



Myndigheten för  
samhällsskydd  
och beredskap

# Att lära stort från små incidenter

– en handledning med fokus på att utvärdera effektiviteten i lärandet



Att lära stort från små incidenter  
– en handledning med fokus på att utvärdera effektiviteten i lärandet

Myndigheten för samhällsskydd och beredskap (MSB)

Författare: Anders Jacobsson

Kontaktperson: Thomas Gell, Marianne Stålheim

Layout: Advant Produktionsbyrå AB  
Tryckeri: DanagårdLiTHO

Publikationsnummer: MSB430 - juli 2012  
ISBN: 978-91-7383-252-6

## Förord

Att vi tjänar på att lära av inträffade oönskade händelser – incidenter – är en sanning som har få opponenter. Därför har de flesta organisationer någon typ av tillbuds- eller incidentrapportering. Krav på detta ingår dessutom som en principiell grundbult i lednings- eller regelsystem avseende säkerhet-hälsa-miljö. Oftast består lärande-systemet av ett datorstöd för den administrativa hanteringen och en uppsättning rutiner för hur rapporter om inträffade händelser ska hanteras i organisationen.

System kan emellertid fungera olika bra. Om man inte på något sätt försöker utvärdera lärande-systemets effektivitet vet man egentligen inget om hur väl det fungerar. Det är lätt hänt att system av denna typ efter en inledande entusiasm då de introducerats, degenereras till något som i värsta fall kan liknas vid trötta ritualer.

Som sagt: hur bra fungerar dessa system? Hur kan de utnyttjas effektivare? Hur kan organisationen bli bättre på att ta vara på de lärdomar som incidenterna innebär, dvs. hur kan man lära sig bli bättre på att lära? Vad är potentialen, vad är bra?

Det finns en ganska omfattande teoribildning inom området, men få handfasta metoder eller verktyg som kan användas praktiskt av den organisation som vill ta sin "lärande-temp".

Denna handledning är avsedd att fylla denna lucka, dvs. vara ett praktiskt stöd för organisationer som vill fördjupa sina kunskaper om lärande från incidenter och på sikt förbättra lärandeprocessen och lärandenivån.

Inriktningen har gjorts generell och handledningen riktar sig till alla sorters organisationer/verksamheter som är intresserade av att lära av och förbättra sitt arbete kring inträffade händelser, liksom till myndigheter och andra organ med uppföljande ansvar i detta avseende.

Den läsare, som redan är väl insatt i ämnet kan utan svårighet direkt tillämpa de metoder och verktyg som utarbetats för att ta tempen på hur effektiv organisationen är i sitt arbete med lärande från incidenter.

Handledning har utarbetats av Anders Jacobsson, en av Sveriges mest erfarna konsulter inom processsäkerhetsområdet och författare till en rad skrifter inom området Säkerhet-Hälsa-Miljö.

Den baseras på resultaten från ett forskningsprojekt "Lärande från incidenter för säkerhet inom farliga verksamheter" (LINS), vilket utförts vid Lunds Universitets centrum för riskforskning (LUCRAM) och finansierats av Myndigheten för Samhällsskydd och Beredskap.

*Myndigheten för samhällsskydd och beredskap  
Enheten för lärande av olyckor och kriser*



## Läsanvisning

Handledningen är uppdelad i två delar

- Del 1, En allmän beskrivande del som behandlar de faktorer som är viktiga för ett bra lärande från incidenter; och
- Del 2, Konkreta hjälpmedel i form av
  - Metoder med verktyg för att bedöma effektiviteten i lärandet från incidenter och
  - Checklistor med tips om vad som är särskilt viktigt att beakta i lärprocessen och vad som bör ingå i ett incidenthanteringssystem

Metodikerna som ingår i handledningen finns också presenterade i författarens doktorsavhandling (se referenslistan).



# Innehåll

Förord.....	3
Läsanvisning.....	5
<b>DEL 1 - Beskrivning av lärprocessen från incidenter .....</b>	<b>10</b>
<b>Inledning .....</b>	<b>11</b>
Syften med handledningen.....	11
Målgrupper .....	12
<b>Nyckelfrågor för framgång .....</b>	<b>13</b>
<i>Specifikt för olika steg i lärcykeln .....</i>	<i>14</i>
<b>Teori och begrepp kring organisatoriskt lärande .....</b>	<b>15</b>
Organisatoriskt lärande .....	15
Lärande som produkt och som process.....	15
Klassificering av lärandet .....	16
Det organisatoriska minnet och dess delar.....	16
<i>Anläggning och utrustning, inklusive teknisk dokumentation .....</i>	<i>17</i>
<i>Personal .....</i>	<i>17</i>
<i>Procedurer .....</i>	<i>17</i>
Verksamheten som ett socio-tekniskt system .....	17
Säkerhetskultur, säkerhetsklimat och lärandekultur .....	18
Ledarskap inom verksamheten .....	20
<b>Begrepp/element i lärandet från incidenter .....</b>	<b>21</b>
Incident, olycka, tillbud, störning .....	21
Olycksmodeller .....	21
Lärcykeln.....	23
Läxa, lärdom (lesson learned).....	24
Tröskel för rapportering.....	25
Mörkertal i rapporteringen .....	25
Lärandenivå .....	27
Lärpotential .....	27
Lärandeagent .....	27
<b>Element och innehåll i ett system för rapportering och hantering av incidenter ..</b>	<b>29</b>
<b>Att analysera/utreda incidenter .....</b>	<b>31</b>
Resurser.....	31
Faktainsamling .....	31

Händelseförloppet .....	32
Orsaker .....	32
Rekommendationer .....	33
<b>Överföring av lärande från system för incidenthantering till organisationens minne .....</b>	<b>34</b>
<b>Rutin och administrativt system för incidenthantering .....</b>	<b>35</b>
<b>Hur skapar, inför och upprätthåller man ett incidenthanteringssystem? .....</b>	<b>36</b>
<b>Kopplingar till andra element i verksamhetens säkerhetsarbete .....</b>	<b>38</b>
<b>Hur man kan undersöka effektiviteten i lärandet från incidenter .....</b>	<b>40</b>
Effektiviteten i lärcykeln .....	41
Effektiviteten i lärprodukten, lesson learned; Lärandenivån .....	42
<i>Steg 1: Verkligt lärande .....</i>	<i>42</i>
<i>Steg 2: Potentiellt lärande .....</i>	<i>43</i>
<i>Steg 3: Jämförelse mellan verklig och potentiell lärandenivå .....</i>	<i>44</i>
<i>Steg 4: Korrektions för mörkertal, dvs ej rapporterade incidenter .....</i>	<i>44</i>
<i>Steg 5: Hänsyn till lärande från incidenter på en aggregerad nivå – 2:a loopen .....</i>	<i>44</i>
<i>Steg 6: Hänsyn till andra mekanismer för lärande från incidenter .....</i>	<i>45</i>
Tröskeln för rapportering .....	45
Mörkertal .....	45
<b>Hantering av "Stora olyckor" .....</b>	<b>46</b>
<b>Viktiga punkter till hjälp för myndigheter .....</b>	<b>47</b>
<b>Litteraturreferenser .....</b>	<b>48</b>
<b>DEL 2 - Metoddel .....</b>	<b>50</b>
<b>Inledning .....</b>	<b>51</b>
<b>Förteckning över metoder och checklistor .....</b>	<b>52</b>
<b>Procedur .....</b>	<b>53</b>
Praktisk användning av metodiken och dess metoder .....	53
<b>1. ANALYS AV EFFEKTIVITETEN I LÄRANDET FRÅN INCIDENTER .....</b>	<b>53</b>
Förenklad tillämpning .....	53
<i>Arbetsgrupp (förslag) .....</i>	<i>53</i>
<i>Material (urval) .....</i>	<i>54</i>
<i>Arbetsätt .....</i>	<i>54</i>
<i>Resultat .....</i>	<i>54</i>
<i>Tidsåtgång .....</i>	<i>55</i>
Fullständig tillämpning .....	55
<b>2. INVENTERING AV FÖRBÄTTRINGSFÖRSLAG .....</b>	<b>55</b>



<b>Metod 1. Bedömning av effektiviteten i lärcykeln</b> .....	<b>56</b>
<b>Metod 2. Bedömning av lärandenivå</b> .....	<b>64</b>
<i>Steg 1: Verkligt lärande</i> .....	64
<i>Steg 2: Potentiellt lärande</i> .....	66
<i>Steg 3: Jämförelse mellan verklig och potentiell lärandenivå</i> .....	69
<i>Steg 4: Korrektionsfaktor för mörkertal, dvs ej rapporterade incidenter</i> .....	69
<i>Steg 5: Hänsyn till lärande från incidenter på en aggregerad nivå – 2:a loopen</i> .....	69
<i>Steg 6: Hänsyn till andra mekanismer för lärande från incidenter</i> .....	70
<b>Metod 3. Bedömning av tröskel för rapportering</b> .....	<b>71</b>
<b>Checklista 1. Viktiga påverkansfaktorer, allmänt och för lärcykeln olika steg</b> .....	<b>73</b>
Allmänna faktorer .....	73
Faktorer för enskilda steg .....	73
<i>Rapportering</i> .....	73
<i>Analys/utredning</i> .....	74
<i>Beslut</i> .....	75
<i>Implementering</i> .....	75
<i>Uppföljning</i> .....	76
<i>2:a loopen</i> .....	76
<b>Checklista 2. Viktiga element/innehåll i ett incidenthanteringsystem</b> .....	<b>77</b>
Rapportering .....	77
Analys (främst orsaksanalys) .....	77
Beslut om åtgärd .....	78
Implementering .....	78
Uppföljning .....	79
2:a loop .....	79

**DEL 1**  
**Beskrivning av lärprocessen  
från incidenter**

## Inledning

Som titeln "Lära stort från små incidenter" låter förstå, handlar denna skrift om hur organisationer kan lära från de "små" incidenter som uppträder i praktiskt taget alla verksamheter. De små incidenterna är många, de stora är få. Rätt hanterade är de små incidenterna en källa till mycken lärdom. Även djupare liggande svagheter i en organisation och dess system kan spåras upp vid en bra hantering av de små incidenterna. Genom att ta rätt hand om de många små incidenterna får man lärdomar som täcker de allra flesta områden som har betydelse för att upprätthålla hög säkerhet. Den stora olyckan ska inte behöva inträffa!

Med incidenter förstår vi i denna handledning i första hand ett brett spektrum av händelser som har resulterat i eller hade kunnat resultera i negativa konsekvenser med avseende på säkerhet, hälsa och/eller miljö i en verksamhet. Begreppet incident kan emellertid enkelt utvidgas eller anpassas för olika verksamheter till vad som är relevant i sammanhanget. För vissa verksamheter kan konsekvenser för "kunder" till verksamheten stå i fokus, t.ex. skada på vårdtagare inom sjukvården, skada på elever i skolor eller brister i leveranser inom kommunala eller statliga sektorn till medborgarna.

Synsättet på och mekanismerna i lärandet från incidenter samt metodiken för att undersöka effektiviteten i lärandet är i allt väsentligt desamma oberoende av verksamhetens art. Därför kan denna handledning anses vara generell och tillämpbar inom de flesta verksamheter; ibland med smärre anpassningar. En springande punkt i allt arbete med att förbättra en situation är att kunna mäta befintligt läge. Därför har i handledningen lagts en hel del kraft på att tillhandahålla konkreta verktyg för att mäta/utvärdera effektiviteten i befintligt lärande från incidenter. Dessa presenteras mot slutet av handledningen.

### Syften med handledningen

Handledningen har som syfte att förmedla kunskap om vad som krävs för att hanteringen av incidenter ska vara effektiv och hur man kan ta reda på om den är det, genom att

- Anvisa verktyg för att undersöka effektiviteten av befintligt lärande från incidenter
- Skapa förståelse för mekanismerna kring lärandet från incidenter
- Peka på de viktigaste faktorerna för att nå framgång med lärandet från incidenter
- Ge en praktisk handledning med handfasta råd och tips om vad ett system för lärande från incidenter bör innehålla.

## Målgrupper

Målgruppen för handledningen är i första hand företag och andra verksamheter inom branscher med farliga verksamheter, exempelvis

- Processindustrin
- Transportsektorn
- Byggindustrin
- Verkstadsindustrin
- Vårdsektorn
- Kommunala sektorn

men i stort sett alla verksamheter, som vill lära av inträffade händelser på ett systematiskt sätt genom att hantera dem i ett incidenthanteringssystem, kan ha stor nytta av handledningen.

Handledningen är främst tänkt för att användas på enhetsnivå (industriell anläggning, "site", sjukhus eller motsvarande), men är användbar på både lägre organisatorisk nivå (avdelning eller grupp) och högre nivå (koncern). Den vänder sig framför allt till personer ansvariga för säkerhetsfunktioner och till personer i ledningen.

En andra målgrupp är myndigheter som utövar tillsyn i olika farliga verksamheter.

Handledningen är emellertid inte avsedd att täcka de krav som finns i lagstiftningen om formell rapportering och utredning av vissa typer av olyckor till myndigheter. Ur ett myndighetsperspektiv skall handledningen mera vara en hjälp i att kunna bedöma hur verksamheternas incidenthantering i allmänhet fungerar i förhållande till kraven som finns i lagstiftningen – dels allmänna krav om incidenthantering, dels specifika krav om incidenthantering som del i ledningssystem för säkerhet.

## Nyckelfrågor för framgång

### Allmänt

Nedan följer i punktform ett antal frågor som kan betraktas som nyckelfrågor för att nå framgång i lärandet från incidenter. Frågorna är inte i absolut prioriteringsordning, men ordningsföljden återspeglar författarens uppfattning om vikten av respektive fråga. De flesta av punkterna har stöd i den forskning som genomförts i LINS-projektet samt i annan forskning.

Vissa begrepp som nämns i det följande behandlas och förklaras närmare längre fram i handledningen.

- **Säkerhetskultur**

En god säkerhetskultur, präglad av tillit, förtroende, öppenhet och en icke-straffande attityd är en absolut förutsättning för ett gott lärande från incidenter. Personer som skall rapportera, kanske egna tillkortakommanden, måste känna att inget de rapporterar kommer att hållas emot dem. Ett bra sätt att öka förtroendet från de anställdas sida gentemot ledningen i denna fråga är att låta de anställda delta i och få påverka utformningen av incidenthanterings-systemet.

- **Ledningens stöd och engagemang**

Som i de flesta andra frågor behövs ledningens uttalade stöd och engagemang för processen och systemet för lärande från incidenter för att lärande ska bli bra. Ledningen måste efterfråga en hög rapporteringsfrekvens och ge positiv feedback. Framför allt måste ledningen visa att man tar hand om de inrapporterade incidenterna på ett bra och något så när snabbt sätt.

- **Enkelhet i själva incidenthanteringssystemet**

I synnerhet skall rapporteringen av en incident vara enkel för rapportören. Rapporteringsformulär i elektronisk eller pappersform ska vara lätt tillgängliga och vara utformade så att alla anställda utan problem och utan alltför stor tidsåtgång kan fylla i dem. Även övriga steg bör göras så enkla och användarvänliga som möjligt. Onödig komplexitet och byråkrati är starkt hämmande för framför allt rapporteringsviljan.

- **Resurser och kompetens i varje steg i lärcykeln (Rapportering – Analys – Beslut – Implementering – Uppföljning)**

Verksamheten måste vara beredd att satsa på tillräckliga resurser och god kompetens för att incidenthanteringssystemet ska leverera de förväntade resultaten. Framför allt gäller detta i det krävande analyssteget. Att utföra arbetsuppgifter i incidenthanteringssystemet är i allmänhet tilläggsuppgifter för berörda anställda, men den nödvändiga tiden måste inrymmas i den totala tiden för befattningarna. Annars riskerar man att incidenthanteringen får låg prioritet.

- **Ägare/lärandeagenter i varje steg i lärcykeln**  
Alla rapporterade incidenter behöver i varje steg i lärcykeln en ägare, en lärandeagent, som skall se till att aktiviteten blir ordentligt utförd och att lärdomarna kommer in på alla relevanta ställen i verksamhetens minne. Tydliga roller och ansvar behövs med avseende på informations spridning, vidare hantering, uppföljning och avslut. Särskilt incidenter som leder till omfattande och kanske tidskrävande aktiviteter för många personer måste ha en ansvarig koordinator.
- **Kontroll av att alla aktiviteter utförts i varje steg i lärcykeln**  
Det behövs en mekanism som säkerställer att alla åtgärder som erfordras i ett steg verkligen vidtagits, innan man släpper frågan vidare till nästa steg.
- **Effektiv informations spridning**  
Alla som berörs av incidenten skall erhålla information om den, från det att den hänt till beslut och genomförande av åtgärder. Informationen skall inte bara ske inom incidenthanteringssystemet självt på t.ex. intranät, utan också genom att man har fora för diskussion kring incidenter.
- **Existensen av en effektiv 2:a loop i lärcykeln**  
Eftersom det inte är att begära att hanteringen av varje enskild incident ska leda till maximalt utnyttjad lärdom, är det nödvändigt att ha en regelbunden aktivitet kring ett samlat material av många incidenter för att utvinna ytterligare lärdomar. Vid analys av ett samlat material bör man kunna se trender, typiska incidenter och gemensamma underliggande orsaker. Kraven på resurser och kompetens för denna 2:a loop är höga, och helt avgörande för framgång. Obs! Beteckningen 2:a loop ska inte förväxlas med double-loop lärande.
- **Utbildning av alla i organisationen i att tänka i olycksmodell**  
Om alla i organisationen, och särskilt anställda i 1:a linjen, har en förståelse för hur en olycksmodell fungerar, t.ex. en schweizerostmodell kombinerad med en socio-teknisk nivåmodell, kan detta generera fler incidentrapporter och dessutom med bättre och mer relevant information.

### **Specifikt för olika steg i lärcykeln**

Utöver ovanstående generella punkter finns en rad frågor och faktorer i de specifika stegen i lärcykeln, från rapportering till uppföljning, som är väsentliga för framgången med lärandet från incidenter. Dessa är samlade i **Checklista 1** i del 2 av handledningen.

## Teori och begrepp kring organisatoriskt lärande

Här följer en kort beskrivning av några centrala begrepp för organisatoriskt lärande.

### Organisatoriskt lärande

Det mesta lärandet börjar som individuellt lärande, innan det kan bli organisatoriskt lärande. En organisation lär genom sina medlemmar. Det är precis vad lärande från incidenter handlar om – att plocka upp informationen från den (de) individ(er) som varit inblandade i eller av annan anledning iakttagit en incident och omvandla informationen till generell kunskap för hela organisationen.

Organisatoriskt lärande för säkerhet äger normalt rum genom många aktiviteter och instrument. Lärandet kan anses vara en integrerad del i många aktiviteter. Bland dessa kan nämnas, förutom lärandet från incidenter även säkerhetsrevisioner, skyddsronder, arbete i säkerhetskommittéer, riskanalyser, inspektioner och beteendebaserat säkerhetsarbete. Det mesta av den grundläggande kunskapen för säkerhet erhålls via mer eller mindre formell utbildning inom verksamheten.

I lärandet från incidenter finns det ofta en inbyggd konflikt i utredningsfasen av händelsen mellan att få fram den fulla ohöjda sanningen och att finna den ”skyldiga” personen.

Detta är särskilt uttalat vid större olyckor. I sammanhang med denna handlednings fokus – verksamhetsinternt lärande från mindre incidenter – är det rimligt att anta att denna konflikt är mindre uttalad än när det handlar om större olyckor, även om den kan tänkas vara närvarande också i verksamhetens utredningar av mindre incidenter. Den avgörande faktorn för hur komplett bilden blir är starkt relaterad till verksamhetens säkerhetskultur. Ju mer öppen, ju mindre straffande, ju rättvisare kulturen är, desto fullständigare blir bilden och desto bättre blir lärande. En förutsättning för ett bra lärande är vidare att spridningen av den vunna informationen sker på ett effektivt sätt in i organisationens system så att informationen når alla berörda. I det sammanhanget spelar lärandeagenterna en stor roll.

### Lärande som produkt och som process

I denna handledning behandlar vi lärandet både som en produkt och som en process. Produkten är lärdomen som extraherats ur händelsen och processen utgörs av alla de aktiviteter som behövs för att driva på lärprocessen från rapportering av incidenten till omvandlingen av erfarenheterna till genomförda åtgärder.

## Klassificering av lärandet

Lärandet från inträffade händelser brukar traditionellt beskrivas i termer av antingen

- Enkel-loop lärande och dubbel-loop lärande; eller
- 1:a, 2:a och 3:e ordningens lärande

Enkel-loop-lärande innebär att man ändrar tillvägagångssättet för en aktivitet efter en inträffad händelse, men fortfarande inom tidigare gällande ramar, t.ex. en ändring i en instruktion. För att kallas dubbel-loop-lärande krävs att organisationen som ett resultat av händelsen ändrar sina grundläggande principer och/eller värderingar om hur man utför sina aktiviteter. Med 1:a ordningens lärande menas genomförande av åtgärder som fokuserar på att korrigera situationen på ett sådant sätt att de ursprungliga målen uppnås med den ursprungliga planen. 2:a ordningens lärande innebär att de ursprungliga målen fortfarande uppnås men med en ny plan. I vissa fall, där åtgärder genomförs, som innebär att också målen ändras och medelst en ny plan, talar vi om 3:e ordningens lärande.

Ovanstående begrepp är mycket viktiga och relevanta i anslutning till stora olyckor med ofta komplexa orsaksbilder. För de allra flesta händelser som är aktuella inom ramen för denna handledning är endast enkel-loop-lärande, respektive 1:a eller möjligen 2:a ordningens lärande aktuellt. För att få ett mera differentierat och användbart resultat används i denna handledning (för huvudsakligen mindre incidenter) en något annorlunda klassificeringsmodell. Den bygger i första hand på den geografiska spridningen av lärdomen och i andra hand på graden av organisatoriskt lärande och graden av långtidsminne inom verksamheten.

## Det organisatoriska minnet och dess delar

Det organisatoriska minnet är massan av data, information och kunskap, som är relevant för en organisations existens. Det består huvudsakligen av två "förvaringsplatser" – en organisations arkiv, inkluderande dess elektroniska databaser, och individernas minnen.

När den användbara informationen från en incident har utvunnits skall denna omsättas i praktiken och lagras i organisationens minne som en lärdom (eller "lesson learned" på engelska).

Innehållet i ett organisatoriskt minne kan ges en enkel struktur enligt följande: Anläggning, Personal och Procedurer. Några exempel på system, som kan utgöra delar av organisationens minne och som kan beröras och behöva uppdateras med erfarenheten från en incident är följande (exempel från processindustri, som lätt kan överföras på andra verksamheter):



### **Anläggning och utrustning, inklusive teknisk dokumentation**

- Grundläggande designspecifikationer och konstruktionsstandarder
- Verksamhets/processbeskrivning
- Externa, föreskrivande dokument – lagstiftning, standarder etc.

### **Personal**

- System för ansvar och befogenheter (befattningsbeskrivningar, delegeringshandlingar mm.)
- Utbildningsprogram/-material
- Kompetens hos personal på alla nivåer

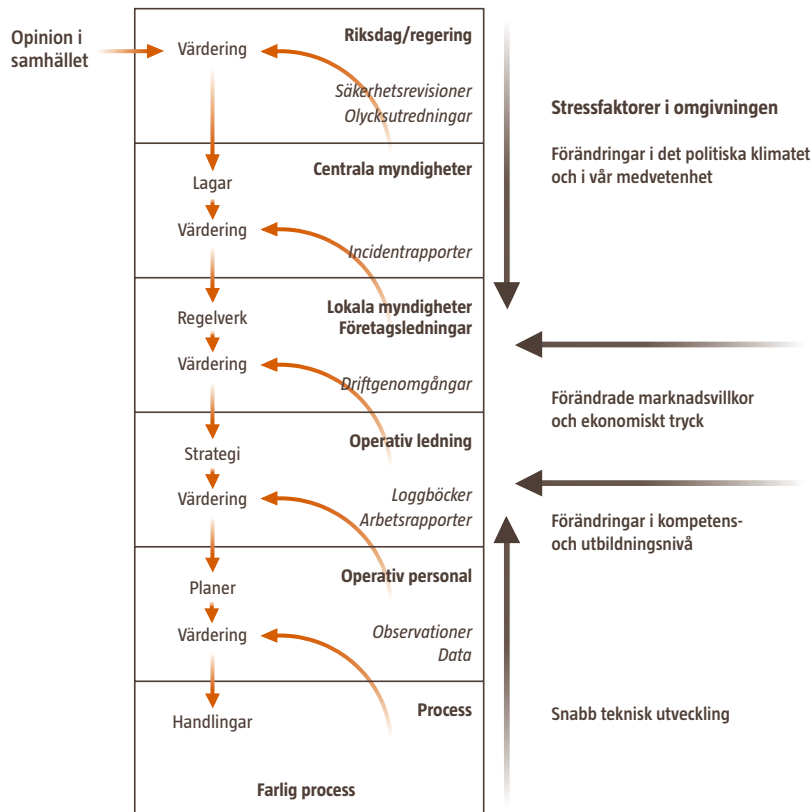
### **Procedurer**

- Ledningssystem
- Instruktioner för drift och underhåll eller motsvarande
- Program för förebyggande underhåll, inspektion med tillhörande arkiv
- Loggar och loggböcker
- Incidenthantering

## **Verksamheten som ett socio-tekniskt system**

En verksamhet kan ses som en hierarki av organisatoriska nivåer som samverkar med varandra. Styrmedlen för verksamheten utgår från toppen av organisationen och blir alltmer detaljerade ju närmare den rent utförande nivån man kommer. Samtidigt som det finns en "top-down"-struktur i sättet att styra verksamheten finns det också återföringsmekanismer av typen "bottom-up".

De flesta incidenter berör mer än en person eller organisatorisk nivå, och förklaringarna och orsakerna till incidenter är oftast fördelade mellan olika anställda och flera organisatoriska nivåer och bland de system och procedurer som är i bruk (exempelvis arbetsinstruktioner, konstruktionsregler och hela ledningssystem). Synsättet med företaget som ett socio-tekniskt system brukar vara till stor hjälp vid analysen av incidenter. Figur 1 visar en sådan uppbyggnad som inkluderar regelverk och lagar från myndigheter och politiska instanser.



FIGUR 1. Företaget som ett socio-tekniskt system (Rasmussen & Svedung).

## Säkerhetskultur, säkerhetsklimat och lärandekultur

En av de viktigaste förutsättningarna som brukar framhållas för att en organisation ska kunna ha ett framgångsrikt lärande är att där finns en kultur som i olika avseenden främjar lärandet. Enligt James Reason består säkerhetskulturen av fyra kritiska delkulturer, nämligen en rapportrande kultur, en rättvis kultur, en flexibel kultur och en lärande kultur. Tillsammans samverkar de till att skapa en informerad kultur, som Reason likställer med säkerhetskultur. Reason definierar en lärande kultur som organisationens vilja och kompetens att dra de riktiga slutsatserna från sitt informationssystem för säkerhet och viljan att genomföra större reformer när behov för detta föreligger.

Definitioner av säkerhetskultur brukar ofta utgå från gemensamma värderingar och attityder som finns i en organisation beträffande säkerhet. En god säkerhetskultur bör präglas av tillit, förtroende, öppenhet och icke-straffande attityder. Vi förutsätter att kärnan i säkerhetskulturen utgörs av gemensamma värdegrunder (värderingar) inom organisationen om vad som är en lämplig nivå för Säkerhet/Hälsa/Miljö (SHM) att bedriva verksamheten på. Vanligtvis är de gemensamma värdegrunderna t.ex. att verksamheten skall bedrivas på ett sådant sätt att ingen människa eller den omgivande miljön kommer till skada. Detta kan ibland preciseras närmare. I en god säkerhetskultur genomsyrar dessa värdegrunder alla medarbetare i verksamheten och resulterar i attityder, engagemang, beteende-

mönster, och åtaganden som kontinuerligt och utan undantag motsvarar värdegrunderna.

För att tydliggöra vad de gemensamma värdegrunderna betyder i praktiken – hur processer och anläggningar skall utformas och hur arbetet skall utföras för att ge det SHM-resultat som överenskommit – brukar det i allmänhet konkretiseras och stadfästas i skrift i form av policies, generella rutiner och detaljerade instruktioner (vi kan för enkelhetens skull kalla det för ledningssystemet för SHM för verksamheten). Förutsatt att man i all denna dokumentation har lyckats fånga den kultur man vill ha och lyckats definiera vad den betyder i praktisk utformning och praktisk handling, har vi fått ett konkret uttryck för hur man vill att säkerhetskulturen i verksamheten skall vara.

Huruvida den kultur man säger sig vilja ha i verksamheten – och som vi antar att man lyckats åskådliggöra i det interna regelverket (ledningssystemet) – verkligen också råder i verksamheten, borde kunna utläsas genom att mäta i vilken grad utformningen av processer och anläggningar samt medarbetarnas arbete följer det uppsatta regelverket. Efterlevnad av (konsistens med) regelverket bör kunna vara en mätare – och en mycket viktig sådan – bland flera andra av säkerhetskulturen.

Tre frågor behöver besvaras för att kunna uttala sig om säkerhetskulturen på en arbetsplats eller inom en verksamhet.

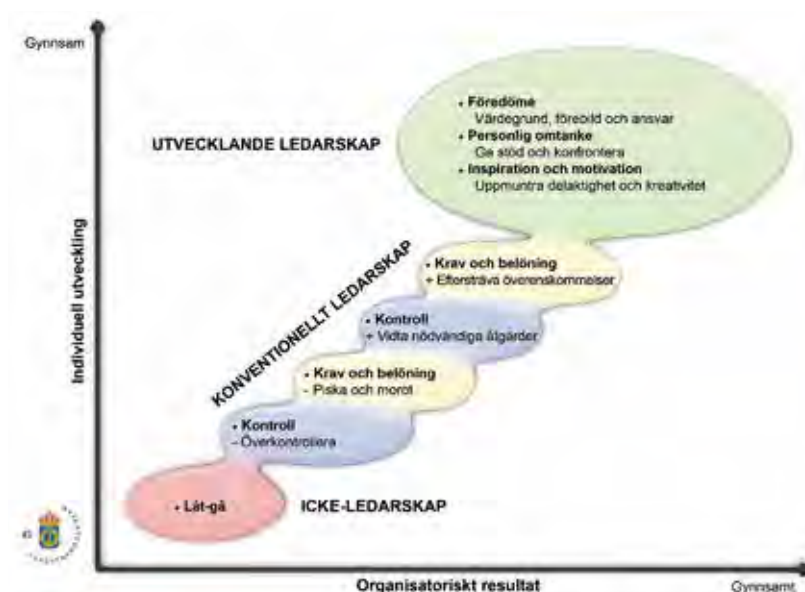
1. Vilka är de gemensamma värdena (värdegrunderna) som organisationen bekänner sig till, och är de uttryck för vad som allmänt anses vara kärnan i, och i övrigt karakteristiska uttryck och egenskaper för, en god säkerhetskultur?
2. Är innehållet och kraven på hur processer och anläggningar skall utformas och på hur arbete skall utföras mm, som det beskrivs i ledningssystemet, en god översättning av organisationens värderingar?
3. I vilken grad motsvarar processer och anläggningar och arbetet som utförs av medlemmarna i organisationen det regelverk man satt upp?

Säkerhetskulturen i en organisation är inte statisk utan kan förändras när organisationen exempelvis genomför omstruktureringar, står inför nya utmaningar, utvecklar eller byter ut sina system m.m. En god säkerhetskultur kan bibehållas genom att organisationen antar en proaktiv inställning till säkerhet, vilket bland annat innebär att man kontinuerligt samlar in information kring säkerhetsaspekter inom organisationen, lär sig från denna information och introducerar förändringar när situationen så kräver. Några av nyckelaspekterna för att en organisation skall upprätthålla en god säkerhetskultur innefattar bland annat att det finns utrymme och kanaler för utbyte av information och diskussion kring säkerhetsaspekter i det vardagliga arbetet och att det genomförs kontinuerliga säkerhetsutbildningar och kompetensutbildningar för personalen.

Många forskare skiljer på säkerhetskultur och säkerhetsklimat. Förenklat kan man säga att säkerhetsklimatet är de synliga yttringarna av säkerhetskulturen. Säkerhetsklimatet låter sig därför i någon mån mätas, medan kulturen är mera svåråtkomlig.

## Ledarskap inom verksamheten

Åtskilliga studier har visat att ledarskapet har en betydande påverkan på anställdas säkerhetsattityder och säkerhetsrelaterade beteenden och har därigenom också en central påverkan på säkerhetskulturen. Under de senaste åren har forskare framförallt fokuserat på betydelsen av två olika typer av ledarskapsbeteenden och dess betydelse för säkerhetsrelaterade aspekter. Det ena ledarskapsbeteendet benämns säkerhetsspecifikt utvecklande ledarskap och det andra benämns säkerhetsspecifikt passivt ledarskap (benämns även "låt-gå"-ledarskap). Modellen nedan ger en överblick över dessa och andra typer av ledarskapsstilar. Modellen placerar in olika typer av ledarskapsstilar i ett koordinatsystem med axlarna organisatoriskt resultat (x-axeln) och individuell utveckling (y-axeln).



FIGUR 2. Individuell utveckling och organisatoriskt resultat vid olika ledarskapsstilar. (G. Larsson, 2006, S. 50 i Direkt ledarskap, Försvarsmakten)

De samlade fynden från studier som undersökt relationen mellan dessa två typer av ledarskapsbeteenden och säkerhetsrelaterade frågor visar att det säkerhetsspecifika utvecklande ledarskapet har en positiv påverkan på säkerhetskulturen, är relaterat till en högre grad av säkerhetsbeteenden hos anställda och en lägre grad av arbetsskador/olyckor. Det passiva ledarskapet uppvisar ett direkt motsatt mönster.

Vidare visar forskningen att det i synnerhet är gynnsamt om arbetsledarna inom organisationen har ett utvecklande ledarskap som präglas av en god förmåga att ge stöd, coacha och konfrontera anställda "på golvet" men också att uppmuntra delaktighet från anställda i säkerhetsarbetet. Dessa ledare är en central kommunikationslänk mellan högre ledning och anställda i att förmedla visioner, policies och procedurer rörande säkerhetsarbetet. Arbetsledarna måste också vara goda förebilder och följa de säkerhetsföreskrifter som råder inom organisationen.

## Begrepp/element i lärandet från incidenter

I handledningen används en hel del begrepp, av vilka några av de viktigaste förklaras nedan.

### Incident, olycka, tillbud, störning

Det finns en hel del olika benämningar och definitioner inom detta område – vad man ska kalla olika typer av händelser. Nomenklaturen varierar beroende på sammanhang, verksamheter och andra förhållanden. Vi väljer här att definiera som *incidenter* ”alla tillfälliga, och från normala förhållanden avvikande händelser i en verksamhet, som resulterar i eller kan resultera i skadliga konsekvenser för säkerhet, hälsa och/eller miljö”.

För vissa verksamheter bör ovanstående definition av incident anpassas till vad som är mest relevant i sammanhanget. För vissa verksamheter kan exempelvis konsekvenser för ”kunder” till verksamheten stå i fokus. Detta är t.ex. fallet vid patientskador inom sjukvården, olycksfall bland elever i skolor eller brister i leveranser inom kommunala eller statliga sektorn till medborgarna.

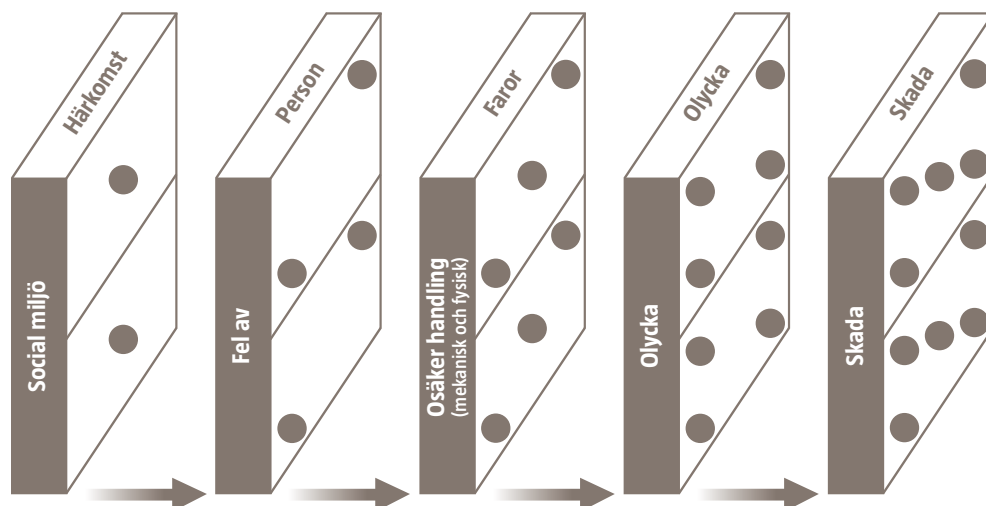
Katastrof, olycka, tillbud (eller med engelska ord incident eller near-miss), störning och avvikelse ingår alla i ovanstående definition av incident. Storleken på konsekvensen är inte avgörande. Den gemensamma nämnaren i sammanhanget är att händelserna oavsett vad vi kallar dem och oavsett var på konsekvensskalan de ligger innehåller mer eller mindre potential för lärande.

### Olycksmodeller

Det finns huvudsakligen tre olika typer av olycksmodeller:

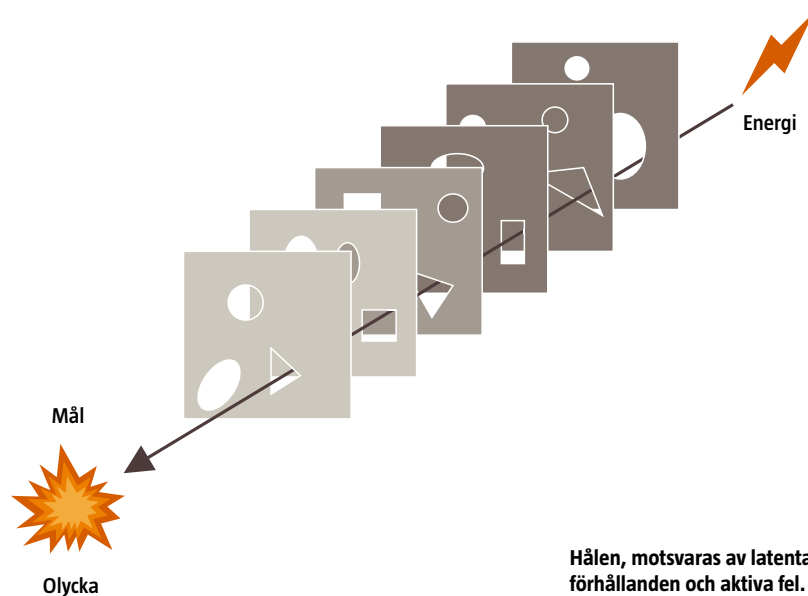
- Sekventiella,
- Epidemiologiska; och
- Systemiska

De sekventiella modellerna är de äldsta och de som i vardagslag används flitigast. Utgångspunkten i dessa, vi kan kalla dem ”domino”-modeller, är helt enkelt att en incident inträffar p.g.a. en *direkt orsak*, som i sin tur beror på en annan orsak och eventuellt ytterligare bidragande eller *underliggande orsaker* i en mer eller mindre sammanhängande följd, ungefär som ett antal uppställda dominobrickor, som alla faller om den första faller. Den djupast liggande orsaken brukar betecknas som grundorsak (”root cause”).



FIGUR 3. Domino-modellen (efter Heinrich, 1959).

De epidemiologiska modellerna kan representeras av den välkända "schweizerost"-modellen. I denna tänker man sig att det finns ett antal *skyddsbarriärer* som ska förhindra en initierande händelse från att fortplanta sig och slutligen åstadkomma skada. Skivorna i schweizerosten har hål, vilket här illustrerar de svagheter (sjukdomssymptom, därav benämningen epidemiologisk modell) som kan finnas i skyddsbarriärerna. Barriärerna kan vara både tekniska, fysiska, barriärer och olika former av administrativa och organisatoriska barriärer.



FIGUR 4. Schweizerostmodellen (efter James Reason).

Vi bör också nämna begreppen *latenta förhållanden* och *situationsfaktorer*. Latenta förhållanden innebär oftast mindre uppenbara förhållanden, som ofta kan vara slumrande under lång tid, men som kan bidra till händelseförloppet. Typiska exempel på latenta förhållanden är svagheter i design och konstruktion av utrustning, otillräcklig utbildning, brister i procedurer och instruktioner, brister i förebyggande underhåll – förhållanden som alla härrör från beslut på ett högre organisatoriskt plan. Även väl underbyggda och rationella beslut kan leda till latenta förhållanden. Det gäller att identifiera de latenta förhållandena och bygga barriärer. Situationsfaktorer är sådana förhållanden som kan dyka upp då och då och som kan försvåra utförandet av ett arbete på ett säkert sätt, och som därmed kan bidra till att initiera en händelse.

Även i de epidemiologiska modellerna finns ett stort mått av stegvist tänkande. En initierande händelse ger fortsatta händelser som bryter igenom den ena barriären efter den andra. I de nyaste modellerna, de systemiska modellerna, har man helt frångått det sekventiella synsättet och ser förklaringar till att olyckor sker mer som att ett antal saker sammanträffar vid ett givet tillfälle – saker eller tillstånd som var för sig kan anses vara mer eller mindre normala. Det handlar alltså om hur systemkomponenter och processer samspelar med varandra och inom vilka gränser dessa tillåts variera genom att vi utövar kontroll och sätter begränsningar på dem. I den systemiska modellen ska varje händelse snarare ses som en del av det hela, än som ett distinkt steg på vägen. I den systemiska modellen kan varje händelse såväl föregås som följas av flera händelser. Varje händelse påverkas av personer på olika nivåer i organisationen från direkt utförande nivå (sharp end) till mera övergripande nivåer (blunt end).

De olika olycksmodellernas för- och nackdelar debatteras en hel del. I själva verket kan alla modellerna ha sitt berättigande och de kan komplettera varandra.

I det arbete som ligger bakom denna handledning har ett synsätt som ligger nära schweizerostmodellen tillämpats. De viktiga underliggande orsakerna till händelser och brister i skyddsbarriärer låter sig i allmänhet väl analyseras med denna modell för de incidenter som denna handledning huvudsakligen är inriktad på, nämligen den stora mängden incidenter i en verksamhet, vilka oftast bara har begränsade eller inga konsekvenser alls.

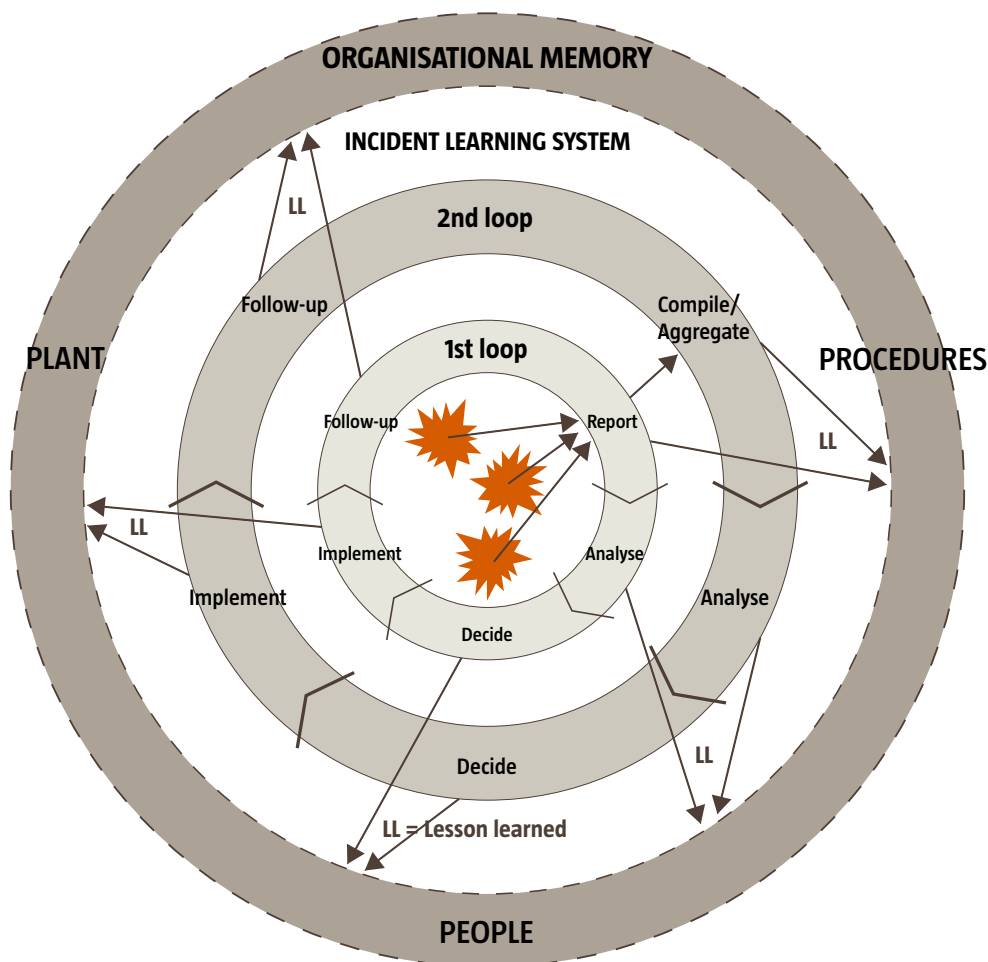
## Lärcykeln

För att en organisation ska lära någonting från en händelse behövs det i allmänhet att många aktörer blir engagerade i ett antal steg i vad vi kan kalla *lärcykeln*.

Typiska steg i cykeln är:

- Rapportering med datainsamling
- Analys och utvärdering
- Beslut
- Implementering av beslut
- Uppföljning

Dessa fem steg utgör en primär loop för varje enskild incident. En sekundär loop bör normalt genomföras på ett samlat material av många incidenter för en djupare analys och utvärdering av underliggande orsaker, gemensamma nämnare och trender. Man kan också lägga till ett steg 0 för identifiering av händelsen som rapportervärd. Här inkluderar vi detta i steg 1, Rapportering.



FIGUR 5. Lärcykeln (figuren innehåller begrepp som beskrivs under respektive rubrik i det följande).

### Läxa, lärdom (lesson learned)

Avsikten med att rapportera incidenter är ju att ta vara på de erfarenheter som finns i dessa – att lära läxan, att skaffa sig lärdom. Det engelska uttrycket i sammanhanget är "lesson learned". Läxan, som skall läras kan sägas bestå av att fånga upp förekomsten av för säkerheten negativa, olämpliga arbetssätt och/eller utformningar av processen eller utrustningen och finna bättre arbetssätt och utformningar samt att informera och upplysa om detta i organisationen för att undvika upprepningar av liknande händelser. En lärdom behöver inte nödvändigtvis vara en korrigerings utifrån en negativ händelse utan kan också vara en positiv förstärkning av ett arbetssätt utifrån en allmän iakttagelse.



Det är viktigt att konstatera att det är först när läxan har implementerats, som den kan kallas en lärdom, en "lesson learned". Fullt ut, innebär det att informationen har förmedlats till alla som kan vara berörda, och att dessa har tagit den till sig och är beredda att agera utifrån den. Att kunna konstatera i vilken omfattning alla berörda har lärt sig läxan blir i praktiken ett omöjligt mätproblem. Vid bedömning av om organisationen verkligen lärt sig läxan får man normalt utgå från de beslut som fattats och hur dessa implementerats samt en bedömning, utifrån de informationssystem och utbildningssystem som finns, av hur effektivt detta trängt ut i organisationen.

## Tröskel för rapportering

I många verksamheter finns det skriftliga definitioner av vad som ska betraktas som en rapporterbar incident, oftast i stil med "Alla händelser som leder till personskada eller till utsläpp av farliga kemikalier eller andra händelser med allvarliga konsekvenser, eller som skulle kunna leda till sådana händelser". Även med en sådan definition blir beslutet att rapportera en incident eller inte en avvägning för den anställde, påverkat av många saker som bl.a. säkerhetsprocedurer och rådande säkerhetsklimat, men också av personliga uppfattningar och preferenser.

Idealt, skall alla incidenter med en potential för lärande rapporteras, vilket innebär en låg tröskel för rapportering. Rapporteringen borde egentligen vara baserad på hur mycket det finns att lära, och det är inte alls detsamma som allvarligheten av den aktuella konsekvensen – det handlar mer om möjliga konsekvenser av identifierade orsaker. En mindre avvikelse kan ibland innehålla värdefullare lärdomar än en stor olycka. Väl utbildade och motiverade anställda kan hjälpa till att välja vad som bör rapporteras med detta kriterium. I praktiken bör man dock också ha en konsekvensnivå, för en allvarlig konsekvens pekar på att något bör förbättras. Allt kan inte rapporteras, än mindre analyseras; därför är det viktigt att välja så effektivt som möjligt.

I verkligheten baseras rapporteringen i de flesta organisationer på graden av konsekvens eller störning. Därför blir rapporterade incidenter (uppfyller organisationens definition) inte nödvändigtvis desamma som rapportervärda incidenter (har en potential för lärande). Omfattningen av rapporteringen blir ofta ett resultat av individens vilja att rapportera och ledningens vilja att utreda och åtgärda.

## Mörkertal i rapporteringen

En fråga som hänger nära samman med tröskeln för rapportering är mörkertalet i rapporteringen. Mörkertalet är ett uttryck för hur många incidenter som inte rapporteras, men som varit "rapportervärda" eller åtminstone "rapporterbara" och alltså borde ha rapporterats.

Antalet rapportervärda incidenter varierar säkert ganska mycket i praktiken och beror bland annat på

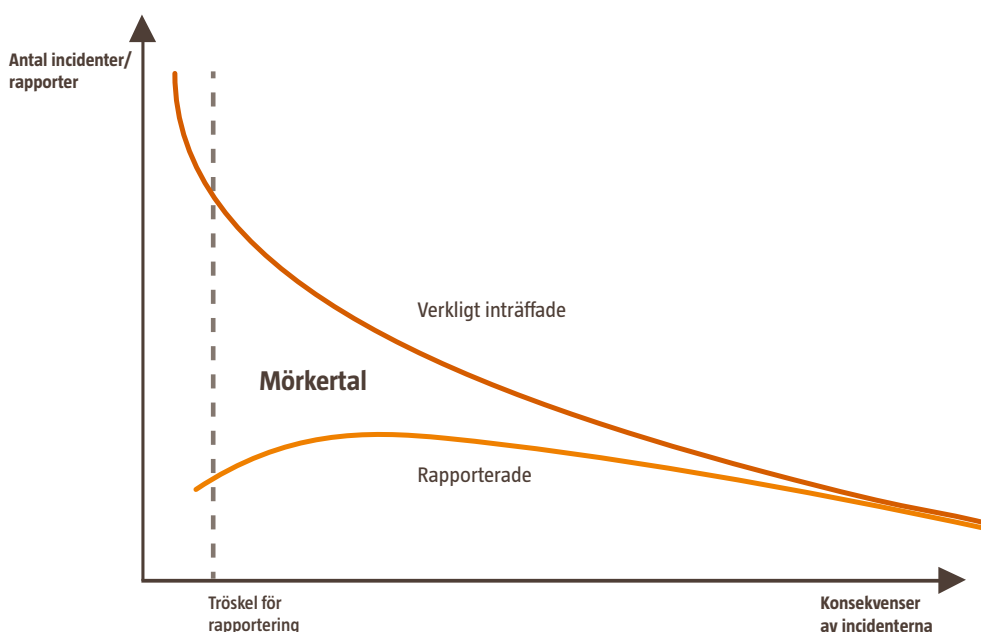
- storlek på verksamhet – ju fler anställda med riskfylld exponering, desto fler rapportervärda incidenter sannolikt

- typ av verksamhet – ju komplexare, desto fler rapportervärda incidenter sannolikt
- typ av verksamhet – ju mer manuella insatser, desto fler rapportervärda incidenter sannolikt
- typ av fysisk anläggning – ju mer komplicerad (t.ex. tätare, svåråtkomligare, mer svårarbetad), desto fler rapportervärda incidenter sannolikt (i viss mån relaterat till ålder; inomhus eller utomhus etc.)
- rådande säkerhetskultur – ju bättre säkerhetskultur, desto färre rapportervärda incidenter sannolikt
- rådande säkerhetskultur – ju bättre säkerhetskultur, desto större andel rapporterade incidenter av de rapportervärda incidenterna sannolikt
- verksamhetens definition av vad som är rapporterbart (inte nödvändigtvis detsamma som rapportervärt)

Det kommer alltid att inträffa incidenter med en potential för lärande som inte rapporteras. Detta mörkertal skall vara så lågt som möjligt. I realiteten blir det dock alltid en avvägning mellan kvantitet och kvalitet. Det är sannolikt bättre med färre rapporter som hanteras bra än många rapporter som hanteras sämre.

Med tanke på variationer i ovan nämnda faktorer kan siffran för rapportervärda incidenter variera betydligt mellan olika verksamheter och även mellan avdelningar inom samma verksamhet.

Mörkertalet och tröskeln för rapportering kan åskådliggöras i en figur med antal incidenter/rapporter och konsekvensen av incidenterna.



FIGUR 6. Mörkertal och tröskel för rapportering.

## Lärandenivå

När man analyserar incidenter finner man ofta att många av lärdomarna (läxorna) bara implementeras i den allra närmaste omgivningen inom verksamheten där incidenten hände. Av och till appliceras lärdomarna bredare. Det organisatoriska lärandet efter en incident innehåller ofta tekniska åtgärder, och/eller förändringar i arbetsinstruktioner och/eller utbildning. Ibland vidtas även åtgärder för att försäkra sig om ett djupare organisatoriskt lärande, ibland t.o.m. så att det påverkar organisationens säkerhetskultur. Vissa åtgärder kommer bara att vara verksamma under en kortare tid, andra under längre tid. Från en praktisk utgångspunkt kan dessa tre aspekter – geografisk applicering, grad av organisatoriskt lärande och tidsaspekten – användas för att klassificera lärdomarna (läxorna) i olika lärandenivåer.

Det är i detta sammanhang begreppen 1:a, 2:a och 3:e ordningens lärande och enkel-loop lärande och dubbel-loop lärande också kommer in i bilden.

## Lärpotential

Den lärdom som maximalt kan utvinnas från en incident varierar naturligtvis en hel del beroende på incidentens typ och karaktär. Vissa incidenter kan bara ge en mycket begränsad lärdom, kanske bara en mycket lokal ändring av en teknisk anordning, d.v.s. den potentiella lärdomen ligger på en låg lärandenivå. Andra incidenter däremot kan ge lärdomar över hela verksamheten och påverka hela sättet för säkerhetsarbetet, d.v.s. den potentiella lärdomen ligger på en hög lärandenivå. Det är viktigt att kunna bedöma den potential för lärande som finns i en incident.

Man kan anta att det är möjligt att bedöma den potentiella lärdomen och därmed den potentiella lärandenivån om man har den fulla förklaringen och orsaksbilden till en incident. För att kunna göra en sådan bedömning skulle man behöva göra en grundorsaksanalys av varje incident. Detta är tidskrävande och kan normalt endast utföras på ett begränsat antal av de rapporterade incidenterna. Man kan emellertid, utgående från de direkta orsakerna till en incident, göra en bedömning av vilka underliggande (bidragande) orsaker som sannolikt bidragit till incidenten med hjälp av relativt enkla och mindre tidskrävande hjälpmedel/verktyg (se nedan). Utgångspunkten för ett sådant verktyg kan tas i beskrivningen av en verksamhet som ett socio-tekniskt system. Direkta orsaker på utförande-nivå har ofta bidragande orsaker på närmast ovanförliggande organisatoriska nivå, som i sin tur kan ha ytterligare bidragande orsaker på nästa nivå ovanför osv, ibland ända upp till verksamhets- eller koncernledningen. Användning av ett sådant verktyg, som ger en övergripande bild med fördelning av sannolika direkta och bidragande orsaker på olika organisatoriska nivåer, kan då också användas för att bedöma lärpotentialen för en incident.

## Lärandeagent

För att systemet för incidenthantering ska generera bra läxor, som kan överföras till lärdomar, behöver vi aktörer – vi kallar dem lärandeagenter – i varje steg av lärandecykeln. Dessa agenter måste ha tillräcklig kompetens och förståelse för

de aspekter som är relevanta för att få ut ett bra lärande ur händelsen. Särskilt i stegen från och med analys av incidenten och vidare i lärcykeln behöver vi kompetenta lärandeagenter (funktioner, personer) i organisationen genom vilka orsaker och andra omständigheter kring en incident kan analyseras och omvandlas till en lärdom, som lagras i det organisatoriska minnet.

## Element och innehåll i ett system för rapportering och hantering av incidenter

En förutsättning för ett effektivt lärande från incidenter är att det finns ett strukturerat sätt att hantera informationen kring en incident och att överföra erfarenheterna från incidenten till läxor och till lärdom för alla som är berörda genom både individuellt och organisatoriskt lärande. Med andra ord, det behövs ett formellt system för incidenthantering. Ett sådant system ingår normalt som en av verksamhetens procedurer inom säkerhetsledningssystemet, där en administrativ instruktion beskriver strukturen, innehållet, arbetsgången, ansvarsförhållanden, formulär som ska användas etc.

Strukturen för ett sådant system bygger lämpligen på stegen i lärcykeln, nämligen

- Datainsamling och rapportering
- Analys och utvärdering
- Beslut om åtgärd
- Implementering av åtgärd
- Uppföljning

För att lära från incidenter måste hanteringen i de olika stegen vara baserad på god information kring incidenten, både avseende omfattning, kvalitet och detaljeringsgrad. I **Checklista 1** i del 2 finns för vart och ett av stegen i lärcykeln de dimensioner som kan vara aktuella att fylla med innehåll (olika aspekter), samt exempel på en del av dessa aspekter.

I ett system för incidenthantering måste det, som redan nämnts, även finnas en aktivitet, som innebär att man utvärderar ett mera samlat material av incidenter för att söka efter mer lärdomar än vad enskilda incidenter kan generera, en aktivitet som vi kallar den 2:a loopen. Det handlar om att sammanställa, statistiskt behandla och analysera en större mängd incidenter och leta efter mönster, trender, gemensamma underliggande faktorer etc. och utifrån detta föreslå och genomföra ytterligare säkerhetsbefrämjande åtgärder. De viktigaste aspekterna som bör behandlas är:

- Typer av inträffade incidenter. (Ser vi något mönster? Har vi exempelvis många ögonskador eller belastningsskador eller t.ex. feldoseringar inom sjukvården? Är någon speciell yrkeskategori ofta inblandad? Är någon del av anläggningen eller enheten, typ av utrustning eller arbetsaktivitet särskilt drabbad?)
- Tidstrender. (Ser vi förändringar i något avseende över tid?)
- Direkta och indirekta orsaker. (Har vi många incidenter relaterade till exempelvis bristande utbildning, stress, avsaknad av riskanalys, konflikt mellan säkerhet och "produktion" eller kan vi även ana djupare liggande problem?)

- Typer av åtgärder. (Finns tendens till att åtgärda mest tekniskt? Stannar åtgärden med enbart lite muntlig information? Appliceras åtgärderna på alla relevanta ställen eller bara högst lokalt? Påverkar åtgärderna den grundläggande tekniska dokumentationen och framtida utformningen av utrustning?)
- Kvalitet i rapportering, analys, beslut, genomförande och uppföljning (enligt punkterna ovan för 1:a loopen).
- Framgång i genomförda åtgärder. (Blev resultatet det som vi avsåg?)
- Kopplingar till ledningssystem och säkerhetskultur etc. (Lär vi oss på djupet? Kommer lärdomarna in i relevanta delar av ledningssystemet och förs de ut i organisationen genom utbildning mm?)

2:a loopen bör genomföras regelbundet, kanske en gång i kvartalet eller åtminstone en gång om året, beroende på verksamhet och antalet inträffade incidenter. För detta arbete krävs kvalificerade resurser med god kompetens i incidentanalys och i frågor kring ledningssystem och säkerhetskultur. Sannolikt är det ett arbete där mer än en person bör vara inblandad. Resultaten från denna övning bör självklart presenteras och diskuteras i t.ex. skyddskommittéer och i verksamhetens ledningsgrupper och generera mera övergripande åtgärder.

Ett nödvändigt element i systemet för incidenthantering är ett verktyg för att avgöra om en händelse skall rapporteras som en incident eller ej. Det behövs alltså en definition om vad som menas med en rapporterbar incident. Definitionen skall framför allt användas och förstås av första linjens aktörer – operatörer, underhållstekniker, vårdbiträden/sjuksköterskor eller motsvarande. Det är lämpligt att tolka en sådan definition genom att komplettera den med ett antal exempel på händelser som skall bedömas som incidenter och andra som ej bedöms som incidenter.

Med tanke på att antalet incidenter kan bli stort, speciellt om tröskeln för rapportering sätts lågt, och belastningen på utredare kan bli stor, kan det vara bra att också definiera kriterier för att avgöra om en fullständig analys och vidare hantering av en rapporterad incident är motiverad, eller om en förenklad hantering kan räcka. En sådan bedömning bör vara baserad på lärpotentialen i incidenten och inte på den aktuella konsekvensen.

Ytterligare ett element som bör finnas i systemet för incidenthantering är kriterier för vilken väg i organisationen en incident skall gå och på vilka nivåer den skall behandlas. Även detta bör styras i första hand av lärpotentialen i incidenten, kanske i kombination med hur allvarlig konsekvensen är.

## Att analysera/utreda incidenter

Analysen/utredningen av en incident är nyckelsteget för att få fram läxorna som skall överföras till lärdomar. Ju ”större och allvarligare” incidenten är desto större omfattning får i allmänhet utredningen. De flesta av de många små incidenterna behandlas i praktiken enbart utifrån de fakta som ges i den ursprungliga rapporten.

Här följer en beskrivning av olika viktiga aspekter i analyssteget för en incident. Beskrivningen är anpassad till vad som kan vara relevant för incidenter med lite större konsekvenser eller större lärpotential. Flertalet av de incidenter som normalt förekommer i den stora mängden av incidenter behöver inte en så formell behandling som beskrivs nedan, även om själva aspekterna som beskrivs alltid finns med. För att analysera/utreda riktigt allvarliga incidenter, eller sådana som hade kunnat bli allvarliga (eller egentligen sådana som kunnat avslöja latent förhållanden med potential att bidra till olyckor) kan det behövas en ännu mer omfattande beskrivning av tillvägagångssätt och metoder än vad som ges nedan.

### Resurser

Framför allt analyssteget ställer höga krav på resurser och god kompetens på den (de) som skall utföra det. Analysen bör ledas av någon med status och god kompetens för att de rekommendationer man kommer fram till skall ha tillräcklig tyngd och trovärdighet i organisationen. Vanligtvis är detta en linjeförman och oftast den ansvariga chefen för avdelningen där incidenten hände. Denna kan behöva ha stöd av en säkerhets- och hälsospecialist, teknisk specialist och andra resurser. Ur ett arbetsmiljöperspektiv är det viktigt att verksamhetens representanter och de anställda samarbetar i utredningen av incidenterna. Skyddsombud kan ofta bidra med värdefulla synpunkter. Resurserna anpassas efter incidentens karaktär och allvarlighet.

### Faktainsamling

Utgångspunkten för den (dem) som ska analysera incidenten är beskrivningen som ges i rapportsteget. Även om denna beskrivning är fyllig behöver den ofta kompletteras med mer fakta för att få en tillräckligt bra bild av incidenten.

Typiska inslag i detta kan vara att:

- Observera förhållanden på platsen för incidenten (i direkt anslutning till incidenten, där platsen eventuellt säkras, fotografier tas, skisser görs mm. eller senare efter incidenten)
- Insamla och sammanställa drift- och underhållsinformation (t.ex. loggar, datautskrifts och underhålls-/inspektionsprotokoll)
- Undersöka tekniska system (materialprov, kontrollberäkningar, simuleringar mm.)
- Intervjua direkt berörda och andra personer

Fakta av ovanstående typer i samband med en incident är naturligtvis färskvara, och därför bör den insamlas så fort som möjligt efter att händelsen skett. Vid allvarliga incidenter blir omfattningen av faktainsamlingen stor.

## Händelseförloppet

Utredarens uppgift är att rekonstruera händelseförloppet för att förstå incidenten och därmed kunna analysera fram orsaker. Vid de allra flesta av de incidenter som avses i denna handledning brukar det räcka med en ganska enkel rekonstruktion av händelseförloppet. Man utgår helt enkelt från själva sluthändelsen – incidenten med sin skada (ibland utan skada) och arbetar sig bakåt i tid med aktiviteter/händelser som föregått sluthändelsen. När alla relevanta delhändelser ordnats i tidsföljd går man igenom dem och letar efter delhändelser som på något sätt avviker från det normala och som påverkat utgången av incidenten. Fallande skyddsbarriärer tas också med i kedjan av händelser.

I utvärderingen av incidenten bör utredaren fråga sig

- Vad kunde ha hänt som värst?
- Vad förhindrade det värsta från att hända?
- Hur ofta kan det hända?

för att ännu bättre komma fram till vilka erfarenheter som kan dras av incidenten.

## Orsaker

Orsaksanalysen får betraktas som den viktigaste delen av analysen/utredningen av incidenten. Framför allt gäller det att komma fram till vilka underliggande orsaker som kan förklara händelsen. De direkta orsakerna innehåller

- personfaktorer, som t.ex. olämpliga beteenden, direkta felgrepp, otillräcklig kompetens hos dem som utför arbetet, och
- jobbfaktorer, som t.ex. brister i säkerhetssystem, brister i utformningen av utrustningen, plötsligt uppträdande försvårande omständigheter (situationsfaktorer), samt
- tekniska faktorer, som t.ex. fallande utrustning.

De underliggande orsakerna innehåller ledningsfaktorer och organisatoriska faktorer som t.ex. brister i instruktioner, brister i utbildning, brister i underhåll, brister i ledningssystem och till sist i brister i engagemang från ledning och i säkerhetskultur.

I praktiken används i de allra flesta fall av smärre incidenter ingen formell metod för orsaksanalys. De flesta utredarna skulle antagligen hänvisa till allmän slutledningsförmåga och sunt förnuft. Man ställer sig antagligen frågan "Varför?" och hittar en som man tycker trolig förklaring. Ofta stannar man vid att få svar på ett "Varför?".



En utmärkt och samtidigt mycket enkel metod är att fortsätta att ställa frågan "Varför?" för varje orsak ända tills man inte längre har några bra svar, som kan åtgärdas i den egna organisationen. Rätt använd brukar denna metod generera värdefulla underliggande orsaker. Metoden brukar ibland kallas "Fem varför" ("5 Why's"). Man bygger i denna metod ett *fritt orsaksträd* genom "brainstorming". Risken är naturligtvis att man förbiser något viktigt. För att försöka undvika detta kan man till sin hjälp ha någon form av checklista med möjliga orsaker. En sådan metod är SMORT (Safety Management and Organisational Review Technique). Mer om SMORT finns i **Prevention of Accidents Through Experience Feedback**. Urban Kjellén, Taylor and Francis, 2000 och i **Granskningsmetodik: Menneske-teknologi-organisasjon**. SINTEF (Tinnmannsvik et al.), 2004.

Man kan också använda sig av *förutbestämda orsaksträd*, i vilka det finns förslag på framför allt sannolika underliggande orsaker, utgående från givna direkta orsaker. En förhållandevis enkel sådan metod beskrivs under "Hur man kan undersöka effektiviteten i lärandet från incidenter", och som återfinns i sin helhet i **Metod 2** i Del 2. Metoden bygger på att från direkta orsaker på utrustningsnivå och nivån 1:a linjens aktörer (exempelvis driftoperatörer) söka sannolika underliggande orsaker bland ett antal förslag, betrakta dessa underliggande orsaker som mera direkta orsaker på en högre organisatorisk nivå, söka nya sannolika underliggande orsaker på denna nivå, och på så sätt klättra uppåt i organisationen tills det inte längre känns meningsfullt att konkretisera orsakerna. En klassisk metod inom området förutbestämda orsaksträd är MORT (Management Oversight and Risk Tree). Mer om MORT kan bl.a. läsas i **Prevention of Accidents Through Experience Feedback**. Urban Kjellén, Taylor and Francis, 2000. MORT-metoden är emellertid ganska tungarbetad och rekommenderas bara i samband med utredningar av större olyckor.

Man brukar prata om stopp-regler när det gäller hur långt man skall gå i att finna underliggande orsaker. Normalt bör man sluta leta efter underliggande orsaker när det inte längre är möjligt för den aktuella organisationen att påverka de faktorer som ger upphov till orsakerna.

## Rekommendationer

Vid incidenter med allvarliga konsekvenser bör en formell rapport innehållande en redovisning av själva händelsen, en ordentlig orsaksanalys och slutsatser och rekommendationer skrivas. I de flesta fall med incidenter räcker det med att slutprodukten av analysen/utredningen uttrycks i tydliga rekommendationer om vad som bör göras för att ta hand om läxorna från incidenten i dokumenten i själva incidenthanteringssystemet. Viktigt är att rekommendationerna är realistiska och genomförbara.

## Överföring av lärande från system för incidenthantering till organisationens minne

För att erfarenheterna som analyserats fram från en incident skall bli ett effektivt lärande i en organisation fordras att dessa omsätts till kunskap i de olika delarna av organisationens minne, från vilket de kan tas fram vid behov.

Följande exempel, hämtat från processindustrin, kan illustrera några typiska system som är aktuella vid lagring av erfarenheten från en enskild incident. Exemplet handlar om en förslitning av en detalj i ett produktionssystem, som leder till en farlig situation. För att konkretisera detta mer väljer vi att betrakta en händelse där en rörbøj i ett rörsystem springer läck p.g.a. korrosion/erosion och ger brännskada eller frätskada på en anställd. Man kan välja att bara reparera eller ersätta den trasiga rörböjen i samma material som tidigare och ingenting mer. Lärdomen blir då ganska begränsad och förmodligen kortvarig. Man kan också välja att ersätta rörböjen med en ny i mer motståndskraftigt material. För att en sådan åtgärd ska resultera i ett bra och långsiktigt lärande måste informationen kring beslutet gå in dels i underhållssystemet så att man vid nästa tillfälle också byter till det bättre materialet, dels i designspecifikationerna för rörsystem vid nykonstruktion. Man kan också tänka sig att beslutet blir att även inspektera övriga rörböjar i rörsystemet och ersätta dessa vid behov och/eller att upprätta en plan för regelbunden inspektion av alla rörböjar. Även en sådan åtgärd kräver att man går in i de administrativa systemen, i detta fall systemet för förebyggande underhåll och kontroll, och uppdaterar dessa och även säkerställer att dessa konsulteras av berörda personer.

Samma exempel (förslitning av detalj, t.ex. rörbøj i rörsystem) kan användas för att exemplifiera vad som krävs vid en ändring i handhavande vid produktion. Man finner kanske att det är driftsättet som gör att rörböjarna slits oväntat snabbt. Då kan den bästa åtgärden vara att ändra driftsätt. Kunskap om detta måste då komma alla berörda på driftavdelningen till del. Det sker genom information inom olika fora (regelbundna möten) eller genom mer formell utbildning. Sannolikt skall också en eller flera driftinstruktion(er) uppdateras. Då gäller det att det också finns en administrativ process som gör att alla berörda anställda kommer att ta del av de uppdaterade driftinstruktionerna.

Det har visat sig att det ofta är ganska svårt att nå ut till alla berörda individer och till alla berörda ställen i de administrativa systemen. Lärandeagenten har här en nyckelfunktion, som ska se till att kunskapen verkligen förs ut hela vägen.

## Rutin och administrativt system för incidenthantering

Varje verksamhet bör ha en särskild rutin/procedur för incidenthantering, vilken ska beskriva hur hela hanteringen av incidenter ska gå till. Innehållet och hantlingsgången i denna rutin blir då styrande för hur det administrativa verktyget/systemet skall utformas.

Numera har de flesta verksamheter datoriserade system för detta (från rapportering till uppföljning), men i mindre verksamheter kan man tänka sig att pappersbaserade system kan fungera lika väl. De system som erbjuds kommersiellt har i allmänhet allt man normalt behöver i ett sådant system och ofta mer därtill. Väljer man ett kommersiellt system bör man ha möjlighet att kunna anpassa det efter sina egna behov. Vägledande vid utformningen av system bör vara att hålla det så enkelt som möjligt att arbeta i för de personer som blir berörda. Ett stort system med många finesser tenderar till att avskräcka många medarbetare från att använda det. Speciellt bör det första steget – att rapportera – göras enkelt för att inte hämma rapporteringen.

## Hur skapar, inför och upprätthåller man ett incidenthanteringssystem?

I många organisationer finns redan ett incidenthanteringssystem. Därför görs här bara några summariska konstateranden kring processen att skapa, införa och upprätthålla ett incidenthanteringssystem.

Det finns ett antal principer som måste följas för att ett system för incidenthantering vid sitt införande skall ha en möjlighet att bli väl mottaget och fungera. Några av de viktigaste är:

- Sälj in konceptet hos ledningen och dess VD eller motsvarande och kräv aktivt stöd och engagemang.
- Utse en person som kan fungera som "primus motor" för projektet.
- Engagera hela organisationen i arbetet.
- Arbeta genom en projekt- och/eller en styrgrupp.
- Gör en tidplan med mål och delmål.
- Bygg systemet på verksamhetens redan existerande rutiner, instruktioner mm., om sådana finns, t.ex. i befintligt kvalitetssystem.

Själva införandet är ett kritiskt skede och bör ägnas stor uppmärksamhet och planeras väl. Följande är några viktiga punkter:

- Ett stegvis införande kan vara lämpligt i större verksamheter för att testa systemet och dess mottagande.
- Projektledaren måste följa upp mycket noga hur rutinerna tas emot och fungerar.
- Linjeorganisationen ska följa och engagera sig i införandet av systemet.
- En primus motor måste fortsatt finnas. Denne kan vara densamme som projektledaren eller t.ex. SHM-chefen.
- Utbildning av all personal (chefer, övriga anställda, entreprenörer, transportörer och motsvarande) ska genomföras.

För att arbetet med incidenthantering skall bli framgångsrikt på sikt krävs bl.a. att man

- kontinuerligt följer arbetet i ledningen och återkopplar till rapportörerna.
- gör periodisk kontroll i form av intern granskning/revision.
- kontinuerligt utbildar och motiverar personalen.
- ser till att tillräckliga resurser finns, särskilt för analys av incidenterna och analys och uppföljning av det samlade materialet.

- ser till att de incidenter som rapporteras behandlas på ett bra sätt i hela kedjan fram till implementerade åtgärder. Kvalitet är viktigare än kvantitet. Dock bör eventuellt misstänkt höga mörkertal uppmärksammas och bearbetas.
- undviker onödig byråkrati kring data.

Hela tiden måste det finnas en pådrivande person som har ansvar för att övervaka, kontrollera och utveckla systemet. Detta kan t.ex. vara chefen för verksamhetens SHM-funktion.

## Kopplingar till andra element i verksamhetens säkerhetsarbete

Systemet eller proceduren för incidenthantering är bara ett av många system eller en av många procedurer i en verksamhets ledningssystem för säkerhet. Incidenthanteringssystemet har kopplingar till de flesta procedurerna i säkerhetsledningssystemet, eftersom det genererar input till förbättringar i alla möjliga delar av verksamhetens arbete för ökad säkerhet. Man kan bara nämna några viktiga sådana, som

- Drift- och underhållsinstruktioner
- Program för förebyggande underhåll
- Tekniska specifikationer för design och konstruktion
- Utbildningsprogram
- Riskanalyser
- Modifieringsrutiner

Procedurer som är nära besläktade med incidenthanteringssystemet är procedurer för "säkerhetsindikatorer", "skyddsronder" och "beteendebaserad säkerhet".

Säkerhetsindikatorer är ju mätetal för att fånga säkerhetsprestanda i en organisation. Dessa kan antingen vara proaktiva eller reaktiva indikatorer. En proaktiv indikator innehåller någon form av mätning av aktiviteter som utförs för att förbättra säkerheten, inkluderande de utfall/resultat man kan erhålla under sådana aktiviteter, vilket innebär

- mätning av aktiviteten i sig (t.ex. graden av genomförande av tester av säkerhetsutrustning), eller
- mätning av resultaten från aktiviteten (t.ex. graden av genomförda tester som höll måttet)

En reaktiv indikator innehåller typiskt mätning av antal falleranden under normal drift (t.ex. antal utsläpp av farliga kemikalier per kvartal eller antal felordinationer i sjukvården).

Av detta framgår att ett system för incidenthantering är väl lämpat för att generera input till systemet för säkerhetsindikatorer, särskilt för de reaktiva indikatorerna.

Skyddsronder eller SHM-ronder är en självklar aktivitet på de flesta arbetsplatser. Normalt rapporteras iakttagelserna under sådana ronder i särskild ordning. Eftersom avvikelser från standard funna under skyddsronder till sin natur är snarlika incidenter, är det emellertid ingenting som hindrar att dessa rapporteras in i systemet för incidenthantering.

Arbete med beteendebaserad säkerhet innebär i allmänhet att man på planerad basis utför observationer av en person i arbete och konstaterar eventuella avvikelser från bästa, säkra sätt att utföra detta arbete. Även detta brukar dokumenteras i särskild ordning, och bör antagligen så göras för att undvika för mycket utpekande av person. Aktiviteten som sådan påminner en hel del om incidenthantering, dock med den viktiga skillnaden att det i beteendebaserat arbete handlar om planerade observationer.

I många verksamheter finns system för rapportering av avvikelser med fokus på kvalitet och "produktion". Rapporteringsfrekvensen i sådana system brukar vara betydligt högre än i system för incidenthantering med fokus på säkerhet, hälsa och miljö. Arbetsinsatsen för de flesta sådana avvikelser är också oftast betydligt lägre än i system för incidenthantering för säkerhet, hälsa och miljö. I grunden är det emellertid ingen egentlig skillnad på dessa två system. Vissa verksamheter hanterar alla sorters avvikelser i ett och samma system.

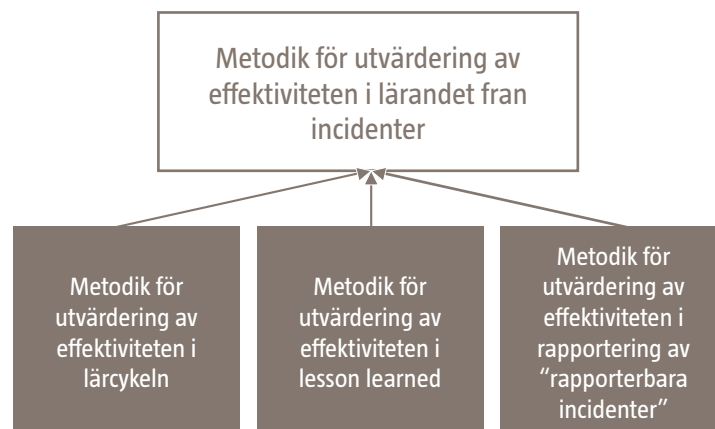
## Hur man kan undersöka effektiviteten i lärandet från incidenter

Att mäta själva lärandet från incidenter är mycket svårt. Enligt tidigare definition av en lärdom har lärandet ägt rum först när läxan är implementerad. Det innebär att alla anställda och ibland även andra som kan vara berörda av läxan från incidenten skall ha tagit till sig kunskapen som utvunnits, och dessutom i framtiden agera utifrån denna. Det säger sig självt att det är nästan omöjligt att mäta om detta har uppnåtts. Man kan möjligen genom intervjuer och enkäter mäta i hur hög grad informationen gått fram.

Man kan dock uppskatta hur pass bra effektiviteten är i själva incidenthanteringssystemet, vilket i sig ger en viss uppfattning om åtminstone hur förutsättningarna för lärande är.

Det är framför allt tre frågor som är intressanta.

1. Har vi en effektiv hantering av de incidenter som rapporteras i vårt system? Fungerar de olika stegen i lärcykeln effektivt?
2. Hur mycket lär vi oss av de incidenter som rapporteras i förhållande till vad som potentiellt går att lära sig av dem? Vilken lärandenivå ligger vi på, vilken skulle vi kunna ligga på och vilken skulle vi vilja ligga på?
3. Rapporterar vi de incidenter som är värda att rapportera? Vad är tröskeln för rapportering? Hur stort är mörkertalet?



Här följer en sammanfattning av en metodik som utarbetats för ändamålet och som täcker alla väsentliga aspekter i både lärprocessen och lärprodukten. **Metoderna 1, 2 och 3** i Del 2 ger en detaljerad vägledning för användning av de olika metoderna och tillhörande verktyg. I **Proceduren** i Del 2 "Praktisk användning av metodiken och dess metoder" ges ytterligare information om användningen, både i en förenklad och i en fullständig tillämpning.



## Effektiviteten i lärcykeln

En självklar förutsättning för att lärandet från incidenter skall fungera åtminstone hyggligt är att själva processen i lärcykeln alla steg fungerar, vilket i sin tur betyder att det administrativa systemet för incidenthantering måste fungera. Alla steg är viktiga. En detaljerad beskrivning av en metod för att undersöka detta ges i **Metod 1** i Del 2. Här görs en något förkortad beskrivning med huvudragen i metoden.

Metoden baseras på att för varje steg bedöma hur väl olika dimensioner och aspekter i dessa behandlas. Genom att bedöma effektiviteten för alla rapporterade incidenter över en viss tidsperiod (säg ett halvår eller ett år) blir det möjligt att ”mäta” en genomsnittlig effektivitet i varje steg i lärcykeln. Dessa mätetal kan användas som sådana för att bedöma om förbättringar behöver införas. De kan också vara till nytta vid jämförelser mellan olika avdelningar inom en verksamhet eller mellan verksamheter.

Metoden innehåller fyra komponenter:

- stegen i lärcykeln;
- dimensioner i varje steg;
- aspekter i varje dimension; och
- mallar med skalor för att bedöma numeriska värden på de olika dimensionerna som ett mått på effektiviteten i varje steg.

Metoden bygger på vad som tidigare sagts i avsnittet om ”Element och innehåll i ett system för rapportering och hantering av incidenter” och på informationen i **Checklista 2** i Del 2.

För alla stegen ingår följande fyra dimensioner (vilka används för beräkning av ett numeriskt värde), vilka i sin tur innehåller flera aspekter, som alla bör vara täckta för en fullgod behandling av en incident.

1. Omfattning (aspekterna varierar beroende på steg)
2. Kvalitet (detaljeringsgrad och djup vid behandlingen av aspekterna under ”Omfattning”);
3. Tid (tid från ett steg till nästa); och
4. Information (informationsspridning i organisationen).

I tillägg till dessa fyra dimensioner innehåller metoden för flera steg ytterligare dimensioner, vilka används mer för att förklara resultatet från de fyra första dimensionerna.

### Poängsystem

För att kunna uttrycka effektiviteten av hanteringen av incidenter har skapats ett poängsystem. De olika aspekterna för varje dimension beskrivs på ett semi-kvantitativt sätt på en skala (mellan 0 och 10) för att kunna mäta effektiviteten så objektivt som möjligt. Kraven för att uppfylla en viss poäng beskrivs genom att

använda vissa ledord för fyra nivåer på 0 – 10-poängsskalan – 2 (Bristfälligt), 4 (Bör förbättras), 7 (Bra) och 10 (Utmärkt). Poängsystemet framgår i detalj i **Metod 1** i Del 2.

## Effektiviteten i lärprodukten, lesson learned; Lärandenivån

Slutprodukten av lärandet från incidenter är ju den implementerade läxan, lärdomen. Här följer en beskrivning av en metod som i sex steg utvärderar lärandet från incidenter baserat på begreppet lärandenivå.

I **Metod 2** i Del 2 finns en detaljerad beskrivning. Här görs en något förkortad beskrivning med huvuddragen i metoden.

Metoden innehåller följande steg

1. Utvärdering av *verklig* lärandenivå hos rapporterade incidenter
2. Utvärdering av *potentiell* lärandenivå hos rapporterade incidenter
3. *Jämförelse* av verklig och potentiell lärandenivå
4. *Korrektion* av resultaten i steg 1 – 3 för mörkertal, dvs. incidenter som ej rapporterats
5. Hänsyn till lärande från behandling av incidenter på en aggregerad nivå – här kallad *2:a loopen*.
6. Hänsyn till andra mekanismer för lärande från incidenter

Även denna metod är tänkt att användas på alla rapporterade incidenter under en viss tidsperiod för att kunna bedöma fördelningen av lärandenivåer och att bilda medelvärden och göra jämförelser.

### Steg 1: Verkligt lärande

Det första steget innebär att klassificera lärdomen (eller läxan, om inte lärdomen kan säkert fastställas) i rapporterade incidenter enligt ett system som baseras på

- primärt, hur brett lärdomen appliceras geografiskt i verksamheten (från mycket lokalt där incidenten inträffade till över hela verksamheten, "siten", där liknande förhållanden råder),
- sekundärt, hur mycket organisatoriskt lärande som är inblandat (tekniska, procedurmässiga och personalmässiga åtgärder)
- tertiärt, hur mycket organisatoriskt långtidsminne som är inblandat.

Det finns inga skarpa gränser mellan de tre aspekterna; viss överlappning mellan den geografiska aspekten och de andra två aspekterna förekommer.

Klassificeringen i sex klasser framgår av Tabell 1. Som jämförelse har i denna tabell också angivits vilken motsvarande klassificering som erhålls om klassificering enligt systemen med 1:a, 2:a och 3:e ordningens lärande samt enkel-loop- och dubbel-loop-lärande används.

Nivå	Karakteristika	1:a, 2:a, 3:e ordningen	Enkel-loop Dubbel-loop
<b>0</b>	Inget egentligt lärande	-	-
<b>I</b>	<i>Primärt:</i> Begränsat lokalt lärande <i>Tillägg:</i> Nästan inget organisatoriskt lärande; Korttidsminne.	(1:a)	(SLL)
<b>II</b>	<i>Primärt:</i> Lokalt lärande <i>Tillägg:</i> Begränsat organisatoriskt lärande; Huvudsakligen långtidsminne.	1:a	SLL
<b>III</b>	<i>Primärt:</i> Lärande på avdelningsnivå (t.ex. processenhet) <i>Tillägg:</i> Substantiellt organisatoriskt lärande; Långtidsminne.	2:a	SLL
<b>IV</b>	<i>Primärt:</i> Lärande på enhetsnivå, t.ex. "site" <i>Tillägg:</i> Substantiellt organisatoriskt lärande; Långtidsminne.	3:e	DLL
<b>V</b>	<i>Primärt:</i> Högre lärande, Koncernlärande; <i>Tillägg:</i> Substantiellt organisatoriskt lärande; Långtidsminne.	3:e	DLL

**Tabell 1**

Resultatet av steg 1 är en procentuell fördelning av incidenterna på de olika klasserna. Ur detta kan en hel del slutsatser dras om hur väl lärandet fungerar. För att gå vidare i metoden kan också ett "medelvärde" beräknas.

### **Steg 2: Potentiellt lärande**

För att bedöma effektiviteten i lärandet bättre än bara genom att utvärdera det verkliga lärandet enligt steg 1 bör det verkliga lärandet jämföras med det lärande som hade kunnat uppnås om den fulla lärlpotentialen i incidenterna hade utnyttjats. De flesta incidenter, om än inte alla, innehåller en potential för högre lärande. Vi antar här att om man kan klarlägga orsaksbilden kring en incident fullt ut, bör man kunna utvärdera de potentiella lärdomarna som kan utvinnas ur incidenten. Nästa steg i metoden är därför att med hjälp av ett verktyg, som är snabbt och effektivt att använda, utvärdera de mest sannolika direkta och bidragande orsakerna till incidenterna utöver vad som redan

finns angivet i incidentrapporterna. Verktøget bygger på att verksamheten kan beskrivas som ett socio-tekniskt system med olika hierarkiska nivåer. Följande exempel på nivåer kan tillämpas på många typer av verksamheter.

- Högsta ledningen, företagsledning (typiskt site-ledning)
- Andra påverkande nivåer (typiskt stabs- och stödfunktioner)
- Arbetsledning på högre nivåer (middle management/typiskt avdelning, fabriksenhet)
- Arbetsledning på utförandenivå (typiskt 1:a linjens arbetsledare)
- Direkt utförandenivå (typiskt operatörer, sjuksköterskor/vårdbiträden)
- Process/Utrustning

I **Metod 2** i Del 2 finns det fullständiga verktøget för orsaksanalys av incidenter med exempel på direkta och underliggande orsaker.

Genom att applicera detta verktøg på samma incidentrapporter som i steg 1 kan man få fram de troliga bidragande orsakerna och därmed de lärdomar som hade kunnat utvinnas ur incidenterna. Därefter kan man på nytt använda verktøget i Tabell 2 för att bedöma vilken lärandenivå som hade varit möjlig att uppnå om man utnyttjat hela potentialen i incidenterna.

Resultatet av steg 2 är en ny uppsättning siffror som anger fördelningen av potentiellt lärande från rapporterade incidenter. Även här kan ett ”medelvärde” för potentiellt lärande beräknas.

### **Steg 3: Jämförelse mellan verklig och potentiell lärandenivå**

Med de två uppsättningarna av värden för verkligt lärande och potentiellt lärande från steg 1 och steg 2 kan man göra jämförelser och dra slutsatser om effektiviteten i lärandet. Siffrorna fördelade på lärandenivåer kan jämföras och kvoten av ”medelvärdena” kan beräknas som ett enkelt mått på effektiviteten, och eventuella förbättringsåtgärder kan övervägas.

### **Steg 4: Korrektion för mörkertal, dvs ej rapporterade incidenter**

Vi bör även ta hänsyn till att vissa incidenter inträffar men inte rapporteras, vilket alltså innebär att vi missar en del lärdomar. Frågan om mörkertalet har beskrivits delvis tidigare. Man kan nöja sig med att behandla denna fråga övergripande som en egen företeelse eller också att gå vidare i metoden och introducera en ”matematisk” korrektion för mörkertalet (för detta se **Metod 2** i Del 2).

### **Steg 5: Hänsyn till lärande från incidenter på en aggregerad nivå – 2:a loopen**

Förekomsten och kvaliteten av en 2:a loop bör naturligtvis påverka bedömningen av lärandenivån, förutsatt att en sådan behandling av samlade incidenter väsentligen ökar lärandenivån. Samma verktøg som utvecklats för att bedöma effektiviteten i 2:a loopen under rubriken ”Lärcykeln” kan vara ett hjälpmedel här (se **Metod 1** i Del 2). En bra behandling av incidenterna i 2:a loopen kan delvis kompensera för ett sämre utfall av lärandenivå baserat på bedömning av de individuella incidenterna enligt steg 1 ovan.

### Steg 6: Hänsyn till andra mekanismer för lärande från incidenter

Som ett sista steg i metoden ingår att ta hänsyn till eventuella andra sätt att lära från incidenter än genom incidenthanteringssystemet (se vidare i **Metod 2** i Del 2).

### Tröskeln för rapportering

En uppfattning om var tröskeln för rapportering ligger, kan man få med användning av ett verktyg som presenteras i **Metod 3** i Del 2. Verktøget ger en kvalitativ utsaga om var på en 0-10-skala en rapporterad incident befinner sig. Utgångspunkten i verktyget är olika typer av händelser, som är vanliga i framför allt processindustrisammanhang, men som direkt kan användas även i andra sammanhang eller i modifierad form på de allra flesta verksamheter.

Kategorierna är:

1. Händelser som lett till faktiska personskador
2. Händelser som lett till någon form av utsläpp av farliga kemikalier (kategorin är specifik och central för processindustri; kan ersättas med annan relevant kategori)
3. Händelser som hade kunnat leda till händelser av kategori 1 eller 2 om ytterligare en eller flera omständigheter varit för handen
4. Avvikelse från procedurer (utan olycka)
5. Andra avvikelser (utan olycka)

### Mörkertal

Tidigare har nämnts att antalet rapportervärda incidenter sannolikt varierar starkt mellan olika verksamheter. Eftersom frågan om mörkertal är viktig, bör man trots svårigheterna att uppskatta vad som kan vara ett rimligt värde på antalet rapportervärda incidenter i sin verksamhet göra en ansats att bedöma detta. I LINS-projektet, som behandlat sex olika processindustrier, har gjorts vissa bedömningar om vad som kan vara en rimlig siffra på hur många incidenter som inträffar per anställd, per år. Den siffra som har använts som ett standardvärde är 3 incidenter per anställd per år. I arbetet tillfrågades såväl en extern, neutral expertpanel som företagen som ingick i studien om detta. Experternas siffra blev 3 incidenter per anställd, per år som medelvärde med ett spann mellan 1 och 7.5. Företagens egna bedömningar blev 2.3 med ett spann från 0.75 till 5.

I andra verksamheter kan ett rimligt antal incidenter per anställd per år vara både högre och lägre än 3. Varje verksamhet gör bäst sin egen uppskattning av hur många rapportervärda incidenter som borde förekomma i verksamheten.

Redan en diskussion inom verksamheten om hur många incidenter som de facto rapporteras i förhållande till hur många incidenter som är rapportervärda är en nyttig övning. Resultatet kan bli att man höjer rapporteringsfrekvensen. Det måste då emellertid tillses att det finns resurser att ta hand om en ökad rapportering. Annars kan den goda ambitionen att lära mer bli ett slag i luften, och i värsta fall resultera i en sänkt motivation för rapportering, om de anställda upplever att organisationen inte tar hand om rapporterna på ett bra sätt.

## Hantering av "Stora olyckor"

Som framgått tidigare avser denna handledning inte att behandla hanteringen av "stora olyckor". Med stora olyckor avser vi oftast olyckor där konsekvenserna är stora. Dock kan det finnas incidenter med mindre konsekvenser, men med hög lärpotential, som också kan motivera en grundlig behandling och utredning. Vid stora olyckor blir det ökat fokus på alla delar av hanteringen, speciellt i olycksutredningssteget. Det som beskrivs tidigare i "Att analysera/utreda incidenter" blir då fullt tillämbart. Oftast kopplas mycket kompetenta, gärna externa, resurser in för utredningen. Faktainsamlingen blir ofta omfattande för att klarlägga händelseförloppet och ge en god grund för att kunna identifiera alla sorters orsaker och latenta förhållanden. Rekommendationerna blir oftast mer omfattande och berör ofta mer djupgående företeelser i organisationen.

I litteraturlistan finns ett antal referenser som huvudsakligen inriktar sig på utredning av olyckor.

## Viktiga punkter till hjälp för myndigheter

Det finns ett antal lagrum som ålägger olika verksamheter att rapportera olyckor och tillbud till olyckor till tillsynsmyndigheter.

I följande checklista finns ett antal punkter som kan vara lämpliga för myndigheter att vid tillsyn kontrollera i vilken grad den granskade verksamheten uppfyller rimliga krav. För flera av punkterna är det lämpligt att konsultera de verktyg som tagits fram i denna handledning.

- Finns ett formellt incidenthanteringssystem?
- Finns alla steg i lärcykeln med i verksamhetens incidenthanteringssystem?  
(Se verktyg)
- Hur fungerar de olika stegen i lärcykeln? Är något eller några steg svaga?  
(Se verktyg)
- Finns det personer som kan fungera som agenter i alla steg?
- Är resurserna och kompetensen för alla agenter tillräckliga?
- Finns en utvecklad och effektiv 2:a loop i systemet?  
(Se verktyg)
- Vad är tröskeln för rapportering? Är den rimlig och hur är den jämfört med verksamhetens definition av rapporterbar incident?  
(Se verktyg)
- Är mörkertalet för icke-rapporterade incidenter stort? En tumregel kan vara att det i de flesta verksamheter bör vara åtminstone 1 rapport per anställd per år.
- Görs egentliga orsaksanalyser? Hur djupa är de? Finns hjälpmedel?  
(Se verktyg)
- Var ligger den genomsnittliga lärandenivån på rapporterade incidenter? Om företrädesvis 0-nivå och en del 1-nivå är den sannolikt för låg.  
(Se verktyg)
- Är överföringen till det organisatoriska minnet effektiv? Uppdateras olika instruktioner och standards och genomförs utbildning?
- Är tiden för behandlingen av de olika stegen i lärcykeln rimliga?  
(Se verktyg).

## Litteraturreferenser

**Methodology for assessing learning from incidents  
– a process industry perspective.**

Anders Jacobsson. Department of Design Sciences, Lund University, Lund.

**Human Error.**

James Reason. Cambridge University Press, 1990.

**Managing the Risks of Organizational Accidents.**

James Reason. Ashgate, 1997.

**The Human Contribution – unsafe acts, accidents and heroic recoveries.**

James Reason. Ashgate, 2008.

**The Field Guide to Understanding Human Error.**

Sidney Dekker. Ashgate, 2006.

**Just Culture – balancing safety and accountability.**

Sidney Dekker. Ashgate, 2007.

**Prevention of Accidents Through Experience Feedback.**

Urban Kjellén. Taylor and Francis, 2000.

**Learning from Accidents.**

Trevor Kletz. Gulf professional publishing, 1988. 3<sup>d</sup> edition, 2001.

**Ledarskapsteori, Direkt ledarskap (s. 30 – 55).**

Gerry Larsson. I G. Larsson & K. Kallenberg (red.), Försvarsmakten, Stockholm, 2006.

**Lessons from Disaster**

**– How organisations have no memory and accidents recur.**

Trevor Kletz. Institution of Chemical Engineers, 1993.

**Investigating Human Error – incidents, accidents and complex systems.**

Barry Strauch. Ashgate, 2002, 2004.

**Barriers and Accident Prevention – or how to improve safety by understanding the nature of accidents rather than finding their causes.**

Erik Hollnagel. Ashgate, 2004.

**Sitting in the hot seat – leaders and teams for critical incident management.**

Rhona Flin. John Wiley & Sons, 1996.



## **Utredningsmetodik**

### **Olycksundersökning.**

Särdqvist. Räddningsverket, 2005.

### **Methods for accident investigation.**

Sklet, NTNU, Norwegian University of Science and Technology, Trondheim, 2002.

### **Utreda tillbud och olyckor i processindustrin.**

IPS (Weibull), 2008.

### **Investigating accidents with STEP.**

Hendrick and Benner. Occupational safety and health, Marcel Dekker. 1987.

### **Granskningsmetodikk: Menneske-teknologi-organisasjon.**

SINTEF (Tinmannsvik et al), 2004.

### **Att utreda olycksfall.**

Rollenhagen. Studentlitteratur, 2003.

### **After the event – From accident to organisational learning.**

Hale, A., Wilpert, B. and Freitag (editors). Pergamon, Oxford. 1997.

# **DEL 2**

## **Metoddel**

## Inledning

Syftet med del 2 av handledningen är att i första hand tillhandahålla praktiska hjälpmedel för organisationer som är intresserade av att undersöka effektiviteten i sitt lärande från incidenter.

Del 2 kan betraktas som en fristående del av handledningen, och de presenterade hjälpmedlen kan användas direkt utan att läsa Del 1 av läsare, som redan är insatta i ämnet.

Metodiken för att fastställa effektiviteten i lärandet från incidenter består av tre delar, vardera med sina metoder och verktyg, som tillsammans svarar på de tre fundamentala frågorna:

1. Har vi en effektiv hantering av de incidenter som rapporteras i vårt system? Fungerar de olika stegen i lärcykeln effektivt?
2. Hur mycket lär vi oss av de incidenter som rapporteras i förhållande till vad som potentiellt går att lära sig av dem? Vilken lärandenivå ligger vi på, vilken skulle vi kunna ligga på och vilken skulle vi vilja ligga på?
3. Rapporterar vi de incidenter som är värda att rapportera? Vad är tröskeln för rapportering? Hur stort är mörkertalet?

I en särskild procedur redogörs för hur metodiken med sina tre metoder kan användas praktiskt, både i en förenklad och i en fullständig tillämpning.

Här finns också hjälpmedel i form av en

- Checklista för viktiga faktorer som påverkar effektiviteten i lärandet från incidenter generellt och i lärcykeln olika steg och som kan användas som utgångspunkt för idéer, när behov för förbättringar i lärande från incidenter konstaterats, och
- Checklista som för de olika stegen i lärcykeln visar vilka dimensioner som kan vara aktuella att fylla med innehåll (olika aspekter), samt exempel på en del av dessa aspekter. Checklistan kan alltså användas vid kontroll av att det egna incidenthanteringssystemet innehåller relevanta dimensioner/aspekter.

## Förteckning över metoder och checklistor

<b>Procedur</b>	<b>Praktisk användning av metodiken och dess metoder</b>
<b>Metod 1</b>	<b>Bedömning av effektiviteten i lärcykeln</b>
<b>Metod 2</b>	<b>Bedömning av lärandenivå</b>
<b>Metod 3</b>	<b>Bedömning av tröskel för rapportering</b>
<b>Checklista 1</b>	<b>Viktiga påverkansfaktorer i lärcykeln's olika steg</b>
<b>Checklista 2</b>	<b>Viktiga element/innehåll i ett incidenthanteringssystem</b>

## Procedur

### Praktisk användning av metodiken och dess metoder

Metodiken för utvärdering av effektiviteten i lärandet från incidenter innebär att ett antal incidenter går igenom och analyseras med de metoder och verktyg som presenteras här i handledningens del 2. För att få en representativ bild bör man inkludera alla inträffade incidenter under en viss tidsperiod. Antalet incidenter som behöver analyseras för att man ska kunna uttala sig om resultatet är beroende av vilken säkerhet man vill ha i sina slutsatser. Erfarenheterna från arbete med metoderna i LINS-projektet pekar på att minst några tiotal incidenter, gärna 50 – 100 incidenter, per analyserad organisatorisk enhet, är önskvärd. Är man bara intresserad av statusen för lärandet i stort för en verksamhet räcker det antagligen med en förhållandevis begränsad insats med ett 50-tal incidenter. Vill man däremot få fram representativa resultat för flera olika avdelningar inom en större verksamhet behövs minst några tiotal incidenter per avdelning.

Informationen för analysen hämtas huvudsakligen ur incidenthanterings-systemets databas, som alltså måste innehålla rimligt god dokumentation om analysen ska vara möjlig att göra. Som komplement till incidenthanterings-systemet kan det behövas tillgång till annan dokumentation, om delar av hanteringen av incidenter dokumenterats på annat håll än i själva incidenthanteringssystemet. Så kan t.ex. skyddskommittéprotokoll, särskilda utredningar mm. innehålla relevant information för analysen.

### 1. ANALYS AV EFFEKTIVITETEN I LÄRANDET FRÅN INCIDENTER

Metodiken för utvärdering av effektiviteten i lärandet från incidenter innehåller

1. Metod med verktyg för utvärdering av effektiviteten i *lärcykeln*
2. Metod med verktyg för utvärdering av effektiviteten (lärandenivån) i *lärdomen* ("lesson learned")
3. Metod med verktyg för utvärdering av effektiviteten i rapportering av "rapporterbara incidenter"

### Förenklad tillämpning

Här beskrivs en förenklad tillämpning av metodiken (jämfört med vad som praktiserats i forskningsprojektet som genererat metodiken). Analysen blir då inte särskilt tidskrävande men genererar ändå ett kvalitativt bra resultat. Även detta förenklade tillvägagångssätt har tillämpats i praktiken med gott resultat.

#### Arbetsgrupp (förslag):

Ordförande, som är väl insatt i metodiken. 2-3 ytterligare personer med kompetens på området, t.ex. skyddsombud, SHM-chef, Arbetsmiljöingenjör. Alla deltagarna skall ha satt sig in i metodiken på förhand för att snabbt och effektivt kunna använda den.

**Material (urval):**

De 50 senast inträffade incidenterna, som blivit slutbehandlade i incidenthanteringsystemet.

**Arbetsätt:**

1. Förbered genom att lista incidenterna t.ex. i Excel med utrymme för Lärandenivå ("Verklig" och "Potentiell") samt för varje steg i lärcykeln dimensionerna Omfattning, Kvalitet, Tid, Information mm. Detta arbete görs på förhand av någon av deltagarna.
2. Gå igenom i gruppen incident för incident med hjälp av metoden i **Metod 1** för lärcykeln olika steg och **Metod 2** för lärandenivå ("Verklig" och "Potentiell"). OBS! Alla stegen i lärcykeln skal utvärderas, även 2:a loopen. I denna förenklade tillämpning kan korrigeringen för mörkertal enligt **Metod 2** lämpligen utelämnas.
3. Beräkna medelvärden, utvärdera och kommentera resultaten av 2.
4. Bedöm tröskeln för rapportering och mörkertalet med hjälp av **Metod 3**.
5. Sammanfatta resultaten inklusive övriga iakttagelser från arbetet.
6. Presentera hela arbetet för ledning och anställda.

**Resultat:**

För effektiviteten i lärcykeln erhålls resultat uttryckta i poäng enligt bedömningsmallarnas skalor och den kvalitet som dessa uttrycker. 5 poäng kan anses vara godkänt och 7 poäng kan sägas vara bra och eftersträvansvärt.

För lärandenivå erhålls bl.a. en fördelning mellan olika lärandenivåer som i sig innehåller intressant information. "Verklig" lärandenivå bör ha sin tyngdpunkt åtminstone åt nivå 2 för att betraktas som bra. Framför allt bör kvoten mellan medelvärden för "Verklig lärandenivå" och "Potentiell lärandenivå" inte vara alltför låg; en kvot  $< 0.5$  signalerar att det finns en hel del mer att ta till vara som lärdomar i incidenterna än vad som görs.

För tröskeln för rapportering erhålls resultat uttryckt i poäng enligt bedömningsmallens skala och den kvalitet som den uttrycker. Poäng  $\leq 4$  indikerar att många fler rapportervärda incidenter sannolikt inträffar än vad som rapporteras. På samma sätt torde en rapporteringsgrad på mindre än 1 rapport per år per anställd också indikera att många fler rapportervärda incidenter finns.

Resultaten medger också (i och med att incidenterna bedöms individuellt) att vissa jämförelser mellan t.ex. olika avdelningar kan göras. Dock kan det begränsade antalet analyserade incidenter göra en sådan jämförelse väl osäker i denna förenklade tillämpning.

Resultaten bör sammanfattas i en kort rapport.

**Tidsåtgång:**

C:a 2 arbetsdagar för grupparbetet inklusive sammanfattning och presentation. (Detta har visat sig vara fullt möjligt i praktiken.) Förberedelserna enligt punkt 1 ligger utanför denna tid.

**Fullständig tillämpning**

Med en fullständig tillämpning avses här en djupare, men också mer tidskrävande genomgång av ett större material av incidenter för en verksamhet. Om man är särskilt intresserad av att undersöka olika avdelningars effektivitet i lärandet från incidenter eller om man vill undersöka om förändringar sker över tid krävs i allmänhet analys av fler incidenter än vad som angetts under "Förenklad tillämpning". Även för att se eventuella effekter av vissa genomförda åtgärder krävs också normalt analys av ett större material.

Lämpligt material kan vara incidenterna under ett par års tid, eventuellt uppdaterade i perioder baserade på förändringar av organisation, bemanning eller andra faktorer som kan ha påverkat rapportering och lärande från incidenter. Här bör **Metod 1, 2 och 3** följas i alla detaljer.

En sådan mera fullständig tillämpning kan också göras av en arbetsgrupp med större arbetsinsats, men istället föreslås att i detta fall lämna merparten av arbetet till en lämplig person att ensam utföra detta. Personens arbete och resultat bör dock förankras med andra personer insatta i verksamhetens system genom att testa ett urval av personens bedömningar och slutsatser i en lämplig arbetsgrupp enligt ovan under "Förenklad tillämpning".

Resultaten från en fullständig tillämpning ger givetvis en säkrare bedömning av alla aspekter i lärandet från incidenter och en djupare insikt i saker som påverkar detta och hur det kan förbättras.

**2. INVENTERING AV FÖRBÄTTRINGSFÖRSLAG**

Om analysen av effektiviteten i lärandet från incidenter enligt punkt 1 ovan visar på ett otillräckligt resultat, i förhållande till den ambitionsnivå man har eller siktar på, vidtar nästa steg – att söka förklaringar till varför lärandet i vissa avseenden är sämre än önskat. Precisa diagnoser om orsaker och exakta recept för hur förbättringar ska genomföras är svåra att ge, men idéer till förklaringar och därmed också till möjliga förbättringsåtgärder kan sökas i checklistorna som inkluderats i handledningen.

Checklista 1 kan användas för att kontrollera att både de allmänna förutsättningarna för ett gott lärande från incidenter och de som gäller för de enskilda stegen i lärcykeln är uppfyllda genom att gå igenom listan med påverkansfaktorer.

Checklista 2 kan användas för att kontrollera att organisationens incidenthanteringsystem innehåller och de facto hanterar de dimensioner och aspekter som där definieras.

## Metod 1. Bedömning av effektiviteten i lärcykeln

En förutsättning för att lärandet från incidenter ska fungera är givetvis att själva processen i lärcykeln alla steg fungerar, vilket i sin tur betyder att det administrativa systemet för incidenthantering måste fungera. Alla steg är viktiga.

Metoden baseras på att för varje steg bedöma hur väl olika dimensioner och aspekter i dessa behandlas. Till hjälp finns en skala med krav för olika grad av effektivitet. Genom att bedöma effektiviteten för alla rapporterade incidenter över en viss tidsperiod (med tillräckligt antal incidenter), säg ett halvår eller ett år, blir det möjligt att "mäta" en genomsnittlig effektivitet i varje steg i lärcykeln. Dessa måttetal kan användas för att bedöma om förbättringar behöver införas. De kan också vara till nytta vid jämförelser mellan olika avdelningar inom en verksamhet eller mellan verksamheter.

Metoden innehåller fyra komponenter:

- stegen i lärcykeln;
- dimensioner i varje steg;
- aspekter i varje dimension; och
- mallar med skalor för att bedöma numeriska värden på de olika dimensionerna som ett mått på effektiviteten i varje steg.

För alla stegen ingår följande fyra dimensioner (vilka används för beräkning av ett numeriskt värde), vilka i sin tur innehåller flera aspekter, som alla bör vara täckta för en fullgod behandling av en incident.

1. Omfattning (aspekterna varierar beroende på steg; se aspekterna för varje steg i tabellerna längst bak bland bilagorna);
2. Kvalitet (detaljeringsgrad och djup vid behandlingen av aspekterna under "Omfattning");
3. Tid (tid från ett steg till nästa); och
4. Information (informationsspridning i organisationen)

I tillägg till dessa fyra dimensioner innehåller metoden för flera steg ytterligare dimensioner, vilka används mer för att förklara resultatet från de fyra första dimensionerna.

### *Poängsystem*

För att kunna uttrycka effektiviteten av hanteringen av incidenter finns ett poängsystem (Se följande tabeller). De olika aspekterna för varje dimension beskrivs på ett semi-kvantitativt sätt på en skala (mellan 0 och 10) för att kunna mäta effektiviteten så objektivt som möjligt. Kraven för att uppfylla en viss poäng beskrivs genom att använda vissa ledord för fyra nivåer på 0 – 10-poängsskalan – 2 (Bristfällig), 4 (Bör förbättras), 7 (Bra) och 10 (Utmärkt).



Avsikten med den föreslagna skalan med sin beskrivande text är att leda utvärderaren i bedömningen av de individuella incidentrapporterna. I bedömningen av en incident jämförs beskrivningen och innehållet i en incidentrapport med beskrivningen för poängnivåerna i mallen, och den nivå som bäst motsvarar incidentrapportens innehåll väljs som relevant i det specifika fallet. Interpolering mellan de i mallen beskrivna nivåerna ska naturligtvis göras när så är relevant. Beskrivningen ska inte tolkas bokstavligt, men användas som en riktlinje. Efter bedömning av varje dimension i varje steg har man en uppsättning data, som kan användas för beräkning av medelvärden av effektiviteten i varje steg i lärcykeln för en specifik incidentrapport. Med ett visst antal incidentrapporter bör man kunna uttala sig om en medelnivå för effektiviteten för en verksamhet för en viss tidsperiod.

#### *Viktning av aspekterna i dimensionerna*

Metoden kan användas utan att tillskriva de olika dimensionerna någon speciell vikt. Vissa dimensioner är emellertid förmodligen viktigare för läroprocessen, särskilt dimensionerna som innehåller många aspekter, t.ex. "Omfattning" och "Kvalitet". Som ett enkelt förslag kan följande viktning användas för alla steg:

- Omfattning 35 %
- Kvalitet 35 %
- Tid 15 %
- Informationsspridning 15 %

De andra dimensionerna, t.ex. "Aktör" bör också utvärderas men bör inte ingå i beräkningen av effektivitet. Dessa andra dimensioner påverkar dock utfallet för de fyra grundläggande dimensionerna och kan därför användas för att förklara resultaten vid beräkningen av effektiviteten.

Om man önskar vara ännu noggrannare kan viktningen differentieras för olika steg, t.ex. enligt följande förslag.

#### STEG I LÄRCYKLEN

Dimension	Rapportering	Analys	Beslut	Implementering	Uppföljning
Omfattning	35	35	30	30	35
Kvalitet	35	45	30	30	35
Tid	15	10	20	20	15
Information	15	10	20	20	15

*Tabell M1:1 Förslag till viktning av olika dimensioner (uttryckta i %) i lärcykeln olika steg. I tabellen inkluderas för Besluts-steget dimensionen Grad i Omfattning och Kvalitet.*

1. RAPPORTERING				
	2 (Bristfälligt)	4 (Bör förbättras)	7 (Bra)	10 (Utmärkt)
<b>1.1 OMFATTNING</b>	Endast ett fåtal av de relevanta aspekterna (se nedan) täckta. Dåligt strukturerat.	De mest relevanta aspekterna (se nedan) täckta, men inte särskilt väl strukturerade.	Alla typer av relevanta aspekter (se nedan) täckta.	Som för 7 + ytterligare aspekter när detta kan bidra till användbarheten av rapporten.
<b>1.2 KVALITET</b>	Relevant information om många av aspekterna saknas.	Bara mest uppenbara fakta rapporterade. Svårt att göra en djup analys av orsaker etc.	Alla aspekter under omfattning täckta, men vissa aspekter inte fullt detaljerat, utan ytterligare information behövs.	Alla aspekter under omfattning täckta i detalj, vilket gör en genomgripande analys möjlig.
<b>1.3 TID</b>	> 1 vecka	Några dagar.	Samma dag/skift.	Omedelbart (timmar)
<b>1.4 INFORMATION</b>	Praktiskt taget ingen.	Individuell läsning (på intranät eller liknande).	Som för 4 + möten.	Som för 7 + riktad information till utvald personal.
<b>1.5 VEM (rapporterar)</b>	Enbart en administratör, ej direkt involverad i incidenten.	Direkt involverad person(er) + skyddsombud. Även entreprenörer täcks.	Direkt involverad person(er) + skyddsombud + arbetsledare.	Som för 7 + särskilt utbildad rapportör.
<b>1.6 TRÖSKEL FÖR RAPPORTERING (se också separat, detaljerat verktyg för detta.)</b>	Enbart olyckor som leder till allvarliga personskador och frånvaro från arbetet.	Alla personskador, större utsläpp, bränder.	Alla personskador, alla utsläpp, fallande säkerhetsutrustning, avvikelser från procedurer.	Alla "lärande-erfarenheter" inklusive mindre störningar, som kunde ha utvecklats mot allvarigare konsekvenser
<p><b>OMFATTNING</b> innehåller aspekter som följande: Beskrivning av händelsen; Arbetsituation; Stressnivå; Kompetens hos inblandade person(er); Stöd av instruktioner etc; Typ av utrustning/position inblandad; Placering; Datum och tid; Meteorologiska förhållanden; Direkt orsak och bidragande orsaker; Skador (personskador, materiella, brand, miljö, produktionsförlust); Bekämpningsinsatser; Omedelbara förbättringsförslag; Namn på rapportör.</p> <p><b>KVALITET</b> är ett mått på detaljerna i rapporteringen av de olika aspekterna under Omfattning.</p> <p><b>TID</b> är tiden från händelsen till när rapporten skrevs.</p> <p><b>INFORMATION</b> är ett mått på spridningen av information om händelsen i direkt anslutning till händelsen, speciellt till berörda anställda.</p> <p><b>VEM</b> (rapporterar) betecknar den person som faktiskt skriver rapporten.</p>				

## 2. ANALYS (OCH REKOMMENDATIONER)

	2 (Bristfälligt)	4 (Bör förbättras)	7 (Bra)	10 (Utmärkt)
<b>2.1 OMFATTNING</b>	Endast aspekter som "mänskligt fel" och "tekniskt fel" tas upp.	Tekniska aspekter i allmänhet + några organisatoriska aspekter.	Tekniska + organisatoriska aspekter rimligt väl täckta.	"Alla" aspekter väl täckta.
<b>2.2 KVALITET</b>	Analysen grund. Stoppar vid första direkta orsaken, ofta "mänskligt fel" eller "tekniskt fel". Mycket lokalt synsätt. Rekommendationerna inriktas bara på att förhindra exakt samma händelse på samma plats.	Analysen något djupare än för 2, inkluderande vissa aspekter kring procedurer och utbildning etc. Mestadels ganska lokalt synsätt.	Analysen djup beträffande direkta orsaker och också underliggande orsaker. Analysen omfattar design, procedurer, utbildning etc. Rekommendationerna är på avdelningsnivå.	Analysen djup beträffande direkta orsaker, olika underliggande orsaker, situationer etc. Analysen omfattar generell design, generella procedurer och säkerhetsledningssystem. Rekommendationerna är breda, på verksamhetsnivå, "site".
<b>2.3 TID</b>	> 1 år	3-6 månader	2-3 veckor	< 1 vecka
<b>2.4 INFORMATION</b>	Praktiskt taget ingen.	Individuell läsning (på intranät eller liknande).	Som för 4 + möten.	Som för 7 + riktad information till utvald personal.
<b>2.5 VEM (analyserar)</b>	Enbart direkt inblandad person. Mycket begränsad tid.	Arbetsledare/avdelningschef + skyddsombud, men ingen med särskild utbildning i analysmetoder. Begränsad tid.	Intern, men oberoende person, med viss utbildning i incidentanalys + assistans från personer = för 4. Rimligt med tid.	Särskilt kompetent personal med bred erfarenhet, utbildad i incidentutredningar + assistans från personer = för 7. Användning av externa specialister i vissa fall. Gott om tid att göra jobbet.
<b>OMFATTNING</b> innehåller aspekter som följande: Personliga tillkortakommanden – Tekniska tillkortakommanden – Design – Utbildning – Procedurer – Ergonomiska faktorer – Situationsfaktorer – Underhåll/inspektioner – Andra underliggande orsaker – Ledningssystem – Säkerhetskultur etc.				
<b>KVALITET</b> är ett mått på spridningen av information i organisationen om resultatet av analysen, speciellt till berörda anställda.				
<b>TID</b> är tiden från händelsen till när analysen är färdig.				
<b>INFORMATION</b> är ett mått på spridningen av information i organisationen om resultatet av analysen, speciellt till berörda anställda.				
<b>VEM (analyserar)</b> betecknar den person(er) som utför analysen inklusive resurser (personal, kompetens, tid).				

3. BESLUT				
	2 (Bristfälligt)	4 (Bör förbättras)	7 (Bra)	10 (Utmärkt)
<b>3.1 OMFATTNING</b>	Beslut begränsade till reparationer och/eller enkel ändring i procedur.	Beslut begränsade till ett fåtal aspekter, mest tekniska och/eller procedurer. Inga organisatoriska eller administrativa aspekter.	Flerfasettade aspekter beaktade.	”Alla” aspekter väl beaktade: som för 7 + <ul style="list-style-type: none"> <li>• Ledningssystem</li> <li>• Förändringar i organisation</li> <li>• Säkerhetskultur etc.</li> </ul>
<b>3.2 KVALITET</b>	Beslut ”grunda”. Enbart mindre ”kosmetiska” ändringar i procedurer eller tekniska installationer. Åtgärderna är bara för att förhindra exakt samma incident att inträffa på samma ställe.	Beslut något djupare än för 2, inkluderande några aspekter kring procedurer och utbildning etc. Mestadels ganska lokalt synsätt.	Väl underbyggda beslut baserade på slutsatserna och rekommendationerna från analyssteget. Hänsyn till underliggande orsaker. Besluten innehåller design-, procedur-, utbildningsaspekter etc. Besluten appliceras på avdelningsnivå.	Som för 7 + ytterligare beslut på högre chefsnivå beträffande ledningssystem och säkerhetskultur. Besluten är breda, på verksamhetsnivå, ”site”.
<b>3.3 GRAD (till vilken beslut följer analys och rekommendationer)</b>	Slutsatser och rekommendationer följs bara till en mycket liten grad.	Slutsatser och rekommendationer följs till en rimlig grad.	Flerfasettade slutsatser och rekommendationer följs.	Alla slutsatser och rekommendationer följs noga + utökade beslut på högre organisatorisk nivå.
<b>3.4 TID</b>	> 3 månader	1 månad	1-2 veckor	< 2 dagar
<b>3.5 INFORMATION</b>	Praktiskt taget ingen.	Individuell läsning (på intranät eller liknande).	Som för 4 + möten.	Som för 7 + riktad information till utvald personal.
<b>3.6 VEM (beslutar)</b>	Låg, otydlig nivå.	Arbetsledarnivå.	Avdelningschefsnivå	Verksamhetschefsnivå, ”site”.
<p><b>OMFATTNING</b> innehåller aspekter som följande, inklusive relevans av dem: Tekniska – Design – Utbildning – Ergonomi – Underhåll/inspektion – Andra underliggande orsaker – Ledningssystem – Säkerhetskultur etc.</p> <p><b>KVALITET</b> är ett mått på detaljerna beträffande djup och bredd i besluten kring de olika tekniska och organisatoriska aspekterna under Omfattning.</p> <p><b>TID</b> är tiden från färdig analys till beslutet är taget.</p> <p><b>INFORMATION</b> är ett mått på spridningen av information i organisationen om resultatet av besluten, speciellt till berörda anställda.</p> <p><b>VEM (beslutar)</b> betecknar de(n) person(er) eller organisatorisk nivå som de facto fattar besluten inklusive resurser (personal, kompetens, tid). Basen för utvärdering av denna punkt är ”relevant beslutsnivå” jämfört med läroptimalen för incidenten.</p>				

4. IMPLEMENTERING				
	2 (Bristfälligt)	4 (Bör förbättras)	7 (Bra)	10 (Utmärkt)
<b>4.1 OMFATTNING</b>	Endast ett fåtal beslut implementeras.	Hälften av besluten implementeras.	Nästan alla beslut implementeras.	Alla beslut implementeras fullt ut.
<b>4.2 KVALITET</b>	Låg. (t.ex. kvaliteten i procedur-, utbildnings-, underhålls-/inspektionsaktiviteter.)	Medium.	Hög.	Mycket hög.
<b>4.3 TID</b>	Lång.	Medium.	Kort.	Mycket kort.
<b>4.4 INFORMATION</b>	Praktiskt taget ingen.	Individuell läsning (på intranät eller liknande).	Som för 4 + möten.	Som för 7 + riktad information till utvald personal.
<b>4.5 VEM (implementerar)</b>	Låg, otydlig nivå.	Arbetsledarnivå.	Avdelningschefsnivå.	Verksamhetschefsnivå, "site".
<b>4.6 RESURSER</b>	Svaga, starkt begränsande implementeringen.	I viss mån begränsande implementeringen.	Bra; ej begränsande implementeringen i praktiken.	"Obegränsade"
<p><b>OMFATTNING</b> innebär här andelen av faktiskt implementerade åtgärder jämfört med beslutade åtgärder.</p> <p><b>KVALITET</b> är ett mått på detaljerna beträffande djup och bredd i faktiskt implementerade åtgärder.</p> <p><b>TID</b> är tiden från beslut till implementering. Tiden beror på typen av åtgärder som skall genomföras.</p> <p><b>INFORMATION</b> är ett mått på spridningen av information i organisationen om resultatet av implementeringen, speciellt till berörda anställda.</p> <p><b>VEM (implementerar)</b> betecknar de(n) person(er) eller organisatorisk nivå som de facto implementerar åtgärderna inklusive resurser (personal, kompetens, tid). Basen för utvärdering av denna punkt är "relevant implementeringsnivå" jämfört med läroptimalen för incidenten.</p> <p><b>RESURSER</b> är ett mått på de resurser som är tillgängliga för att genomföra de beslutade åtgärderna.</p>				

## 5. UPPFÖLJNING (KONTROLL)

	2 (Bristfälligt)	4 (Bör förbättras)	7 (Bra)	10 (Utmärkt)
<b>5.1 OMFATTNING</b>	Ingen egentlig uppföljning.	Hälften av besluten följs upp.	Nästan alla beslut följs upp.	Alla beslut följs upp.
<b>5.2 KVALITET</b>	Mycket grund uppföljning; ingen åtgärd om det finns avvikelser från intentionen i beslutet.	Viss begränsad uppföljning; begränsade åtgärder om det finns avvikelser från intentionen i beslutet.	Grundlig uppföljning; åtgärder om det finns avvikelser från intentionen i beslutet.	Mycket grundlig uppföljning; direkta åtgärder om det finns avvikelser från intentionen i beslutet.
<b>5.3 TID</b>	> 2 år	1 år	3-6 månader	2 veckor – 2 månader
<b>5.4 INFORMATION</b>	Praktiskt taget ingen.	Individuell läsning (på intranät eller liknande).	Som för 4 + möten.	Som för 7 + riktad information till utvald personal.
<b>5.5 VEM (följer upp)</b>	Ingen specifik person för uppföljning.	Respektive linjechef.	Linjechef + oberoende intern person (när relevant).	Som för 7 + högre ledning (när relevant).
<b>5.6 RESURSER</b>	Svaga, avsevärt begränsade uppföljningen.	Något så när, till viss grad begränsade uppföljningen.	Bra, ej begränsade uppföljningen i praktiken.	”Obegränsade”
<b>5.7 VERKLIGT RESULTAT (Fungerade det?)</b>	Endast i mindre grad och/eller med dålig kvalitet.	I viss grad och med rimlig kvalitet.	I hög grad och med god kvalitet.	Helt och hållet och med högsta kvalitet.
<p><b>OMFATTNING</b> innebär här andelen av aspekter som följs upp.</p> <p><b>KVALITET</b> är ett mått på detaljerna beträffande djup och bredd i uppföljningen.</p> <p><b>TID</b> är tiden från implementering till uppföljning. Tiden beror på typen av åtgärder som skall genomföras.</p> <p><b>INFORMATION</b> är ett mått på spridningen av information i organisationen om resultatet av uppföljningen, speciellt till berörda anställda.</p> <p><b>VEM (följer upp)</b> betecknar de(n) person (er) eller organisatorisk nivå som de facto följer upp inklusive resurser (personal, kompetens, tid). Basen för utvärdering av denna punkt är ”relevant uppföljningsnivå” jämfört med läropten-tialen för incidenten.</p> <p><b>RESURSER</b> är ett mått på de resurser som är tillgängliga för att genomföra uppföljningen.</p> <p><b>VERKLIGT RESULTAT (Fungerade det?)</b> är ett mått på hur väl de implementerade åtgärderna fungerar i förhållande till intentionen.</p>				

## 6. 2:A LOOPEN PÅ AGGREGERADE INCIDENTER

	2 (Bristfälligt)	4 (Bör förbättras)	7 (Bra)	10 (Utmärkt)
<b>6.1 Omfattning</b>	Endast mycket begränsad statistik och trender kring <ul style="list-style-type: none"> <li>• Typer av händelser</li> <li>• Direkta orsaker</li> </ul>	Viss statistik och trender kring <ul style="list-style-type: none"> <li>• Typer av händelser</li> <li>• Direkta orsaker</li> <li>• Genomförda åtgärder</li> </ul>	Statistik och trender kring <ul style="list-style-type: none"> <li>• Typer av händelser</li> <li>• Direkta orsaker</li> <li>• Genomförda åtgärder</li> <li>• Grad av framgång</li> </ul>	Som för 7 + fokus på gemensamma orsaker, organisatoriska frågor.
<b>6.2 Kvalitet</b>	Endast mycket begränsad analys av underliggande orsaker; mycket begränsade åtgärder.	Viss analys av underliggande orsaker och med rimliga åtgärder i anslutning till resultatet.	Djup analys av underliggande orsaker, inkluderande vissa aspekter i säkerhetsledningssystem och med relevanta åtgärder i anslutning till resultatet.	Som för 7 + analys av effekten på säkerhetsledningssystem och säkerhetskultur + kraftfullt agerande från högsta ledningen om implementerade åtgärder inte varit framgångsrika.
<b>6.3 Tid (från incident till uppföljning/utvärdering)</b>	Sällan och godtyckligt.	Ibland, men inte schemalagd utvärdering av aggregerade resultat; ett år efter speciella händelser.	En gång per år för utvärdering av aggregerade resultat och 3 månader efter speciella händelser.	4 gånger per år för utvärdering av aggregerade resultat och 1-2 månader efter speciella händelser.
<b>6.4 Information</b>	Praktiskt taget ingen.	Individuell läsning (på intranät eller liknande).	Som för 4 + möten.	Som för 7 + riktad information till utvald personal.
<b>6.5 Vem (organisatorisk nivå)</b>	Ingen specifik person för denna aktivitet.	Viss utvärdering görs av skyddscommitte.	Högsta ledningen + intern specialist.	Som för 7 + oberoende extern specialist.

## Metod 2. Bedömning av lärandenivå

Slutprodukten av hanteringen av en incident är ju själva läxan, som också skall överföras i lärdom. Denna kan vara mer eller mindre omfattande och kvalitetsmässigt bra. Här följer en utförligare beskrivning av en metod som i sex steg utvärderar lärandet från incidenter baserat på begreppet lärandenivå.

Metoden innehåller följande steg

1. Utvärdering av *verklig* lärandenivå hos rapporterade incidenter
2. Utvärdering av *potentiell* lärandenivå hos rapporterade incidenter
3. *Jämförelse* av verklig och potentiell lärandenivå
4. *Korrektion* av resultaten i steg 1 – 3 för mörkertal, dvs. incidenter som ej rapporterats
5. Hänsyn till lärande från behandling av incidenter på en aggregerad nivå – här kallad *2:a loopen*.
6. Hänsyn till andra mekanismer för lärande från incidenter

Denna metod är tänkt att användas på alla rapporterade incidenter under en viss tidsperiod för att kunna bedöma fördelningen av lärandenivåer och att bilda medelvärden och göra jämförelser.

### Steg 1: Verkligt lärande

Det första steget innebär att klassificera lärdomen i rapporterade incidenter enligt ett system som baseras på

- primärt, hur brett lärdomen appliceras geografiskt i verksamheten (från mycket lokalt där incidenten inträffade till över hela "siten", där liknande förhållanden råder),
- sekundärt, hur mycket organisatoriskt lärande som är inblandat (tekniska, procedurmässiga och personalmässiga åtgärder)
- tertiärt, hur mycket organisatoriskt långtidsminne som är inblandat.

Det finns inga skarpa gränser mellan de tre aspekterna; viss överlappning mellan den geografiska aspekten och de andra två aspekterna förekommer.

Nedan visas ett system (Tabell M2:1) för klassificering av lärande från incidenter baserat på lärandenivåer. Det baseras på de lärdomar (läxor) som genomförs. Systemet har tagits fram för att passa den normala stora mängden av incidenter som rapporteras i många verksamheter. Exempelen är hämtade från processindustrin.



Nivå	Karakteristika	Beskrivning	Exempel
<b>0</b>	Inget lärande.	Inget egentligt lärande.	Endast reparation av fallerande utrustning eller acceptans av "mänskligt fel".
<b>I</b>	<i>Primärt:</i> Begränsat lokalt lärande.  <i>Tillägg:</i> Nästan inget organisatoriskt lärande; Korttidsminne.	Lärande enbart på mycket lokal nivå, bara på den speciella plats i anläggningen där incidenten inträffade. På sin höjd begränsad dokumentation. Begränsat organisatoriskt lärande. Företrädesvis endast korttids organisatoriskt minne.	Diskussioner inom ett skift och möjligen anteckningar i loggbok.
<b>II</b>	<i>Primärt:</i> Lokalt lärande.  <i>Tillägg:</i> Begränsat organisatoriskt lärande; Huvudsakligen långtidsminne.	Lärandet på lokal nivå, något bredare än I, men fortfarande begränsat till den specifika plats i anläggningen där incidenten inträffade. Normalt dokumenterad. En del organisatoriskt lärande. Normalt långtids organisatoriskt minne.	Förändringar i en specifik procedur med dokumentation, och viss information/utbildning, eller byte av material i specifik utrustning.
<b>III</b>	<i>Primärt:</i> Lärande på processenhetsnivå.  <i>Tillägg:</i> Substantiellt organisatoriskt lärande; Långtidsminne.	Lärande på processenhetsnivå (undantagsvis site-nivå). Lärdomarna appliceras på andra, liknande platser/system eller procedurer i en processenhet. Dokumenterat. Organisatoriskt lärande. Långtids organisatoriskt minne.	Utbyte av alla pumpar av en specifik typ, eller förändring av procedurer och utbildning för provtagning generellt.
<b>IV</b>	<i>Primärt:</i> Lärande på site-nivå.  <i>Tillägg:</i> Substantiellt organisatoriskt lärande; Långtidsminne.	Lärande på en typisk site-nivå. Lärdomarna appliceras på andra, liknande platser/system över hela siten, inkluderande generiska läxor generellt och SHM-ledningssystem och normer (policy, mål, specifikationer etc.). Dokumenterat. Organisatoriskt lärande. Långtids organisatoriskt minne.	Väsentliga förändringar i konstruktionsspecifikationer, arbetsprocedurer, utbildningsprogram.
<b>V</b>	<i>Primärt:</i> Högre lärande: Koncernlärande; Långtidsminne.	Lärande på högre nivå (koncernnivå). Lärdomarna uppmärksammas i koncernens högsta ledning och fundamental omvärdering av SHM-aktiviteter äger rum. Dokumenterat. Organisatoriskt lärande. Långtids organisatoriskt minne.	Fundamentala ändringar i koncernens SHM-policy.

Tabell M2:1

Resultatet av steg 1 är en procentuell fördelning av incidenterna på de olika klasserna. Ur detta kan en hel del slutsatser dras om hur väl lärandet fungerar. För att gå vidare i metoden kan också ett ”medelvärde” beräknas. Eftersom vi har använt en ordinal-skala är medelvärdet inte helt strikt ett aritmetiskt medelvärde, vilket dock i sammanhanget torde spela mindre roll.

### **Steg 2: Potentiellt lärande**

För att bedöma effektiviteten i lärandet bättre än bara genom att utvärdera det verkliga lärandet enligt steg 1 bör det verkliga lärandet jämföras med lärandet som hade kunnat uppnås om den fulla lärpotentialen i incidenterna hade utnyttjats. Givetvis innehåller inte alla incidenter lärdomar på en hög lärandenivå. Vissa motiverar åtgärder endast på en lägre nivå – en lokal teknisk åtgärd eller begränsad procedurmässig eller organisatorisk åtgärd – eller ingen åtgärd alls. De flesta incidenter innehåller emellertid en potential för högre lärande. Vi antar här att om man kan klarlägga orsaksbilden kring en incident fullt ut, bör man kunna utvärdera de potentiella lärdomarna som kan utvinnas ur incidenten. En fullständig grundorsaksanalys är mycket tidskrävande. Därför är nästa steg i metoden att med hjälp av ett verktyg, som är snabbt och effektivt att använda, utvärdera de mest sannolika direkta och bidragande orsakerna till incidenterna. Verktyget ska bidra till att klarlägga orsaksbilden ytterligare utöver de orsaker som redan finns angivna i incidentrapporterna. Verktyget är baserat på att verksamheter kan beskrivas som socio-tekniska system med olika hierarkiska nivåer. Exemplet nedan visar lämpliga nivåer, som kan tillämpas på många typer av verksamheter.

- Högsta ledningen, företagsledning (typiskt site-ledning)
- Andra påverkande nivåer (typiskt stabs- och stödfunktioner)
- Arbetsledning på högre nivåer (typiskt fabriksenhet/middle management)
- Arbetsledning på utförandenivå (typiskt 1:a linjens arbetsledare)
- Direkt utförandenivå (typiskt operatörer)
- Process/Utrustning

Verktyget presenteras i följande tabell.

Analysnivå	Avdelning/ organisation	Direkta orsaker	Underliggande orsaker (svagheter i säkerhetskulturen)
5. Toppnivå	Företagsledning	Otillräcklig granskning av system och säkerhetsresultat i organisationen; Behov för utbildning/kompetens inses och uppskattas inte; Oförenliga mål och felaktiga prioriteter ges till lägre organisatoriska nivåer; Dålig kommunikation av säkerhetsprioriteringar; Ansvar och befogenheter oklara; Svaga val av chefer; Otillräckliga procedurer för riskanalys; Otillräckliga system för utformning och konstruktion enligt goda tekniska standarder, applicering av inherent-safety.	Otillräckligt eller svagheter i säkerhetsledningssystemet; svagheter i säkerhetskulturen. Dåligt säkerhetsengagemang och ledarskap i företaget eller koncernen. Allmänt undermåligt tänkande för säkerhet.
	Andra (om tillämpliga)	(Att utveckla)	(Att utveckla)
4. Andra påverkande nivåer (stöd-funktioner etc.)	Teknisk avdelning	Design otillräcklig; Riskanalyser otillräckliga.	Otillräckliga system för utformning och konstruktion enligt goda tekniska standarder, applicering av inherent-safety; Otillräckliga rutiner för riskanalys; Otillräckliga resurser/kompetens.
	Inköpsavdelning	Inspektion otillräcklig; Inköpsrutiner otillräckliga.	Otillräcklig granskning av system och säkerhetsresultat i organisationen.
	Andra (om tillämpliga)	(Att utveckla)	(Att utveckla)
3. Arbetsledning på högre nivå (ofta linjechefer)	Drift	Arbetsledning/övervakning/kontroll av system och organisation otillräcklig; Otillräckliga driftprocedurer; Otillräcklig kompetens och utbildning förmedlas; Otillräckliga resurser; Riskanalyser otillräckliga; Chefer "bryr sig inte" eller visar inte att de gör det.	Svaga resurser och kompetens; Otillräckligt engagemang (från högre ledningsnivå); Otillräcklig översyn och kontroll av högre ledningsnivå; Ingen tid för relevant utbildning. Otillräckligt riskmedvetande; Behov för utbildning/kompetens inses och uppskattas inte; Ingen systematisk rutin för riskanalys.
	Underhåll	Arbetsledning/övervakning/kontroll av system och organisation otillräcklig; Underhåll/inspektions-program otillräckliga; Otillräcklig kompetens och utbildning förmedlas; Otillräckliga resurser; Chefer "bryr sig inte" eller visar inte att de gör det.	Otillräcklig insikt om behovet av underhållsprogram eller medvetet åsidosättande; Otillräckligt engagemang (från högre ledningsnivå); Otillräcklig översyn och kontroll av högre ledningsnivå; Otillräcklig riskanalys; Procedurer endast för tillfredsställelse av systemet; Behov för utbildning/kompetens inses och uppskattas inte;
	Andra (om tillämpliga)	(Att utveckla)	(Att utveckla)

Tabell M2:2 Verktyg för orsaksanalys av incidenter, exempel på orsaker. (fortsätter på s. 68)

2. Arbetsledning på utförande- nivå	Drift	Övervakning/kontroll vid utförande otillräcklig; Bemanning otillräcklig; Otillräcklig utbildning av operatörs-personal; Andra prioriteringar högre än säkerhet; Attityder hos individer bristfälliga; Arbetsledare "bryr sig inte" eller visar inte att de gör det.	Otillräckligt engagemang (från högre ledningsnivå); Otillräckliga resurser; Behov för utbildning/kompetens inses och uppskattas inte; Ingen tid för relevant utbildning; Otillräcklig översyn och kontroll av system och säkerhetsprestanda.
	Underhåll	Underhålls/inspektionsprogram följs inte; Arbetsledning/kontroll av utförande otillräcklig; Utbildning av underhållspersonal otillräcklig; Otillräckliga underhållsprocedurer; Andra prioriteringar högre än säkerhet; Attityder hos individer bristfälliga; Arbetsledare "bryr sig inte" eller visar inte att de gör det.	Otillräckligt engagemang (från högre ledningsnivå); Otillräckliga resurser; Behov för utbildning/kompetens inses och uppskattas inte; Ingen tid för relevant utbildning; Otillräcklig översyn och kontroll av system och säkerhetsprestanda.
	Andra (om tillämpliga)	(Att utveckla)	(Att utveckla)
1. Direkt utförande nivå ("Sharp-end operators")	Drift (operatör)	Drift utanför designförhållanden; Procedurer följs ej; Direkt operatörsfel; Tillkortakommande hos individer; Otillräcklig kompetens; Attityder hos individer bristfälliga.	Procedurer otillräckliga; Utbildning otillräcklig; Otillräcklig arbetsledning och kontroll; Bemanning otillräcklig; Andra prioriteter än säkerhet; Situationsfaktorer: Hög arbetsbelastning, stress eller andra försvärande faktorer.
	Underhåll (tekniker)	Procedurer följs ej; Direkt teknikerfel; Tillkortakommande hos individer; Otillräcklig kompetens; Attityder hos individer bristfälliga.	Procedurer otillräckliga; Utbildning otillräcklig; Otillräcklig arbetsledning och kontroll; Bemanning otillräcklig; Andra prioriteter än säkerhet; Situationsfaktorer: Hög arbetsbelastning, stress eller andra försvärande faktorer.
	Entreprenörer (tekniker)	Procedurer följs ej; Direkt teknikerfel; Tillkortakommande hos individer; Otillräcklig kompetens; Attityder hos individer bristfälliga.	Procedurer otillräckliga; Utbildning otillräcklig; Otillräcklig arbetsledning och kontroll; Bemanning otillräcklig; Andra prioriteter än säkerhet; Situationsfaktorer: Hög arbetsbelastning, stress eller andra försvärande faktorer.
	Andra (om tillämpliga)	(Att utveckla)	(Att utveckla)
0. Process/ Utrustning		Fallerande processkär/containern/annan utrustning; Felfungerande komponent/maskin; Förlust av processkontroll; Fallerande instrument-/kontroll-/övervakningsutrustning.	Tillverkningsfel; Korrosion/erosion/utmattning; Otillräckliga eller ej följda underhålls-/inspektionsprogram; Drift utanför designförhållanden.

Genom att applicera detta verktyg på alla incidentrapporter för en viss tid kan man få fram de troliga bidragande orsakerna och därmed de lärdomar som hade kunnat utvinnas ur incidenterna. När detta väl är gjort kan man på nytt använda verktyget i tabell M2:1 för att bedöma vilken lärandenivå som hade varit möjlig att uppnå om man utnyttjat hela potentialen i incidenterna.

Resultatet av steg 2 är en ny uppsättning siffror som anger fördelningen av potentiellt lärande från rapporterade incidenter. Även här kan ett "medelvärde" för potentiellt lärande beräknas.

### **Steg 3: Jämförelse mellan verklig och potentiell lärandenivå**

Med de två uppsättningarna av värden för verkligt lärande och potentiellt lärande från steg 1 och steg 2 kan man göra jämförelser och dra slutsatser om effektiviteten i lärandet. Siffrorna fördelade på klasser kan jämföras och kvoten av "medelvärdena" kan beräknas som ett enkelt mått på effektiviteten. Här bör slutsatser om hur effektivt lärandet är i verkligheten kunna dras och eventuella förbättringsåtgärder övervägas.

### **Steg 4: Korrektion för mörkertal, dvs ej rapporterade incidenter**

Resultatet efter steg 3 är emellertid inte hela bilden av hur lärandet fungerar. Vi bör ta hänsyn till att ett visst antal incidenter inträffar men inte rapporteras, vilket alltså innebär att vi missar en del lärdomar. Man kan nöja sig med att behandla denna fråga övergripande som en egen företeelse eller också att gå vidare i metoden och introducera en "matematisk" korrektion för mörkertalet.

Varje verksamhet är själv bäst lämpad att göra en bedömning av hur stort mörkertal man har. Här fortsätter vi metoden med att anta att det i många verksamheter är rimligt att anta att det förekommer 3 rapportervärda incidenter per anställd per år. Vidare måste man göra ett antagande om vad lärandenivån för dessa ej rapporterade incidenter är.

När man korrigerar resultaten från steg 1 och steg 2 för mörkertalet måste dessa ej rapporterade incidenter åsättas ett visst värde beträffande lärandenivå. För *verkligt* lärande antas dessa ha 0-nivå. När det gäller *potentiellt* lärande antas de ej rapporterade incidenterna ha en något lägre lärandenivå i snitt än de som faktiskt rapporteras. Ett rimligt antagande kan vara en genomsnittlig lärandenivå på 1.7 med fördelningen 50 % på nivå I, 30 % på nivå II och 20 % på nivå III. På detta sätt kan man fortsätta en beräkningsmässig behandling av utvärderingen av lärandenivåer. Visserligen ökar osäkerheten i själva siffrorna, men det kan ändå ha ett värde att se hur mycket lärandenivån påverkas om mörkertalet tas med i bilden. Siffervärdena kan ha en fördel om man vill göra jämförelser mellan olika avdelningar i en verksamhet eller mellan verksamheter.

### **Steg 5: Hänsyn till lärande från incidenter på en aggregerad nivå – 2:a loopen**

Så här långt har vi bara tagit hänsyn till lärandet från individuella incidenter. Som nämnts tidigare i del 1 av handledningen under "Element och innehåll i ett system för rapportering och hantering av incidenter" bör det ingå i ett system för incidenthantering att regelbundet göra en utvärdering av ett samlat material för att om möjligt lära mer genom att se mönster, trender, gemensamma nämnare etc.

Förekomsten av en sådan aktivitet bör naturligtvis påverka bedömningen av lärandenivån, förutsatt att en sådan behandling väsentligen ökar lärandenivån. Samma verktyg som utvecklats för att bedöma effektiviteten i 2:a loopen under rubriken "Läracykeln" kan vara ett hjälpmedel här (se **Metod 1**, steg 6). En bra behandling av incidenterna i 2:a loopen kan delvis kompensera för ett sämre utfall av lärandenivå baserat på bedömning av de individuella incidenterna enligt steg 1 ovan.

#### **Steg 6: Hänsyn till andra mekanismer för lärande från incidenter**

Som ett sista steg i metoden ingår att ta hänsyn till eventuella andra sätt att lära från incidenter än genom incidenthanteringssystemet. Det är inte ovanligt att andra funktioner än de som normalt hanterar incidenthanteringssystemet också är aktiva när det gäller incidenter. Säkerhetskommittén eller en motsvarande grupp tar ibland på sig denna roll särskilt för allvarigare incidenter. Om denna grupp hanterar och fattar beslut som går vid sidan av det normala systemet för incidenthantering måste givetvis hänsyn tas till detta i en utvärdering av lärandenivå. Också eventuella andra sätt att hantera incidenter bör tas hänsyn till. Så kan ibland vissa tekniska incidenter passera förbi det formella systemet för incidenthantering och gå direkt via verksamhetens underhållssystem.

## Metod 3. Bedömning av tröskel för rapportering

Nedanstående tabell är utvecklad för att passa i en processindustri, men det mesta av innehållet är generellt och den bör lätt kunna anpassas till i stort sett alla verksamheter.

Idén är att tröskeln för rapportering kan bedömas genom att utvärdera ett stort antal incidentrapporter och se vilken lägsta nivå på tröskeln som fortfarande ger rapporter.

En rapporterad incident av någon av typerna 1-5, får en "poäng" som närmast motsvarar beskrivningen i tabellen (med möjlighet att interpolera). Exempelvis får en rapport om en avvikelse från en driftinstruktion, där avvikelsen i sig betraktas som liten, men där närvaron av ytterligare två omständigheter (t.ex. fallerande säkerhetsbarriärer) kunde ha lett till en olycka (med t.ex. personskada, utsläpp, brand, miljöpåverkan eller kostnad) en poäng = 7.

För typ 3, 4 och 5 behövs en viss ingenjörsmässig bedömning av personen som använder verktyget att bedöma möjligheterna för eskalering av den rapporterade händelsen till allvarigare konsekvenser. För att avgöra var tröskeln ligger bör ett visst minsta antal incidenter ligga där; endast någon eller några enstaka händelser kan inte anses vara tillräckligt. Tröskelvärdet kan vara en signifikant information om organisationens ambitionsnivå att lära från incidenter. Ju lägre tröskel, desto högre poäng och desto bättre är rapporteringen och sannolikt möjligheterna för lärande.

Den aktuella nivån som verktyget förmedlar kan också jämföras med definitionen som verksamheten har för vad som är en rapportierbar händelse.

## POÄNG

	2	4	7	10
<b>TYP AV HÄNDELSE</b> (Konsekvens eller effekt)				
1. Personskada (verklig)	Större personskada, normalt sjukhusvård	LTI (Lost Time Incident) = frånvaro från arbetet 1 dag eller mer.	Enkel medicinsk behandling, 1:a hjälpen.	
2. Utsläpp, "Loss of containment" (LOC) av farlig substans, brand etc (verklig).	Större utsläpp. Större brand. Större miljöpåverkan och/eller ekonomisk förlust.	Mindre utsläpp. Mindre brand. Mindre miljöpåverkan och/eller ekonomisk förlust.	Utsläpp, som skulle ha kunnat utvecklas till brand, miljöpåverkan och/eller ekonomisk förlust, om ytterligare 1 barriär fallerat.	Utsläpp, som skulle ha kunnat utvecklas till brand, miljöpåverkan och/eller ekonomisk förlust, om ytterligare 2 barriärer fallerat.
3. Händelsen + en eller flera omständigheter kunde ha lett till...	Ej tillämpligt på denna typ av händelse.	Händelsen + 1 ytterligare omständighet kunde ha lett till en allvarlig olycka (större personskada, större utsläpp, större brand, större miljöpåverkan och/eller ekonomisk förlust).	Händelsen + 2 ytterligare omständigheter kunde ha lett till en olycka (personskada, utsläpp, brand, miljöpåverkan och/eller ekonomisk förlust).	Händelsen + 3 ytterligare omständigheter kunde ha lett till en olycka (personskada, utsläpp, brand, miljöpåverkan och/eller ekonomisk förlust).
4. Avvikelse från procedurer (utan olycka)	Ej tillämpligt på denna typ av händelse.	Större avvikelse från procedur + 1 ytterligare omständighet kunde ha lett till en allvarlig olycka (större personskada, större utsläpp, större brand, större miljöpåverkan och/eller ekonomisk förlust).	Mindre avvikelse från procedur + 2 ytterligare omständigheter kunde ha lett till en olycka (personskada, utsläpp, brand, miljöpåverkan och/eller ekonomisk förlust).	Mindre avvikelse från procedur + 3 ytterligare omständigheter kunde ha lett till en olycka (personskada, utsläpp, brand, miljöpåverkan och/eller ekonomisk förlust).
5. Andra avvikelser (utan verklig olycka), som fallande säkerhetsutrustning, kommunikationssystem etc.	Ej tillämpligt på denna typ av händelse.	Avvikelsen + 1 ytterligare omständighet kunde ha lett till en allvarlig olycka (större personskada, större utsläpp, större brand, större miljöpåverkan och/eller ekonomisk förlust).	Avvikelsen + 2 ytterligare omständigheter kunde ha lett till en olycka (personskada, utsläpp, brand, miljöpåverkan och/eller ekonomisk förlust).	Avvikelsen + 3 ytterligare omständigheter kunde ha lett till en olycka (personskada, utsläpp, brand, miljöpåverkan och/eller ekonomisk förlust).

Tabell M3:1



## Checklista 1. Viktiga påverkansfaktorer, allmänt och för lärcykeln olika steg

Följande sammanställning av faktorer är tänkt att dels

- allmänt belysa och öka förståelsen för vad som kan tänkas påverka effektiviteten i lärandet från incidenter, generellt och i lärcykeln olika steg; och dels
- utgöra en checklista för att finna möjliga områden och detaljer att fokusera på, när behov för förbättringar i lärande från incidenter konstaterats.

### Allmänna faktorer

- En god säkerhetskultur, präglad av tillit, förtroende, öppenhet och en icke-straffande attityd är en absolut förutsättning för ett gott lärande från incidenter.
- Ledningens uttalade stöd och engagemang för processen och systemet för lärande från incidenter behövs.
- Incidenthanteringssystemet bör vara enkelt; framför allt skall rapporteringen av en incident vara enkel för rapportören.
- Resurser och kompetens behövs i varje steg i lärcykeln (Rapportering – Analys – Beslut – Implementering – Uppföljning).
- Alla rapporterade incidenter behöver i varje steg i lärcykeln en ägare, en lärandeagent, som skall se till att aktiviteten blir ordentligt utförd och att lärdomarna kommer in på alla relevanta ställen i verksamhetens minne.
- Det behövs en mekanism som säkerställer att alla åtgärder som erfordras i ett steg verkligen vidtagits, innan man släpper ärendet vidare till nästa steg.
- Alla som berörs av incidenten skall erhålla information om den, från det att den hänt till beslut och genomförande av åtgärder.
- En effektiv 2:a loop i lärcykeln, dvs. en regelbunden genomgång av ett samlat material av incidenter är nödvändig.
- Utbildning av alla i organisationen i att tänka i olycksmodell främjar rapporteringen och dess kvalitet.

### Faktorer för enskilda steg

#### Rapportering

Vi söker rapportering av "alla rapportervärda" incidenter på ett sådant sätt att de kan utredas/analyseras vidare för att kunna utvinna maximalt med lärande för individ och organisation. Frågan om vem eller vilka som skall rapportera är viktig. Vi utgår här från att det normalt är de personer som är direkt inblandade i incidenten ("1:a linjens aktörer"), ibland i samarbete med arbetsledare och/eller skyddsombud.

*Påverkansfaktorer:*

- "1:a linjens aktörers"/rapportörernas utbildning för att rapportera – ju bättre utbildning desto bättre rapporter och underlag för bra lärande.
- "1:a linjens aktörers" förståelse för ett organisatoriskt lärande – ju bättre förståelse desto bättre förutsättningar för bra lärande.
- Gemensam uppfattning i organisationen om tröskeln för "rapporterbarhet" och lärandepotential – ju mer samsyn desto bättre underlag för bra lärande.
- Snabbhet – ju snabbare rapportering desto bättre underlag för bra lärande (med viss risk för sämre kvalitet vid alltför snabb rapportering).
- Rapporteringssystemets utformning, omfattning och formalia – ju enklare och informellare desto större rapporteringsvilja (med risk för bristande information om alltför enkelt). Formulär bör vara utformade så att de hjälper rapportören i att komma med god information om händelsen, och även förslag till förbättringar.
- Möjligheter till tilläggsinformation – utrymme för tilläggsinformation ger större möjligheter till bättre lärande.
- Förväntningarna hos rapportören om hur rapporteringen förvaltas – ju bättre och snabbare återföring och meningsfulla åtgärder desto större rapporteringsvilja.

**Analys/utredning**

Vi letar efter de grundläggande orsakerna hos de rapporterade händelserna, de som kan ge oss idéer för ett aktivt individuellt och organisatoriskt lärande, framför allt generiska underliggande orsaker som kan vara utgångspunkt i ett organisatoriskt lärande. Utredaren bör alltid ställa sig följande frågor (formell punkt i rutinen) för att ge perspektiv på analysen:

- Var mer kan vi ha liknande förhållanden som kan generera liknande problem? Om sådana finns, påpeka dessa och uppmärksamma ansvariga eller agera själv på dessa.
- Vem mer i organisationen kan ha anledning att uppmärksamma liknande frågeställningar?

*Påverkansfaktorer:*

- Utredarens intresse – ju mer engagerad och intresserad desto bättre möjligheter för bra lärande.
- Utredarens kompetens (multidisciplinär kunskap) – ju större kompetens desto bättre möjligheter för bra lärande.
- Utredarens resurser, främst tid – ju större resurser desto bättre möjligheter för bra lärande.
- Utredarens objektivitet inför den inträffade incidenten och dess orsaker – ju mera fristående från personligt ansvar i frågan, desto bättre möjligheter för bra lärande. Att peka ut svagheter inom det egna ansvarsområdet är alltid svårare.

- Underlaget för analys, dvs rapporteringen – ju bättre underlag desto bättre möjligheter för bra lärande.
- Tillgång till analysmodeller – ju bättre tillgång till hjälpmedel desto bättre möjligheter för bra lärande.
- Analysmodellernas enkelhet, effektivitet mm – ju enklare och effektivare desto bättre möjligheter för bra lärande. Tidskrävande metoder kan hämma användningen.
- Förväntningarna hos utredaren om hur ärendet förvaltas – ju högre förväntningar desto bättre utredning och möjligheter för bra lärande.
- Snabbhet – ju snabbare utredning desto bättre genomslag och förtroende och vidare möjligheter för bra lärande (med viss risk för sämre kvalitet vid alltför snabb utredning).
- Möjligheter till informationsspridning – ju enklare, naturligare och effektivare fora för informationsspridning desto bättre möjligheter för bra lärande.

### **Beslut**

Vi strävar efter beslut som innehåller bredd och djup så långt man kan nå i organisatoriskt lärande.

#### *Påverkansfaktorer:*

Beslutsfattarens organisatoriska ställning (för att t.ex. kunna se behovet och nyttan av och mandat att kunna fatta beslut om generella åtgärder) – ju högre ställning (inom vissa gränser) desto större möjligheter för bra lärande.

- Beslutsfattarens intresse – ju mer engagerad och intresserad desto bättre möjligheter för bra lärande.
- Beslutsfattarens kompetens (multidisciplinär kunskap) – ju bättre kompetens desto bättre möjligheter för bra lärande.
- Beslutsfattarens resurser, främst tid – ju större resurser desto bättre möjligheter för bra lärande.
- Tillgången på lämpliga och effektiva beslutsfora – ju bättre tillgång desto bättre möjligheter för bra lärande.
- Snabbhet – ju snabbare beslutsfattande desto bättre genomslag och förtroende och vidare möjligheter för bra lärande.
- Kvalitet på underlag för beslut, d.v.s. analys – ju bättre kvalitet desto bättre beslut för bra lärande.
- Möjligheter till informationsspridning – ju enklare, naturligare och effektivare fora för informationsspridning desto bättre möjligheter för bra lärande.

### **Implementering**

Vi vill se en snabb, effektiv och fullständig implementering av fattade beslut.

*Påverkansfaktorer:*

- Tillgången på lämpliga och effektiva implementeringsprocesser – ju effektivare desto bättre möjligheter för bra lärande. Avser implementering som
  - Uppdatering av instruktioner
  - Uppdatering av konstruktionsregler
  - Uppdatering av system för förebyggande underhåll och inspektioner
  - Uppdatering av ledningssystem
  - Uppdatering av ansvarsförhållanden
  - Genomförande av utbildning
- Tillgången på resurser (personella, ekonomiska mm.) – ju större resurser desto bättre möjligheter för bra lärande.
- Organisationens vilja, förmåga och kraft att genomföra fattade beslut – ju större vilja, förmåga och kraft desto bättre implementering för bra lärande.

**Uppföljning**

Vi vill säkerställa att besluten efter implementeringen lever vidare på ett avsett sätt och inte urholkas på längre sikt.

*Påverkansfaktorer:*

- Effektiviteten i uppföljningsprocessen – ju effektivare desto bättre möjligheter för bra lärande på sikt.
- Resurser (personella, tid och andra resurser) på både hög och låg nivå – ju mer resurser desto större möjligheter för bra lärande på sikt.

**2:a loopen**

Vi vill här se en aktivitet, som genomförs regelbundet, och som genom att sammanställa och göra statistik på ett aggregerat antal incidenter, kunna fördjupa lärandet från incidenter. Framför allt kan man genom trendanalyser, analyser av olyckstyper, djupanalys av orsaker och kvalitetsgranskning av hanteringen av de separata incidenterna förbättra lärandet från incidenter.

*Påverkansfaktorer:*

- Innehåll och process i 2:a loopen – ju bättre innehåll och effektivare process desto bättre möjligheter för bra lärande.
- Resurser (personella, tid och andra resurser) – ju mer resurser desto större möjligheter för bra lärande på sikt.
- Kompetens hos deltagare (multidisciplinär kunskap) – ju större kompetens desto bättre möjligheter för bra lärande.
- Insikt, vilja, förmåga etc. hos ledningen att engagera sig i resultatet av 2:a loopen – ju större engagemang desto större möjligheter för bra lärande.

## Checklista 2. Viktiga element/innehåll i ett incidenthanteringssystem

För att lära från incidenter måste hanteringen i själva incidenthanteringssystemet vara baserad på god information, avseende såväl omfattning som kvalitet och detaljeringsgrad i alla stegen i lärcykeln. Följande sammanställning visar för varje steg i lärcykeln vilka dimensioner som kan vara aktuella att fylla med innehåll (olika aspekter), samt exempel på en del av dessa aspekter. Sammanställningen kan användas som en utgångspunkt vid konstruktion av eller kontroll av innehållet i incidenthanteringssystem. Sammanställningen har också använts som utgångspunkt för konstruktion av verktyget för utvärdering av effektiviteten i lärandeprocessen, **Metod 1**.

### Rapportering

- a. **Omfattning**  
Beskrivning av händelsen; Arbetsituation; Stressnivå; Kompetens hos inblandade person(er); Stöd genom instruktioner etc; Typ av utrustning/enhet; Lokalisering; Datum och tid; Meteorologiska förhållanden; Direkt orsak och bidragande orsaker; Skador (personskador, materiella, brand, miljöskada, produktionsförlust); Bekämpningsinsatser; Omedelbara förslag; Namn på rapportör(er).
- b. **Kvalitet**  
Kvalitet och detaljeringsgrad i de olika aspekterna under "Omfattning"
- c. **Tidsaspekt**  
Tiden från händelsen till färdig rapport
- d. **Informationsspridning**  
Spridning av information om incidenten i direkt anslutning till händelsen, speciellt till berörda anställda
- e. **Rapportör**  
Rapportörens ställning, kompetens mm.

### Analys (främst orsaksanalys)

- a. **Omfattning**  
Mänskliga tillkortakommanden; Tekniska svagheter; Design; Utbildning; Procedurer; Ergonomiska faktorer; Situationsfaktorer; Underhåll/inspektion; Andra underliggande orsaker och brister i barriärer; Ledningssystem; Säkerhetskultur etc.
- b. **Kvalitet**  
Kvalitet, detaljeringsgrad och djup av analysen av de olika tekniska och organisatoriska aspekterna under "Omfattning".

- c. **Tidsaspekt**  
Tiden från händelsen till färdig analys.
- d. **Informationsspridning**  
Spridning av information om resultatet av analysen av händelsen, speciellt till berörda anställda.
- e. **Analytiker**  
Resurser, Analytikerns ställning, kompetens mm.

## Beslut om åtgärd

- a. **Omfattning**  
Tekniskt; Design; Utbildning; Ergonomi; Underhåll/inspektion; Administrativa rutiner; Andra underliggande orsaker; Ledningssystem; Säkerhetskultur etc., inklusive relevans av aspekt. Även i vilken omfattning beslut följer rekommendationerna i analysen.
- b. **Kvalitet**  
Kvalitet, detaljeringsgrad och djup av besluten beträffande de olika tekniska och administrativa/organisatoriska aspekterna under "Omfattning".
- c. **Tidsaspekt**  
Tiden från färdig analys till beslut.
- d. **Informationsspridning**  
Spridning av information om resultaten av besluten, speciellt till berörda anställda.
- e. **Beslutsfattarnivå**  
Organisatorisk nivå för beslut, inkluderande resurser, kompetens. Basen för denna punkt är "relevant" beslutsnivå jämfört med lärpotentialen från incidenten.

## Implementering

- a. **Omfattning**  
Omfattning av åtgärder som verkligen genomförts jämfört med fattade beslut om åtgärder.
- b. **Kvalitet**  
Kvalitet, detaljeringsgrad och djup av genomförda åtgärder.
- c. **Tidsaspekt**  
Tiden från beslut till genomförd åtgärd. Tiden beror på typ av åtgärd.
- d. **Informationsspridning**  
Spridning av information om resultat av genomförda åtgärder, speciellt till berörda anställda.
- e. **Genomförandenivå**  
Organisatorisk nivå för genomförande, inkluderande resurser, kompetens. Basen för denna punkt är "relevant" genomförandenivå jämfört med lärpotentialen från incidenten.

## Uppföljning

- a. **Omfattning**  
Omfattning av de aspekter som följs upp
- b. **Kvalitet**  
Kvalitet, detaljeringsgrad och djup av genomförd uppföljning.
- c. **Tidsaspekt**  
Tiden från implementering till uppföljning. Tiden beror på typ av åtgärd
- d. **Informationsspridning**  
Spridning av information om resultat av genomförd uppföljning av åtgärder, speciellt till berörda anställda.
- e. **Uppföljningsnivå**  
Organisatorisk nivå för uppföljning, inkluderande resurser, kompetens. Basen för denna punkt är "relevant" genomförandenivå jämfört med lärpotentialen från incidenten.
- f. **Verkligt resultat**  
Ett mått på hur väl åtgärderna fungerar i förhållande till de avsedda.

## 2:a loop

- a. **Omfattning**  
Omfattning av de aspekter som analyseras och följs upp
- b. **Kvalitet**  
Kvalitet, detaljeringsgrad och djup av genomförd analys och uppföljning
- c. **Tidsaspekt**  
Frekvens.
- d. **Informationsspridning**  
Spridning av information om resultat av genomförd analys och uppföljning, speciellt till berörda anställda.
- e. **Uppföljningsnivå**  
Organisatorisk nivå för uppföljning, inkluderande resurser, kompetens.





