



**Malmö stad**

# Kontinuitetsplanering av IT- verksamheten

IT Advisory  
KPMG AB  
*14 september 2009*  
*Antal sidor: 19*

1.	Inledning och sammanfattning	2
1.1	Inledning	2
1.2	Sammanfattning	2
2.	Syfte och genomförande	4
2.1	Granskningens syfte	4
2.2	Genomförande	5
3.	Metod	5
3.1	Vald rekommendation	5
3.2	Metodens utgångspunkter	6
4.	Kontinuitetsplanering av IT-verksamheten vid Malmö stad	8
4.1	Inledning	8
4.2	Kontinuitetsplanering med stöd av iFACTS	8
4.3	Policy för kontinuitetsplanering	10
4.3.1	Rekommendation	10
4.3.2	Aktuell situation i Malmö stad	11
4.4	Business Impact Analysis (BIA)	11
4.4.1	Rekommendation	11
4.4.2	Aktuell situation i Malmö stad	12
4.5	Klassificering av verksamheter	14
4.5.1	Rekommendation	14
4.5.2	Aktuell situation i Malmö stad	14
4.6	Identifiering av IS processer som stödjer kritiska verksamheter	16
4.6.1	Rekommendation	16
4.6.2	Aktuell situation i Malmö stad	16
4.7	Valet av kontinuitetsbevarande åtgärder	17
4.7.1	Rekommendation	17
4.7.2	Aktuell situation i Malmö stad	17
4.8	Utveckling av en detaljerad BCP (inklusive DRP)	18
4.8.1	Rekommendation	18
4.8.2	Aktuell situation i Malmö stad	18
4.9	Test av planer, träning och medvetandeprogram	19
4.9.1	Rekommendation	19
4.9.2	Aktuell situation i Malmö stad	19
4.10	Oberoende kontroll	19
4.10.1	Rekommendation	19

# 1. Inledning och sammanfattning

## 1.1 Inledning

När det som inte får hända trots allt inträffar är det viktigt att en organisation är förberedd. Alla organisationer drabbas förr eller senare av allvarliga incidenter och som kan leda till att kritiska verksamheter inte längre kan bedrivas som normalt. Utan ett system av skyddande kontroller och detaljerade, testade handlingsplaner för sådana situationer, ökar risken för att konsekvenserna blir avsevärt kostsammare. Graden av beredskap är därför helt avgörande för att säkerställa en organisations långsiktiga framgång och funktion.

Kontinuitetsplanering (*Business Continuity Planning (BCP)*) syftar till att bygga upp en beredskap mot oväntade incidenter. Det är en omfattande process som dels är inriktad mot att utveckla alternativa arbetssätt för kritiska verksamheter, dels mot åtgärder för att inom bestämda tidsmål återställa den normala verksamheten och dels mot att införa preventiva och upptäckande kontroller. Allt syftar till att undvika eller minska konsekvenserna vid incidenter/avbrott.

Eftersom skyddsmöjligheterna idag är många och ofta kostsamma, är det samtidigt viktigt att valet av åtgärder bestäms i förhållande till skyddsvärdet, som i detta sammanhang sammanhänger med de konsekvenser som uppstår vid ett avbrott från den normala verksamheten. Detta framkommer genom att genomföra risk-, och konsekvensanalyser (*Business Impact Analysis (BIA)*) av organisationens olika verksamheter.

Denna granskning är inriktad mot att bedöma kontinuitetsplanering av IT-verksamheten i Malmö stad. Eftersom IT-verksamhet (informationssystem med data och funktionalitet, infrastruktur som nätverk och drift, utrustning mm) enbart är en stödjande funktion till organisationens kärnverksamheter, är det inte möjligt att bedöma kontinuitetsplaner för IT-verksamhetens olika delar utan koppling till kärnverksamheternas kontinuitetsplaner.

Kontinuitetsplanering används idag av allt fler organisationer eftersom man inser att fördelarna vida överstiger kostnaderna. En annan fördel av planeringsarbetet är att det ökar personalens medvetenhet och förståelse för organisationens verksamheter och prioriteringar.

## 1.2 Sammanfattning

Utifrån uppdraget att bedöma om IT-verksamheten i Malmö stad bedöms uppnå ett ”säkerställande av en kontinuerlig drift av verksamhetskritiska system för att kunna ge service åt medborgare och andra intressenter i Malmö stad och begränsa den ekonomiska skadan vid avbrott” har vi granskat organisationens kontinuitetsplanering.

Vi noterar som tillägg till uppdragets syfte att det är viktigt att kontinuitetsplanering utgår från en organisations kärnverksamhet (och dess krav) och att den IT-verksamhet, vars stöd utnyttjas av den aktuella kärnverksamheten, ingår som en naturlig del av denna kontinuitetsplanering. Med denna utgångspunkt är det möjligt att bedöma IT-verksamhetens betydelse och därmed vilka åtgärder som är ändamålsenliga med avseende på kontinuitetssäkrande åtgärder.

För att det skall finnas möjlighet att bygga upp en effektiv kontinuitetsplanering av IT-verksamheten, är det med andra ord helt avgörande att de olika kärnverksamheterna ställer tydliga krav på IT-verksamheten.

Vid granskningen har vi utgått från den rekommendation som Certified Information Systems Auditor (CISA) utformat (CISA Review manual, 2009).

Inledningsvis har vi noterat att Malmö stad saknar övergripande riktlinjer för kontinuitetsplanering av de olika verksamheterna. Vi rekommenderar därför att sådana utvecklas i form av en ”*Policy för kontinuitetsplanering*”. Gemensamma övergripande riktlinjer säkerställer att kontinuitetsplanering genomförs utifrån samma metod, med ett gemensamt arbetssätt och med enhetliga normer och värderingar för samtliga verksamheter inom organisationen. Behovet av sådana gemensamma riktlinjer ökar för en organisation som Malmö stad, med flera olika verksamheter och som till stora delar är lagstyrda och känsliga.

Noterbart är också att det sedan två år pågår ett strukturerat arbete med att kontinuitetsplanera systemverksamheten inom Malmö stad. Detta sker på initiativ av Informationssäkerhetschefen (STK) utifrån ett ledningssystem för informationssäkerhet, iFACTS. Vi har följt upp uppgifterna i iFACTS vilket bland annat gav följande resultat

- Sammantaget 194 system har registrerats i iFACTS
- Riskanalyser har **inte** registrerats i iFACTS för ca 70 % av de registrerade systemen
- Klassificering av konsekvensen vid avbrott för olika bedömningsområden (oförnekbarhet, riktighet, sekretess, spårbarhet, tillgänglighet), visar att drygt 25 % av systemen **inte** bedömts (samt att för endast 2 system har nivån ”kritiskt” valts)
- För de 194 systemen har **endast** ca 10 % noterat att man utvecklat en reservplan som kan användas vid avbrott i den normala verksamheten. För endast tre av systemen anges att tester sker
- För de 194 systemen anges ca 60 – 70 olika driftsställen (interna och externa). Eftersom Malmö stad saknar övergripande riktlinjer/krav för systemdrift, är det vår rekommendation att sådana utvecklas. Nuvarande driftsavtal har inte påverkats av krav från verksamheten (SLA), vilket rekommenderas ske.

Systemet iFACTS (eller andra liknande system) har funktionsstöd för de olika faserna av kontinuitetsplanering. Det finns exempelvis möjlighet att utgå från respektive verksamhet vid kontinuitetsplaneringen, att genomföra riskanalyser (BIA), att klassificera verksamheter, att registrera beroendekopplingar, koppla krav och rapportera avvikelser. Vid arbetet vid Malmö stad används dock inte verksamhetsmodulen, utan arbetet utgår från respektive registrerat system. Modulen för anläggningar har ännu inte införskaffats, varför det för närvarande inte finns möjlighet att registrera hela beroendekedjan i iFACTS, vilket är en väsentlig förutsättning för att kontinuitetsplaneringen skall bli komplett.

Vid granskningen av kontinuitetsplaneringen vid några av Malmö stads verksamheter kunde vi notera att det finns verksamheter som utvecklat ändamålsenliga kontinuitetsbevarande åtgärder och som också testas regelbundet.

Vår sammanfattande bedömning är dock att kontinuitetsplanering, med den inriktning och omfattning som framgår av den rekommendation (CISA) som varit vår utgångspunkt vid granskningen, saknas för de flesta av Malmö stads olika verksamheter. Detta framgår också av sammanställningen ovan utifrån iFACTS.

Nedan framgår våra rekommendationer i punktform. För ökad förståelse av våra synpunkter är det viktigt att hela rapporten läses. Vi rekommenderar Malmö stad att

- utveckla övergripande riktlinjer i form av en ”*Policy för kontinuitetsplanering*”, för att säkerställa enhetlighet vad avser metod, ansvarsfördelning och värderingsprinciper
- fastställa en *metod för kontinuitetsplanering* som exempelvis kan omfatta faserna risk- och konsekvensanalyser (BIA), klassificering, registrering av beroendekedjan (t.ex. IS/IT-komponenter), kontinuitetsbevarande åtgärder/strategier, detaljerade BCP/DRP, tester och oberoende kontroll
- tillse att kontinuitetsplaneringen sker med *utgångspunkt* från Malmö stads olika *kärnverksamheter* och de krav och förutsättningar som gäller för dessa
- tillse att respektive kärnverksamhet ställer *tydliga krav* på de delar av *IT-verksamheten* (t.ex. informationssystem, data, infrastruktur och andra IT-komponenter) som den utnyttjar och att detta är utgångspunkten för kontinuitetsplanering av IT-verksamhet
- klargöra *roller och ansvarsfördelning* i arbetet med kontinuitetsplanering. Det är exempelvis viktigt att ledningen för respektive kärnverksamhet har det yttersta ansvaret för kontinuitetsplanering av verksamheten
- tillse att tillräckligt stöd finns för att uppnå *enhetlighet i bedömningen av klassificeringsnivå* för de olika verksamheterna, eftersom detta är ett viktigt moment för bestämmandet av säkerhetskrav
- utveckla övergripande, gemensamma *riktlinjer för systemdrift*
- tillse att *avtal* för systemdriften flexibelt anpassas utifrån de olika systemens verksamhetskrav (SLA) och inte, som för närvarande, t.ex. utifrån antalet systemanvändare
- utveckla enhetliga, gemensamma riktlinjer för *ändringshantering* inom Malmö stad för systemverksamheten. Inom de verksamheter vi granskat sker ändringshanteringen utifrån olika metoder, vilket bland annat innebär att ändringar inte alltid sker utifrån en tydlig ansvarsfördelning och dokumenterade beslut för de olika faserna av en systemförändring

## 2. Syfte och genomförande

### 2.1 Granskningens syfte

Enligt uppdragsbeskrivningen skall granskningen ge svar på frågan om kontinuitetsplaneringen av IT-verksamheten inom Malmö stad bedöms uppnå ett ”*säkerställande av en kontinuerlig drift av verksamhetskritiska system för att kunna ge service åt medborgare och andra intressenter i Malmö stad och begränsa den ekonomiska skadan vid avbrott*”.

Som också framgår under föregående avsnitt kan inte de olika delarna av IT-verksamheten värderas utan dess koppling till den del av kärnverksamheten som utnyttjar IT-stödet. Därför måste kontinuitetsplanering av IT-verksamhetens olika delar ingå som en naturlig del av kontinuitetsplanerna för de kärnverksamheter som utnyttjar IT-stödet. Detta präglar därför också granskningen.

## 2.2 Genomförande

Granskningen har skett genom intervjuer och genom att ta del av fastställda instruktioner, arbetsbeskrivningar och motsvarande med betydelse för kontinuitetsplaneringen i Malmö stad. Vi har inte verifierat, genom tester, att beskrivna rutiner också är de som tillämpas.

Vid inledande diskussioner med företrädare för såväl revisionskontoret som informationssäkerhet (STK) inom Malmö stad, bestämdes vilka verksamhetssystem som skulle väljas för granskning och som därmed utgör en del av underlaget för våra bedömningar av kontinuitetsplaneringen. De system som valts ut för närmare granskning är Origo (Vård och omsorg), Elit (Skola), Marval (Support), SAM3001 (Trafikövervakning), SiteVision (Malmö.se och KomIn) och Carewin (Larmcentralen).

Intervjuer har genomförts med Informationssäkerhetschef Peter Johansson, Systemförvaltare Avdelning Vård och Omsorg (Origo) Lena Rosenberg, Kvalitetscontroller Avdelning Vård och Omsorg Lars-Åke Borgström, Systemförvaltare och Administratör IT Service (Marval) Mona Karlsson, Systemtekniker Larmcentralen (Carewin) Anders Kjellberg, Systemförvaltare Skola (Elit) Anders Ljungdahl, IT-sekreterare TÖC (SAM3001) Torbjörn Lindstedt, Systemförvaltare (Sitevision) Mattias Nordgren, Enhetschef Kundenheten ITS Markus Öhlin och Produktionschef ITS Davor Periac.

Dessutom har vi tagit del av funktionalitet och innehåll i systemet iFACTS, som används som ledningssystemstöd för informationssäkerhet med funktionalitet för ledningsstöd för kontinuitetsplanering.

Granskningen har genomförts av Jan-Inge Hedin under augusti och september 2009.

## 3. Metod

### 3.1 Vald rekommendation




På marknaden finns ett antal rekommendationer kring kontinuitetsplanering och där tillvägagångssätt och terminologi har vissa variationer. Utgångspunkten för vårt granskningsförslag är den rekommendation som Certified Information Systems Auditor (CISA) utformat (CISA Review manual, 2009).





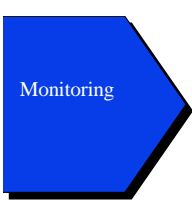
I enlighet med granskningsförslaget är det vår avsikt att, som en del av avrapporteringen, återge de väsentligaste delarna av den av CISA rekommenderade metoden (Se under "Rekommendation" vid respektive avsnitt nedan), dels eftersom detta ökar förståelsen för kontinuitetsplaneringens olika delar och tillvägagångssätt, men också eftersom det ger möjlighet

till kunskapsöverföring, förhoppningsvis till gagn vid uppdragsgivarens fortlöpande granskning av området inom Malmö stads verksamhet.

### 3.2 Metodens utgångspunkter

Kontinuitetsplanering är en pågående process (till skillnad mot tidsbegränsade projekt) och kan indelas i nedan beskrivna faser.

Faser	Översikt
 <p>Policy för kontinuitets- planering</p>	<p>En framgångsrik kontinuitetsplanering omfattar organisationens samtliga verksamheter och sker med ett gemensamt arbetssätt utifrån enhetliga normer och värderingar. För att uppnå detta utvecklas en för organisationen gemensam och övergripande <b>Policy för Kontinuitetsplanering</b> och som fastställs av organisationens ledning.</p>
 <p>Business Impact Analyzis (BIA)</p>	<p>Genom <b>risk-, och konsekvensanalyser (BIA)</b> identifieras och bedöms de olika scenarier som riskerar att äventyra kontinuiteten i verksamheterna. Förutom hotbilder beskrivs och analyseras konsekvenserna såväl finansiellt som med avseende på efterföljnad av lagar och regler samt hur det påverkar omvärldens förtroende för verksamheten. Sådana analyser genomförs av verksamhetsansvariga och banar väg för en kostnadseffektiv kontinuitetsplanering, som även inkluderar stödjande verksamheter, exempelvis IT-verksamheten.</p>
 <p>Klassificering av verksamheter</p>	<p><b>Klassificering</b> av organisationens olika verksamheter rekommenderas ske genom att relatera olika incidenters konsekvenser med sannolikheten att en incident skall inträffa (exempelvis under nästa femårsperiod). Härigenom kan organisationens olika verksamheter klassificeras utifrån de värden som riskeras vid avbrott.</p>

 <p>Identifiering av IS processer som stödjer kritiska verksamhetsprocesser</p>	<p><b>Beroendekedjan</b> mellan kritiska verksamheter och samtliga stödjande processer och hjälpmedel (inklusive IS-system, infrastruktur och IT-komponenter) måste beskrivas som en förutsättning för att säkerställa kontinuitetsplaneringen</p>
 <p>Valet av kontinuitetsbevarande åtgärder</p>	<p>Valet av kontinuitetsbevarande åtgärder rekommenderas ske utifrån en vald <b>strategi för att säkerställa kontinuiteten</b> i olika verksamheter. Genom att beskriva de olika åtgärdsalternativ, med dess inneboende risker, kan ledningen bestämma åtgärdsvalen. Detta inkluderar stödjande processer för respektive verksamhet, inom exempelvis IT-verksamheten.</p>
 <p>Utveckling av en detaljerad BCP (inklusive DRP)</p>	<p>Valet av strategi, enligt ovan, ger möjlighet att utveckla en i detalj fastställd <b>BCP</b> för de olika kärnverksamheterna. Detta inkluderar även reservrutiner och planer för återställning av den normala verksamheten efter avbrott.</p>
 <p>Tester och träning av fastställda planer</p>	<p>Det är viktigt att <b>testa</b> fastställda kontinuitetsplaner regelbundet eftersom förutsättningarna hela tiden ändras. Testerna visar om planerna är aktuella och om de fungerar i praktiken. Resultatet av tester bör dokumenteras, bevaras och vid behov utveckla befintliga planer. Det är dessutom nödvändigt att berörd personal får möjlighet att <b>träna in sina roller</b> i kontinuitetsplaneringen genom att testa olika åtgärder.</p>
 <p>Monitoring</p>	<p>Löpande <b>kontroll</b> av processen för kontinuitetsplanering bör utföras av en oberoende funktion.</p>

## 4. Kontinuitetsplanering av IT-verksamheten vid Malmö stad

### 4.1 Inledning

I det följande sker beskrivningen utifrån metodens fasindelning enligt avsnitt 3.2, ovan. Inom respektive avsnitt återges dels rekommendationen och dels den aktuella situationen inom Malmö stad.

Nedan (avsnitt 4.2) beskrivs kontinuitetsplanering av systemverksamheten inom Malmö stad, som pågår med stöd av systemet iFACTS.

### 4.2 Kontinuitetsplanering med stöd av iFACTS

Inom Malmö stad pågår ett arbete med att kontinuitetsplanera systemverksamheten utifrån systemet iFACTS. iFACTS är ett ledningssystemstöd för informationssäkerhet och som anskaffats på initiativ av tidigare IT-säkerhetsansvarig vid Stadskontorets IT-avdelning. Arbetet har pågått under knappt två år.

Bakgrunden till det aktuella informationssäkerhetsarbetet är ”Handlingsplan för Basnivå Informationssäkerhet” (2008-04-12) som utformades utifrån en GAP-analys av IT-verksamheten i förhållande till den internationella standarden för informationssäkerhet ISO/IEC 17799: 2005. GAP-analysen inkluderade även kontinuitetsplanering. För kontinuitetsplanering framgår två målnivåer, dels att uppnå en överensstämmelse med standarden på 80 % till våren 2008 och dels till 95 % till hösten 2008. Vid GAP-analysens genomförande konstaterades kontinuitetsplaneringen ligga på en nivå som motsvarade 63 % av standarden. Arbetet med att minska skillnaden mot standarden har försenats.

iFACTS har funktionsstöd för de flesta av kontinuitetsplaneringens olika delar (se avsnitt 3.2, ovan). Det finns exempelvis möjlighet att registrera samtliga verksamheter inklusive dess beroendekedja (Beroendekedja uppifrån: Verksamhet, Informationssystem, IT-tjänster, IT-infrastruktur och anläggningar (t.ex. noder och serverhallar)), att göra konsekvensanalyser (BIA), att klassificera av de olika verksamheterna och att rapportera incidenter/avvikelser. Modulen för registrering av anläggningar har dock ännu inte införskaffats.

Dessutom används inte verksamhetsmodulen i iFACTS. Det betyder att kontinuitetsplaneringen utgår från de system som används. Ansvariga för genomförandet är systemförvaltarna inom de olika förvaltningarna och stöds av Informationssäkerhetschefen (STK).

Följande uppgifter/bedömningar skall registreras för varje informationssystem

- **Allmän beskrivning** om systemet inklusive uppgift om var systemet drifas
- **Klassificering** innebär att betydelsen (nivåer) skall anges inom 6 områden
  - Oförnekbarhet (2 nivåer)
  - Riktighet (4 nivåer)

- Sekretess (4 nivåer)
- Spårbarhet (4 nivåer)
- Tillgänglighet 1 (särskilda tidpunkter)
- Tillgänglighet 2 (4 nivåer)

Val av nivå triggas automatiskt krav för systemet och dess användning.

- **Kritiska tider** under vilka systemet är särskilt känsligt för avbrott. Avsikten är att detta skall påverka utformningen av driftsavtal (i form av SLA (Service Level Agreement)).
- **Lag/norm 2.** I systemet finns lagar inlagda som bedöms vara aktuella för de olika verksamheterna. För verksamheten gällande lagar kan triggas krav på det aktuella systemstödet. För varje lag skall i iFACTS ett av följande tre val göras:
  - Ej tillämpbar
  - Tvingande
  - Undersöker
- **Kontinuitet och kris (riskanalys).** Här registreras en risk- och konsekvensanalys (BIA) vid avbrott (dessutom beroende på avbrottets tidslängd). Områden som bedöms med avseende på konsekvenserna är kostnader, efterföljnad av lagar och normer samt förtroendet från omvärlden.
- Dessutom skall förekomsten av **reservrutin vid avbrott** registreras liksom hur den är utformad och när den **testades** senast. Även förekomsten av plan för återställning skall anges per system.
- Registreringen av uppgifter i iFACTS innebär att olika val automatiskt genererar ett antal **krav** beroende på nivåer registrerade vid klassificering, efterföljnad av lagar och normer och konsekvenser vid avbrott. Avsikten är att ansvariga skall kunna följa upp om de olika kraven är uppfyllda och i annat fall ange ett senaste datum för när detta beräknas ske.

Vi har följt upp iFACTS och konstaterade att kontinuitetsplanering (åtminstone) har påbörjats för 194 informationssystem. Utgångspunkt för arbetet med iFACTS är de system som används inom de förvaltningar där det finns systemförvaltare. I det följande redovisas vissa uppgifter kring de 194 system som registrerats i iFACTS.

**Notering:** iFACTS ger ett bra stöd för kontinuitetsplanering. Eftersom det finns möjlighet att anpassa systemet utifrån den process som väljs erhålls flexibla möjligheter att stödja vald metod inom Malmö stad.

Som tidigare noterats är det vår rekommendation att kontinuitetsplaneringen utgår från verksamheterna och inte informationssystemen. Därför bör ansvaret för att genomföra kontinuitetsplaneringen överföras på de olika verksamhetsledningarna. Informationschefen inom, liksom andra IT-specialister inom organisationen, kan stödja verksamheterna i detta arbete.

Genom att kontinuitetsplanera systemverksamhet som en naturlig del av kontinuitetsplanerna för de verksamheter som utnyttjar systemverksamheten sker detta utifrån systemens verkliga betydelse. Detta inkluderar då inte bara förekommande system utan även informationstillgångar utifrån dess betydelse och känslighet.

## 4.3 Policy för kontinuitetsplanering

### 4.3.1 Rekommendation

Kontinuitetsplaneringen inom en organisation bör ske utifrån gemensamma riktlinjer för organisationens samtliga verksamheter. Därför är det viktigt att utveckla en **Policy för kontinuitetsplanering** och som fastställs av organisationens ledning. Härigenom kommunicerar ledningen dels hur organisationen skall förhålla sig till aktuella risker och hot, men också den metod som skall användas (kontinuitetsplaneringens olika faser) för att etablera en beredskap mot incidenter som annars riskerar att leda till allvarliga konsekvenser för verksamheternas normala servicenivå.

Denna övergripande styrning är särskilt viktig för komplexa organisationer med verksamheter av flera olika slag (t.ex. Malmö stad).

Viktiga mål för kontinuitetsplaneringen och som bör prägla policyns utformning är att

- tydliggöra **roller** och ansvarsfördelning kring planeringsarbetet
- förmedla kunskap om **prioriteringar** vid en kris (t.ex. genom klassificeringssystem)
- besluta om kritiska verksameters **alternativa arbetsätt** under en kris
- besluta om **tids- och andra mål** för kritiska verksamheter
- **beslutstiden** under en kris skall minimeras

Eftersom skyddsåtgärder kan vara väldigt kostsamma, är det samtidigt viktigt att skapa förutsättningar som leder till att man utvecklar en **kostnadseffektiv** kontinuitetsplan. Det innebär att valet av skyddsåtgärder och dess kostnader, sker utifrån de konsekvenser/kostnader som beräknas/bedöms om den aktuella verksamheten drabbas av ett avbrott i den normala servicenivån.

För att kontinuitetsplaneringen skall vara ändamålsenlig, bör den inte bara omfatta åtgärder som säkerställer alternativa arbetsätt för kritiska verksamheter under ett avbrott, utan den bör dessutom omfatta

- **Preventiva** kontroller, varigenom konsekvenser vid incidenter till och med kan undvikas helt (t.ex. utrustning för reservström när elleveranser avbryts)
- **Detektiva** kontroller, varigenom potentiella incidenter upptäcks på ett tidigt stadium för att minimera konsekvenser (ex larm av olika slag eller granskning av loggar för att i förväg upptäcka ökad risk för intrång)

- **Återställande** kontroller, som syftar till att återställa avbruten verksamhet inom fastställda tidsmål (t.ex. avtal om återställande av lokaler, hård- och mjukvara)

Beslut om skyddsgärder (kontinuitetsplaner) bör fattas av respektive verksamhetsledning, dels eftersom detta är en naturlig del av verksamhetsansvaret men också eftersom valet samtidigt innebär en accept av de olika åtgärdernas inneboende risker.

#### 4.3.2 Aktuell situation i Malmö stad

Malmö stad saknar en ”Policy för Kontinuitetsplanering”, eller motsvarande övergripande styrmedel för kontinuitetsplanering, med den omfattning och inriktning som avses enligt rekommendationen ovan.

**Notering:** Vi rekommenderar Malmö stad att utveckla en ”Policy för kontinuitetsplanering”. Gemensamma övergripande riktlinjer säkerställer att kontinuitetsplaneringen genomförs utifrån samma metod, med ett gemensamt arbetssätt och med enhetliga normer och värderingar för samtliga verksamheter inom organisationen.

Behovet av gemensamma riktlinjer ökar för en organisation som Malmö stad, som innehåller flera olika verksamheter och som till stora delar är lagstyrda och känsliga.

### 4.4 Business Impact Analysis (BIA)

#### 4.4.1 Rekommendation

BIA är en fas där incidenter som bedöms kunna påverka kontinuiteten i verksamheterna identifieras och beskrivs. Förutom en realistisk hotbild förutsätter detta en djup kunskap om de olika verksamheternas delprocesser och dess betydelse utifrån de konsekvenser som uppstår vid avbrott. För en komplett analys förutsätts att delprocessernas beroendekopplingar, exempelvis till IT-verksamheten är beskriven. Arbetet förutsätter ett aktivt deltagande från såväl verksamhetsansvariga som olika personalkategorier beroende på verksamhetsprocess. Detta inkluderar även IT-personal och slutanvändare.

De viktigaste frågorna som skall besvaras under analysen är

- *Vilka är de olika verksamhetsprocesserna.* Varje process skall bedömas och utvärderas utifrån dess betydelse/konsekvenser vid avbrott/känslighet
- *Vilka kritiska informationsresurser* är relaterade till dessa processer. Eftersom avbrott till information i sig själv inte är kritisk, är kopplingen till verksamhetsprocessen avgörande för att bestämma hur kritiskt ett avbrott mot informationen är
- Vilken är den *kritiska återställningstiden* för de olika delprocesserna innan oönskade konsekvenser drabbar verksamheten. Även andra väsentliga mål bör involveras i denna del beroende på verksamhetsprocess. Detta underlättar utformningen av en detaljerad kontinuitetsplan. Exempel på viktiga användbara mål är

- RTO (Recovery Time Objective), som visar *efter vilken tidsperiod* en verksamhet måste vara återställd för att undvika katastrofala konsekvenser
- RPO (Recovery Point Objective), som visar *till vilken historisk punkt* som verksamheten "minst" måste kunna återställas till informationsmässigt, för att undvika oönskade följder. Utifrån detta mått kan rutinen för backup kopiering av information utformas
- SDO (Service Delivery Objective), som visar *lägsta möjliga servicenivå* för en verksamhetsprocess. Detta mått används för att utforma alternativ rutin för en verksamhet då den normala rutinen är avbruten

Konsekvenser bör beskrivas såväl finansiellt som med avseende på efterföljnad av lagar och regler samt effekten på olika intressenters förtroende för verksamheten.

#### 4.4.2 Aktuell situation i Malmö stad

Intervjuer med systemförvaltare för de utvalda systemen, visade att

- **Origo** (Vård och Omsorg) är ett system för dokumentation av stadsdelsnämndernas ärenden inom vård och omsorg enligt SOL (Socialtjänstlagen), LSS (Lagen om särskilt stöd till vissa funktionshindrade) och HSL (Hälsa- och sjukvårdslagen). Systemet har 50-60 superanvändare och sammantaget ca 4 500 användare. BIA (Kontinuitet och kris), varigenom bedömningar av konsekvenserna som registrerats i iFACTS för de olika bedömningsområdena vid avbrott, har bedömts som "Ej tillämpligt".
- **Elit** (Skola) är ett system för att hantera elevuppgifter, klasser, kurser, grupper för fyra olika verksamheter, barnomsorg, grundskola, gymnasium och komvux. Systemet har ca 750 användare. BIA har inte registrerats i iFACTS.
- **Carewin** (Larmcentralen, Limhamns Industriby) är ett system för att bevaka trygghetslarm dygnet runt (ca 5 800 larm) utifrån uppdrag inom 9 av 10 stadsdelar (undantag för Fosie SDF som använder annat system med drift i egen lokal).

BIA för Carewin har inte registrerats i iFACTS, men arbete pågår för att ISO-certifiera verksamheten, för vilket färdigtidpunkt är planerad till oktober 2009. Eftersom Carewin driftas i egen lokal på Larmcentralen, finns planer på att dessutom SSF-certifiera verksamheten. Detta beror på att ISO-certifieringen inte beaktar process- och miljökrav kring systemdriften i tillräcklig omfattning.

- **SAM 3001** (Trafikövervakningscentralen) är ett planerings- och samordningsverktyg som klarar av att hantera stora mängder transporter. Man har utvecklat och dokumenterat avbrottsplaner (Nödlägesberedskap och Reservrutiner) för olika händelser med olika följd. De är dock inte registrerade i iFACTS vilket man nu planerar att göra. Eftersom planerna utvecklades för några år sedan, finns nu planer på att uppdatera dem. Man har bedömt att verksamheten kräver att systemet alltid skall vara tillgängligt.
- **Marval** (Support) är ett ärendesystem för support- och systemdriften inom Malmö stad. Samtliga användare vänder sig till ITS, tel. 34 27 27 eller [342727@malmo.se](mailto:342727@malmo.se). ITS har ca 85 personer som använder Marval. Användare kan följa sitt ärende i Marval på Komin. Alla anmälda incidenter registreras i Marval. Ärende som avser handhavande i

applikation som ITS inte har support på hänvisas till superanvändare. Alla anmälda incidenter klassas i Prio 3, men det finns en koordinator som övervakar exempelvis äldre ärenden. BIA har inte registrerats i iFACTS.

- **SiteVision** (Intranätet) är ett administrativt stöd för extern och intern web-publicering (Malmö.se och KomIn). BIA har registrerats i iFACTS, med bedömningar för "Negativ mediauppmärksamhet": Dag 1; och för "Allvarlig och utbredd förtroendeförlust": Dag 6-10. För övriga områden har "Ej tillämpligt" registrerats.

En sammanställning av BIA (**Risakanalys**) för samtliga de system som registrerats i iFACTS framgår dessutom av nedanstående tabell

Risikområde/ Konsekvens	Allvarliga konsekvenser (kopplat till alternativ för avbrottets längd i dagar)	Ej tillämpligt	Blankt
"Negativ mediauppmärksamhet"	13	45	136
"Allvarlig och utbredd förtroendeförlust"	12	46	136
"Brott mot lagstiftning"	2	56	136
"Verksamhetens budget äventyras"	24	34	136
"Verksamhetens mål äventyras"	25	33	136

**Notering:** Vi vill påminna om att tabellen visar bedömda konsekvenser vid avbrott (BIA) i systemverksamheterna och inte avbrott i de olika kärnverksamheterna. För att få en komplett bedömning av konsekvenserna vid avbrott i verksamheternas normala service, är det vår rekommendation att komplettera analyserna med denna utgångspunkt.

Det stora antalet "blanka" alternativ i tabellen över registrerade BIA i iFACTS visar dessutom att konsekvenserna vid avbrott inte bedömts för 70 % av de i iFACTS registrerade systemen.

En iakttagelse vid intervjuerna var att ändringshanteringen inte sker utifrån en enhetlig metod för de olika verksamheterna. För någon verksamhet tillämpas systemstöd vid ändringshantering, varigenom det är möjligt att följa statusen för pågående ändringsarbeten, notera dokumenterade krav, ta del av testarbete, notera vem som fattar beslut o.s.v. Inom vissa verksamheter saknas metod för ändringshantering. Ändringshantering utan tydlig ansvarsfördelning, dokumenterade krav, godkänd testverksamhet mm, kan medföra risker som till och med kan äventyra systemets

stabilitet och funktionalitet. Därför bör man fastställa en enhetlig metod för ändringshanteringen inom Malmö stad.

## 4.5 Klassificering av verksamheter

### 4.5.1 Rekommendation

Klassificering av organisationens olika verksamheter rekommenderas ske utifrån konsekvenser inom olika väsentlighetsområden (se beskrivning av de olika områdena för iFACTS).

Rekommendationen för att bestämma nivåerna inom respektive bedömningsområde genom att relatera konsekvenser (t.ex. kostnader, lagbrott) till sannolikheten att konsekvenserna skall utfalla inom ett antal år. Härigenom bestäms således de olika verksamheternas kritiska betydelse för organisationen utifrån dess bedömda ”skadenivåer” vid avbrott.

Detta utgör samtidigt grunden för att välja kontinuitetssäkrande åtgärder (krav) exempelvis genom förhindrande, lindrande och återställande kontroller.

### 4.5.2 Aktuell situation i Malmö stad

Klassificeringen i iFACTS av de sex utvalda systemen framgår av tabellen nedan

Klassificerings- område/Väsentlig- hetsnivå	Kritisk	Mycket viktig	Viktig	Mindre viktig	Blank
<b>Oförnek- barhet</b>			Origo, Marval, SAM3001		Elit, Carewin, Sitevision
<b>Riktighet</b>		Carewin, Sitevision, Origo	Elit, Marval, SAM3001		
<b>Sekretess</b>		Elit, Carewin, Origo, Sitevision, SAM3001		Marval	
<b>Spårbarhet</b>		Carewin, Sitevision	Elit, Origo, Marval, SAM3001		
<b>Tillgänglighet 2</b>		Elit, Carewin, Origo,	Marval		

		SAM3001, Sitevision			
<b>Klassificerings- område/Väsentlig- hetsnivå</b>	<b>Vardag 0700-1700, Vardagar 0000-2400</b>	<b>Alla dagar 0700-2200</b>	<b>Alla dagar 0700-1700</b>	<b>Alla dagar 0000-2400</b>	<b>Blankt</b>
<b>Tillgänglighet 1</b>	Marval			Origo, SAM3001	Elit, Carewin, Sitevision

Klassificeringen av samtliga (194) registrerade system i iFACTS framgår av nedanstående tabell.

<b>Klassificerings- område/Väsentlighets- nivå</b>	<b>Kritisk</b>	<b>Mycket viktig</b>	<b>Viktig</b>	<b>Mindre viktig</b>	<b>Blank</b>
<b>Oförnekbarhet</b>		31	9		154
<b>Riktighet</b>	0	30	87	29	48
<b>Sekretess</b>	2	24	39	82	44
<b>Spårbarhet</b>	0	17	48	81	48
<b>Tillgänglighet 2</b>	0	29	53	64	48
<b>Klassificerings- område/Väsentlighets- nivå</b>	<b>Vardagar 0700-1700, Vardagar 0000-2400</b>	<b>Alla dagar 0700-2200</b>	<b>Alla dagar 0700-1700</b>	<b>Alla dagar 0000-2400</b>	<b>Blankt</b>
<b>Tillgänglighet 1</b>	25, 1	3	5	6	154

**Notering:** Liksom för tidigare faser inom kontinuitetsplaneringen rekommenderar vi att arbetet sker utifrån konsekvenser för verksamheten och inte systemverksamheten.

Det relativt sett stora antalet blanka nivåer i iFACTS (se tabellerna ovan) är troligen en kombination av att man endera inte genomfört klassificeringsfasen, eller att det finns en osäkerhet för vissa bedömningsområden (t.ex. oförnekbarhet).

Det är också noterbart att endast 2 system bedöms vara ”kritiska” oavsett bedömningsområde, vid avbrott. Eftersom klassificeringsnivåerna har stor betydelse för de säkerhetskrav som uppkommer

på systemen är detta ett viktigt moment i kontinuitetsplaneringen. Man bör därför utvärdera behovet av stöd vid klassificeringsarbetet för att uppnå enhetlighet i bedömningarna.

## 4.6 Identifiering av IS processer som stödjer kritiska verksamheter

### 4.6.1 Rekommendation

**Beroendeförhållandet** mellan kärnverksamheterna och den stödjande IT-verksamheten (informationssystem med dess informationstillgångar, infrastruktur och IT-komponenter), måste beskrivas för att säkerställa att samtliga förutsättningar blir involverade i planeringsarbetet.

Detta kan brytas ner till olika nivåer beroende på verksamhet, men detaljeringsgraden har betydelse dels vid utvecklandet av reserv- och återställningsrutiner, men också för att ha möjlighet att skydda väsentliga processer och tillgångar på ett ändamålsenligt sätt. Detta avser inte minst informationsstillgångar.

### 4.6.2 Aktuell situation i Malmö stad

Vid kontinuitetsplanering med stöd av iFACTS används inte verksamhetsmodulen och dessutom har man inte anskaffat modulen för anläggningar. Beroendekedjan för de olika verksamheterna har således inte registrerats i iFACTS.

Som en del av uppgifterna i iFACTS anges även informationssystemens **driftsställe**. Uppföljning kring detta visade att de 194 system som registrerats i iFACTS hade ca 65 – 70 olika driftsställen (egentligen finns ett drygt 80-tal driftsställen registrerade, men eftersom det saknas indatakontroll för driftsplats har samma driftsställe registrerats med olika benämning för ett antal system). Malmö stad har två stora serverhallar (Rönnen och Stadshuset) som driftas genom ITS försorg. Förutom de system som driftas där förekommer således ytterligare ett stort antal, både interna och externa, driftsställen. Dessutom är uppgiften om driftsställe blankt för 7 system medan man angivit "Vet ej" för ytterligare 7 system.

Detta är ett sätt att spegla komplexiteten och därmed behovet av att registrera hela beroendekedjan för varje verksamhet. Registrering av hela beroendekedjan skapar också förutsättningar för kompletta kontinuitetsplaner.

**Notering:** Vi rekommenderar Malmö stad att anpassa kontinuitetsplaneringen så att alla delar av en verksamhet (beroendekedjan) kan inkluderas i verksamhetens kontinuitetsplanering.

Nuvarande driftsavtal, exempelvis med ITS (Rönnen och Stadshuset), har inte anpassats till de särskilda krav som framkommer genom klassificering och BIA som registrerats i iFACTS, vilket man har för avsikt att göra i framtiden. Vi rekommenderar dessutom Malmö stad att utveckla övergripande, generella riktlinjer för systemdrift (med t.ex. säkerhetskrav) som stöd för organisationen. Behovet av detta ökar genom det stora antalet driftsställen som används idag.

## 4.7 Valet av kontinuitetsbevarande åtgärder

### 4.7.1 Rekommendation

Valet av kontinuitetsbevarande åtgärder för en verksamhet bör variera med de konsekvenser som framkommit under BIA. Ju mer som riskeras desto mer ambitiösa kan också skyddsåtgärderna vara.

Rekommendationen är att utveckla olika skyddande strategier för respektive verksamhet, låta verksamhetsledningen ta del av de olika strategierna som beskrivs inklusive de olika åtgärdernas inneboende risker. Det innebär att ledningarna fattar beslut om strategi väl medvetna om alternativ och risker. En strategi består av en kombination av preventiva, detektiva och återställande kontroller/åtgärder.

Valet av strategi skall avgöras utifrån verksamhetens kritiska betydelse, kostnader, tillgänglig tid för återställande och säkerhet.

### 4.7.2 Aktuell situation i Malmö stad

Intervjuer med systemförvaltare för de sex utvalda systemen visar att man saknar dokumenterade strategier för kontinuitetsplanering i enlighet med rekommendationen (möjligtvis med undantag för Larmcentralen), ovan.

Avseende reservrutiner vid avbrott framkom följande

- För **Origo** (Vård och Omsorg) har en avbrottsplan utvecklats som dessutom kortfattat beskriver hur verksamheten skall bedrivas vid olika långa avbrott. Tester av avbrottsplanen har inte dokumenterats.
- För **Elit** (Skola) har inga avbrottsplaner utvecklats.
- För **Carewin** (Larmcentralen, Limhamns Industriby) har reservrutin vid avbrott utvecklats genom att man har byggt upp en backupcentral vid Tygelsjö Äldreboende, med 4 ständigt utrustade operatörsplatser. Systeminformationen speglas (med ett dygns förskjutning) till server placerad i den alternativa lokalens elcentral. Vid några tillfällen per år testas reservrutinen genom att personal flyttar till Tygelsjö och startar upp och driver verksamheten därifrån. Larmcentralen har således vidtagit ett antal åtgärder för att minska risken för allvarliga konsekvenser avbrott, som exempelvis redundans av information, reservenergi såväl i form av UPS och dieselkraftverk och inte minst genom en alternativ fullt utrustad lokal.

Serverrummet (tidigare kontorsutrymme i samma lokal som larmcentralen) är dock inte anpassat till serverdrift. Sådana utvecklingsplaner finns dock.

- För verksamheten kring Trafikövervakningssystemet, **SAM3001**, finns som tidigare nämnts dokumenterade reservrutiner vid avbrott. Bland kontinuitetsbevarande åtgärder kan nämnas UPS för några timmars systemdrift vid strömavbrott och bärbara datorer, försedda med mobilkort, att användas exempelvis vid avbrott i det lokala nätverket.

Systemet driftas av Malmator i Älvsjö. Reservrutinerna testas några gånger årligen. Driftsavtal finns med angivna tillgänglighetskrav. Man har inte granskat driftsmiljön för att verifiera om driftsavtalet följs. Reservrutinerna kommer att registreras i iFACTS.

- Supportverksamheten kring **Marval** saknar dokumenterade reservrutiner vid avbrott.
- **SiteVision** (Intranätet) har inte heller dokumenterat reservrutiner vid avbrott.

Uppföljning av uppgifter med avseende på reservrutin och när denna senast testats har skett för samtliga system (194 st.) som registretats i iFACTS. Resultatet framgår av nedanstående tabell

Uppgift om reservrutin/val	Ja	Nej	Blankt
Beskrivning av reservrutin	11	3	180
Rutin för aktivering av reservrutin	20	2	172
Senaste test/övning	3 (Varav ett årtal är 2010)	-	191

**Notering:** Resultatet visar att reservrutin vid avbrott från systemets normala drift endast finns för 11 (möjligt 20) av 194 system. Dessutom har reservrutinens funktion endast testats för 2 system.

Eftersom fungerande (testade) reservrutiner vid avbrott i den normala verksamheten, är en av de mest väsentliga åtgärderna för att säkerställa en önskvärd minsta servicenivå, visar resultatet att mycket arbete återstår innan kontinuitetsplaneringen kan anses fungera inom Malmö stad.

## 4.8 Utveckling av en detaljerad BCP (inklusive DRP)

### 4.8.1 Rekommendation

Utifrån valet av strategi för kontinuitetsplanering för respektive verksamhet kan detaljerade Kontinuitetsplaner utvecklas för de olika kärnverksamheterna, och fastställas av de olika verksamheternas ledningar. Planerna skall inkludera reservrutiner och planer för återställande av den normala verksamheten efter avbrott. Det är också viktigt att de innehåller en beskrivning av roller och ansvarsfördelning.

### 4.8.2 Aktuell situation i Malmö stad

Kontinuitetsplaner enligt rekommendationen ovan saknas för verksamheterna i Malmö stad.

**Notering:** Detaljerade kontinuitetsplaner för varje verksamhet inom Malmö stad bör utvecklas och fastställas, inklusive reservplaner och planer för återställande av normal verksamhet efter avbrott. Dessa planer skall också innehålla en beskrivning av roller och ansvarsfördelning.

## 4.9 Test av planer, träning och medvetandeprogram

### 4.9.1 Rekommendation

Detaljerade kontinuitetsplaner bör testas regelbundet eftersom förutsättningarna hela tiden ändras. Personal byts ut, rutiner ändras, processer, lokaler mm förändras med jämna mellanrum. Därför är det viktigt att testa planer, dokumentera resultatet av testerna och att vid behov utveckla planerna utifrån resultatet av testerna.

Det är dessutom nödvändigt att berörd personal får möjlighet att träna in sina roller i kontinuitetsplaneringen genom de planerade testerna. Detta avser inte minst personal som inte ingår i kontinuitetsteamet, men som ändå påverkas vid en katastrof. Genom att träna och medvetandegöra ökar sannolikheten för att uppsatta planer också skall fungera vid ett avbrott.

### 4.9.2 Aktuell situation i Malmö stad

Som inte minst framgår enligt avsnitt 4.7.2 ovan hör det till ovanligheterna att avbrotts- eller kontinuitetsplaner testas inom Malmö stads verksamheter.

**Notering:** Det är viktigt att detaljerade kontinuitetsplaner testas enligt i förväg bestämt schema och rutin, för att säkerställa att fastställda planer fungerar över tiden trots att verksamheternas förutsättningar förändras.

## 4.10 Oberoende kontroll

### 4.10.1 Rekommendation

Löpande **kontroll** av att processen för kontinuitetsplaneringen, inklusive tester och dokumentation, bör löpande utföras av en oberoende funktion. Vi har dock inte följt upp hur denna kontroll utförs för närvarande.

Malmö som ovan  
KPMG AB

Jan-Inge Hedin  
*IT Advisory*