identifierat sig enligt MSB:s föreskrifter som leverantör av samhällsviktig tjänst.
8. Bedriva ett systematiskt och riskbaserat säkerhetsarbete.
9. Aktivera incidentrapporteringskonto hos MSB (MSB kontaktar den person eller de personer som anmälts i p 7 ovan).

MSBFS 2018:7



Myndigheten för samhällsskydd och beredskaps författningssamling

Utgivare: Anna Asp, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

MSBFS 2018:7
Utkom från trycket den 30 oktober 2018

Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster;

beslutade den 23 oktober 2018.

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.

Begreppsförklaring

3 § I denna författning avses med

inom 3 kap. energi

systemansvarstjänst transmission (TSO) för gas	Systemansvarstjänst transmission (TSO) enligt definitionen i artikel 2.4 i Europaparlamentets och rådets direktiv 2009/73/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för naturgas.

1

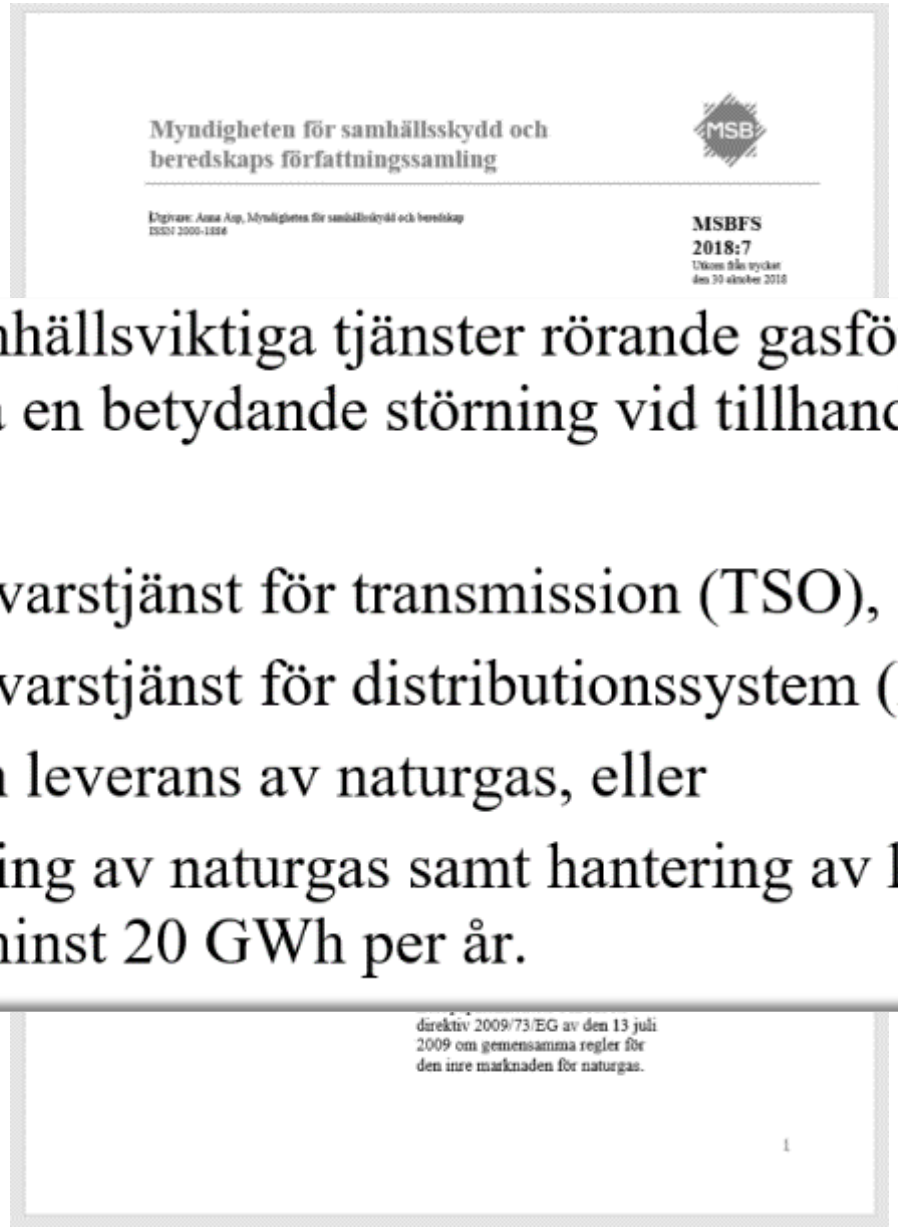
Begreppsförklaring

3 § I denna författning avses med

inom 3 kap. energi

systemansvarstjänst transmission (TSO) för gas	Systemansvarstjänst transmission (TSO) enligt definitionen i artikel 2.4 i Europaparlamentets och rådets direktiv 2009/73/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för naturgas.

3 kap. Energi


Myndigheten för samhällsskydd och beredskaps författningssamling

MSB

Utgivare: Anna Asp, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1836

MSBFS 2018:7
Utkom från trycket den 30 oktober 2018

direktiv 2009/73/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för naturgas.

1

3 § Med samhällsviktiga tjänster rörande gasförsörjningen där incidenter skulle medföra en betydande störning vid tillhandahållandet av tjänsten avses

1. systemansvarstjänst för transmission (TSO),
2. systemansvarstjänst för distributionssystem (DSO),
3. handel och leverans av naturgas, eller
4. kondensering av naturgas samt hantering av kondenserad naturgas som omfattar minst 20 GWh per år.

Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap

Datum	Diarienr	Utgåva
2018-12-24	2018-11619	1.2

Vägledning för anmälan och identifiering av leverantörer av samhällsviktiga tjänster enligt NIS-regleringen

Myndigheten för samhällsskydd och beredskap

Även gas kan i vissa fall hanteras i flytande form, exempelvis LPG eller LBG, men i NIS regleringen behandlas de produkterna som gas.

3 § Med samhällsviktiga tjänster rörande gasförsörjningen där incidenter skulle medföra en betydande störning vid tillhandahållandet av tjänsten avses

1. systemansvarstjänst för transmission (TSO),
2. systemansvarstjänst för distributionssystem (DSO),
3. handel och leverans av naturgas, eller
4. kondensering av naturgas samt hantering av kondenserad naturgas som omfattar minst 20 GWh per år.

I enlighet med gasmarknadsdirektivet inkluderas även biogas i begreppet naturgas. Anläggningar för gas som används som en intern tjänst inom industriområde betraktas inte som samhällsviktig tjänst.

3.6 Leverans och distribution av dricksvatten

1 § Med samhällsviktiga tjänster avseende leverans och distribution av dricksvatten där incidenter skulle medföra en betydande störning vid tillhandahållandet av tjänsten avses

1. leveranser av dricksvatten som en huvudman enligt 2 § lagen (2006:412) om allmänna vattentjänster tillhandahåller
   a) minst 20 000 personer, eller
   b) akutsjukhus.

En huvudman för vattenproduktion/distribution kan ha flera nät som vardera försörjer färre än 20 000 personer, men det är huvudmannens totala leverans som ska utgöra grunden för om aktören berörs av NIS regleringen eller inte. Som beräkningsnyckel kan en förbrukning av 200 liter/dygn räknas som en person.

Akutsjukhus definieras som ”vårdinrättning som är inrättad för sluten vård och som har särskild akutmottagning för den som behöver omedelbar hälso- och sjukvård”.

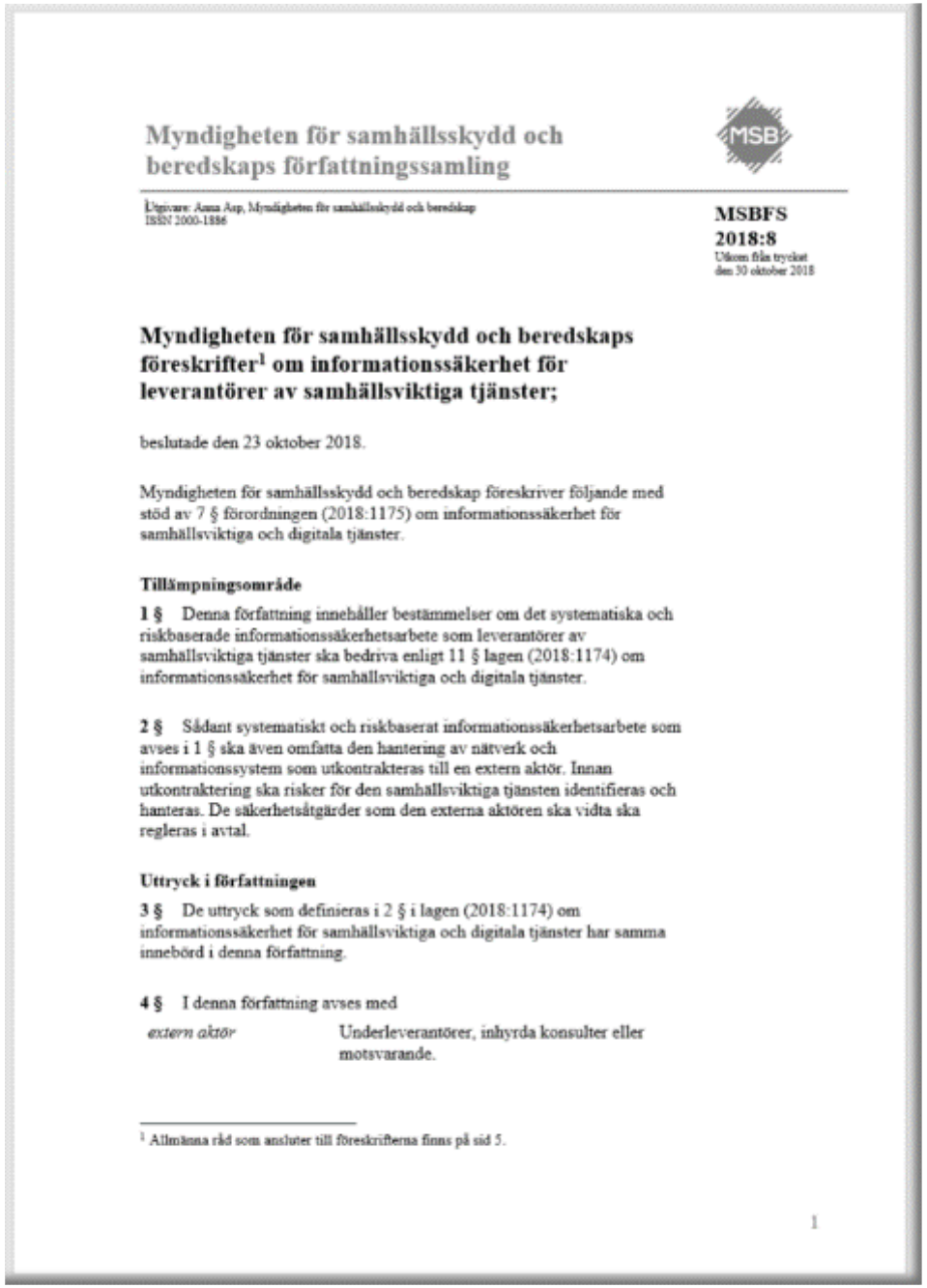
Anmälan

- Leverantörer anmäler sig till TM
- MSB autentiserar kontaktansvariga
- MSB tar emot kontaktuppgifter för rapportörer
- MSB skapar konton för rapportering och skickar ut certifikat

Systematiskt informationssäkerhetsarbete och användning av standarder

- Lagen anger att leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete MSB:s föreskrifter beskriver i mer detalj vad detta innebär.
- Informationssäkerhetsarbetet ska bedrivas med stöd av standarderna om ledningssystem för informationssäkerhet (SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017) eller motsvarande.
- I detta ingår att sätta informationssäkerhetsmål, klassa sin information, göra riskanalys med mera.
- Genom att följa MSB:s metodstöd för systematiskt informationssäkerhetsarbete kommer man att uppfylla kraven i regleringen.
- Kraven gäller även vid utkontraktering.
- För digitala tjänster är kraven annorlunda och beskrivs i EU:s kommissionens så kallade genomförandeförordning

MSBFS 2018:8



Myndigheten för samhällsskydd och beredskaps författningssamling

Utgivare: Anna Aap, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

MSBFS 2018:8
Utkom från trycket den 30 oktober 2018

Myndigheten för samhällsskydd och beredskaps föreskrifter[1] om informationssäkerhet för leverantörer av samhällsviktiga tjänster;

beslutade den 23 oktober 2018.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 7 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Tillämpningsområde

1 § Denna författning innehåller bestämmelser om det systematiska och riskbaserade informationssäkerhetsarbete som leverantörer av samhällsviktiga tjänster ska bedriva enligt 11 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

2 § Sådant systematiskt och riskbaserat informationssäkerhetsarbete som avses i 1 § ska även omfatta den hantering av nätverk och informationssystem som utkontrakteras till en extern aktör. Innan utkontraktering ska risker för den samhällsviktiga tjänsten identifieras och hanteras. De säkerhetsåtgärder som den externa aktören ska vidta ska regleras i avtal.

Uttryck i författningen

3 § De uttryck som definieras i 2 § i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster har samma innebörd i denna författning.

4 § I denna författning avses med

extern aktör	Underleverantörer, inhyrda konsulter eller motsvarande.

[1] Allmänna råd som ansluter till föreskrifterna finns på sid 5.

1

Myndigheten för samhällsskydd och beredskap

MSBFS 2018:8

Föreskrifter informationssäkerhet för leverantörer av samhällsviktiga tjänster

Tillämpningsområde

2§ Utkontraktering

3-4§ Begrepp

Systematiskt och riskbaserat informationssäkerhetsarbete

5§ Arbeta med stöd av SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002

6§ Intern ledning och styrning

Närmare krav på informationssäkerhetsarbetet

7§ Styrande dokument – policy och andra interna regler

8§ Systematiskt arbetssätt -informationsklassning, riskbedömning, val av säkerhetsåtgärder

9§ Kunskap och kompetens

Särskilt om nätverk och informationssystem

10§ Informationssäkerhet för nätverk och informationssystem

11§ Incidenthantering

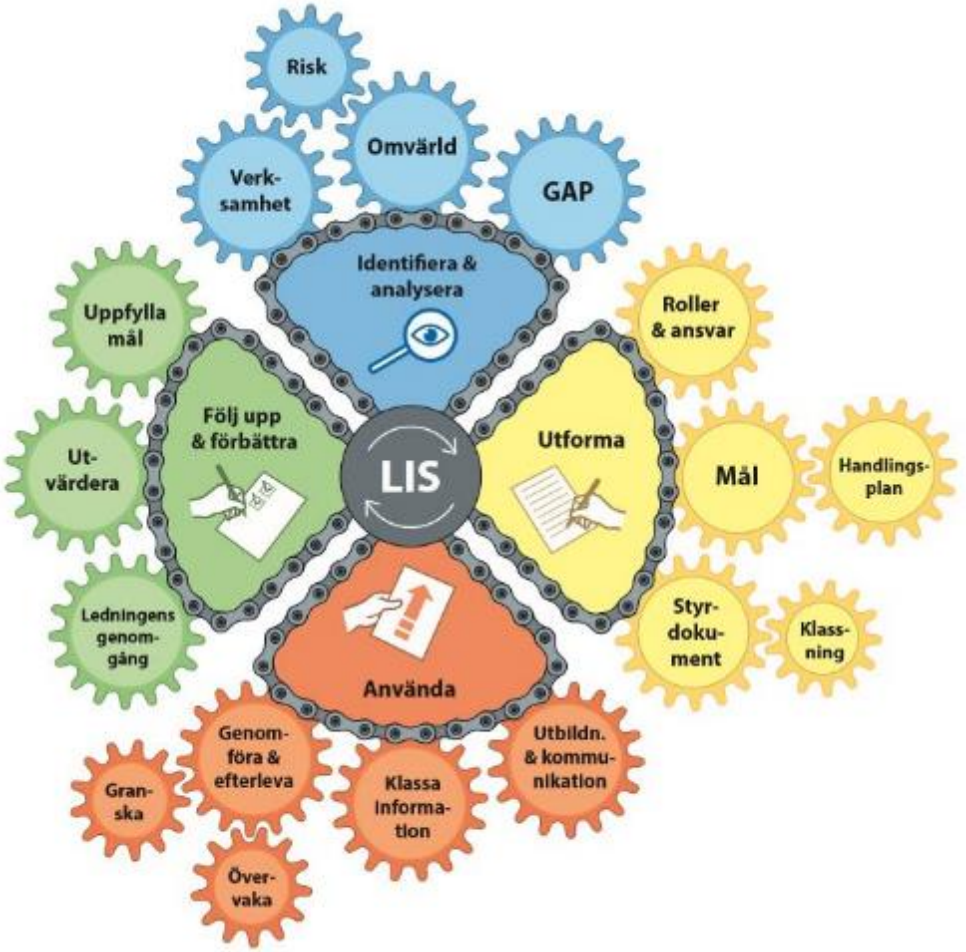
12§ Kontinuitetshantering

MSB's metodstöd för systematiskt informations-säkerhetsarbe

Metodstödet vänder sig till de som arbetar med informationssäkerhet i en organisation

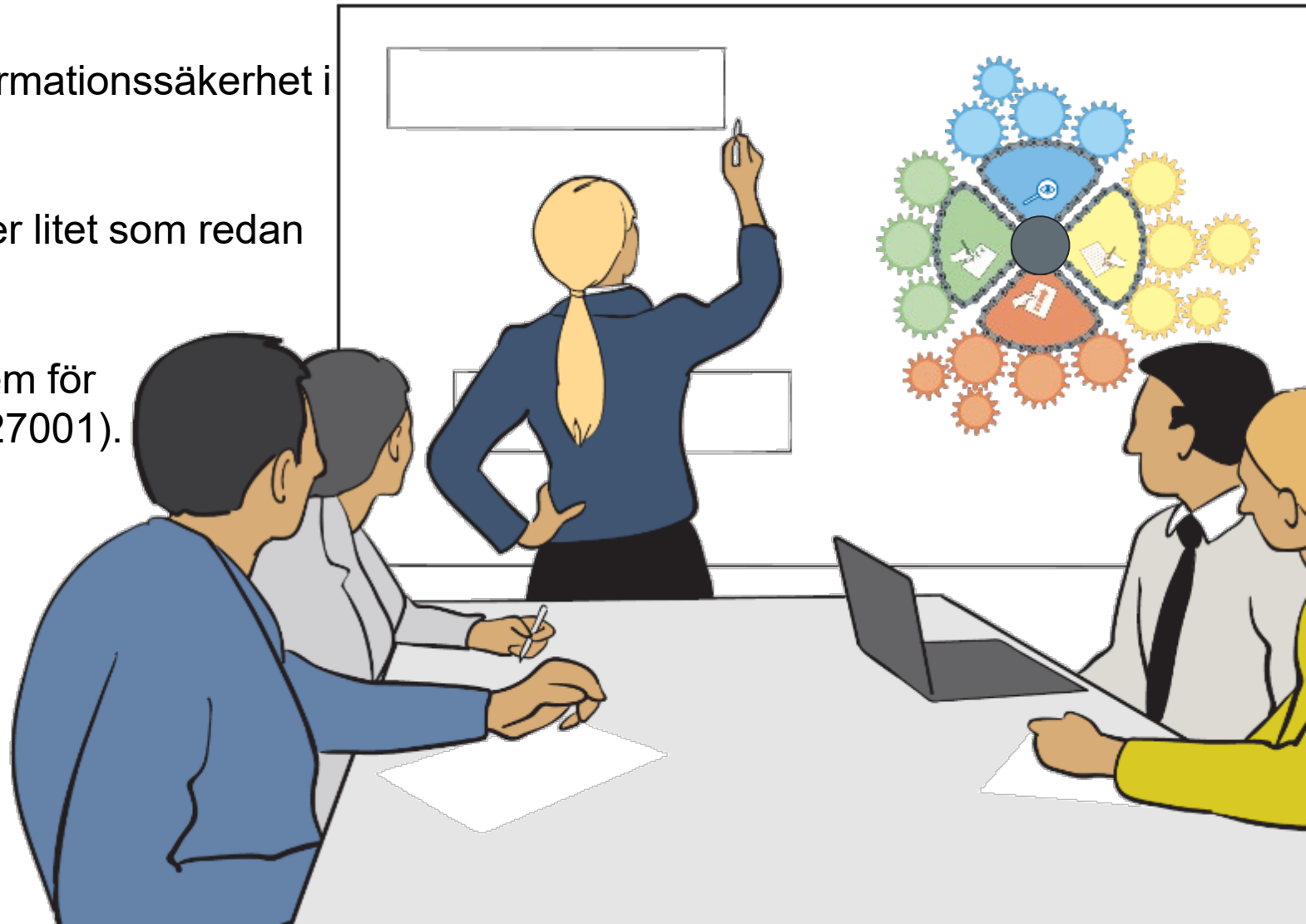
”Från principer till checklistor”

www.informationssäkerhet.se



Metodstöd för systematiskt informationssäkerhetsarbete

- Vänder sig till dig som arbetar med informationssäkerhet i en organisation
- Går att använda oavsett hur mycket eller litet som redan är gjort i din organisation
- Utgår från standarden för ledningssystem för informationssäkerhet (SS-EN ISO/IEC 27001).



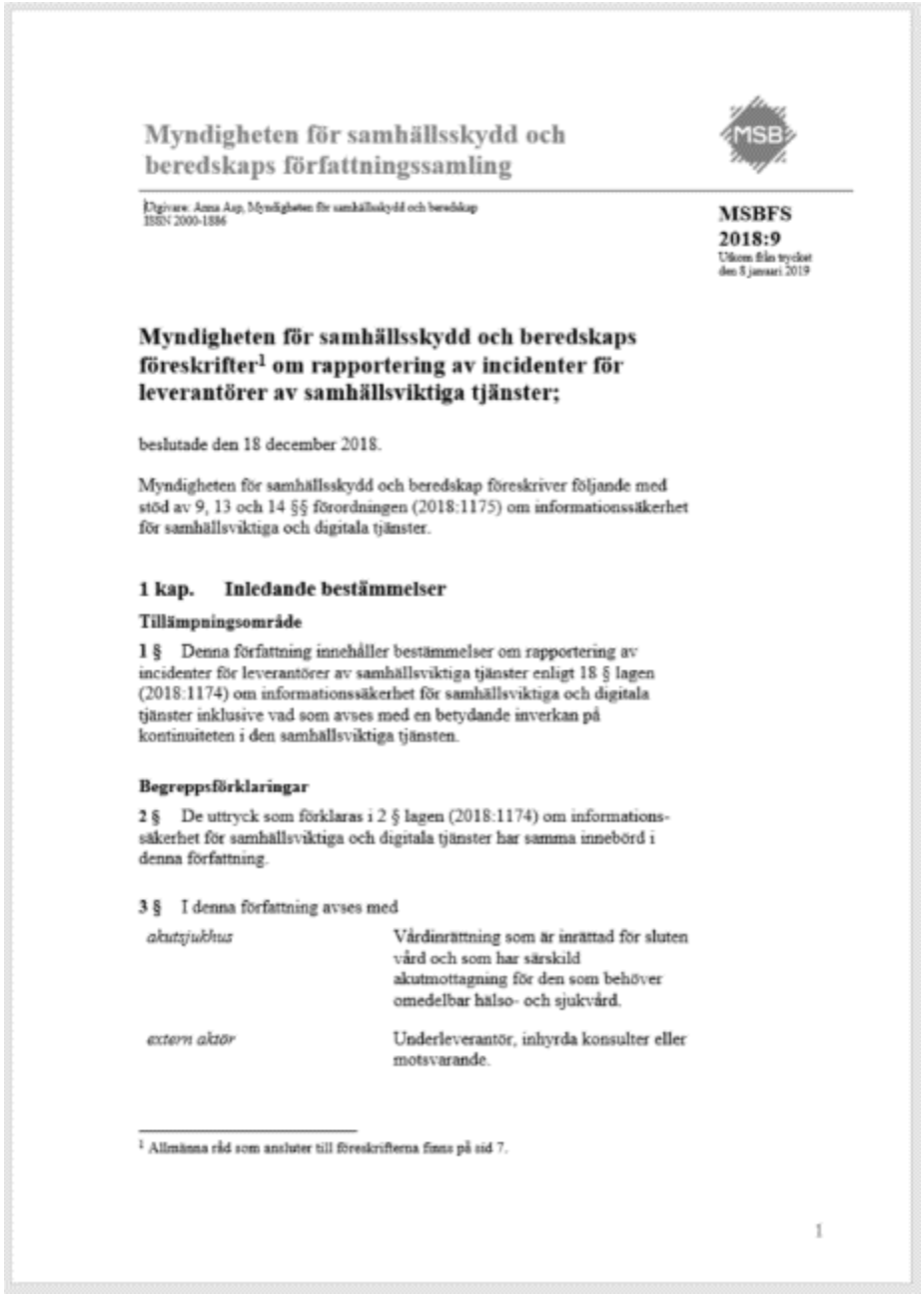
För dig som vill veta mer

Du hittar metodstödet på Informationssäkerhet.se

Skicka frågor och synpunkter till

metodstod@informationssakerhet.se

MSBFS 2018:9



Myndigheten för samhällsskydd och beredskaps författningssamling

Utgivare: Anna Aap, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

MSBFS 2018:9
Utkom från trycket den 8 januari 2019

Myndigheten för samhällsskydd och beredskaps föreskrifter[1] om rapportering av incidenter för leverantörer av samhällsviktiga tjänster;

beslutade den 18 december 2018.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 9, 13 och 14 §§ förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Denna författning innehåller bestämmelser om rapportering av incidenter för leverantörer av samhällsviktiga tjänster enligt 18 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster inklusive vad som avses med en betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten.

Begreppsförklaringar

2 § De uttryck som förklaras i 2 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster har samma innebörd i denna författning.

3 § I denna författning avses med

akutsjukhus	Vårdinrättning som är inrättad för sluten vård och som har särskild akutmottagning för den som behöver omedelbar hälso- och sjukvård.
extern aktör	Underleverantör, inhyrda konsulter eller motsvarande.

[1] Allmänna råd som ansluter till föreskrifterna finns på sid 7.

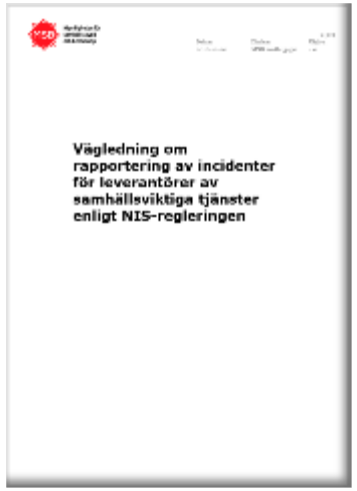
1

Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap

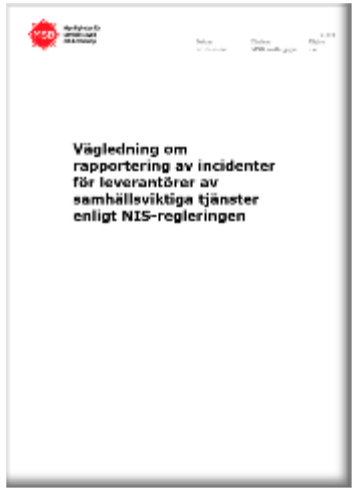
Begreppsförklaringar

incident	en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem
störning i den samhällsviktiga tjänsten	En konsekvens av incidenten som innebär att den samhällsviktiga tjänsten inte levereras i förhållande till normalt tillhandahållande



Innehållsförteckning

Myndigheten för samhällsskydd och beredskap



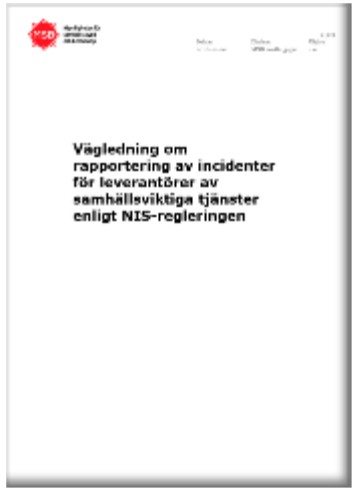
Gas

3 kap. 2 §

Leverantörer inom gasförsörjningen ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som

3. innebär risk för en händelse som resulterar i en avsevärd försämring av försörjningssituationen för gas,
4. kan leda till avbrott i gasförsörjningen, eller
5. har påverkat styrning och övervakning inom ramen för systemansvarstjänst.

Nedan följer ett antal exempel på incidenter som ska rapporteras. Exemplen ska inte ses som uttömmande.

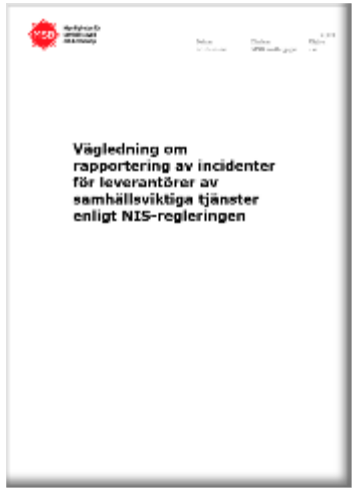


Aktör C är ett kommunalt bolag som äger naturgasledningar som ingår i det västsvenska naturgasnätet. Under en sommarnatt med liten förbrukning inträffar en it-incident som omöjliggör övervakningen av nätet under 4 h då personalen står helt utelåsta från systemet. I efterhand kan man se att flödet i ledningarna inte har påverkats.

- Avbrottet är rapporteringsskyldigt eftersom styrningen och övervakningen har påverkats.

Aktör D är en större gasleverantör till det västsvenska naturgasnätet, ett svenskt dotterbolag till en internationell koncern. Under en väldigt kall februaridag, mitt i arbetsveckan, får handlarna ett kommunikationsavbrott som leder till att de tappar marknadsövervakningen för spotmarknaden och möjligheten att handla under 12 h. Incidenten leder till att nomineringen för kommande dygn hos balansansvariga blir kraftigt missvisande.

- Avbrottet är rapporteringsskyldigt eftersom det har påverkat:
  - handel och leverans av naturgas,
  - det innebär risk för en händelse som resulterar i en avsevärd försämring av försörjningssituationen för gas, samt
  - styrningen och övervakningen har påverkats.



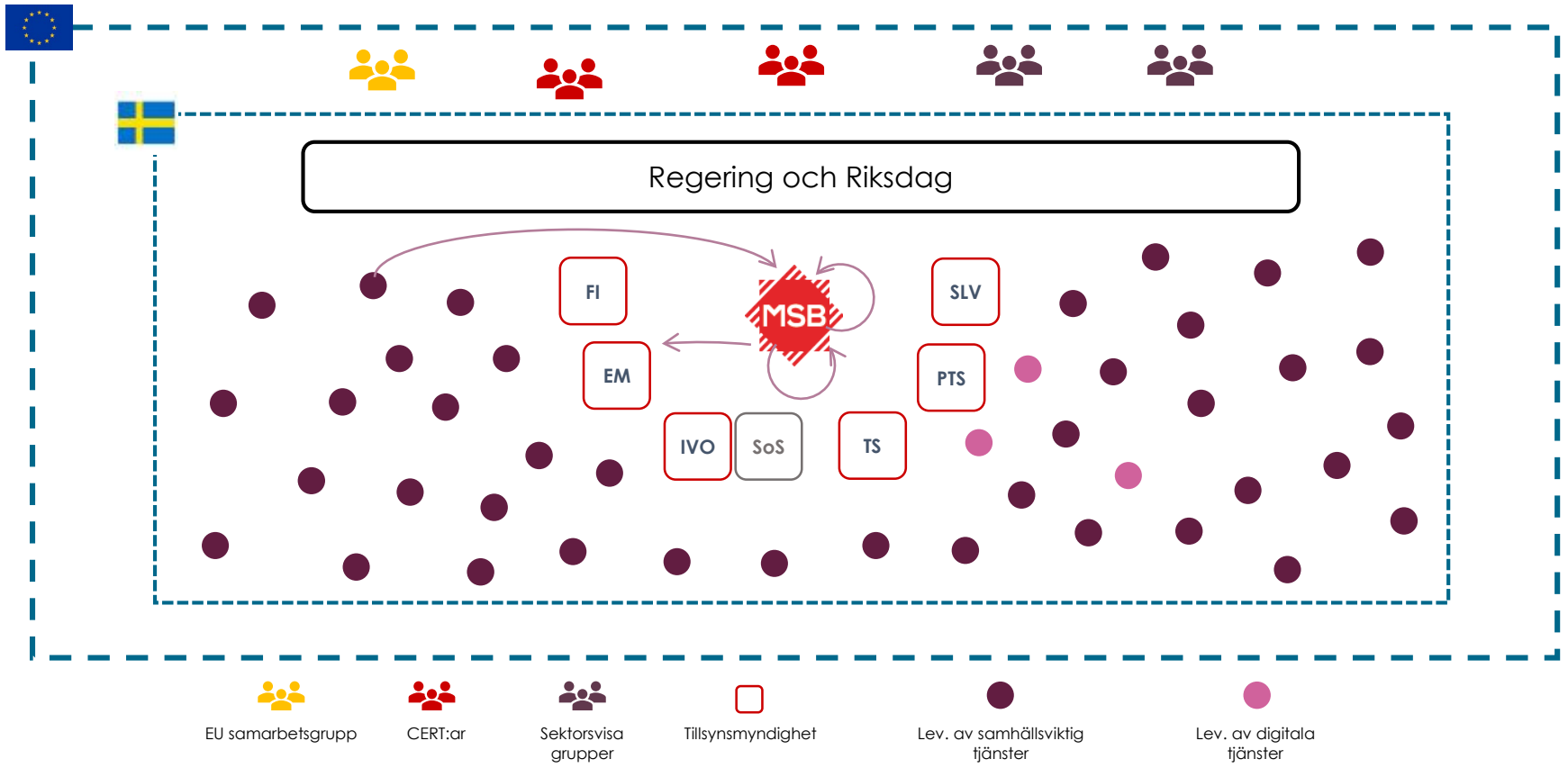
2. har påverkat styrning och övervakning av tjänsten.

Om övervakningen inte är kontinuerlig, ska påverkan bedömas i relation till när och hur övervakning sker i normalfallet.

Påverkan innebär inte enbart driftsavbrott. Beroende på systemets konstruktion finns en risk att felaktig funktion i styr- och reglersystemet skulle kunna både över- och underdosera kemikalier. Exempelvis kan underdosering vara problematiskt när det gäller klor eftersom en mikrobiologisk säkerhetsbarriär då slås ut. På motsvarande sätt kan felaktig funktion orsaka att pumpar antingen stannar eller kör så mycket att det skulle kunna orsaka tryckfall eller översvämningar i distributionen.

Syfte med incidentrapportering

- Förebygga och hantera
- Minska konsekvenser
- Skapa lägesbild
- Förbättra informationssäkerheten


Regering och Riksdag
FI
MSB
SLV
EM
PTS
IVO
SoS
TS
EU samarbetsgrupp
CERT:ar
Sektorsvisa grupper
Tillsynsmyndighet
Lev. av samhällsviktig tjänster
Lev. av digitala tjänster

Skede 1, 6 timmar

- Telefonsamtal tas emot av Desk hos CERT-SE
- Frågor om incidenten och hanteringen
  (Skede 1 i formuläret i kondenserad form)
- Vid incidenthantering kan säkrare kommunikationslösningar användas
- Anteckningar vidarebefordras till TM per telefon nästa kontorstid

Bedömning av ärendet

- CERT-SE bedömmer
  - Informera MSB TiB?
  - Utredning?
  - Incident-team? Mål, plan, åtgärder
- Knoppas av från hanteringen av rapporten

Skede 2, 24 timmar

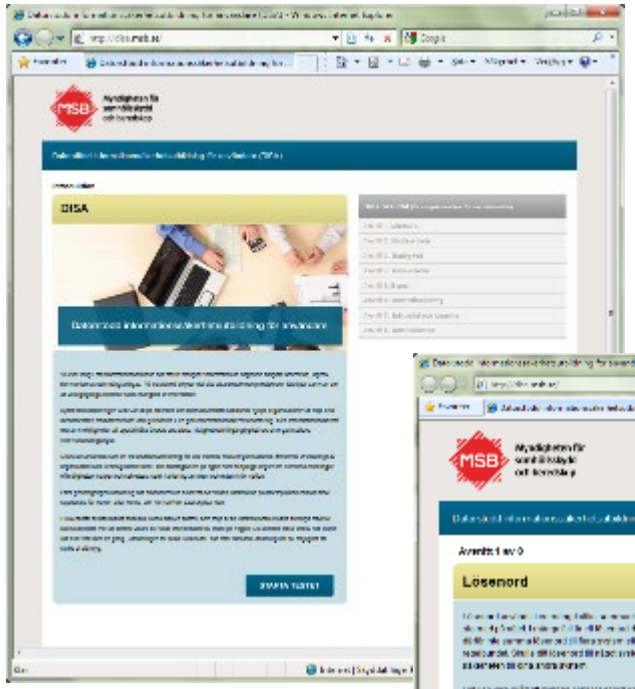
- Rek-brev tas emot av Desk hos CERT-SE
- Formuläret, Skede 1 och 2
- Vidarebefordras till TM med rek-brev

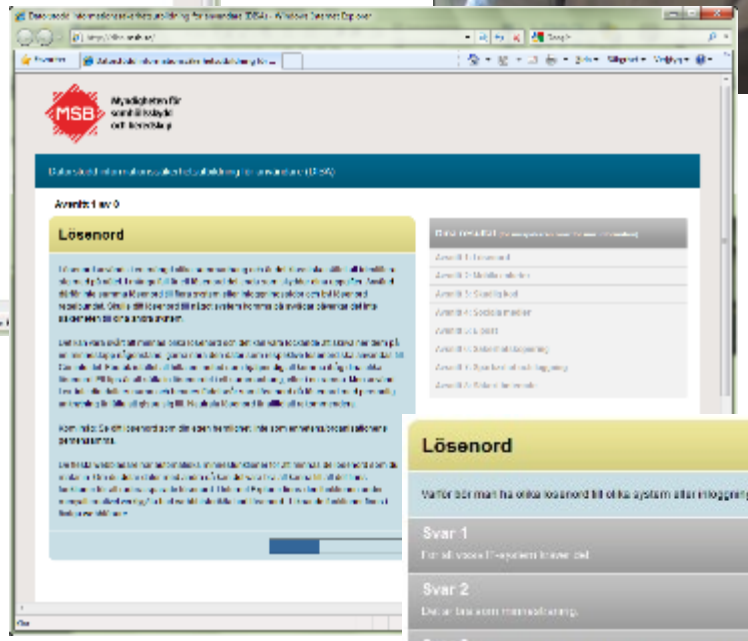
Skede 3, 4 veckor

- Rek-brev tas emot av Desk hos CERT-SE
- Formuläret, Skede (1, 2 och) 3
- Vidarebefordras till TM med rek-brev

DISA

MSB:s informationssäkerhetsutbildning för användare på http://disa.msb.se





Består av:

- Film
- Informationstext
- Frågebank
- Intyg

Avsnitt 1: Lösenord
Avsnitt 2: Mobila enheter
Avsnitt 3: Skadlig kod
Avsnitt 4: Sociala medier
Avsnitt 5: E-post
Avsnitt 6: Säkerhetskopiering
Avsnitt 7: Spårbarhet och loggning
Avsnitt 8: Säkert beteende
Avsnitt 9: Smarta telefoner
Avsnitt 10: Surfplattor

Myndigheten för samhällsskydd och beredskap

Reklam www.msb.se/SCADA

Myndigheten för samhällsskydd och beredskap

Mer information

Om MSB, vår verksamhet och vårt stöd till alla som arbetar med samhällsskydd och beredskap
www.msb.se @MSBse
www.msb.se/nis

Om den enskilda människans säkerhet och beredskap
www.dinsakerhet.se @Dinsakerhet

Samlad myndighetsinformation inför och under kriser
www.krisinformation.se @Krisinformation

Sveriges nationella CSIRT (Computer Security Incident Response Team)
www.cert.se

Stöd för systematiskt arbete med informationssäkerhet i organisationer
www.informationssakerhet.se

fraga.nis@msb.se

www.msb.se/NIS

http://www.energimyndigheten.se/trygg-energiforsorjning/informationssakerhet/

Myndigheten för samhällsskydd och beredskap

Reklam:

Myndigheten för samhällsskydd och beredskap

Kurser och utbildningar

Resurser och anläggningar

- Aeroakustik och vibrationsanalys
- Aerosolkammaren
- Analyser och uppdrag inom CBRN-ämnen
- Atmosfärslidar
- Batteritester
- CRATE - Cyber Range And Training Environment
- Isotoplaboratoriet
- Katastroftoxikologi - KcC
- Laboratoriet för högtoxiska ämnen
- Marin fältförsöksanläggning
- Säkerhetslaboratoriet
- Tanklaboratoriet
- Toxinlaboratoriet

Konferenser och seminarier

CRATE - Cyber Range And Training Environment

För att lyckas med en svår uppgift så måste man träna först. Det kan vara att vinna en tennismatch, bygga ett hus eller lösa uppgifter i termodynamik på universitetet. Första försöken brukar sällan vara lyckade, men allteftersom man övar så blir man bättre och bättre.

I fallet IT-intrång och IT-incidenter gäller det naturligtvis också att det går rätt dåligt första gången man skall hantera dessa, men att det blir bättre med träning och övning. Att öva incidenthantering och att genomföra sårbarhetsexperiment i en verklig miljö är i bästa fall vanskligt och ofta helt omöjligt. Det är därför vi byggt CRATE.

FOI har sedan 2008 byggt upp en av de allra första europeiska träningsanläggningarna speciellt anpassade för cyberförsvar. Tillsammans med våra huvudkunder Försvarsmakten och MSB har vi nu en unik anläggning för att öva IT-säkerhet på alla nivåer, från nybörjare till erfarna systemadministratörer.

Myndigheten för samhällsskydd och beredskap

Kurs | Praktisk incidenthantering i industriella informations- och styrsystem

LINKÖPING 7-10 NOVEMBER 2017

Myndigheten för samhällsskydd och beredskap (MSB) inbjuder i samarbete med Svenska Kraftnät och Energiföretagen/EBITS till kursen *Praktisk incidenthantering i industriella informations- och styrsystem* (14S). Kursen genomförs av Totalförsvarets forskningsinstitut (FOI) som en del av Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3).

Syftet med kursen är att få en ökad förståelse för de krav som ställs på industriella informations- och styrsystem samt kunskap om hur incidenthantering kan ske i IT-miljöer där sådana system finns.

Kursen riktar sig till dem som arbetar med IT i organisationer där processnära IT-miljöer förekommer. Kurstillfällets huvudsakliga målgrupp är operatörer inom elproduktion, eltransmission och eldistribution, men även andra organisationer är välkomna att anmäla sig. Deltagarna ska ha erfarenheter av nätverk, servrar eller operativsystem. Deltagarna kan också befinna sig i en roll där organisationsförståelse är viktigt. Exempel på roller som kan motsvara målgruppen är systemadministratör eller ansvariga för IT-drift och administration.

Kursen ges i FOI:s lokaler i Linköping

Kursinnehåll | Praktisk incidenthantering i industriella informations- och styrsystem

Kursen omfattar 2,5 dagar. De två första dagarna innehåller föreläsningar, demonstrationer och övningar. Under dag tre genomförs en övning där deltagarna, som arbetar med IT-drift för ett företag inom tillverkningsindustrin, ska rapportera de incidenter som upptäcks i företagets IT-miljö. Lärdomar från övningsgenomförandet och

Myndigheten för samhällsskydd och beredskap

Grundläggande kurs | Säkerhet i industriella informations- och styrsystem

TVÅ TILLFÄLLEN: LINKÖPING 16-17 MAJ ALTERNATIVT 22-23 MAJ 2018

Myndigheten för samhällsskydd och beredskap inbjuder i samarbete med Svenska Kraftnät och Energiföretagen/EBITS till två tillfällen av kursen *Grundläggande kurs: Säkerhet i industriella informations- och styrsystem*. Kursen genomförs av Totalförsvarets forskningsinstitut, FOI. Kursen har tidigare genomförts under namnet SIK – Säkerhet i industriella kontrollsystem. Den syftar till att höja medvetenheten om vikten att arbeta systematiskt med säkerhetsfrågor inom informations- och styrsystem. Inbjudan sker i samarbete med Svenska kraftnät och Energiföretagen/EBITS men du är välkommen att söka även om du arbetar inom en annan sektor än energisektorn.

Kursen är praktisk inriktad och vänder sig till operatörer, processingenjörer, utvecklingsingenjörer och underhållspersonal.

Plats | FOI, Olaus Magnus väg 42, Linköping

Kursinnehåll | Grundläggande kurs: Säkerhet i industriell informations- och styrsystem

Kursen omfattar två heldagar och innehåller såväl föreläsningar som praktiska demonstrationer och övningar.

Under kursen kommer bland annat följande frågor att behandlas:

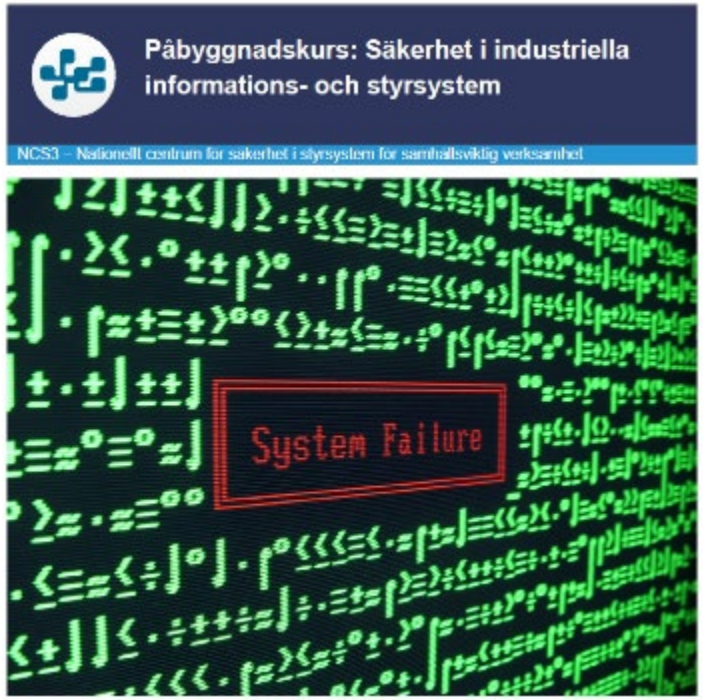
- Vad innebär säkerhet i industriella informations- och styrsystem?
- Vilka typer av sårbarheter finns i programmerbar elektronik?
- Vilka typer av IT-incidenter har uppmärksammats inom informations och styrsystem?
- Hur kan man skydda sig mot angrepp av skadlig kod?

Myndigheten för samhällsskydd och beredskap

SVENSKA KRAFTNÄT

FOI

Myndigheten för samhällsskydd och beredskap



Påbyggnadskurs säkerhet i industriella informations- och styrsystem är en kurs för dig som vill lära dig hur förutsättningar för säkerheten i industriella informations- och styrsystem kan skapas och förbättras. Under kursen får du kunskaper om hur exponeringen av kritiska delar av ett system kan reduceras samt om skydds-åtgärder för att stärka skyddet av ett system.

Industriella informations- och styrsystem används för att styra och kontrollera flera funktioner i vår vardag. Det kan röra sig om allt från övervakning av ventilation till produktion, transmission och distribution av el. Om dessa system utsätts för angrepp kan det få allvarliga konsekvenser för samhället. Det är därför viktigt att de skyddas tillräckligt.

Publikationer

Myndigheten för samhällsskydd och beredskap

Publikationer

Myndigheten för samhällsskydd och beredskap

Hela denna sida är reklam

Myndigheten för samhällsskydd och beredskap

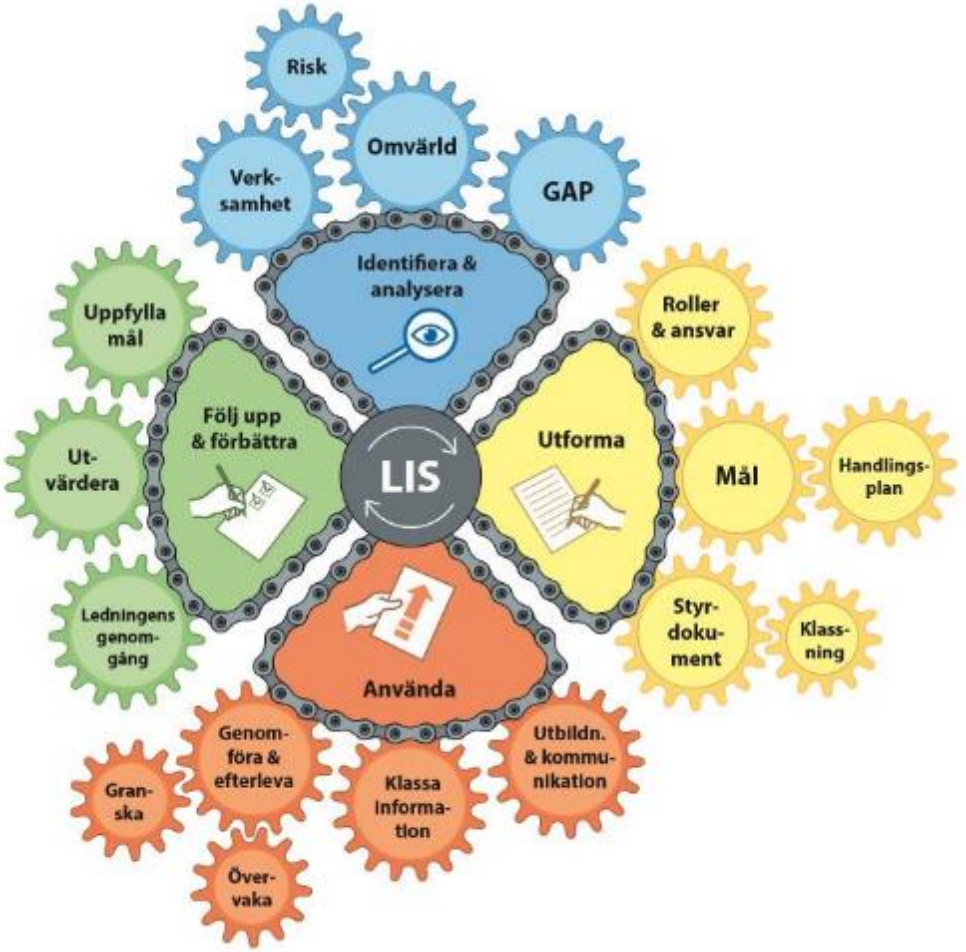
Hela denna sida är en annons

MSB's metodstöd för systematiskt informations-säkerhetsarbe

Metodstödet vänder sig till de som arbetar med informationssäkerhet i en organisation

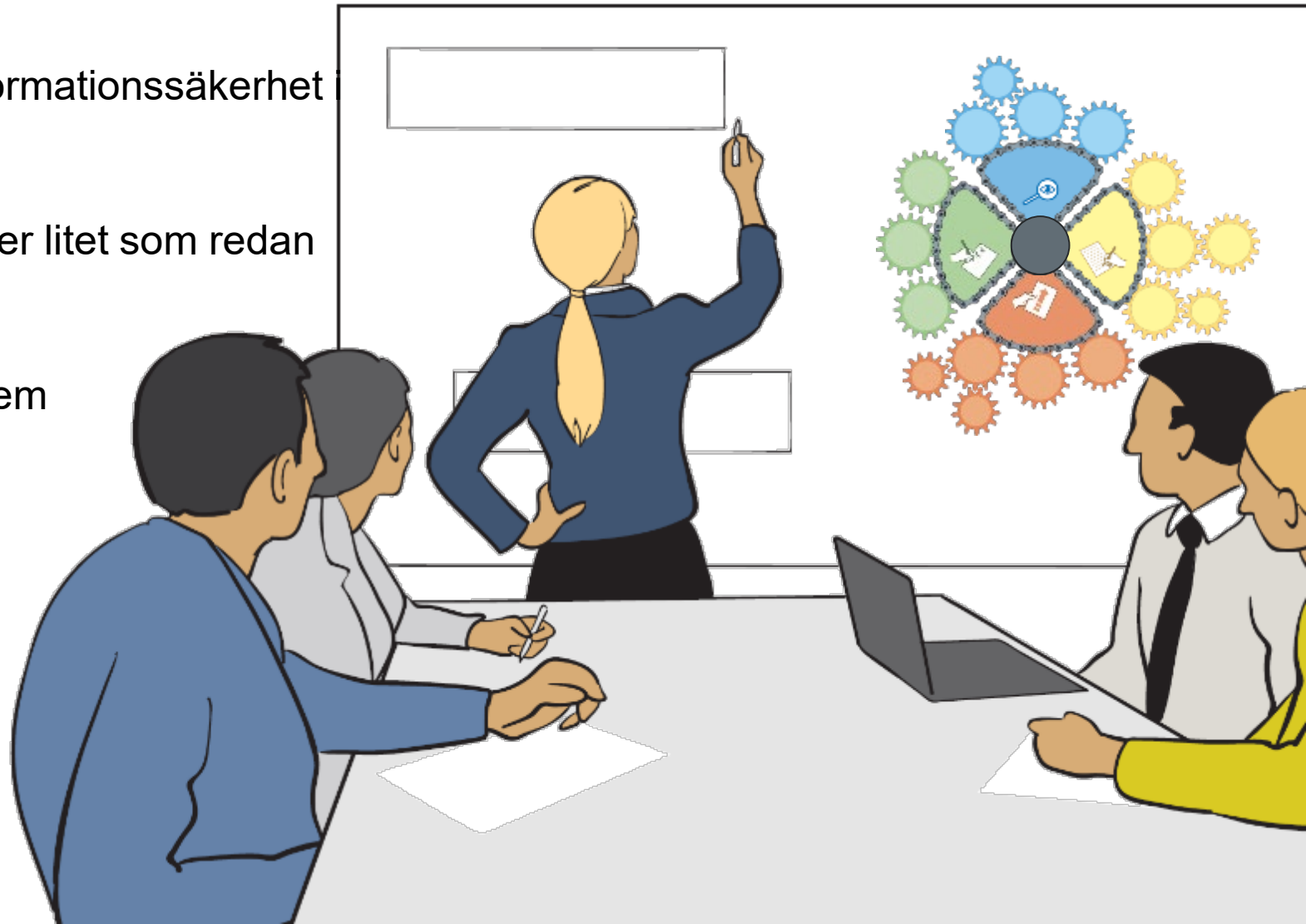
”Från principer till checklistor”

www.informationssäkerhet.se



Metodstöd för systematiskt informationssäkerhetsarbete

- Vänder sig till dig som arbetar med informationssäkerhet i en organisation
- Går att använda oavsett hur mycket eller litet som redan är gjort i din organisation
- Utgår från standarden för ledningssystem för informations-säkerhet (SS-EN ISO/IEC 27001).



Systematiskt informationssäkerhetsarbete

- MSB:s metodstöd för systematiskt informationssäkerhetsarbete har sin utgångspunkt i standarden för ledningssystem för informationssäkerhet (SS-EN ISO/IEC 27001).
- Metodstödet har arbetats fram av en grupp bestående av informations-säkerhetsspecialister från olika organisationer.
- Under arbetets gång har tre öppna seminarier genomförts i syfte att få in kloka synpunkter från ytterligare informationssäkerhetsspecialister och från fler typer av organisationer.

Metodstödets innehåll

- Att arbeta systematiskt med informationssäkerhet
- Vägledningar
- Verktyg
- Utbildningsmaterial
- Exempel
- Kunskapsbank med fördjupningar och komplement
- FAQ

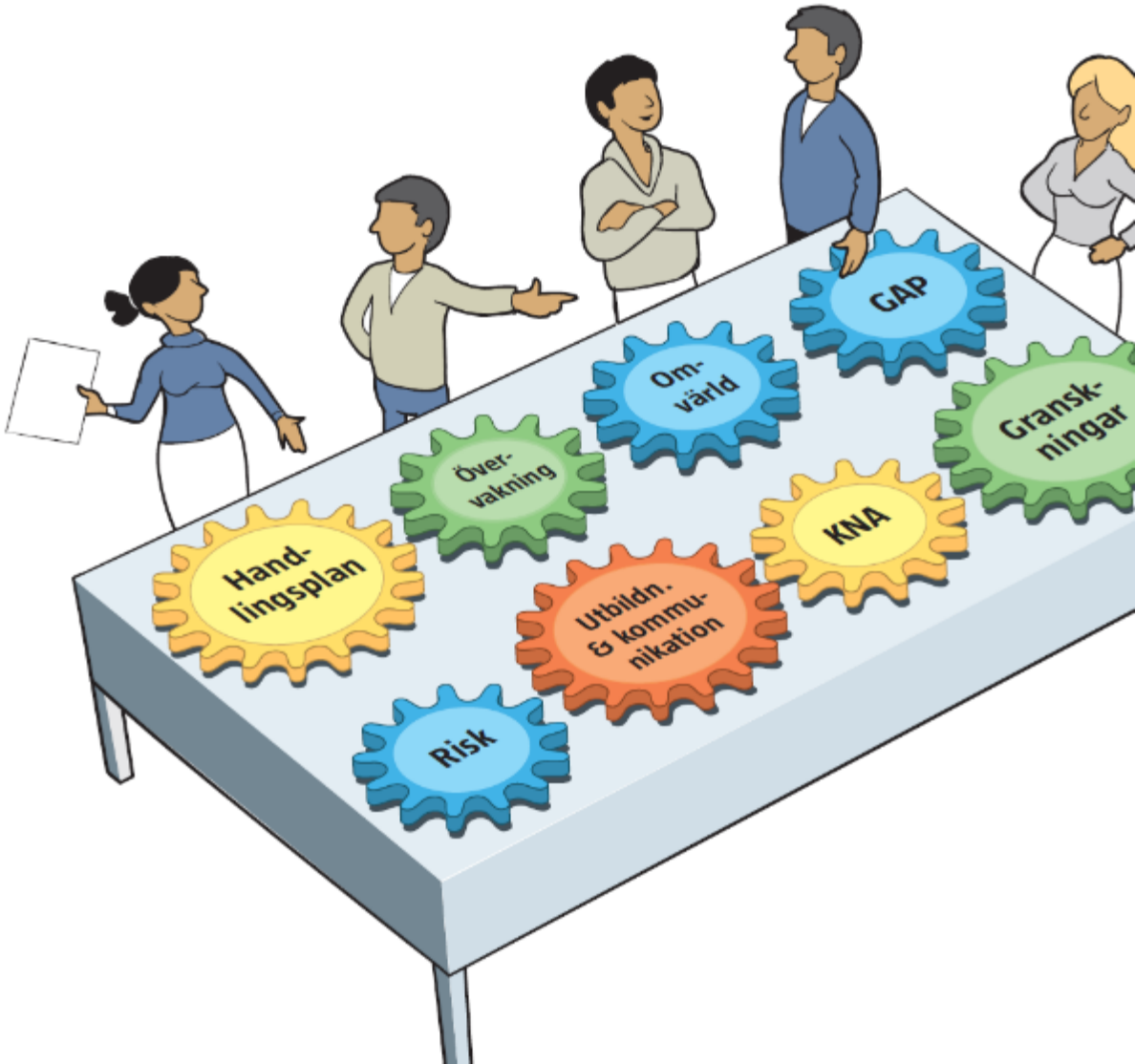
Att använda metodstödet

Metodstödet vänder sig till alla som arbetar med informationssäkerhet

- Arbetet med systematiskt informationssäkerhetsarbete ska påbörjas i din organisation
- Din organisation har redan kommit en bit på väg
- Din organisation ska certifiera sig mot SS-EN ISO/IEC 27001

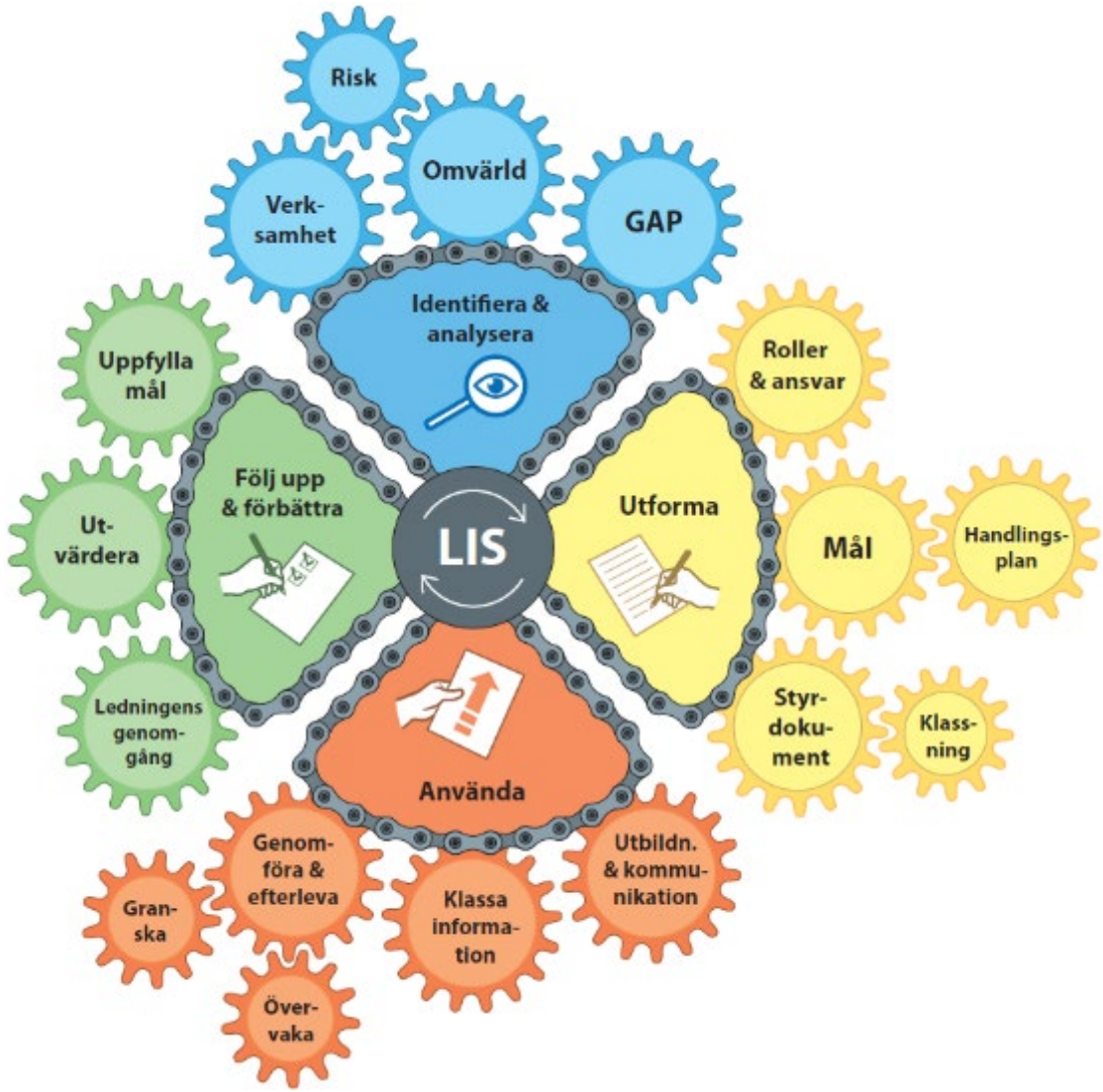
Praktiska tips

- Jobba igenom ”A till Ö” eller välj relevanta steg. Många jobbar i flera steg parallellt.
- Metodstödet är webbanpasset och finns på informationssäkerhet.se
- Text och verktyg går att skriva ut så att du kan använda dem för dina behov
- Dela och återanvänd gärna innehållet. Hela metodstödet är licensierat enligt Creative Commons (Erkännande).



Fyra metodsteg

- Identifiera och analysera
- Utforma
- Använda
- Följa upp och förbättra



Metodsteg – Identifiera och analysera

Ingångsvärde: För att analysera verksamheten, omvärlden, risk och gap krävs kunskap och information om nuläget, dvs. den situation i vilken verksamheten befinner sig.

Beskrivning: Här analyseras verksamheten, omvärlden och informationssäkerhetsrisker. Här identifieras också gapet mellan nuläget och det läge man vill befinna sig i. Utifrån resultatet av dessa analyser väljs lämpliga säkerhetsåtgärder att införa i organisationen.

Resultat:

- lista på interna och externa förutsättningar och aktörer
- lista på informationstillgångar som ska skyddas
- vilka risker de ska skyddas mot
- valda säkerhetsåtgärder och status på dessa

Metodsteg - Utforma

Ingångsvärde: Samtlig information från tidigare verksamhetsövergripande analyser.

Beskrivning: I steget Utforma tar man fram samtliga verksamhetsövergripande komponenter som behövs för det systematiska arbetssättet.

Resultat:

- organisation, dvs. ansvar och roller för informationssäkerhet
- styrdokument och mål för informationssäkerhet
- en organisationsövergripande klassningsmodell för informationstillgångar
- en handlingsplan för informations-säkerhet som i regel ska genomföras på årlig basis

Metodsteg - Använda

Ingångvärde: Allt ovan från Utforma.

Beskrivning: Här realiseras och används det som tagits fram i Utforma. Viktiga delar är att handlingsplanen genomförs och att styr-dokumenten efterlevs. För detta krävs utbildnings- och kommunikationsinsatser, och särskilt stöd ges för att klassa informationstillgångar.

Resultat: Metodsteget Använda resulterar i statusrapporter och slutrapporter gällande genomförande av handlingsplan och efter-levnad av styrdokument, dokumentation av genomförda utbildnings- och kommunika-tionsaktiviteter, faktisk kunskaps- och medvetandehöjning samt klassade informationstillgångar.

Metodsteg – Följa upp och förbättra

Ingångsvärde: Information och resultat från Utforma och Använda.

Beskrivning: Att följa upp och förbättra såväl arbetssättet som nivån på informations-säkerhet genomförs löpande men också vid planlagda och med övrig verksamhetsstyrning integrerade tillfällen. I metodsteget ingår att utvärdera ifall informations-säkerheten i stort är ändamålsenligt utformad, har avsedd verkan, samt att säkerhetsåtgärder existerar och fungerar tillfredsställande. Aktiviteter som ingår kan vara uppföljning av mål och planer, intern och extern revision samt ledningens genomgång.

Resultat: Resultatet från Följa upp och förbättra är ingångsvärde till nya analyser i Identifiera och analysera och ny planering av verksamheten i Utforma.

För dig som vill veta mer

Du hittar metodstödet på Informationssäkerhet.se

Skicka frågor och synpunkter till

metodstod@informationssakerhet.se

fraga.nis@msb.se

www.msb.se/NIS

http://www.energimyndigheten.se/trygg-energiforsorjning/informationssakerhet/

www.livsmedelsverket.se/produktion-handel--kontroll/dricksvattenproduktion/nis

Myndigheten för samhällsskydd och beredskap