Publ.nr: MSB1834 – sept 2021
ISBN 978-91-7927-185-5

Utbildning i systematiskt informationssäkerhetsarbete

Heldagsutbildning för lokala informationssäkerhetssamordnare utifrån MSB:s metodstöd

Myndigheten för samhällsskydd och beredskap

Agenda

Hej och välkommen!

- Presentation av deltagare och praktiska saker
- Målet med utbildningen

- Systematiskt informationssäkerhetsarbete

- Vårt informationssäkerhetsarbete

Paus

MSB:s metodstöd

- Presentation av det fiktiva företaget – underlag för uppgifterna

Identifiera och analysera

- Uppgift 1 – Identifiera informationstillgångar
- Uppgift 2 – Bedöma risker

Utforma

- Diskussion informationssäkerhetspolicy

Lunch

Använda

-Uppgift 3 – Klassa information

-Uppgift 4 – Välja säkerhetsåtgärder

Paus

Följa upp och förbättra

- Uppgift 5 – Presentera resultatet

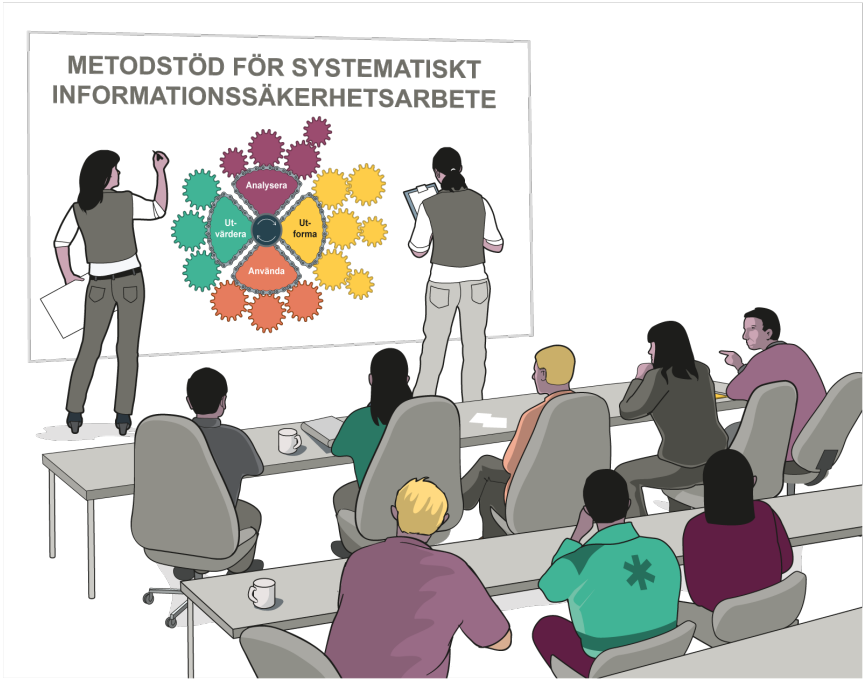
Utvärdering och avslutning

Myndigheten för samhällsskydd och beredskap

Vi som är här och praktiska saker

- Presentation av deltagarna
- Gruppindelning

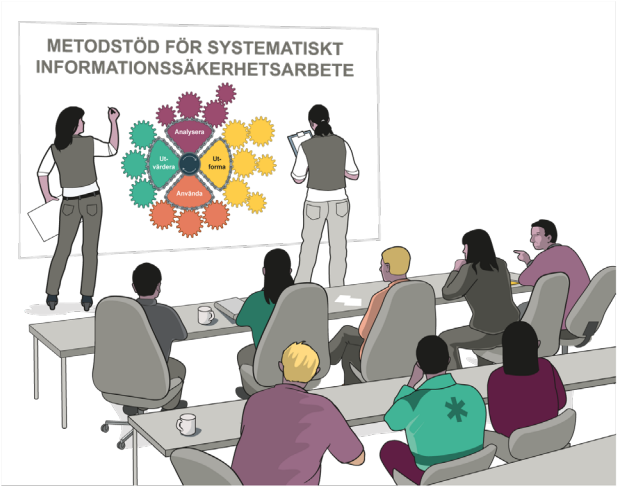
- Nödvändig information
  - Utrymningsvägar och återsamlingsplats
  - Toaletter
  - Om du behöver svara i telefon



Vi som är här och praktiska saker

- Presentation av deltagarna
- Gruppindelning

- Nödvändig information
  - Använd ”mute”-funktionen när du inte pratar
  - Använd chatten för att uppmärksamma mig på att du har frågor under de teoretiska passen
  - Om du behöver svara i telefon



Målet med utbildningen

Efter utbildningen kommer du att:

- Ha fått en grundläggande teoretisk förståelse för vad systematiskt informationssäkerhetsarbete är
- Praktiskt ha prövat på att
  - Identifiera informationstillgångar
  - Genomföra riskbedömning
  - Klassa information
  - Föreslå säkerhetsåtgärder
  - Presentera resultatet

Systematiskt informationssäkerhetsarbete

Varför informationssäkerhet är så viktigt

https://www.youtube.com/watch?v=2EM-dbwkA2Y

Vad är det som ska skyddas?

Information

så att informationens behov av skydd för konfidentialitet, riktighet och tillgänglighet upprätthålls

Korv 10 kronor

Informationen i Larm-systemet

Amanda har brutit benet och är sjukskriven i två månader!!!!

Drottninggatan 11, 132 54 Storköping

Myndigheten för samhällsskydd och beredskap

Vad är konfidentialitet, riktighet och tillgänglighet?

Konfidentialitet	att endast behöriga personer får ta del av informationen
Riktighet	att vi kan lita på att informationen är korrekt och inte manipulerad eller förstörd
Tillgänglighet	att informationen finns tillgänglig när behörig efterfrågar den

Vad ska information skyddas mot?

Felaktig hantering

Här står att min månadslön är 367 kronor – vad har hänt?

Det är alltid bra att veta vad ens kollegor gör

Jag kommer inte åt systemet nu – kan du återkomma?

Om jag bara tittar lite kort så gills det inte

Det är så praktiskt att man kan arbeta överallt t ex på café!

Myndigheten för samhällsskydd och beredskap

Hur skyddar vi informationen?

Med säkerhetsåtgärder

- Arbeta med **informationssäkerhet** på ett **systematiskt** och **riskbaserat** sätt, och
- Införa olika **säkerhetsåtgärde**r som **skyddar informationen** utifrån dess värde.

Systematiskt informationssäkerhetsarbete

Utgår från verksamheten

- Behov och interna krav
- Informationstillgångar
- Risker

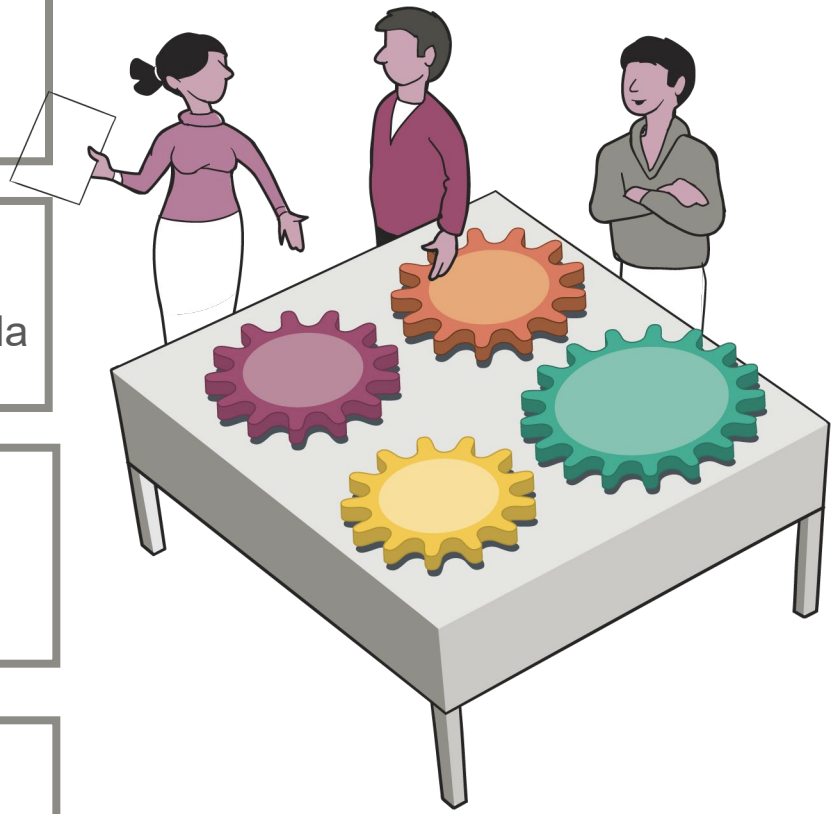
Görs genom att arbeta metodiskt

- Planera
- Analysera
- Dokumentera och använda

Tydliggör behov för organisationen

- Roller & ansvar
- Resurser och kompetens
- Regler och stöd

Utvärdera och förbättra regelbundet



Myndigheten för samhällsskydd och beredskap

Perspektiv på styrning och ansvar

- Leda
- Besluta
- Utföra arbetsuppgifter
- Följa upp

Roller och ansvar i det systematiska informationssäkerhetsarbetet

- Ledningen
- CISO – *Chief Information Security Officer*
- Övriga medarbetare med särskilt ansvar
  - Exempel på roller med särskilt ansvar: verksamhetschef, informationsägare, systemägare, it-säkerhetschef, dataskyddsombud, internrevisionen, lokala informationssäkerhetssamordnare
- Alla medarbetare

CISO och övriga roller med särskilt ansvar

CISO är inte ansvarig för all informationssäkerhet, men för att:

- Samordna informationssäkerhetsarbetet (taktisk nivå)
- Skapa förutsättningar för informationssäkerhet (alla tre nivåerna)

Övriga roller med särskilt ansvar kan ha olika uppgifter, till exempel:

- Fatta beslut
- Ta fram underlag
- Stödja
- Följa upp

Externa krav på att hantera information

Det finns lagar som styr informationshantering

- Offentlighets och sekretesslagen (OSL)
- Dataskyddsförordningen (GDPR)
- Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS)
- …

Andra externa krav kan finnas i till exempel överenskommelser

Systematiskt informationssäkerhetsarbete är ett arbetssätt för alla identifiera krav på och införa säkerhetsåtgärder som ger tillräckligt skydd för informationen.

PAUS

Vårt informationssäkerhetsarbete

Myndigheten för samhällsskydd och beredskap

Status i vårt systematiska informationssäkerhetsarbete

Vi har:

- [tex Informationssäkerhetspolicy]
- ……

Vi arbetar med att:

- [tex utifrån handlingsplanen för året…. uppdatera våra säkerhetsåtgärder]
- ……..

Myndigheten för samhällsskydd och beredskap

Min roll och mitt ansvar som CISO

Mitt ansvar

- X

Organisatorisk placering

- X

Tilldelad tid/antal ansvarsområden

- X

Att stödja verksamheter - en mycket viktig roll!

- Det du gör är avgörande för informationssäkerheten
- Du stödjer verksamheten i det operativa informationssäkerhetsarbetet

- När du träffar verksamheter passa på att:
  - Informera om våra interna regler
  - Lyssna efter problem verksamheterna upplever
  - Uppmuntra att anmäla incidenter

Att stödja verksamheter med informationssäkerhet

Ditt ansvar som lokal informationssäkerhetssamordnare är att

- Stödja verksamheter med metodkunskap och arbetssätt
- Arbeta på uppdrag och tillsammans med verksamheter för att
  - Identifiera informationstillgångar
  - Klassa informationen
  - Genomföra riskbedömningar
  - Föreslå säkerhetsåtgärder

Vad tänker du kring rollen? Vad kan vara svårt och vad finns som stöd?

MSB:s metodstöd

Beskriver ett tillvägagångssätt för att införa och utveckla det systematiska informationssäkerhetsarbetet i en organisation.

Metodstödet består av:

- Vägledningar
- Verktyg
- Utbildningsmaterial
- Exempel
- Kunskapsbank

Myndigheten för samhällsskydd och beredskap

Hur du kommer igång med arbetet med informationssäkerhet

https://www.youtube.com/watch?v=vMjJj07qKmQ

Det fiktiva företaget – underlag för uppgifterna

Företagspresentation

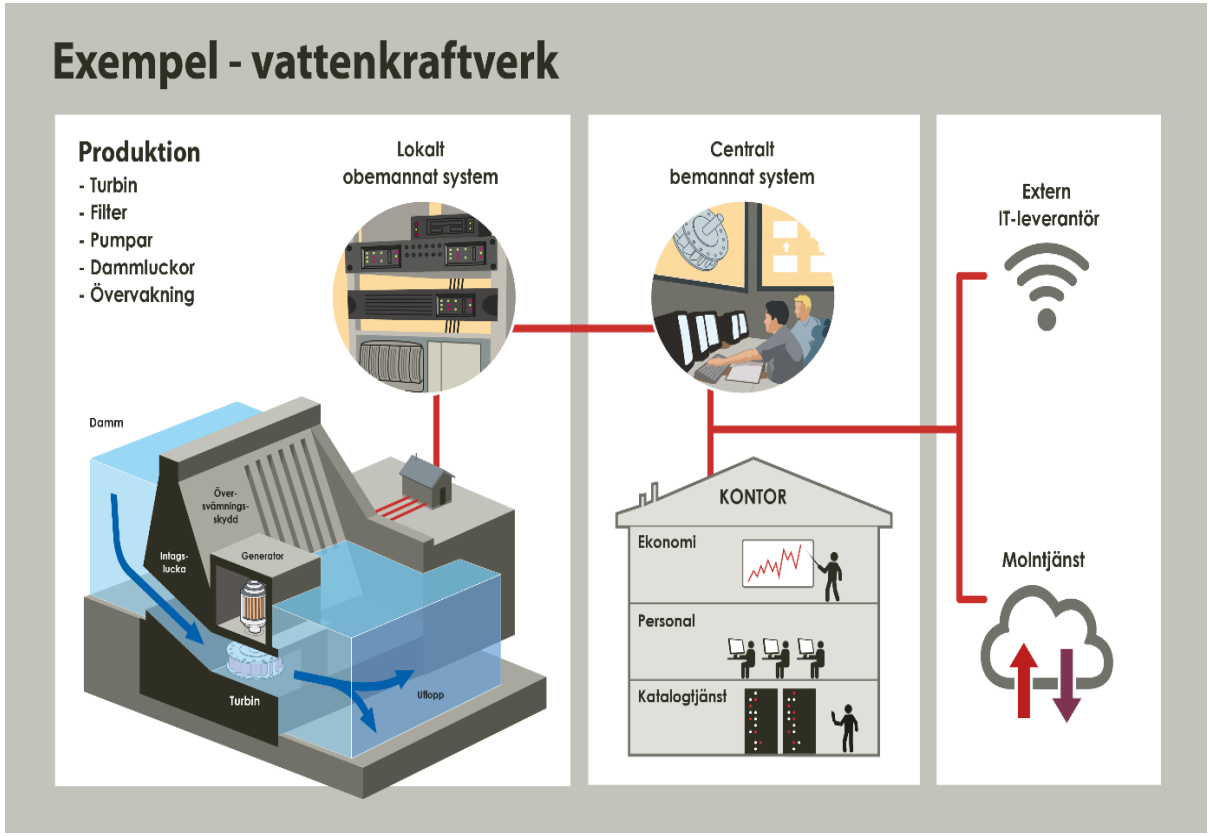
EL-VIS AB

”Vi ger förutsättningar för framtiden”

Myndigheten för samhällsskydd och beredskap

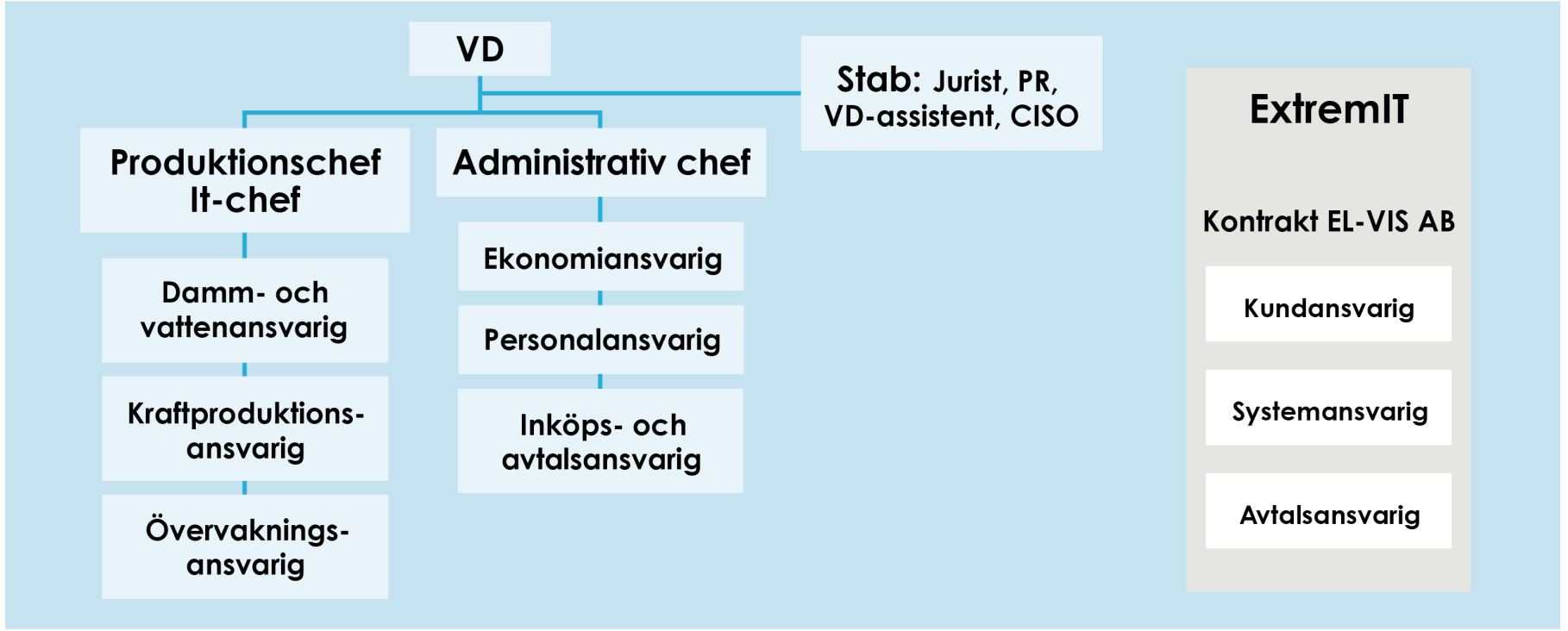
Om EL-VIS AB:s verksamhet

- Vattenkraftverk
- Damm och dammvall
- Genererar en effekt på ca 50MW ut på regionnätet



Myndigheten för samhällsskydd och beredskap

Om EL-VIS AB:s organisation



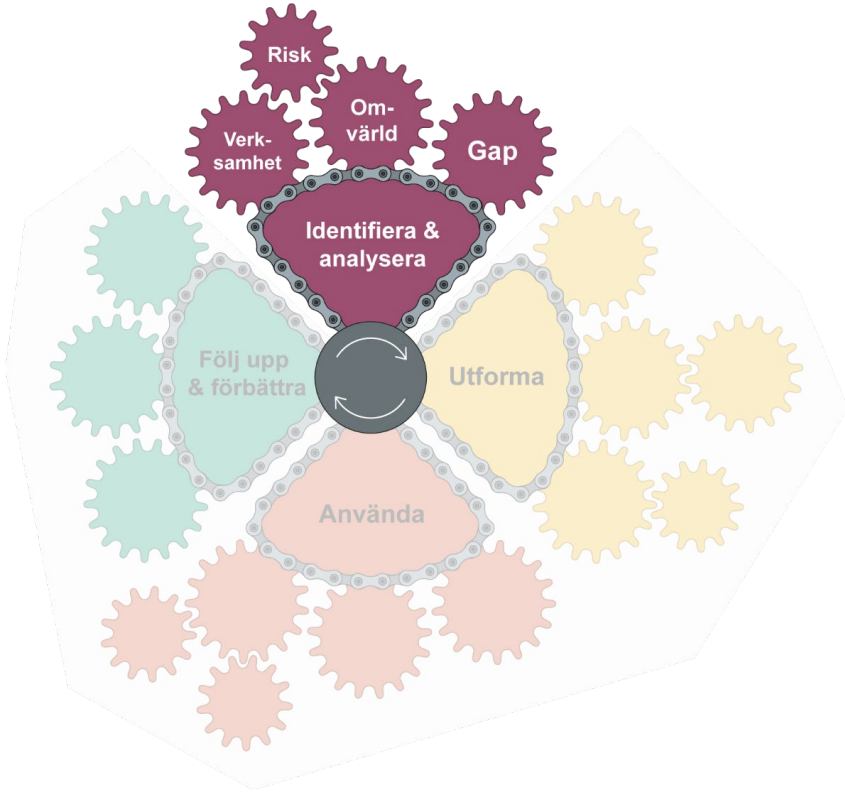
Informationssäkerhetsarbetet på EL-VIS AB

- Vi har en CISO som sitter organisatoriskt i staben.
- Vi har analyserat vilken reglering vi berörs av.
- Vi har tagit reda på vilken hotbild som finns generellt mot el-producenter.
- Vi har identifierat externa intressenter.

I *företagsbeskrivningen* hittar du mer information om företaget.

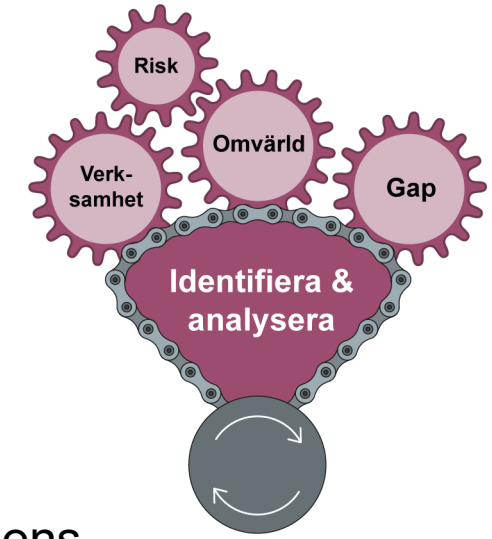
I *rollkorten* hittar du verksamhetsansvarigas kunskap om den information som hanteras i verksamheten.

Identifiera och analysera



Myndigheten för samhällsskydd och beredskap

Metodsteg – Identifiera och analysera



Beskrivning:

Analyser av verksamheten, omvärlden och organisationens övergripande informationssäkerhetsrisker.

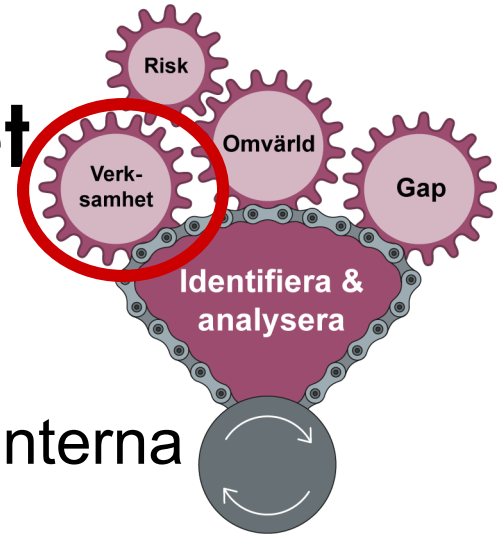
Utifrån resultatet av dessa analyser väljs vilka säkerhetsåtgärder som är relevanta för organisationen.

Här identifieras också skillnaden mellan informationssäkerhetsarbetets nuläge och det läge organisationen behöver befinna sig i.

Resultat:

- Förståelse för interna behov och externa krav
- Sammanställning av organisationens informationstillgångar
- Övergripande informationssäkerhetsrisker för organisationen
- Säkerhetsåtgärder från interna behov och externa krav från bland annat reglering och standarder samt status på dessa

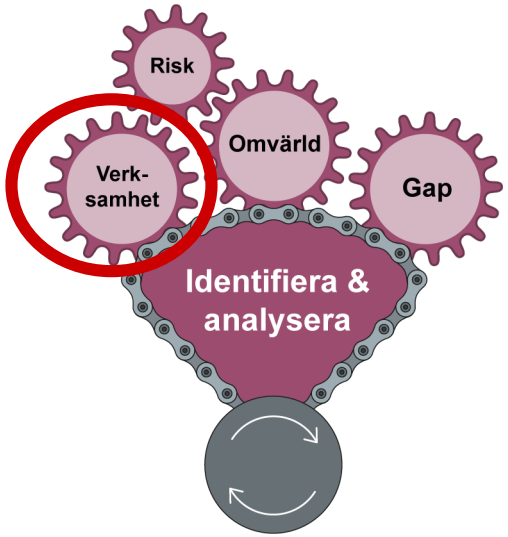
Analysera för att förstå din verksamhet



- Omvärldsanalys
- **Verksamhetsanalys**
- Riskanalys
- Gapanalys

- Identifiera era interna intressenter
- Identifiera era interna förutsättningar
- **Identifiera era informationstillgångar**.

Verksamhetsanalys – Identifiera informationstillgångar



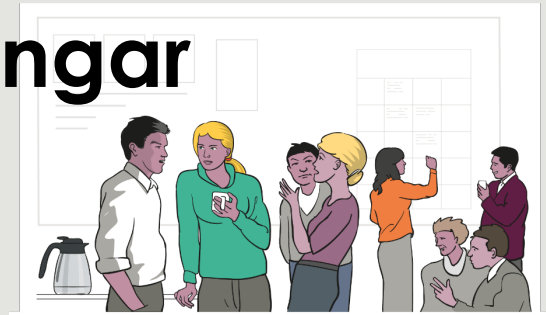
- Informationstillgångar är den information som organisationens olika verksamheter hanterar samt de resurser som behandlar informationen. Exempel på sådana resurser är it-system, usb-minne och utskrifter.
- Genom analysen identifierar vi det som informationssäkerhetsarbetet ska skydda.

Exempel – inventera informationstillgångar

ID	Benämning	Beskrivning	Information / data	Kritisk	Ägare	Kontakt
Info-0001	Exempel: Work&Save	Exempel: Lönesystem	Exempel: Personuppgifter, uppgift om lön samt sjukfrånvaro.	Ja	Anders Andersson	anders@elvisvattenkraft.se
Info-0002				Välj		
Info-0003				Välj		
Info-0004				Välj		

Några frågor?

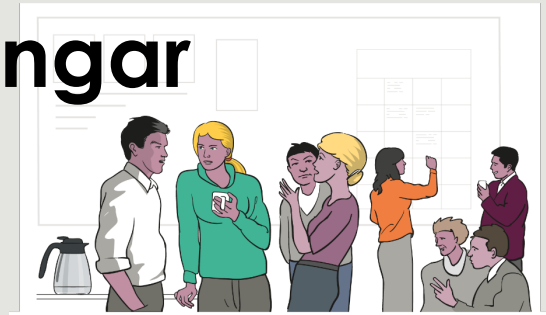
Uppgift 1: Identifiera informationstillgångar



- Arbeta i era grupper
- Intervjua den person som har den roll ni fått tilldelad om vilken information verksamheten hanterar och var den hanteras.
- Läs mer om uppgiften i uppgiftsbeskrivningen för uppgift 1: Identifiera informationstillgångar.
- Dokumentera informationstillgångarna i uppgiftsmallens flik uppgift 1: Identifiera informationstillgångar.

Frågor?

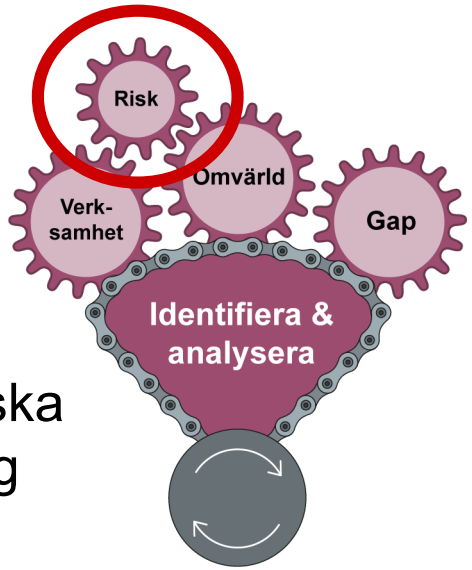
Uppgift 1: Identifiera informationstillgångar



- Arbeta i era grupper
- Utgå från rollkortet för den chef i det fiktiva företaget ni blivit tilldelade och identifiera vilken information verksamheten hanterar och var den hanteras.
- Läs mer om uppgiften i uppgiftsbeskrivningen för uppgift 1: Identifiera informationstillgångar.
- Dokumentera informationstillgångarna i uppgiftsmallens flik för uppgift 1: Identifiera informationstillgångar.

Frågor?

Bedöma risk



- Att identifiera och bedöma risker är en viktig del av det systematiska informationssäkerhetsarbetet och genomförs med olika omfattning och djup beroende på behov.
- Risk bedöms genom att identifiera oönskade händelser, hot mot verksamheter, som kan leda till negativa konsekvenser för organisationen.
- Arbetet går ut på att besvara de tre frågorna **”Vad kan hända?”**, **”Vad blir konsekvenserna?”** och **”Hur sannolikt är det?”**
- Utifrån bedömda risker tas en åtgärdsplan fram. Åtgärderna beskriver vad organisationen kan göra för att minska konsekvensen och/eller sannolikheten.

Bedömning av risk i förhållande till sanningen

- Viktigt att tänka på när man bedömer risker är att resultatet inte är ”sanningen”. Det är inte heller syftet. Bedömningen är en uppskattning av vad som kan hända som vi gör innan något oönskat har hänt, inte när vi vet hur det gick.
- Syftet är att förstå hot och sårbarheter som ger risker för att kunna ta fram underlag för beslut om vilka säkerhetsåtgärder som ska införas.

Definitioner vid bedömning av risk

En **risk** är en *möjlig* oönskad händelse

... till skillnad mot en **incident** som är en *inträffad* oönskad händelse

- **Hot** = något som orsakar eller bidrar till att en oönskad händelse inträffar (vad/vem?)
- **Sårbarhet** = avsaknad av något som skulle kunna förhindra att den oönskade händelsen inträffar (vad saknas/brister?)
- **Konsekvens** = vad händelsen resulterar i för problem för oss
- **Sannolikhet** = hur sannolikt det är att händelsen inträffar

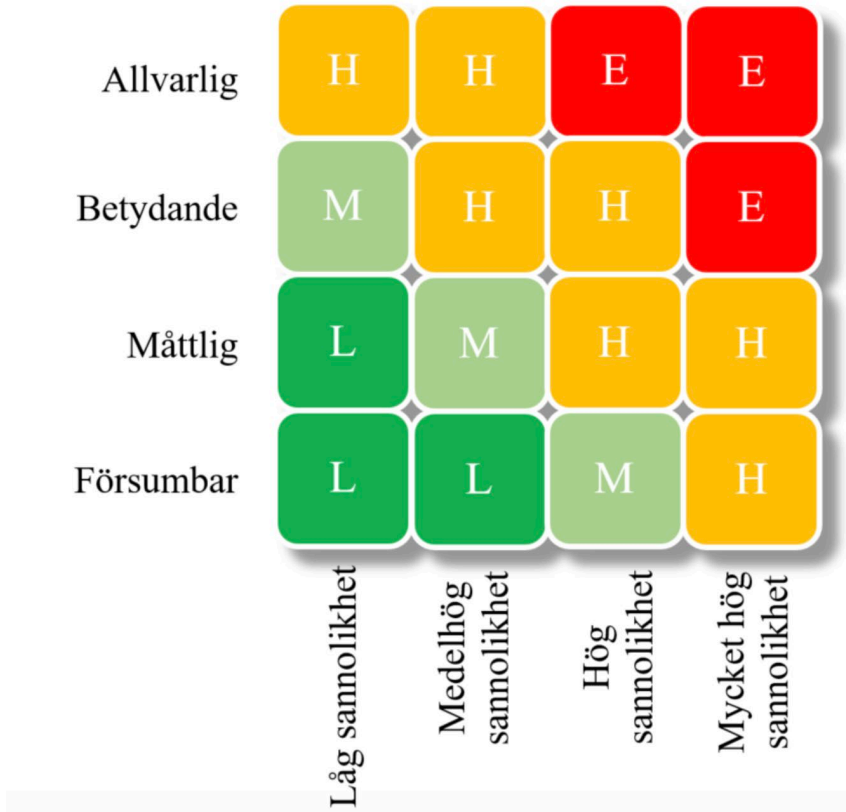
Exempel - konsekvensnivåer

Företagets riskmatris

	Verksamhetsförmåga	Förtroende	Ekonomisk förlust	Efterlevnad av rättsliga krav
Allvarlig	Ingen produktion av el på mer än en vecka. Övervakningen av produktionen fungerar inte på mer än 1 timme. HR-systemet nere under mer än 1 vecka runt löneutbetalning.	Dödsfall eller skada på egen personal som leder till bestående men. Allvarlig miljöskada enligt länsstyrelsens bedömning som leder till omfattande negativ publicitet i mer än en månad.	Förlust på mer än 2 miljoner eller 20% av budget.	Sådana brister i verksamheten att tillsynsmyndighet stoppar verksamheten, eller kräver investeringar på motsvarande kriterier för ekonomisk förlust.
Betydande	Ingen produktion av el på ett dygn. Övervakningen av produktionen fungerar inte på 30-60 minuter. HR-systemet nere under 4-7 dagar.	Skada på egen personal som innebär sjukskrivning upp till 3 månader. Miljöskada som innebär merarbete och negativ publicitet under mindre än en månad.	Förlust på mer än 1 miljon eller 10-20% av budget.	Sådana brister i verksamheten att tillsynsmyndigheten kräver stora investeringar motsvarande kriterier för ekonomisk förlust för att få fortsätta verksamheten.
Måttlig	Ingen produktion av el på upp till 4 timmar. Övervakningen av produktionen fungerar inte på 10-30 minuter. HR-systemet nere under 2-4 dagar.	Skada som leder till sjukskrivning, mindre än en månad. Miljöskada som leder till enstaka kortvarig negativ publicitet.	Förlust på mer än 500 000 kronor eller 5-10% av budget.	Brister som kräver investeringar på motsvarande kriterier för ekonomisk förlust.
Obetydlig/ Försumbar	Ingen produktion av el på 20 minuter. Övervakningen av produktionen fungerar inte på upp till under 10 minuter. HR-systemet nere under 24 timmar.	Obetydande skada på egen personal. Åter i tjänst inom ett par dagar. Miljöskada som kan åtgärdas på mindre än en vecka och som leder till enstaka upprörda inlägg i exempelvis sociala medier.	Förlust på minde än 500 000 kronor eller 5% av budget.	Brister som kräver åtgärder på motsvarande kriterier för ekonomisk förlust.

Exempel – sannolikhetsnivåer och riskmatris

Begrepp	Intervall
Mycket hög sannolikhet	1-10 ggr/år
Hög sannolikhet	0,5-1 ggr/år
Medelhög sannolikhet	0,05-0,5 ggr/år (mellan en gång vartannat till en gång per 20 år)
Låg sannolikhet	< 0,05 ggr/år (mindre än en gång per 20 år)

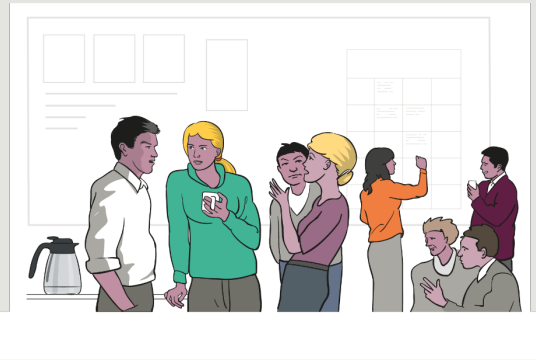


Exempel – bedöma risker

		Risk					
ID	Informationstillgång	Hot	Sårbarhet	Konsekvens	S	K	Kommentar
0	Sjukskrivningslistor	Kollega läser	Ligger i öppna mappar	Känslig information kommer i orätta händer	4	3	
1							
2							

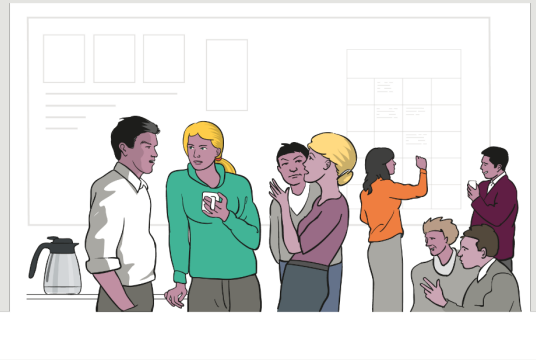
Några frågor?

Uppgift 2: Bedöm risker



- Arbeta i era grupper
- Intervjua den person som har den roll ni fått tilldelad om vilka händelser som skulle kunna påverka dennes verksamhet negativt och på vilket sätt.
- Läs mer om uppgiften i uppgiftsbeskrivningen för uppgift 2: Bedöm risker
- Dokumentera vilka risker ni ser med informationshanteringen och bedöm konsekvenserna utifrån riskmatrisen i uppgiftsmallens flik 2: Bedöm risker.

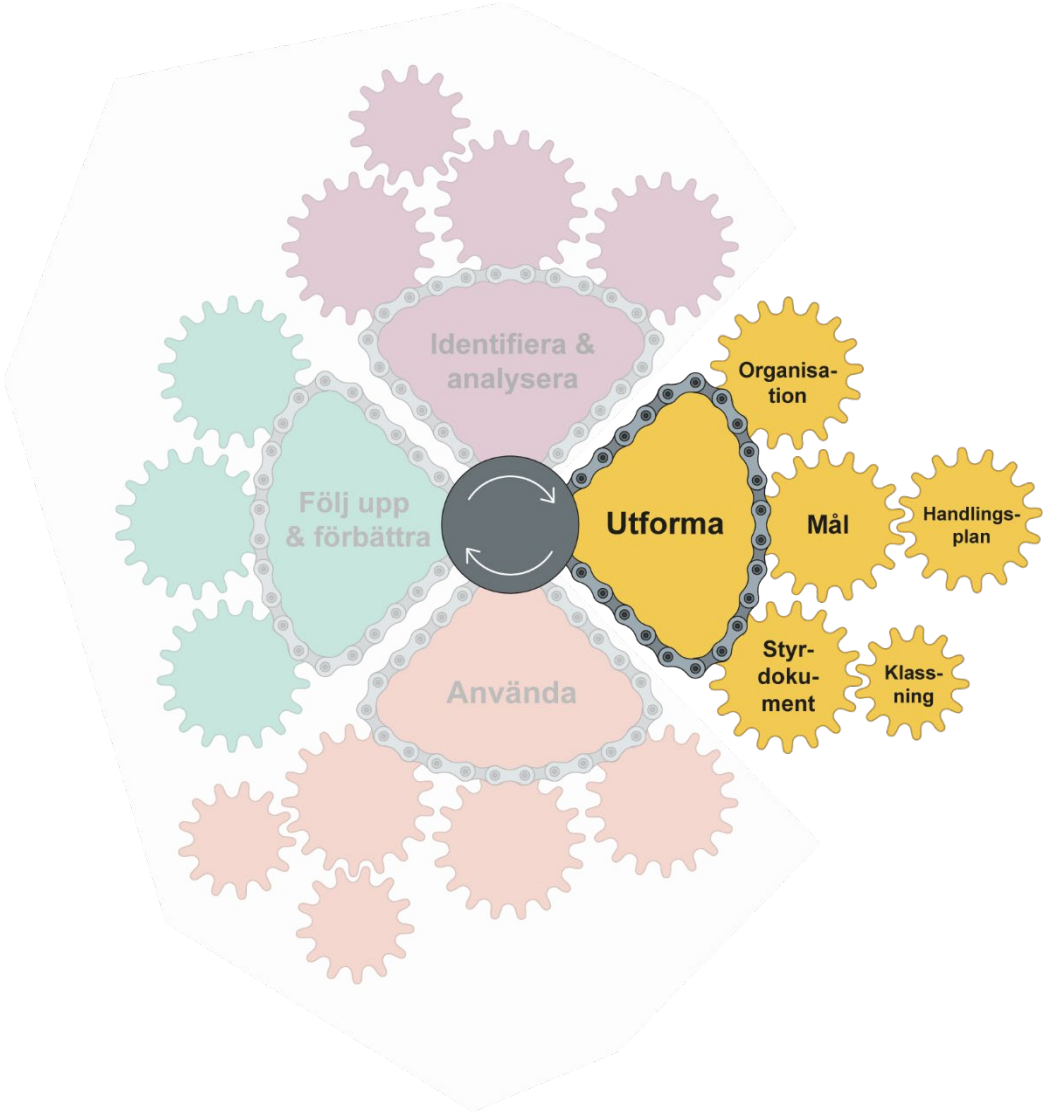
Uppgift 2: Bedöm risker



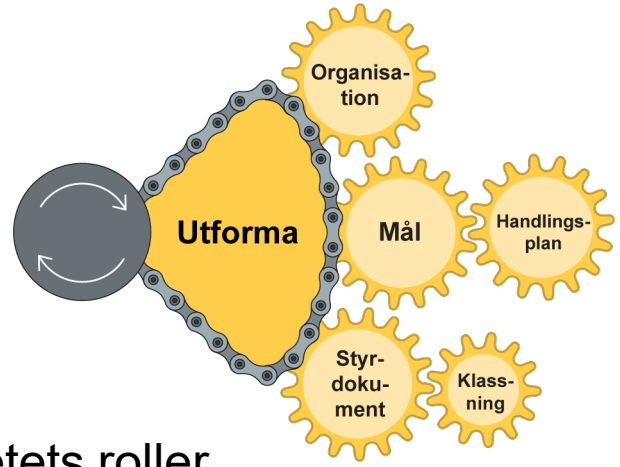
- Arbeta i era grupper
- I rollkortet för den chef i det fiktiva företaget ni blivit tilldelade beskrivs de problem denne ser med verksamhetens informationshantering.
- Läs mer om uppgiften i uppgiftsbeskrivningen för uppgift 2: Bedöm risker
- Dokumentera vilka risker ni ser med informationshanteringen och bedöm konsekvenserna utifrån riskmatrisen i uppgiftsmallens flik 2: Bedöm risker.

LUNCH

Utforma


Identifiera & analysera
Organisa-tion
Följ upp & förbättra
Utforma
Mål
Handlings-plan
Styr-doku-ment
Klass-ning
Använda

Metodsteg – Utforma



Beskrivning:

I steget Utforma utvecklar man material och arbetssätt som behövs för det systematiska informationssäkerhetsarbetet.

Allt material kan inte tas fram på en gång utan tas fram och förbättras utifrån vad som saknas och prioriterats.

Resultat:

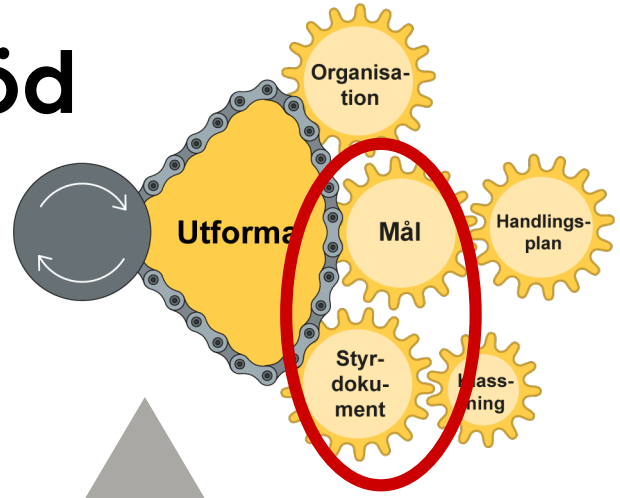
- Informationssäkerhetsarbetets roller och deras ansvar
- Mål för informationssäkerheten
- Styrdokument med tillhörande stöd
- En klassningsmodell för att värdera informationstillgångar
- Handlingsplaner där åtgärder som ska genomföras för att förbättra informationssäkerheten dokumenterats.

Att utforma det material som behövs

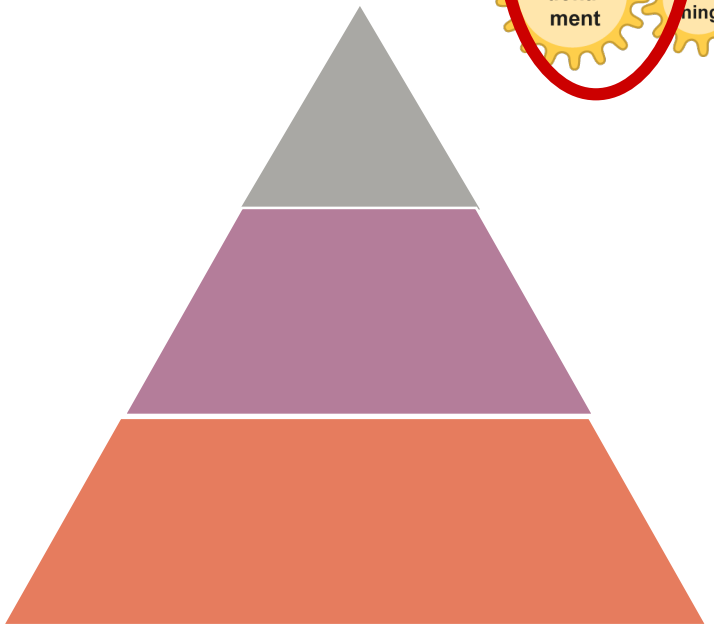
Utformningen sker utifrån strategiska mål och verksamhetens behov

Material på alla nivåer behöver utformas, användas och förbättras

Mål, styrdokument och tillhörande stöd



- **Informationssäkerhetspolicy**
  - Beskriver ledningens mål och inriktning för vad informationssäkerhetsarbetet ska uppnå. Allt informationssäkerhetsarbete utgår från policyn.
- **Anvisningar/riktlinjer**
  - Övergripande krav, regler och rekommendationer.
- **Instruktioner/rutiner**
  - Specifika krav, regler och rekommendationer.
  - Arbetsbeskrivningar för specifika uppgifter.
- **Stöd**
  - Mallar, utbildningsmaterial, planer och annat material som ger stöd i arbetet med att uppfylla kraven.



Myndigheten för samhällsskydd och beredskap

Informationssäkerhetspolicy – ledningens mål

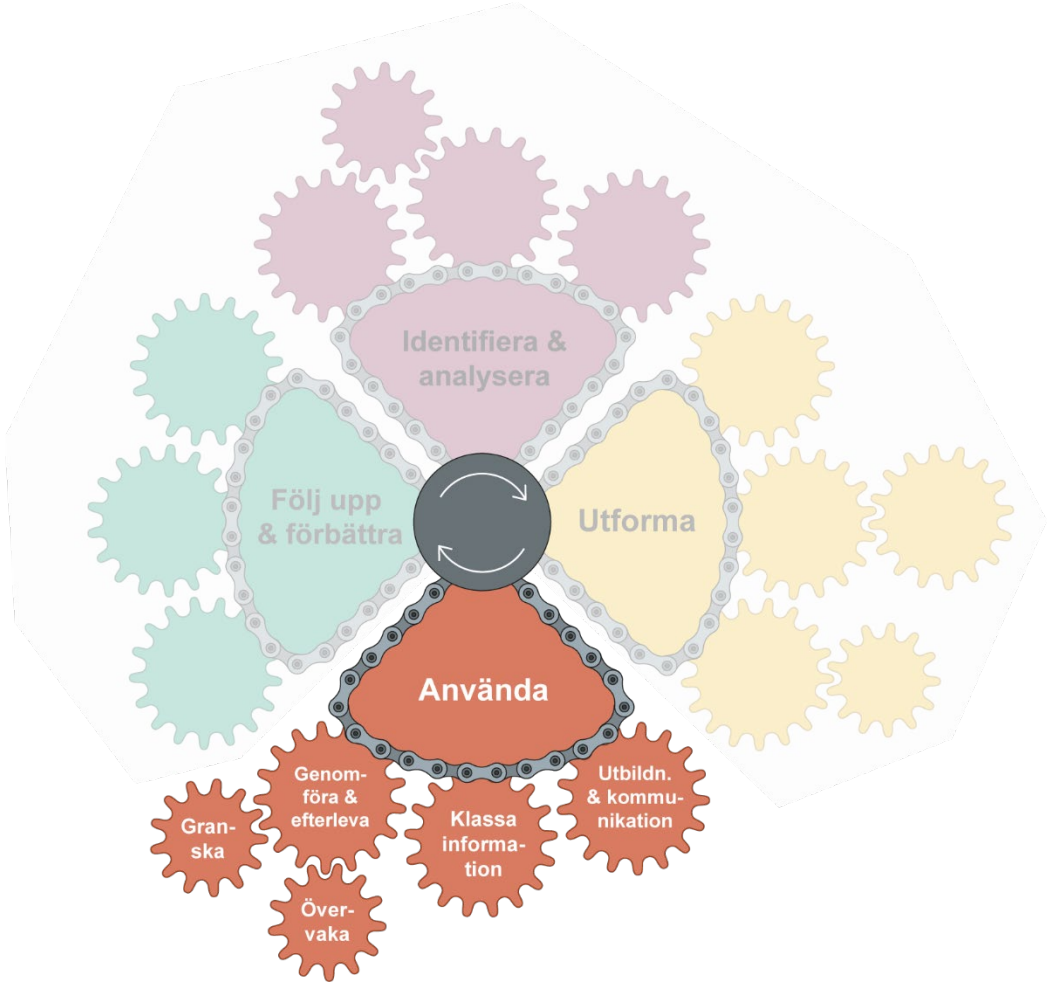
På El-Vis AB skyddar vi vår elproduktion och den data vi behöver för att producera el.

Vi inför tekniska skydd så att ingen annan än vår personal kan förändra informationen för våra styr- och reglersystem.

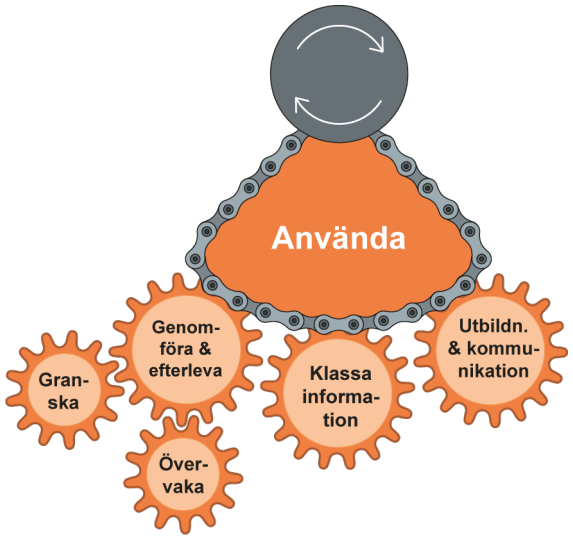
Informationssäkerhetsarbetet stödjer företaget genom att vara effektivt, flexibelt och ge tillräckligt stöd till företagets ledning.

Vad är bra respektive mindre bra med policyn?

Använda


Identifiera & analysera
Följ upp & förbättra
Utforma
Använda
Gran-ska
Genom-föra & efterleva
Över-vaka
Klassa informa-tion
Utbildn. & kommu-nikation

Metodsteg – Använda



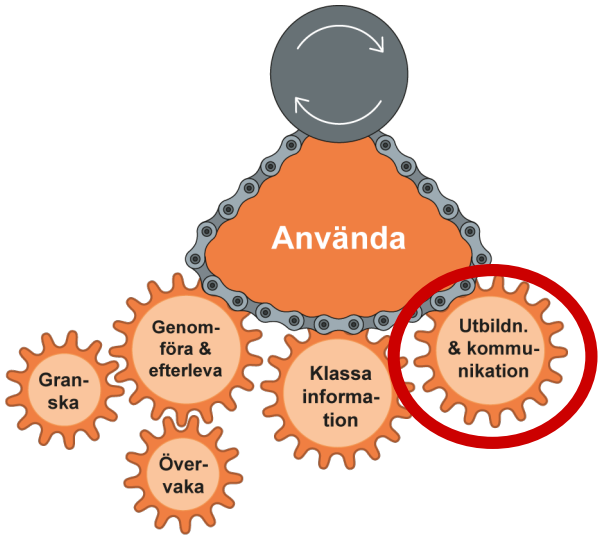
Beskrivning:

Här används styrande dokument, arbetssätt, stöd och övrigt material som tagits fram i Utforma. Åtgärdsplaner genomförs. Utbildnings- och kommunikationsinsatser till olika roller beroende på deras ansvar görs utifrån behov.

Resultat:

- Arbete utifrån styrdokument, stöd och ansvar
- Utbildnings- och kommunikations-aktiviteter
- Klassad information
- Införda säkerhetsåtgärder

Utbilda och kommunicera



Utbilda olika roller utifrån identifierat behov

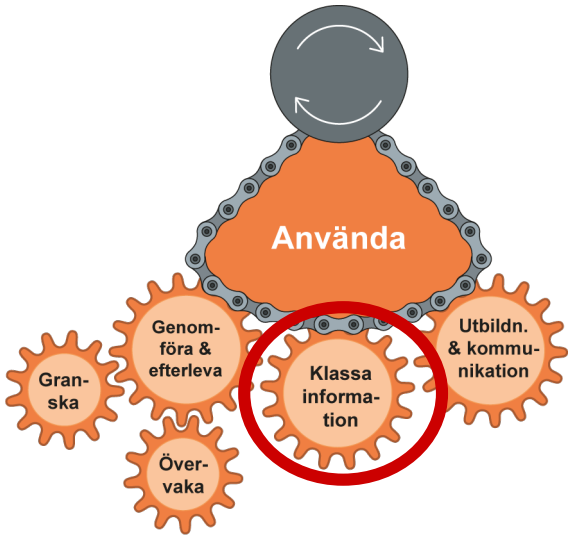
Informera när möjlighet ges om våra:

- styrande dokument
- stödjande dokument
- Arbetssätt

Var lyhörd inför upplevda problem

Följ styrande dokument, ta hjälp av stödjande dokument, fråga om du är osäker och anmäl problem!

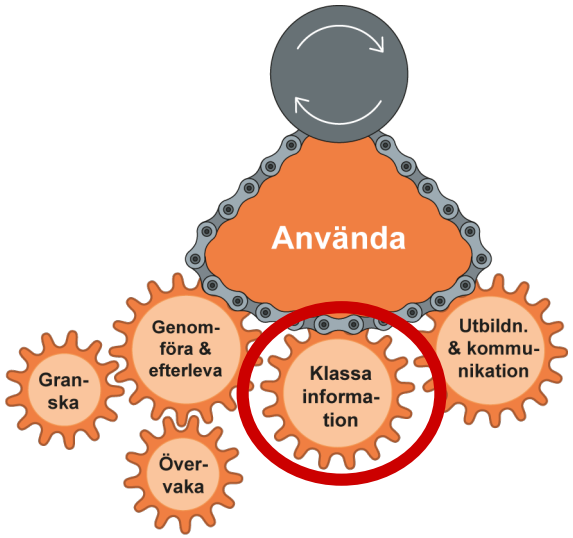
Klassa information



Värdera information utifrån organisationens klassningsmodell för att

- Förstå informationens värde för organisationen
- Hitta kritisk och känslig information
- Få ett underlag inför att välja säkerhetsåtgärder

Klassa information



Värderingen sker utifrån modellens kriterier för:

- Konfidentialitet
- Riktighet
- Tillgänglighet

- Visar på vilket sätt informationen är kritisk och känslig

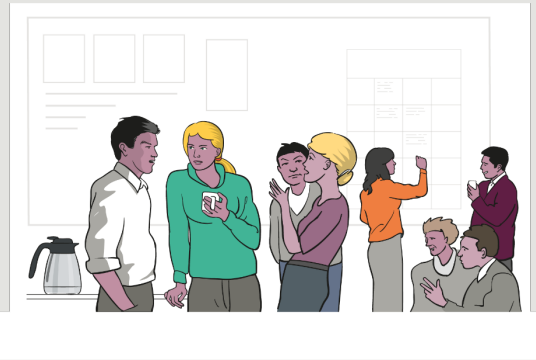
Exempel – informationsklassningsmatris

	Nivå	Konfidentialitet	Riktighet	Tillgänglighet
3	**Allvarlig**	**K3** **Mycket känslig** information där förlust av konfidentialitet kan leda till allvarliga konsekvenser för verksamhetens förmåga, förtroende eller skonomisk förlust.	**R3** Information där förlust av riktighet kan leda till allvarliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	**T3** Information där förlust av tillgänglighet kan leda till allvarliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.
2	**Betydande**	**K2** **Känslig** information där förlust av konfidentialitet kan leda till höga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	**R2** Information där förlust av riktighet kan leda till höga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	**T2** Information där förlust av tillgänglighet kan leda till höga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.
1	**Måttlig**	**K1** **Intern** information där förlust av konfidentialitet kan leda till måttliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	**R1** Information där förlust av riktighet kan leda till måttliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	**T1** Information där förlust av tillgänglighet kan leda till måttliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.
0	**Obetydlig eller försumbar**	**K0** **Öppen** information där förlust av konfidentialitet inte kan leda till några konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	*Krav finns alltid att information ska vara riktig, bedöms ej.*	*Krav finns alltid att information ska vara tillgänglig, bedöms ej.*

Exempel – Klassa information

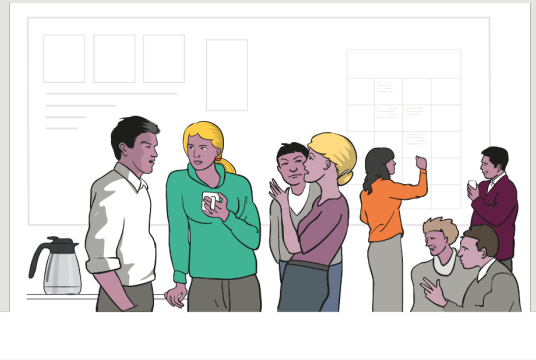
ID	Klassningsobjekt	Beskrivning/innehåll i klassningsobjektet	K	R	T	Kommentar till bedömningen
1	[T.ex. viss handling, fält i databas]	[T.ex. namn, **adress**, artikel-ID, belopp]	Välj	Välj	Välj	[Motiviering, andra viktiga förhållanden, m.m.]
2	[tex informationstyp_adress]		1	2	3	

Uppgift 3: Klassa information



- Arbeta i era grupper
- För över information/data från uppgift 1: Identifiera informationstillgångar till uppgift 3: Klassa information
- Klassa informationen - bedöm de negativa konsekvenser som kan uppstå vid förlust av konfidentialitet, riktighet och tillgänglighet.
- Läs mer om uppgiften i uppgiftsbeskrivningen för uppgift 3: Klassa information
- För in resultatet i uppgiftsmallens flik uppgift 3: Klassa information.

Uppgift 3: Klassa information



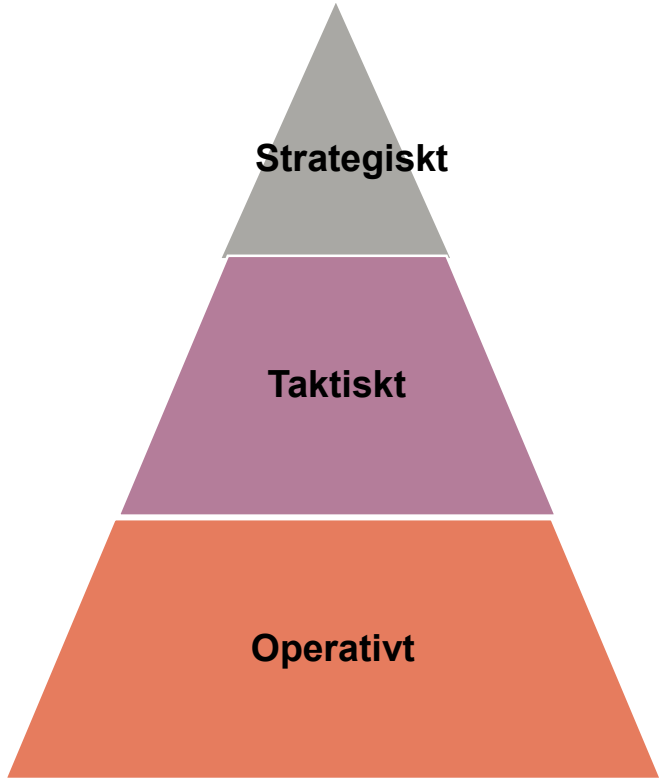
- Arbeta i era grupper
- För över information/data från uppgift 1: Identifiera informationstillgångar till uppgift 3: Klassa information
- Klassa informationen - bedöm de negativa konsekvenser som kan uppstå vid förlust av konfidentialitet, riktighet och tillgänglighet.
- Läs mer om uppgiften i uppgiftsbeskrivningen för uppgift 3: Klassa information
- För in resultatet i uppgiftsmallens flik uppgift 3: Klassa information.

Ta fram förslag på säkerhetsåtgärder

- Säkerhetsåtgärder från olika källor
  - Säkerhetskrav från ISO 27001 bilaga A och rekommendationer från 27002
  - Organisationens egna säkerhetskrav

Säkerhetsåtgärder på olika nivåer

- En säkerhetsåtgärd för hela organisationen
- Olika styrka i säkerhetsåtgärderna utifrån behov
- Anpassning av säkerhetsåtgärder i verksamheten



Olika typer av säkerhetsåtgärder

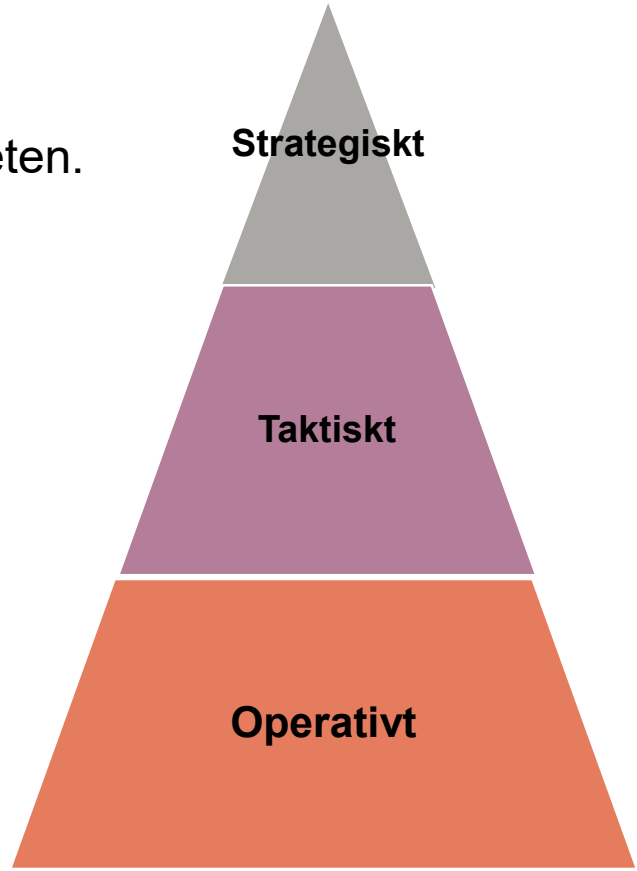
- Organisatoriska
- Administrativa
- Tekniska
- Fysiska

- Kombineras för att få tillräckligt skydd

Handlingsplan

- En handlingsplan
  - Sammanställning av åtgärder som förbättrar informationssäkerheten.
  - Handlingsplaner finns för olika delar av organisationen.
  - Ansvarig beslutar om vilka åtgärder som ska införas och hur de ska följas upp.

- Exempel på handlingsplaner
  - Organisationens övergripande handlingsplan för informationssäkerhetsarbetet (3–5 år)
  - CISOS årliga handlingsplan
  - Chefers handlingsplaner för olika verksamheter



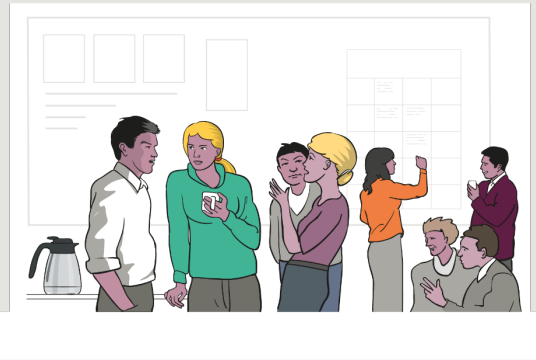
Myndigheten för samhällsskydd och beredskap

Exempel – Ta fram förslag på säkerhetsåtgärder

Säkerhetsåtgärd	Beskrivning	Ja/Nej	Anteckning
6.1.1 Informationssäkerhetsroller och ansvar	Allt ansvar för informationssäkerhet bör definieras och tilldelas.	Välj	
6.1.2 Uppdelning av arbetsuppgifter	Ansvar och ansvarsområden som står i konflikt med varandra bör åtskiljas för att minska möjligheterna för obehörig eller oavsiktlig ändring eller missbruk av organisationens tillgångar.	Välj	
6.2.1 Regler för mobila enheter	Regler och stödjande säkerhetsåtgärder bör antas för att hantera de risker som användning av mobila enheter medför.	Välj	

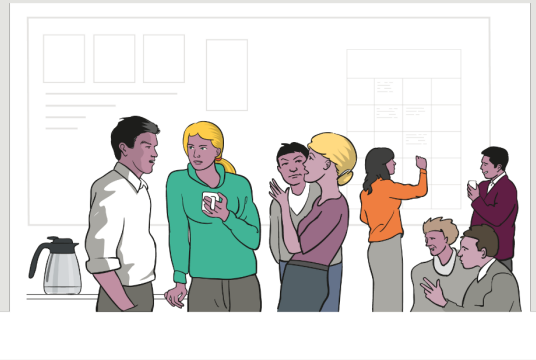
Några frågor?

Uppgift 4: Ta fram förslag på säkerhetsåtgärder



- Arbeta i era grupper
- Ni har klassat information och identifierat risker
- Ta fram lämpliga säkerhetsåtgärder som skyddar informationen på ett tillräcklig sätt
  - Organisatoriska, Administrativa, Tekniska, Fysiska?
  - Kombinationer?
- Läs mer om uppgiften i uppgiftsbeskrivningen för uppgift 4: Ta fram förslag på säkerhetsåtgärder
- Dokumentera era förslag på säkerhetsåtgärder i en hanteringsplanen i uppgiftsmallens flik uppgift 4: Välj säkerhetsåtgärder

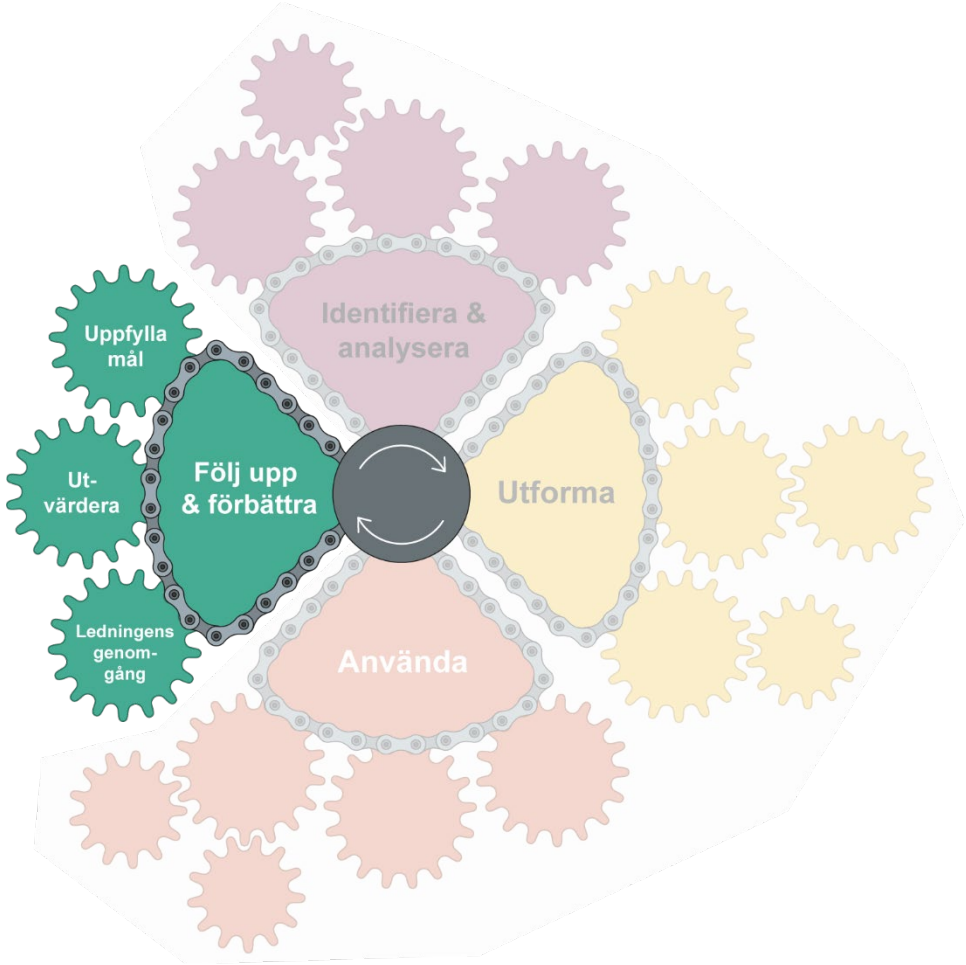
Uppgift 4: Ta fram förslag på säkerhetsåtgärder



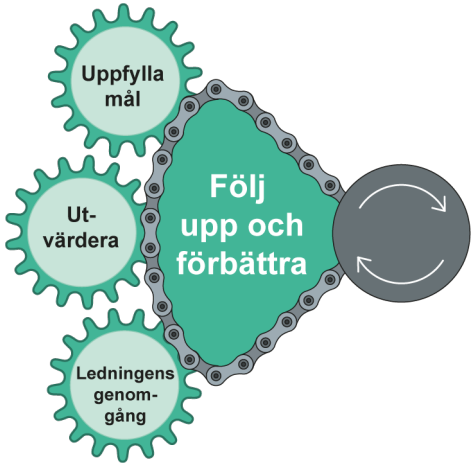
- Arbeta i era grupper
- Ni har klassat information och identifierat risker
- Ta fram lämpliga säkerhetsåtgärder som skyddar informationen på ett tillräcklig sätt
  - Organisatoriska, Administrativa, Tekniska, Fysiska?
  - Kombinationer?
- Läs mer om uppgiften i uppgiftsbeskrivningen för uppgift 4: Ta fram förslag på säkerhetsåtgärder
- Dokumentera era förslag på säkerhetsåtgärder i en hanteringsplanen i uppgiftsmallens flik uppgift 4: Välj säkerhetsåtgärder

PAUS

Följa upp och förbättra



Metodsteg – Följa upp och förbättra



Beskrivning:

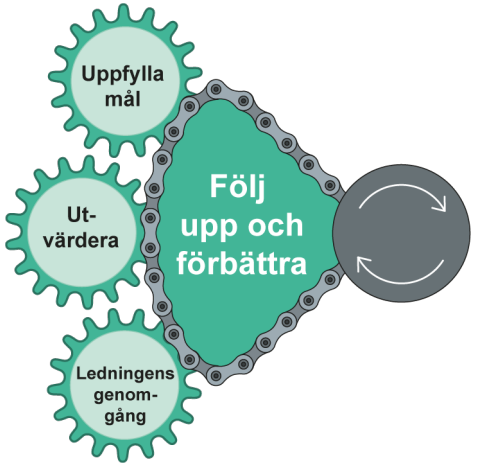
Att följa upp och förbättra såväl arbetssättet som säkerhetsåtgärder genomförs vid behov men också vid planlagda tillfällen.

Resultatet av uppföljningen blir ingångsvärden till att förbättra informationssäkerheten.

Resultat:

- Underlag för att bedöma om säkerhetsåtgärderna är tillräckliga
- Handlingsplanerna uppdaterade med säkerhetsåtgärder beslutade av ansvarig

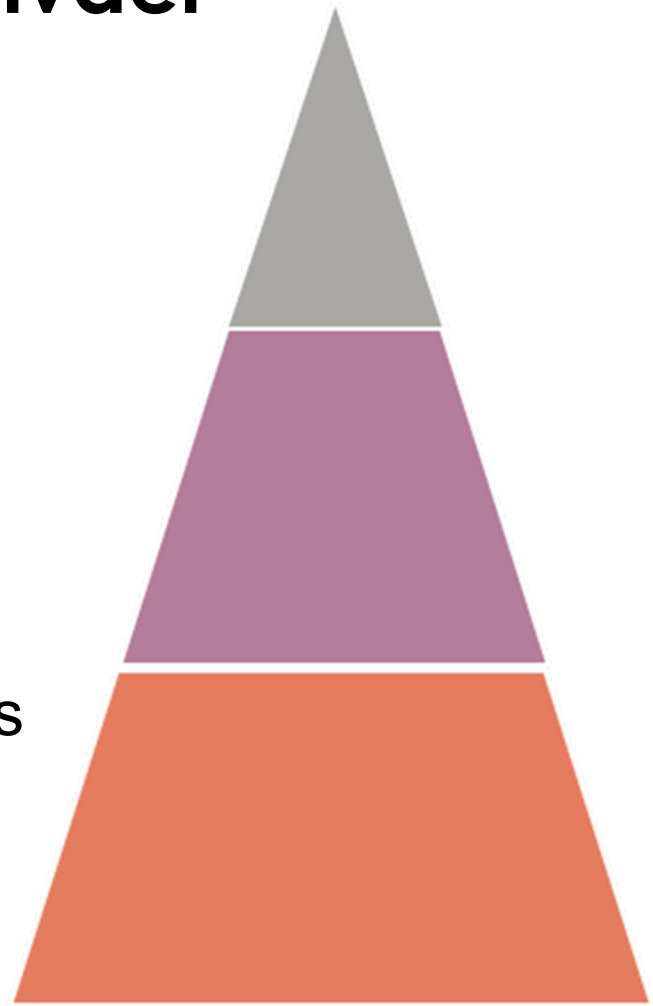
Följa upp och förbättra



- Vad har vi gjort och vad har vi kvar att göra?
- Vad fungerar bra och vad behöver vi ändra?
- Följer vi upp rätt saker på rätt sätt?
- Vad kan vi förbättra/utveckla?

Följa upp och förbättra på olika nivåer

- Hur väl följer vi ledningens beslutade mål
- Hur fungerar arbetssätt för att nå säker informationshantering
- Status på åtgärder i handlingsplaner
- Hur bra är införda säkerhetsåtgärder
- Vilka identifierade risker har ännu inte åtgärdats



Myndigheten för samhällsskydd och beredskap

Exempel – Ta fram underlag för beslut

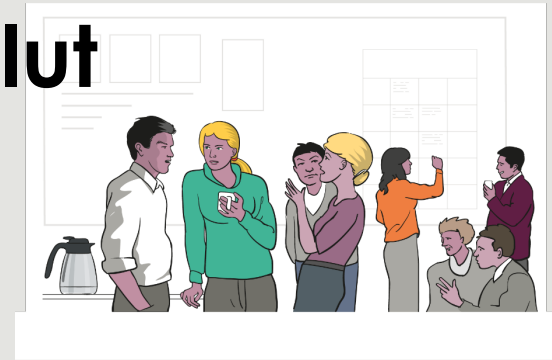
Underlag för beslutsfattande:

Presentera följande för informationsägare/beslutsfattare

- Vilken verksamhet
- Vilka analyser
- Viktiga resultat
    - Vilka informationstillgångar har ni identifierat?
    - Viktiga risker ni har identifierat
    - Resultatet av er informationsklassning
    - Förslag på säkerhetsåtgärder

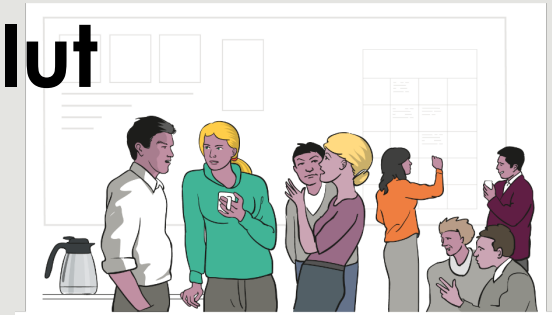
Några frågor?

Uppgift 5: Presentera underlag för beslut



- Presentera för beslutsfattare:
  - Resultatet från identifiering och klassning av information
  - Identifierade risker, fokusera på de allvarligaste riskerna ni funnit
  - Föreslagna säkerhetsåtgärder
- Läs mer om uppgiften i uppgiftsbeskrivningen för uppgift 5: Presentera underlag för beslut
- Håll presentationen på en övergripande nivå
  - Överlämna materialet ni tagit fram för beslut och underlag inför ledningens genomgång.

Uppgift 5: Presentera underlag för beslut



- Presentera för beslutsfattare:
  - Resultatet från identifiering och klassning av information
  - Identifierade risker, fokusera på de allvarligaste riskerna ni funnit
  - Föreslagna säkerhetsåtgärder
- Läs mer om uppgiften i uppgiftsbeskrivningen för uppgift 5: Presentera underlag för beslut
- Håll presentationen på en övergripande nivå
  - Överlämna materialet ni tagit fram för beslut och underlag inför ledningens genomgång.

Sammanfattning av dagen

- Grundläggande teoretisk förståelse för vad systematiskt informationssäkerhetsarbete är
  - Identifiera och analysera
  - Utforma
  - Använda
  - Följa upp och förbättra
- Praktiskt prövat att
  - Identifiera informationstillgångar
  - Klassa information
  - Bedöma risker
  - Föreslå säkerhetsåtgärder
  - Presentera vad du kommit fram till för en beslutsfattare

Myndigheten för samhällsskydd och beredskap

Vad tänker du nu om systematiskt informationssäkerhetsarbete?

Utvärdering - hur var dagen?

- Innehåll: betyg 1–4 (1 inte bra, 4 mycket bra)
- Upplägg: betyg 1–4 (1 inte bra, 4 mycket bra)

- Vad fungerade bra?
- Vad skulle kunna förbättras?

Tack!

Om du vill veta mer om metodstödet

www.informationssakerhet.se/metodstodet

Myndigheten för samhällsskydd och beredskap