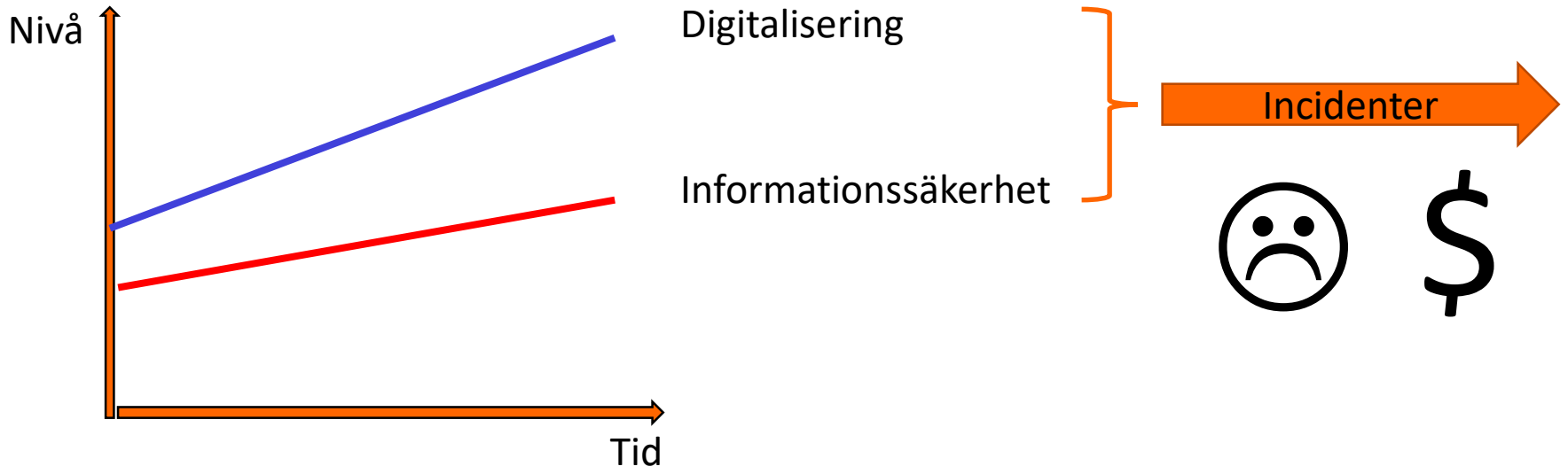
Regelverk och myndighetsstöd för ökad informationssäkerhet inom dricksvattenförsörjningen (NIS)

Anders Östgaard

Livsmedelsverket

Digitalisering



NIS-direktivet

NIS - Network Information Security

Flera skäl, bland annat:
-Ekonomisk och samhällelig verksamhet, inre marknadens funktion
-Minska säkerhetsincidenter (antal, omfattning)
-Säkerställa att de allvarligaste incidenterna rapporteras
-Främja en riskhanteringskultur
-Säkerställa en hög nivå på säkerheten

Livsmedelsverket

NIS-direktivet

Energi

Transporter (väg, järnväg, sjöfart, luftfart)

Bankverksamhet

Finsansmarknadsinfrastruktur

Hälso- och sjukvård

Leverans och distribution av dricksvatten

Digital infrastruktur

Digitala tjänster

Livsmedelsverket

Vilka system avses?

Nätverks- och informationssystem - definieras i direktivet och svensk lag.

För vattensektorn – digitala system som påverkar leveransen av vatten, ex styrsystem (ICS / SCADA).

NIS-lagstiftningen - hierarkin

NIS-direktivet: Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174)

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

Myndigheten för samhällsskydd och beredskaps föreskrifter om identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2018:XXXX)

Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster; (MSBFS 2018:XXXX)

Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:XXXX)

Myndigheten för samhällsskydd och beredskaps föreskrifter om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet (MSBFS 2018:XXXX)

Livsmedelsverkets föreskrifter (LIVSFS)

Livsmedelsverket

Tidslinje

Livsmedelsverket

Lagens tillämpningsområde:

- Samhällsviktiga tjänsteleverantörer och digitala tjänster
- Etablerade i Sverige
- Tillhandahållandet av tjänsten är beroende av nätverk och informationssystem
- En incident medför betydande störning vid tillhandahållandet av tjänsten.

- Gäller ej **verksamhet** som omfattas av säkerhetsskydd

Livsmedelsverket

Vad är en samhällsviktig tjänsteleverantör inom dricksvatten?

Beskrivs i MSBs föreskrifter. **Remissförslag** gällande dricksvatten:

Levererar dricksvatten till

- 20000+ personer
- Akutsjukhus

Vad är en incident med betydande inverkan?

Beskrivs i MSBs föreskrifter. **Remissförslag** för dricksvatten:

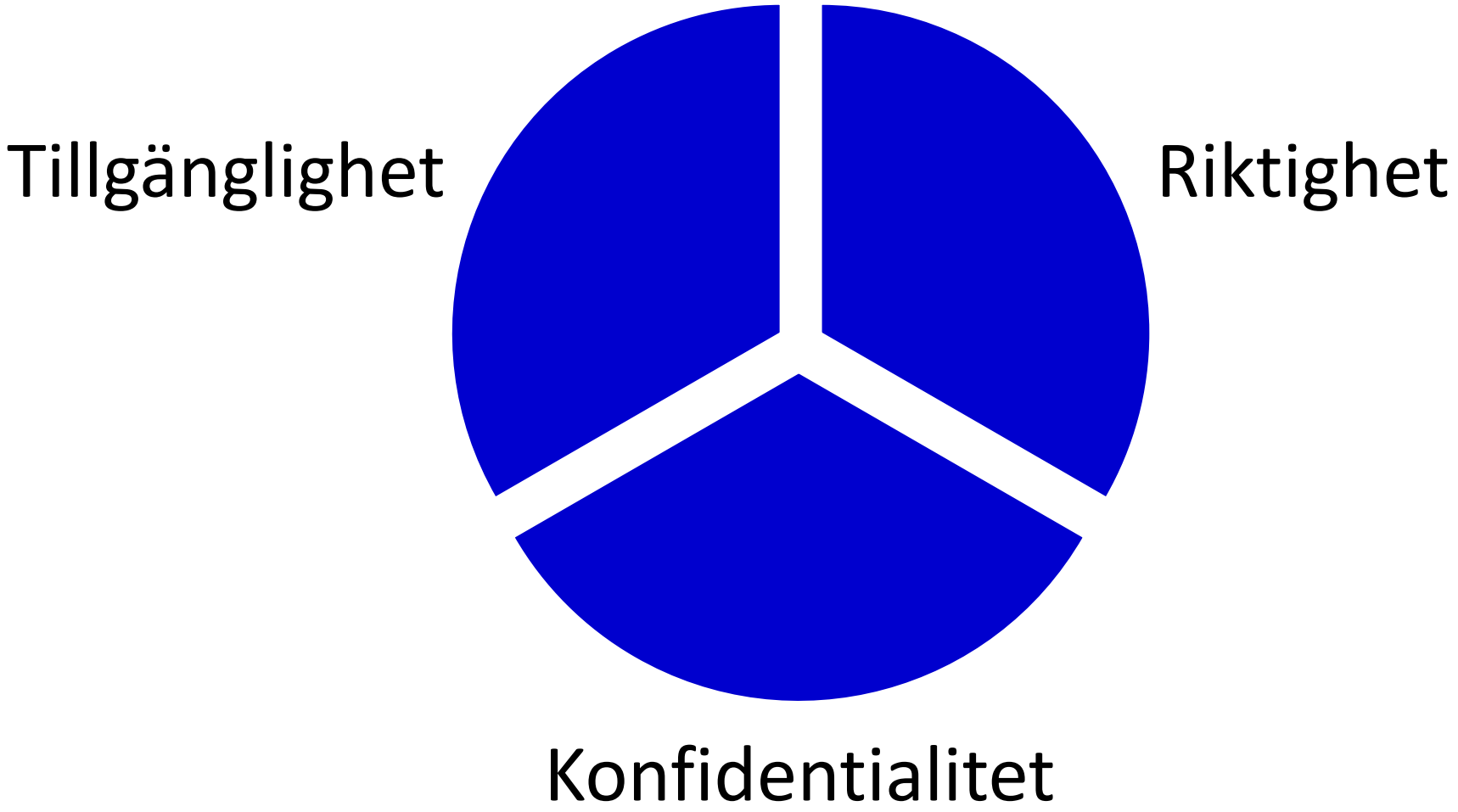
- Vid leveransavbrott i minst två timmar
- Styrning och övervakning av tjänsten inte har kunnat genomföras under en tidsperiod om minst två timmar

Digitala styrsystem (ICS eller SCADA)

De nätverk, datorer och komponenter som styr och övervakar vattenproduktionen och distributionen.

Livsmedelsverket

Informationssäkerhetsaspekter



Vad ska göras?

Några paragrafer att titta på:

Vad (förenklat)	Lag §	Föreskrift	Tillsynsmyndighet
Identifiering och anmälan	23 §	MSB (höst 2018)	Livsmedelsverket
Rapportering av incidenter	18 §	MSB (höst 2018)	Livsmedelsverket
Bedriva systematiskt arbete	11 §	MSB (höst 2018)	Livsmedelsverket
Årliga riskanalyser	12 §	Livsmedelsverket	Livsmedelsverket
Tekniska och organisatoriska åtgärder	13 §	Livsmedelsverket	Livsmedelsverket
Hantera incidenter	14 §	Livsmedelsverket	Livsmedelsverket

Hur anmäla?

De tjänsteleverantörer som utifrån MSBs kommande föreskrifter identifierat att de omfattas ska utan dröjsmål anmäla sig till respektive tillsynsmyndighet.

Leverantörer inom området *Leverans och distribution av dricksvatten* ska anmäla sig till Livsmedelsverket.

Instruktion kommer finnas på www.livsmedelsverket.se/nis

Hur rapportera incidenter?

Tjänsteleverantörerna ska anmäla incidenter som har en betydande inverkan på kontinuiteten av tjänsten till CSIRT (MSB).

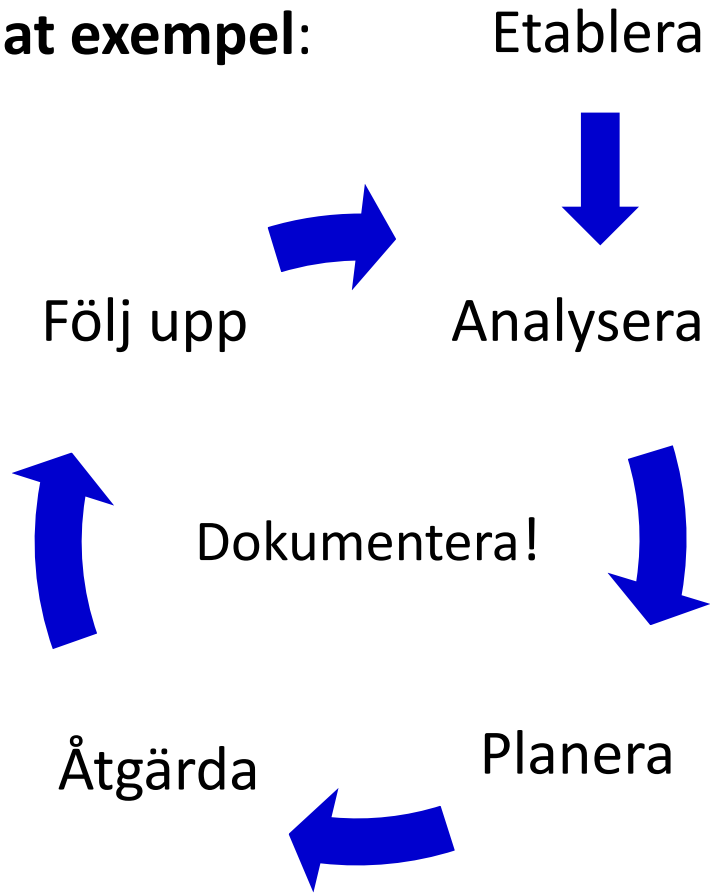
MSB föreskriver om innehåll i rapporten och anvisar metod.

Vad för slags säkerhetsåtgärder ska vidtas?

- 11§ - Systematiskt och riskbaserat informationssäkerhetsarbete.
- 12§ - Göra årlig riskanalys
- 13§ - Säkerhetsåtgärder (tekniska och organisatoriska)
- 14§ - Hantera incidenter

Systematiskt arbete 11§

Förenklat exempel:



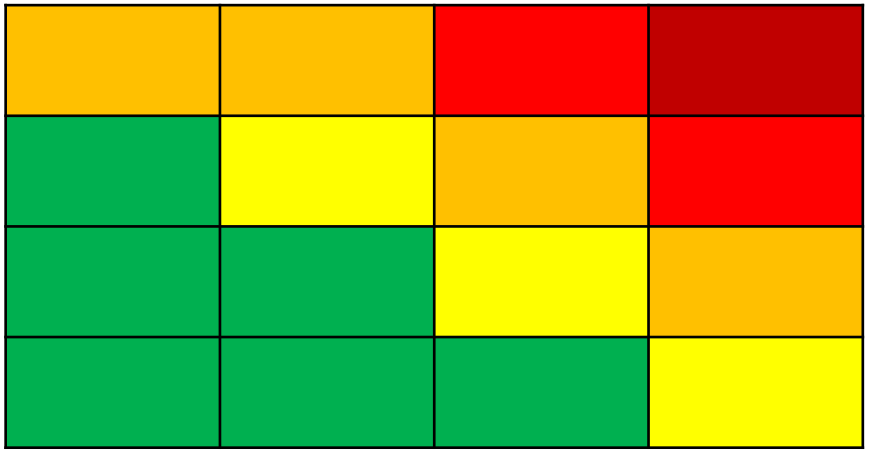
Resultat i form av kontinuitet i tjänsten.

dvs verksamheten kan förebygga och hantera allvarliga störningar.

Riskanalys 12§

Riskanalys som ska ligga till grund för åtgärder enligt 13-14§§.

Ska uppdateras årligen och resulterar i en åtgärdsplan



Livsmedelsverket

Tekniska och organisatoriska åtgärder 13§

Åtgärder för att säkerställa lämplig nivå på säkerheten relativt risken

Exempel på åtgärder (**OBS – beror på er riskanalys**)

Separera administrativa och produktionsnätverk
Säkerställa avtal (ex service och supportavtal, licenser).
Tvåfaktorsautenticering för fjärrstyrning
Förändra processen för förändringshantering
Framtagande av utbildningsprogram

Incidenthantering 14§

Åtgärder för att minimera effekten av incidenter och återställa tjänsten.

Exempel på åtgärder (**OBS – beror på er riskanalys**)

Öva
Tillgänglig reservhårdvara
Undvik snäva marginaler

Livsmedelsverket

Vilket stöd finns?

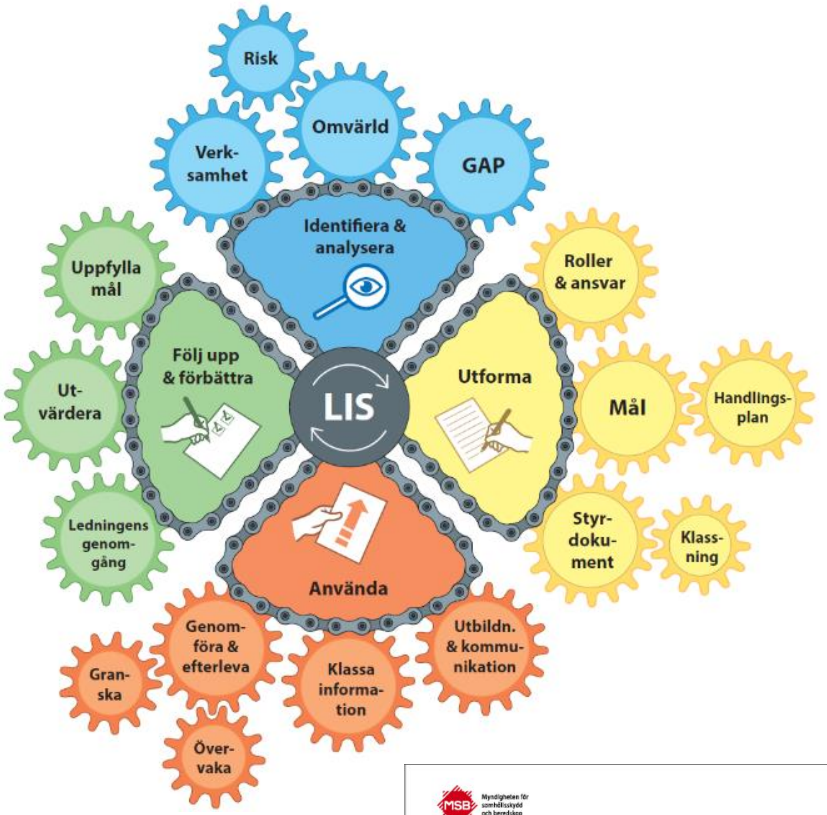
MSB

www.msb.se/nis

Metodstöd för LIS:

www.informationssakerhet.se

Stöd gällande styrsystem:
www.msb.se/ics



Livsmedelsverket

Kontakt med Livsmedelsverket

nistillsyn@slv.se

www.livsmedelsverket.se/nis

Livsmedelsverket