Celab COMMUNICATIONS

# Guide till pålitlig reservkommunikation

## Hur säkerställer man att verksamheten fungerar när ordinarie kommunikationssystem inte längre är tillgängligt?

# Guide till pålitlig reservkommunikation

## Hur säkerställer man att verksamheten fungerar när ordinarie kommunikationssystem inte längre är tillgängligt?

Trots att alla organisationer arbetar mer eller mindre hårt för att skydda sin infrastruktur och olika system finns en obekväm sanning: inga system är hundra procent tillförlitliga.

Du som läser detta är sannolikt en del av en organisation som redan insett och accepterat detta faktum, samt landat i behovet av en Plan B eller med andra ord, ett reservkommunikationssystem.

Den här artikeln är en del av en serie som skall hjälpa er "skottsäkra" er verksamhetskritiska kommunikationsmiljö. Vi rekommenderar att ni tar del av artiklarna i följande ordning.

1. Introduktion till beredskapskommunikation - Varför preparera?
2. Guide till riskanalyser för kommunikationssystem - Vad kan gå fel?
3. Guide till robusta kommunikationssystem - Vad kan vi göra åt det?
4. **Guide till pålitlig reservkommunikation - Vad gör vi när det ändå inte räcker till? (denna artikel)**

Syftet med artikelserien i stort är att ge er ett antal "linser" med vilka ni kan beskåda er kommunikationsmiljö för att kunna urskilja lämpliga åtgärder för just era förutsättningar.

Ni hittar alla våra artiklar på celab.se/kunskapsbank/artiklar.

Reservkommunikation är i stort sett unikt för varje ändamål och behov. I vissa fall räcker det med att säkra talkommunikationen medan i andra fall även dataförbindelserna är kritiska.

## Exempel på reservkommunikationssystem

| Primär kommunikation | Potentiellt reservsystem |
|---|---|
| **RAKEL** | Fristående radiosystem (DMR, Kortvåg, etc) |
| **Telefoni (Publik)** | RAKEL, Privat mobilnät, Fristående radiosystem (DMR, Kortvåg, etc), Infrastruktur-fri lösning |
| **Privat/Dedikerat mobilnät** | Fristående radiosystem (DMR, Kortvåg, etc), Infrastruktur-fri lösning |
| **Fristående radiosystem** | Annat radiosystem (DMR, Kortvåg, etc), Infrastruktur-fri lösning |

För att hitta rätt reservsystem krävs en strukturerad genomlysning av just er situation, och vi vill hjälpa er på vägen med denna ”checklista”.

## 1. Risk- och sårbarhetsanalys

Reservkommunikation är rent krasst bara nödvändigt när er ordinarie kommunikationsmiljö inte kan eliminera eller hantera de risker ni står inför. Ett lämpligt sätt att utvärdera detta är genom att göra en risk- och sårbarhetsanalys på ert/era nuvarande kommunikationssystem – något som vi tipsar om i artikel 2 i denna serie.

Om genomförd granskning påvisar att era system, och i förlängningen er organisation, inte kan leva upp till interna krav och/eller externa förväntningar så har ni hamnat rätt.

# 2. Behovsanalys

Ett reservkommunikationssystem behöver inte kunna allt men ni måste avgöra vad som är väsentligt och vad som är överflödigt i prekära situationer. Kort sagt måste ni bestämma;

- **Vad systemet skall klara av.**
- **Under vilka omständigheter systemet skall klara av det.**
- **På vilket/vilka sätt systemet skall klara av det.**

Nedan följer en - icke uttömmande - lista av aspekter och frågeställning att ta ställning till för att lyckas utforma reservkommunikationssystem som funkar när de behövs;

## 2.1 Scenarion

Först och främst måste det bestämmas under vilka omständigheter som reservkommunikationssystemet skall användas. Detta ger de yttre gränsdragningarna för kommande frågeställningar och ställningstaganden.

- **Vilka förutsättningar råder när reservkommunikationssystemet skall användas?**
- **Vilka olika triggers är aktuella – vad behöver ske för att reservsystemet skall aktiveras?**
- **Hur länge förväntas reservsystemet användas när det väl tas i bruk?**

***Glöm inte att fastställa och värdera eventuella externa förväntningar från kunder, medborgare, myndigheter eller andra viktiga intressenter. Dessa styr såväl direkt som indirekt de scenarion som ni behöver ta ställning till.***

## 2.2 Deltagare

Under denna rubrik skall ni identifiera och lista alla entiteter som behöver använda systemet under de scenarion som registrerats.

### Personer

- **Vilka interna individer - eller roller - behöver kommunicera med varandra?**
- **Vilka behöver leda, samtala respektive lyssna?**
- **Hur behöver de praktiskt/organisatoriskt kunna nå varandra? (inte tekniskt)**
- **Behöver de kunna skicka meddelanden/data mellan varandra?**

### Applikationer & utrustning

- Har ni ledningsstöd, kamerasystem eller annan utrustning som behöver vara tillgänglig även under listade scenarion?
- Hur behöver denna "utrustning" vara tillgänglig i praktiken? (inte tekniskt)
- Vilken prestanda krävs för att använda applikationen eller utrustningen?

### Samverkan

- Behöver vi ha kanaler öppna mot externa parter som exempelvis myndigheter, leverantörer eller kunder?
- Kan vi använda deras system, kan vi tillhandahålla vårt eller behöver dem integreras?
- Vilka externa individer eller utrustning kan tänkas beröras?

## 2.3 Funktioner & Finesser

Nu behöver ni fastställa vilka "kommunikationssätt" och features som behöver/måste fungera för att tillfredsställa ovanstående behov i berörda scenarion.

### Talkommunikation

- Larmsamtal
- Gruppsamtal
- Individsamtal/ Telefonsamtal
- Prioriteringar

### Meddelanden

- SMS/SDS
- Status

### Anslutningar

- Utalarmering?
- Ärendehantering?
- Databas?
- Intranät?
- Internet?

## 2.4 Tillgänglighet

Här skall bestämmas när, var och hur systemet skall tillhandahålla sin funktion under fastslagna scenarion.

### Tillgång

- Hur och när behöver systemet vara tillgängligt?
- Behöver olika deltagare ha olika behörigheter och/eller prioriteringar?

### Täckning & Kapacitet

- Vart behöver systemet vara tillgängligt?
- Vad behöver vara tillgängligt på respektive plats?
- Kan behovet förändras och hur kan det då tänkas ske?

## 3. Systemval

När ni sammanställt de behov som behöver täckas och de risker som behöver undvikas så behöver detta omsättas till en kravlista för att kunna utvärdera och identifiera passande system.

Här gäller det inte bara att identifiera rätt tekniska plattform utan också att undvika flaskhalsar, single-point-of-failures och andra potentiella sårbarheter redan innan implementeringen. Bristande systemdesign, komponenter och installationer kan få stora konsekvenser som kanske inte upptäcks förrän det är för sent.

- **En klassisk fallgrop är exempelvis att "reservlösningen" delar sårbarheter med huvudsystemet. Dessa flaskhalsar kan vara uppenbara men också dolda. Systemen kanske delar på en fiber-anslutning, en server eller en säkring.**

Det gäller alltså att välja en leverantör som utöver att kunna teknologierna också innehar relevant erfarenhet från att leverera en robust (verksamhetskritisk) installation.

När ett systemförslag är framtaget kan det vara lämpligt att genomföra en "simulerad" risk- och sårbarhetsanalys redan före beställning för att försöka lokalisera potentiella bekymmer innan de förverkligas. Undersökningen kan med fördel genomföras tillsammans leverantör för att försäkra att ni delar syn på utmaningarna.

# 4. Förberedelser

Reservkommunikation handlar inte bara om teknik – utan om förmågan att leda, fatta beslut och samverka när allt annat sviktar.

Det medför att arbetet inte är klart när ett behovsanpassat system har installerats. För att vara förberedda för de scenarion som systemet skall användas under så finns ytterligare frågor att ta hänsyn till att för att garantera att systemet faktiskt levererar den trygghet som det är tänkt.

## 4.1 Logistik

Med "logistik" menar vi att ni behöver säkerställa att all berörd reservkommunikationsutrustning är funktionsduglig och disponibel utan dröjsmål när den behövs.

### Fastinstallerad utrustning

- Hur försäkrar ni att den är fungerar på alla platser när den väl aktiveras?
- Plan för förebyggande underhåll?
- Rutiner för regelbundna kontroller?
- Hur ser ni till att konfigureringar är korrekta över tid?

### Flyttbar utrustning

- Hur försäkrar ni att användarenheter, kringutrustning och tillbehör finns där dem behövs - när dem behövs?
- Plan för förebyggande underhåll, så som underhållningsladdning av batterier?
- Rutiner för regelbundna funktionskontroller?
- Hur ser ni till att konfigureringar är korrekta över tid?

## 4.2 Metodik

I detta kapitel skall ni reda ut hur ni tillser att ALLA berörda parter vet vad dem skall göra när reservkommunikationen aktiveras.

### Ansvar

- Finns det en ansvarig för beredskapskommunikation?
- Är frågan förankrad i ledningen?
- Ingår reservkommunikation i kris- och kontinuitetsplaner?

### Rutiner

- Finns systemet dokumenterat i detalj?
- Finns det checklistor för driftsättning?
- Finns det lathundar för användning?
- Finns felsökningsscheman?
- Finns manualer för underhåll och reparation?

### Övning

- Planerar ni för regelbunden träning?
- Kan systemet användas under "skarpa" verksamhetsövningar?
- Inkluderar övningsplan möjlighet att träna på olika scenarion?

# 5. Avslutning

Vi nämnde det redan i första artikeln i denna serien, men det tål att upprepas; "Eftersom hotbilder, behov, krav och tekniska möjligheter förändras konstant så utvecklas också behovet av åtgärder. För att bibehålla resiliens och beredskap över tid så krävs kontinuerligt arbete."

***Även denna artikelserie och dess innehåll kan bli irrelevant på sikt – trots att vi försökt vara så generella som möjligt.***

## Glöm inte ordinarie kommunikation

Även om ni har ett reservsystem som framtaget enligt konstens alla regler så nonchalera inte era ordinarie kommunikationssystem. Se till att stärka upp dessa och gör dem motståndskraftiga mot identifierade risker och hot. Ju längre ni kan bibehålla ordinarie kommunikation i drift desto enklare blir det rimligtvis att hålla verksamheten i gång under incident, kris och krig.

- Länk till Checklista för robust kommunikation

## Plan C

Som vi nämnde alldeles i början så är inga system hundraprocentiga - inte ens reservsystem. Med andra ord kan det vara värt att utforma rutiner och arbetssätt även för scenarion där ingen teknik finns att tillgå.

# Om Celab

+46 (0)303 24 60 00
info@celab.se
https://celab.se

Celab Communications AB är ett företag inom Tången-gruppen som sedan starten 1978 upplevt stora framgångar inom verksamhetskritisk kommunikation.

Med det menar vi kommunikationslösningar för organisationer där sambandet är avgörande för verksamhetens framgång och/eller medarbetarnas säkerhet.

Företagets affärsidé är att tillhandahålla kommunikationssystem baserade på världsledande utrustning som genom vår unika kompetens utvecklas, förädlas och optimeras specifikt för våra kunder och deras unika verksamhet.

Celab COMMUNICATIONS

**Huvudkontor** Rollsbovägen 20, 442 40 Kungälv
**Stockholm** Elsa Brändströms gata 56, 129 52 Hägersten
**Karlstad** Lagergrens gata 2, 652 26 Karlstad