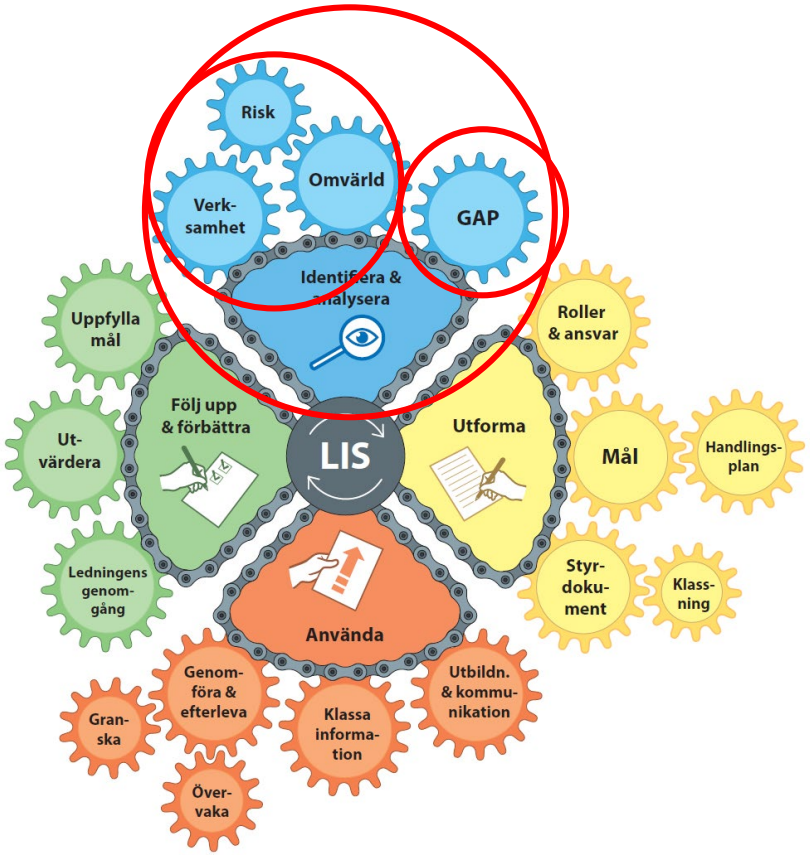
Säkerhetsåtgärder

Så minskar vi gapet

Vad är säkerhetsåtgärder?

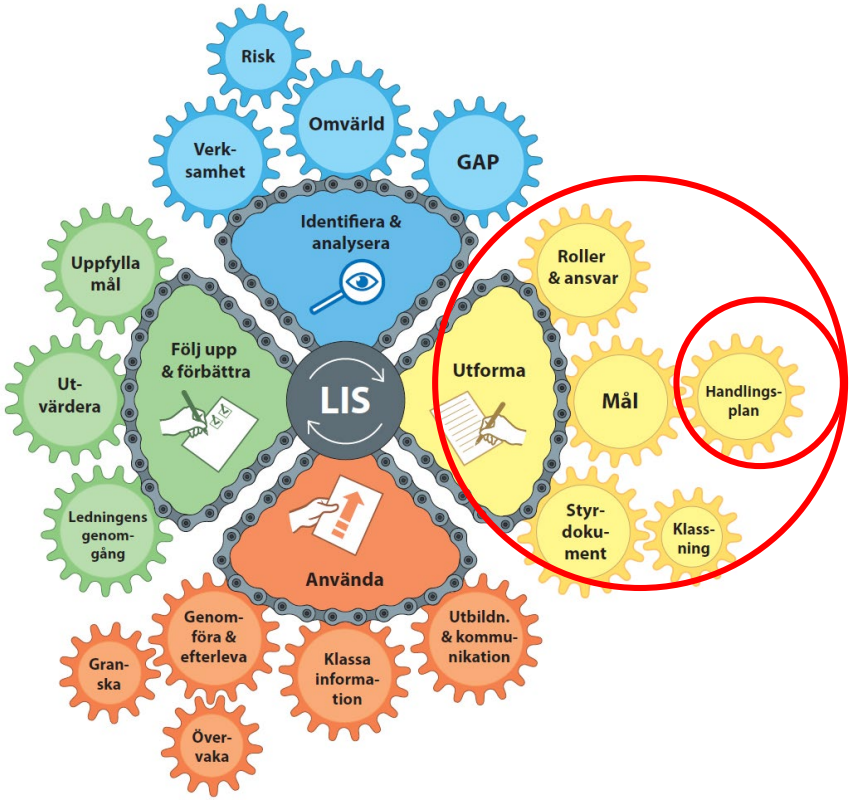
- Åtgärder för att **reducera identifierade risker**
  - För att nå informationssäkerhetsmålen
- Använder oss av analysresultatet
  - Alternativt utgå från SS-EN ISO/IEC 27001 (bilaga A)
    - Alltså säkerhetsåtgärderna från SS-EN ISO/IEC 27002
- Estimerar resurser
- Prioriterar mellan åtgärder
- Motivera åtgärderna

Var i sammanhanget?



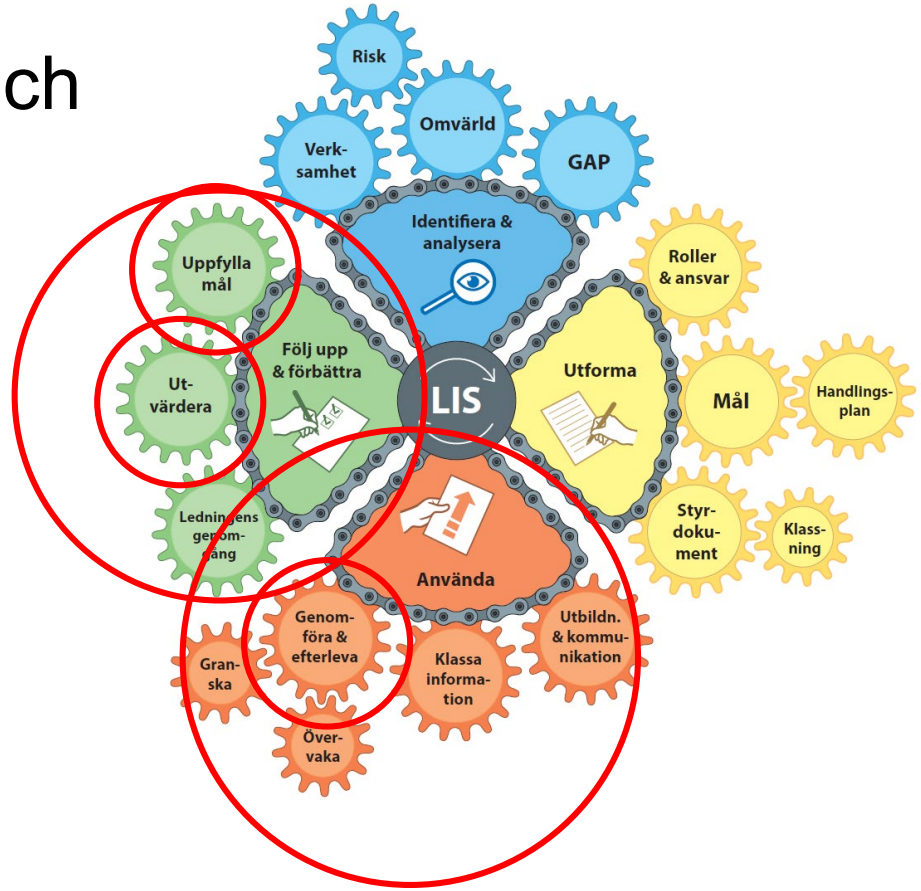
Var i sammanhanget?

Sedan behövs en handlingsplan

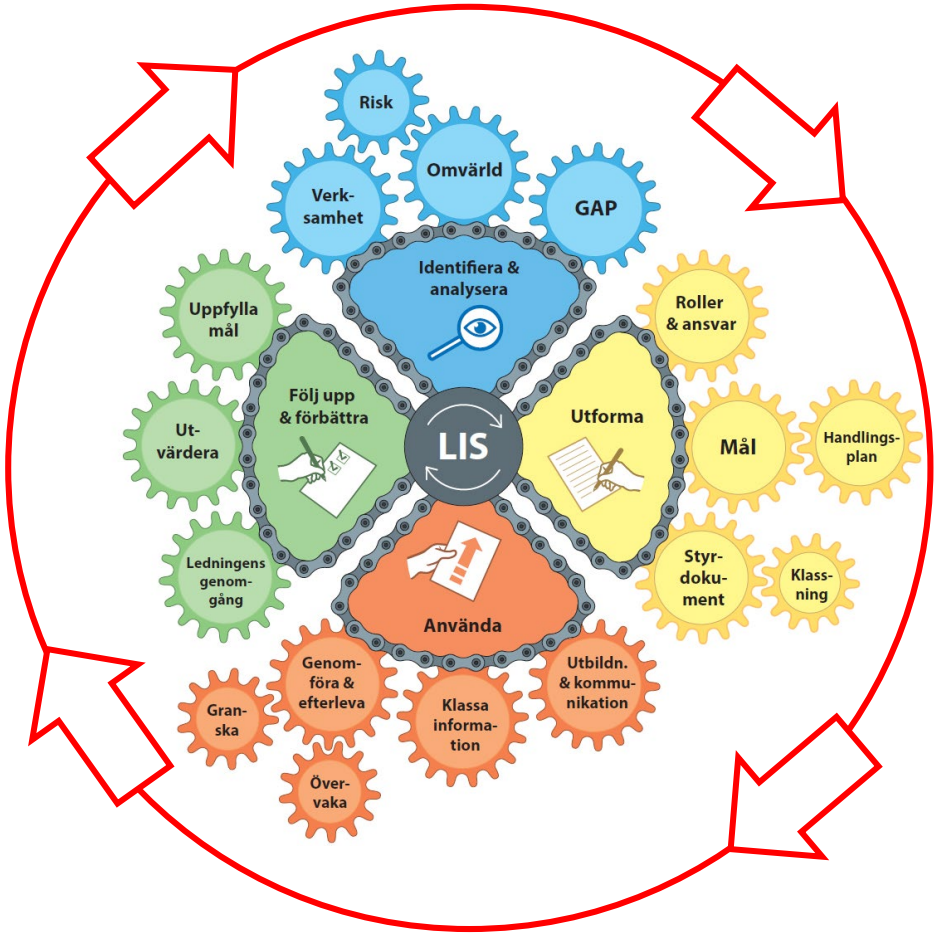


Var i sammanhanget?

Sedan ska riskerna åtgärdas och utvärderas mot målen

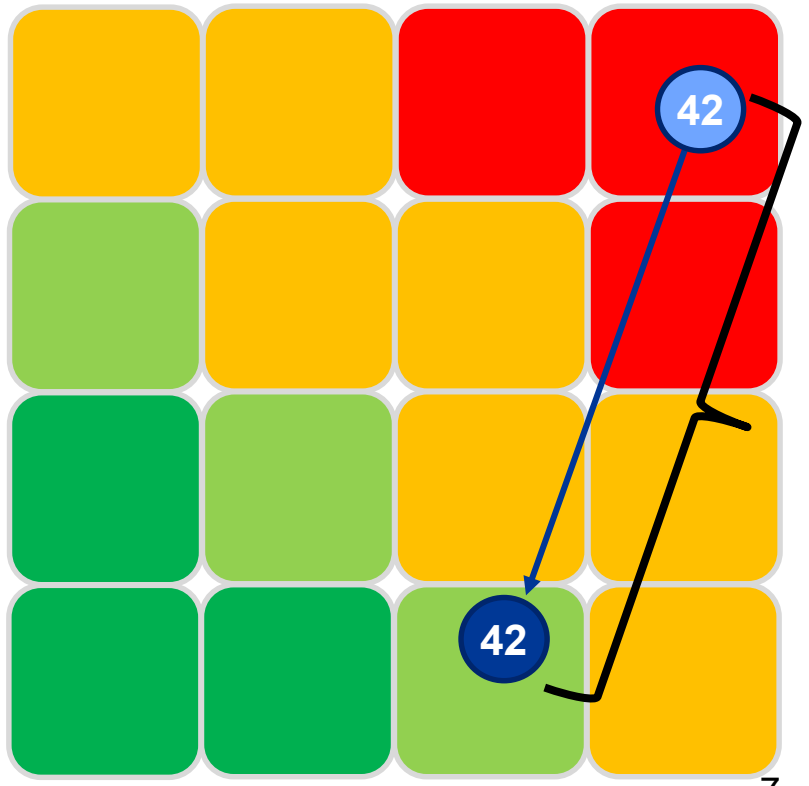


Var i sammanhanget?



Gapanalysen

- Hur stort är gapet mellan nuvarande status och målbilden?
- Har vi redan försökt att åtgärda denna risk?
- Vad behövs göras för att överbrygga gapet?
  - Vilka nya åtgärder kan behövas?



Välja säkerhetsåtgärder

Åtgärdsområden

- **Tekniska** (en förändring i nätverk eller informationssystemen)
- **Organisatoriska** (en resursförändring)
- **Processbaserade** (en förändring i arbetssätt)

Rimlighet och omfång

- **Ekonomiska**
- **Tidsmässiga**
- **Teknisk strategi**
- **Organisationens skyldigheter**
- **Intressenters krav**
- **Organisationens mål**
- **Riskkriterier**
- **Tillgängliga resurser**

Prioriteringar

- Bäst effekt för minsta insats
  - **Tid och pengar** är alltid två viktiga faktorer
- Åtgärder som reducerar de mest **kritiska bristerna**
- Åtgärder som är genomförbara med **tillgängliga resurser**
- Åtgärder inom område som **prioriteras** av organisationen
- Riskhanteringsalternativ utesluter nödvändigtvis inte varandra

Riskhanteringsalternativ

- Ett alternativ kan vara en eller flera av nedan alternativ:
  - Att **inte fortsätta** med aktiviteten
  - Att **inte påbörja** en viss aktivitet
  - Att ta eller öka risken för att kunna **tillvarata** en möjlighet
  - Att **eliminera** riskkällan
  - Att **förändra** sannolikheten
  - Att **förändra** konsekvenserna
  - Att **dela** risktagandet (t.ex. genom avtal eller genom att teckna försäkringar)
  - Att **dela** risken genom att en del tekniska delar bryts ut och läggs på andra system
  - Att **bibehålla** risken genom att fatta informerade beslut

Grundläggande IT-säkerhetsåtgärder

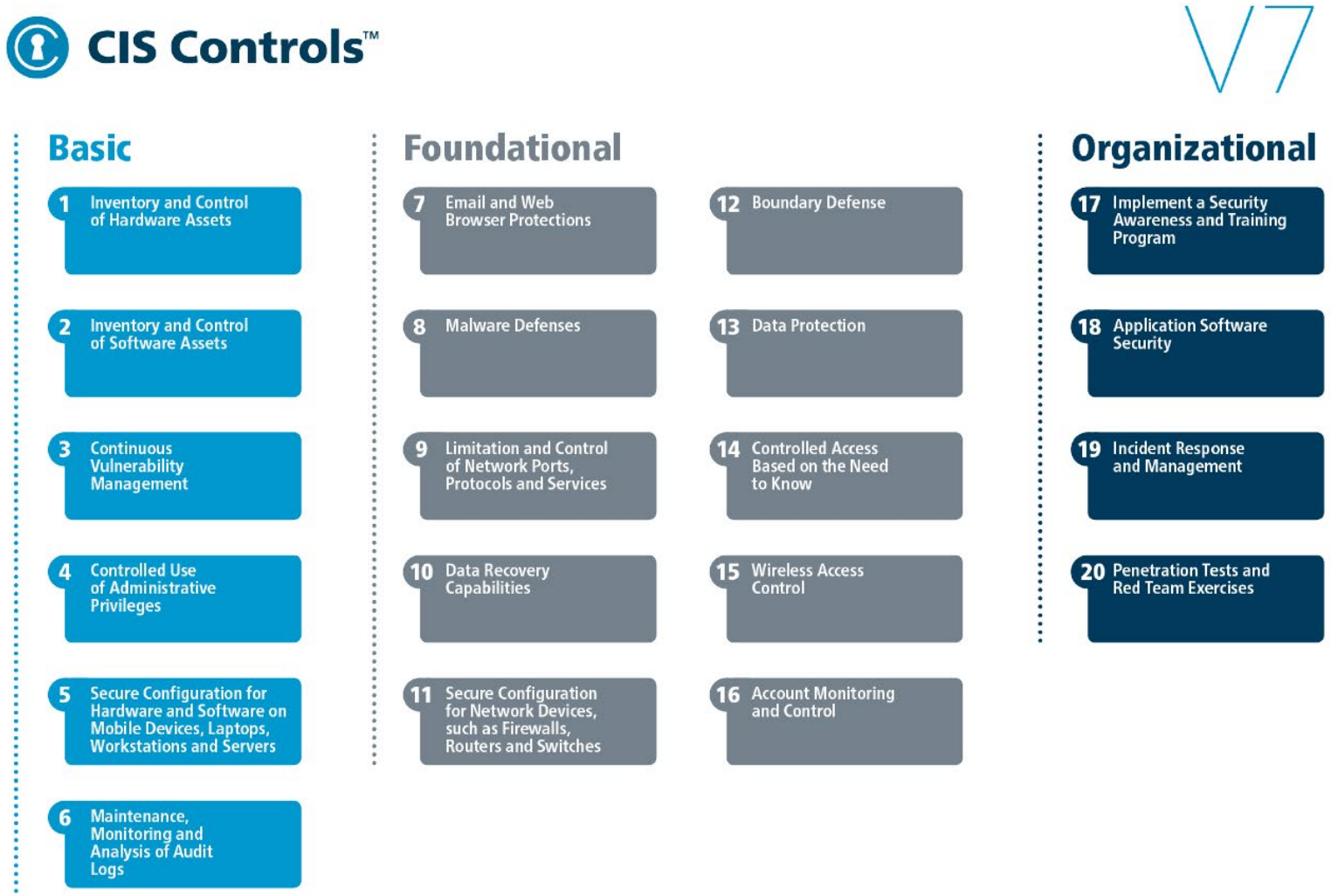
- MSB kommer ut med en lista av rekommenderade säkerhetsåtgärder
  - För de som har begränsade resurser och behöver komma igång

De tio viktigaste säkerhetsåtgärderna

1. Inför flerfaktorsautentisering
2. Installera säkerhetsuppdateringar så fort det går
3. Begränsa användningen av administratörsrättigheter (enligt least privileges)
4. Ändra lösenord som är förinställda vid leverans
5. Segmentera nätverken och filtrera trafiken mellan segmenten
6. Konfigurera säkerhetskopiering och testa återställning
7. Inför att endast godkänd programvara får köras (vitlistning) och inaktivera att makron körs
8. Inaktivera oanvända tjänster och protokoll
9. Konfigurera så att loggar skickas centralt och att dessa analyseras
10. Överväg noga riskerna vid utkontraktering och prioritera ökad säkerhet för inloggningar till externa tjänster (t.ex. molntjänster)

CIS-kontroller för ICS

(*Center for Internet Security*)



Handlingsplan

- *Riskhanteringsplan, riskbehandlingsplan, åtgärdsplan*
- När och hur säkerhetsåtgärderna ska införas
- Motivering av åtgärderna
- Ansvariga personer för godkännande och genomförandet
- Föreslagna aktiviteter
- Nödvändiga resurser
- Hur man gör mätningar av resultatet
- Begränsningar
- Rapportering och övervakning