

Vervas föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte

Wiggo Öberg, tidigare Verva nu KBM,
2008-11-19

Vervas regeringsuppdrag

”Utveckla säkert elektroniskt informationsutbyte”

- Leda och samordna statsförvaltningens utvecklingsarbete
- Ge vägledning
- Utveckla gemensamma riktlinjer och specifikationer
- Bedöma behovet av reglering
- Beakta standarder på området
- **Utfärda föreskrifter vid behov**

Verket för förvaltningsutvecklings författningssamling

ISSN 1654-0832

Utgivare: Lena Jönsson, Verva, Box 214, 101 24 Stockholm

VERVA VERKET FÖR
FÖRVALTNINGS-
UTVECKLING

Vervas föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte;

VERVAFS 2007:2

Utkom från trycket
den 19 november 2007

beslutade den 14 november 2007

Verket för förvaltningsutveckling (Verva) föreskriver följande med stöd av 3 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.

Föreskriftens tillämpningsområde

1 § Denna föreskrift gäller för myndigheter under regeringen.

Verket för förvaltningsutveckling får besluta om undantag från dessa föreskrifter i enlighet med 4 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.

2 § Syftet med föreskriften är att i förvaltningen skapa förutsättningar för ett säkert och förtroendefullt elektroniskt informationsutbyte genom att myndigheterna bedriver sin verksamhet med den säkerhet som är nödvändig med hänsyn till den enskilda myndighetens förutsättningar.

3 § Om det i annan författning finns bestämmelser om statliga myndigheters arbete med säkert elektroniskt informationsutbyte gäller dessa framför denna föreskrift.

4 § En myndighet kan överenskomma med annan myndighet att helt eller delvis fullgöra myndighetens uppgifter enligt bestämmelserna i 5-6 §§.

Grundläggande krav

5 § En myndighet ska i sitt arbete för ett säkert elektroniskt informationsutbyte tillämpa ett ledningssystem för informations-säkerhet. Det innebär att myndigheten ska;

1. upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet,
2. utse en eller flera personer som ansvarar för säkerhetsarbetet och som minst en gång per år för myndighetsledningen redovisar och dokumenterar vilka granskningar och skyddsåtgärder av större betydelse som har vidtagits enligt myndighetens policy- och styrdokument.

Verket för förvaltningsutvecklings författningssamling

ISSN 1654-0832

Utgivare: Lena Jönsson, Verva, Box 214, 101 24 Stockholm

VERVA VERKET FÖR
FÖRVALTNINGS-
UTVECKLING

Vervas allmänna råd till föreskrift om statliga myn- digheters arbete med säkert elektroniskt informa- tionsutbyte, VERVAFS 2007:2;

VERVAFS 2007:2AR

Utkom från trycket
den 19 november 2007

Bakgrund

Regeringens ambition att använda informations- och kommunikations-teknik för att förbättra service, främja demokratiproccessen och öka effektiviteten i offentlig förvaltning bygger på att nödvändig tillit kan etableras i relationen mellan offentlig förvaltning å ena sidan och medborgare och företag å andra sidan. Myndigheter som samverkar kring e-tjänster måste känna förtroende för varandra när det gäller tillit till och utbyte av information. Medborgare och företag måste känna tillit till myndigheternas sätt att tillhandahålla e-tjänster. Detta innebär krav på godtagbar säkerhet så att exempelvis den personliga integriteten skyddas. Brister i informationssäkerhet kan innebära svårigheter att sprida nya e-tjänster och åstadkomma hinder för effektiva processer mellan myndigheter. Att åstadkomma säkerhet vid användning av IT är därmed en nödvändighet för att kunna utvärta tekniken på bästa sätt.

En organisations sammanhållna säkerhet skapas genom en kombination av tekniska respektive administrativa skyddsåtgärder och ger därmed en aggregerad nivå av säkerhet som benämns informationssäkerhet. Informationssäkerhet som begrepp omfattar skydd av information både när den hanteras manuellt av människor och när den behandlas med hjälp av IT. Att åstadkomma god informationssäkerhet är en komplex process som inbegriper hela verksamheten och som därför kräver engagemang och styrning från myndighetens ledning. Utgångspunkten för arbetet med informationssäkerhet är att risk- och sårbarhetsanalyser genomförs för att klarlägga den säkerhetsnivå som ska gälla för skydd av en organisations information och informationssystem.

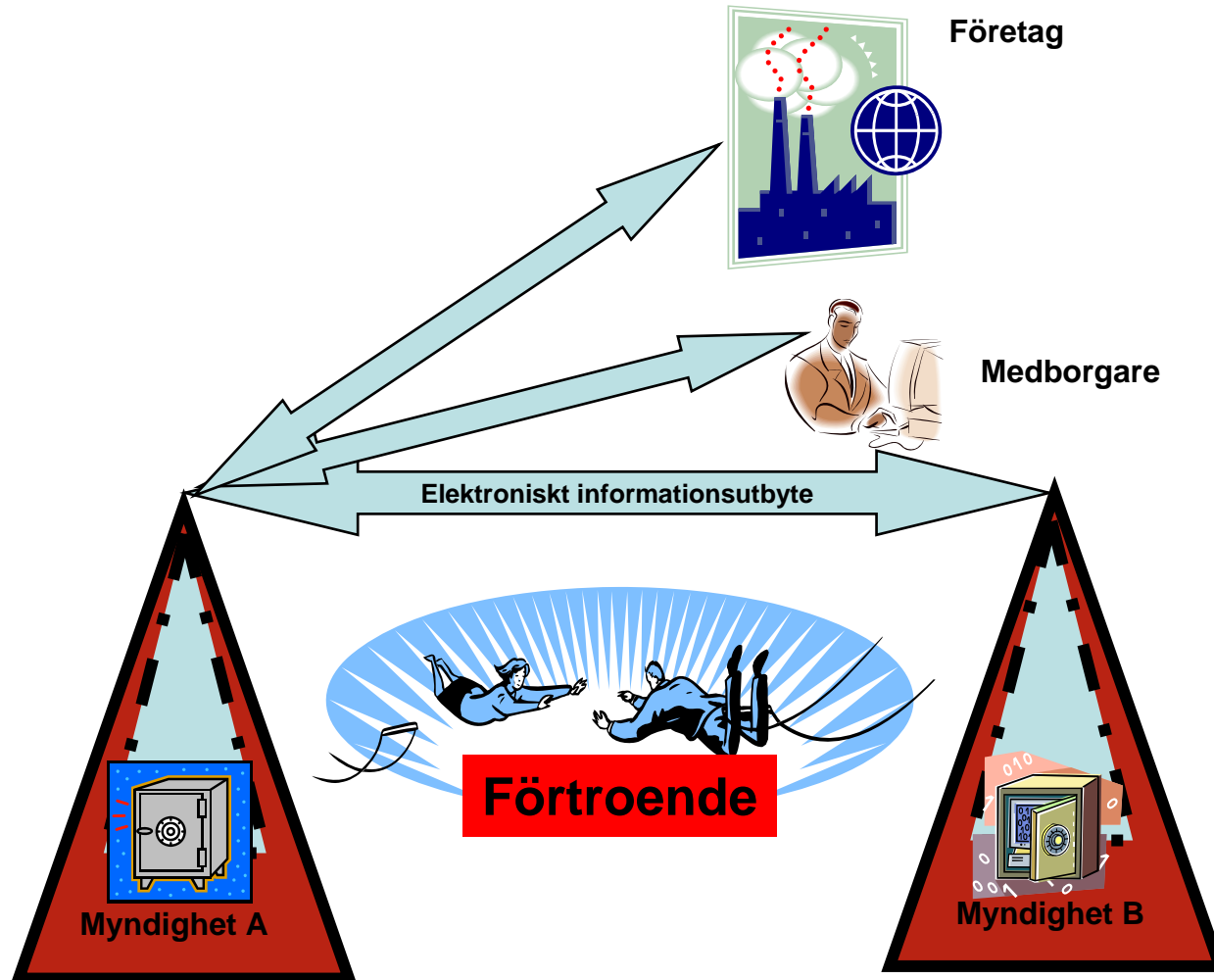
Utveckling av IT-användningen, inte minst den som följer av utvecklingen av e-förvaltningen, innebär stora möjligheter men kan också medföra en ökad sårbarhet. Grunden för att åstadkomma och vidmakthålla en tillräcklig nivå på informationssäkerheten är att det finns fungerande processer som gör att man kan möta nya situationer och möjligheter. Ökad samverkan mellan organisationer, utökad informationsutbyte, flera e-tjänster mot allmänhet och företag ställer krav på att säkerhetsfrågorna behandlas seriöst och kompetent. Detta för att skapa nödvändig kvalitet

Varför en föreskrift som täcker ”all” informationssäkerhet i en myndighet?

Likformighet och samsyn

2 § Syftet med föreskriften är att i förvaltningen skapa förutsättningar för ett säkert och förtroendefullt elektroniskt informationsutbyte genom att myndigheterna **bedriver sin verksamhet med den säkerhet som är nödvändig** med hänsyn till den enskilda myndighetens förutsättningar.

.... gemensam grund, samsyn, omvärldskrav



Varför följa standard ("LIS")?

- Internationellt och nationellt etablerad standard
- Samlad erfarenhet
- "Anpassningsfilosofi" stämmer med svensk modell för styrning
- Process- och beslutsmodell inte detaljstyrning
- Svensk medverkan i vidareutveckling
- EU pekar på LIS som medel
- Informationssäkerhetsutredningen d:o
- Befintliga vägledningar (KBM:s rek. BITS och Datainsp. allmänna råd) anpassade mot LIS-standarderna.
- Grundläggande vid SÄPO-tillsyn för tillämpning av säkerhetsskyddslagen.

Hur ska föreskriften tillämpas?

- Gäller myndigheter under regeringen
- Verva kan besluta om undantag
- Avvikande bestämmelser går före
- Myndigheter kan samarbeta om genomförandet
- **Informationssäkerhet anpassad till myndighetens förutsättningar**

Verket för förvaltningsutvecklings författningssamling

ISSN 1654-0832

Utgivare: Lena Jönsson, Verva, Box 214, 101 24 Stockholm

VERVA | VERKET FÖR
FÖRVALTNINGS-
UTVECKLING

Vervas föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte;

VERVAFS 2007:2

Utkom från trycket
den 19 november 2007

beslutade den 14 november 2007

Verket för förvaltningsutveckling (Verva) föreskriver följande med stöd av 3 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.

Föreskriftens tillämpningsområde

1 § Denna föreskrift gäller för myndigheter under regeringen.

Verket för förvaltningsutveckling får besluta om undantag från dessa föreskrifter i enlighet med 4 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.

2 § Syftet med föreskriften är att i förvaltningen skapa förutsättningar för ett säkert och förtroendefullt elektroniskt informationsutbyte genom att myndigheterna bedriver sin verksamhet med den säkerhet som är nödvändig med hänsyn till den enskilda myndighetens förutsättningar.

3 § Om det i annan författning finns bestämmelser om statliga myndigheters arbete med säkert elektroniskt informationsutbyte gäller dessa framför denna föreskrift.

4 § En myndighet kan överenskomma med annan myndighet att helt eller delvis fullgöra myndighetens uppgifter enligt bestämmelserna i 5-6 §§.

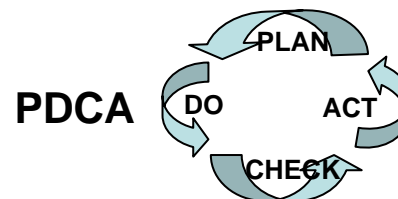
Grundläggande krav

5 § En myndighet ska i sitt arbete för ett säkert elektroniskt informationsutbyte tillämpa ett ledningssystem för informations-säkerhet. Det innebär att myndigheten ska;

1. upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet,
2. utse en eller flera personer som ansvarar för säkerhetsarbetet och som minst en gång per år för myndighetsledningen redovisar och dokumenterar vilka granskningar och skyddsåtgärder av större betydelse som har vidtagits enligt myndighetens policy- och styrdokument.

Grundläggande krav

- Tillämpa ett ledningssystem för informationssäkerhet, vilket innebär:
 - Upprätta informationssäkerhetspolicy och andra styrande dokument
 - Utse en eller flera personer som ansvarar för säkerhetsarbetet
 - Minst en gång per år redovisar för myndighetsledningen och dokumenterar granskningar och skyddsåtgärder av större betydelse som har vidtagits enligt myndighetens policy- och styrdokument



Grundläggande krav

- Utgångspunkt för arbetet med informationssäkerhet är att risk- och sårbarhetsanalyser genomförs för att klargöra den säkerhetsnivå som skall gälla
- Tillämpa etablerade standarder
 - Ledningssystem för informationssäkerhet – Krav (SS-ISO/IEC 27001:2006 fastställd 2006-01-19) och
 - Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005 fastställd 2005-08-12).

Verket för förvaltningsutvecklings författningssamling

ISSN 1654-0832

Utgivare: Lena Jönsson, Verva, Box 214, 101 24 Stockholm

Verfas allmänna råd till föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte, VERVAFS 2007:2;

VERVAFS 2007:2AR

Utkom från trycket
den 19 november 2007

Bakgrund

Regeringens ambition att använda informations- och kommunikationsteknik för att förbättra service, främja demokratiprocessen och öka effektiviteten i offentlig förvaltning bygger på att nödvändig tillit kan etableras i relationen mellan offentlig förvaltning å ena sidan och medborgare och företag å andra sidan. Myndigheter som samverkar kring tjänster måste känna förtroende för varandra när det gäller att kunna till och utbyta av information. Medborgare och företag måste kunna tillit till myndigheternas sätt att tillhandahålla e-tjänster. Detta innebär krav på godtagbar säkerhet så att exempelvis den personliga integriteten skyddas. Brister i informationssäkerhet kan innebära svårigheter att sprida nya e-tjänster och åstadkomma hinder för effektiva processer mellan myndigheter. Att åstadkomma säkerhet vid användning av IT är därmed en nödvändighet för att kunna utnyttja tekniken på bästa sätt.

En organisations sammanlagda säkerhet skapas genom en kombination av tekniska respektive administrativa skyddsåtgärder och ger därmed en aggregerad nivå av säkerhet som benämns informationssäkerhet. Informationssäkerhet som begrepp omfattar skydd av information både när den hanteras manuellt av människor och när den behandlas med hjälp av IT. Att åstadkomma god informationssäkerhet är en komplex process som inbegriper hela verksamheten och som därför kräver engagemang och styrning från myndighetens ledning. Utgångspunkten för arbetet med informationssäkerhet är att risk- och sårbarhetsanalyser genomförs för att klarlägga den säkerhetsnivå som ska gälla för skydd av en organisations information och informationssystem.

Utveckling av IT-användningen, inte minst den som följer av utvecklingen av e-förvaltningen, innebär stora möjligheter men kan också medföra en ökad sårbarhet. Grunden för att åstadkomma och vidmakthålla en tillräcklig nivå på informationssäkerheten är att det finns fungerande processer som gör att man kan möta nya situationer och möjligheter. Ökad samverkan mellan organisationer, utökat informationsutbyte, flera e-tjänster mot allmänhet och företag ställer krav på att säkerhetsfrågorna behandlas seriöst och kompetent. Detta för att skapa nödvändig kvalitet

Vad säger de allmänna råden

- Föreskriften är avsedd att tillämpas där motsvarande reglering saknas
- Föreskriften ger möjlighet för varje organisation att utifrån sin **storlek, inriktning** och **andra unika förhållanden** samt genomförd **riskanalys** besluta omfattning
- Utgångspunkt för arbetet med informationssäkerhet är att risk- och sårbarhetsanalyser genomförs för att klargöra den säkerhetsnivå som skall gälla

...för stora och små...

Störst:

RPS

Försvarsmakten

Försäkrings-

Kassan

Skatteverket



..och vad kostar det då ??

Kommentar:

Om du har bra informationssäkerhet kan du luta dig tillbaka

Om du har brister är det kanske dags att ta tag i dessa – Säkerhet kostar mer ju senare man upptäcker problemen

Oavsett:

Detta kommer att vara en nyttig övning för att få reda på status – och du kommer troligtvis att bli överraskad åt något håll

Hur startar jag upp ??

- Läs igenom de allmänna råden noga
- Använd standarden som "förlaga" – du kommer att uppskatta både helheten och de delar som berör dig

Kommentarer:

Anta utmaningen

Fundera ut vem som är lämpad att ta större ansvar för dessa frågor

Blanda in flera – ökad medvetenhet hos personalen är en förutsättning

Se möjligheterna – en tryggare vardag

Allmänna råden - detaljerna

- Upprätta informationssäkerhetspolicy och andra styrande dokument
- Organisation, roller och ansvarsförhållanden
- Personalens medverkan
- Risk- och sårbarhetsanalyser
- Informationsklassificering/Informationsvärdering
- Skyddsåtgärder

Grundläggande för beslut om verksamhetens skyddsnivå

Upprätta informationssäkerhetspolicy och andra styrande dokument

- Informationssäkerhetspolicyn är ett "måste"
- "Andra styrande dokument" - utifrån verksamhetens behov

Goda råd:

Policyn anger riktningen, och det är viktigt att det också finns en "hur"-beskrivning så att personalen förstår.

Lägg tid på att sprida information till personalen.

Strukturera befintliga regler/riktlinjer/instruktioner. Standarden ger vägledning och hjälp.

Viktigt att prioritera dvs. ta hand om det som är mest kritiskt först

Undvik att överarbeta

Organisation, roller och ansvarsförhållanden

- Myndighetsledningen måste vara involverad och delaktig
- Myndighetsledningen skall tilldelas underlag för att kunna fatta "kloka" beslut
- Ansvarig utses
- Informationssäkerheten är en integrerad del av verksamheten och ansvaret skall ligga där det passar bäst

Personalens medverkan

- "What's in it for me??" Var tydlig med att beskriva nyttan
- Det är personalen som hanterar informationen – blanda in dem så mycket som möjligt
- Ställ krav på personalen
- Utbildning och information en förutsättning för "framgång"

Kommentarer:

Det finns alltid omvägar att undvika säkerhet – och vi vet alla hur man gör.

Därför är det förutsättning att personalen är medvetna om VARFÖR befintliga regler och riktlinjer finns och HUR de skall användas.

Information och utbildning är färskvara – det skadar inte att påminna.

Risk- och sårbarhetsanalys

- Enda möjligheten att få en bild över vilka risker som finns i just min organisation
- Förutsättning för att avgöra vilka risker som skall
 - elimineras,
 - reduceras eller
 - accepteras

Kommentar:

**En enkel riskanalys kan göras i anslutning till ett enhetsmöte
Inte helt lätt första gångerna – en bra idé är att låta någon få lära sig tekniken**

Större riskanalyser kräver metoder och tar tid

Hjälp finns på Internet och ”ute på stan”

Informationsklassificering (värdering av informationstillgångar)

- Nära sammanknuten med riskanalysen
- Lagkrav kan styra
- Syftet är att ta fram förutsättningar för en lämplig skyddsnivå för myndighetens informationstillgångar

Kommentarer:

Behöver inte vara krångligt

Finns ett antal tekniker och produkter ”ute på stan”

Läs i BITS – BITS Plus

Projekt KBM, SIS, FMV, FRA, m fl för ny generell vägledning.

Skyddsåtgärder

- Drift, datakommunikation
- Åtkomst- och behörighetsstyrning
- Systemutveckling, systemanskaffning och systemavveckling
- Kontinuitetsplanering
- Incidenthantering
- Granskning

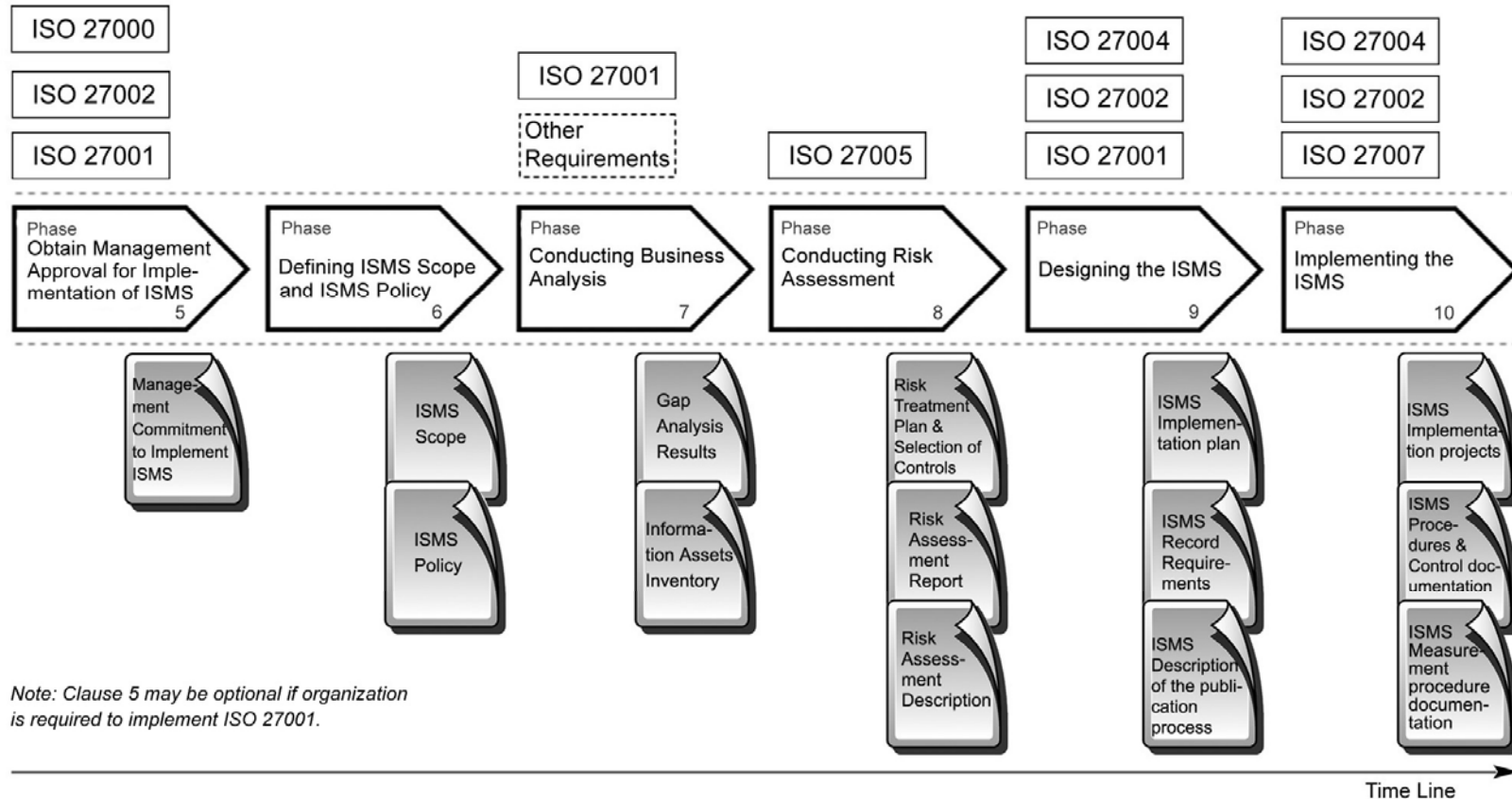
Kommentarer:

Sammanställ vad som finns idag på myndigheten – behöver anpassning göras ?

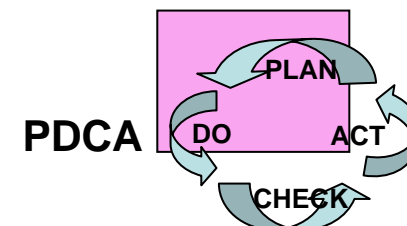
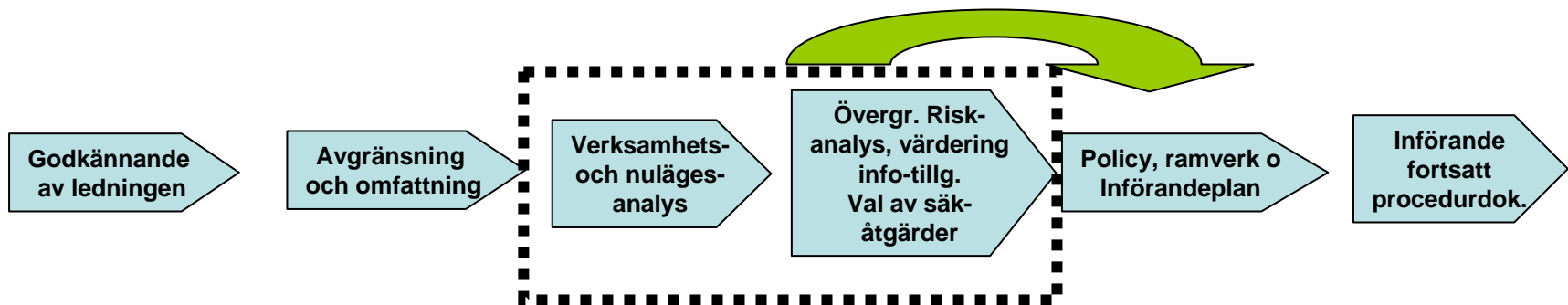
Ofta finns bra regelverk framtagna för hantering av IT-system, men behöver kanske ses över.

BITS ger goda råd eller kan vara en tillämpningsmetod för stora delar.

Ny standard på gång (ISO 27003) – ”vägledning för införande”



Införandesteg - översikt

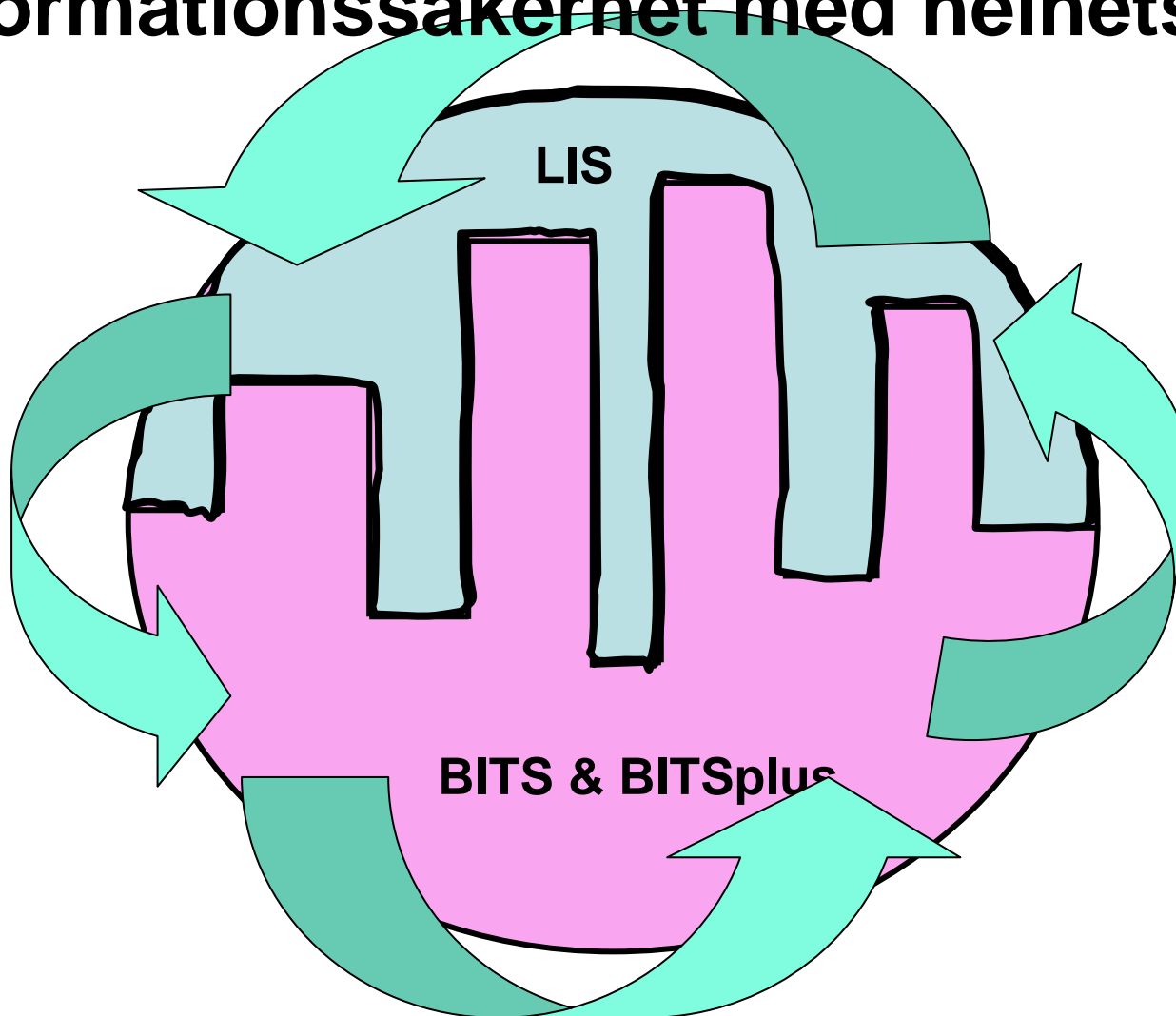


Planera – Genomföra – Följa upp - Förbättra

*Ansvar*et för föreskriften avses flyttas
Under 2009 till den nya
**Myndigheten för Samhällskydd
och Beredskap (MSB)**
som också får föreskriftsrätt när det
gäller informationssäkerhet



Informationssäkerhet med helhetssyn



”Ät elefanten i bitar”

Frågor ?

Kontakter på Krisberedskapsmyndigheten och Verva

Frågor om informationssäkerhet

- Wiggo Öberg, 08-593 71287, wiggo.oberg@kbm-sema.se

Juridiska frågor

- Martin Brinnen, 08-55 05 57 76, martin.brinnen@verva.se