Celab
COMMUNICATIONS

Guide to reliable backup communications

How do you ensure that your organisation continues to function when the primary communication system is no longer available?

Guide to reliable backup communications

How do you ensure that your organisation continues to function when the primary communication system is no longer available?

Although all organisations work more or less actively to protect their infrastructure and systems, there is an uncomfortable truth: no system is one hundred percent reliable.

You are probably reading this because you are part of an organisation that has already recognised and accepted this fact, and has identified the need for a Plan B — in other words, a backup communication system.

This article is part of a series intended to help you "bulletproof" your mission- or business-critical communications environment. We recommend reading the articles in the following order:

- Introduction to Preparedness Communications — Why prepare?
- Guide to Risk Analysis for Communication Systems — What can go wrong?
- Guide to Robust Communication Systems — What can we do about it?
- Guide to Reliable Backup Communications — What do we do when that is still not enough? (this article)

The overall purpose of this article series is to give you a number of "lenses" through which you can examine your communications environment, making it easier to identify appropriate measures for your specific conditions.

Backup communications are, in practice, almost unique to each purpose and need. In some cases, securing voice communication is sufficient. In other cases, data connections are also critical.

Examples of backup communication systems:

Primary communication	Potential backup system
National public safety coms (like Rakel)	Standalone radio system, such as DMR or HF radio; DMO-based solution
Telephony / public networks	National public safety networks, private cellular, standalone radio system such as DMR or HF radio, infrastructure-free solution
Private / dedicated cellular network	Standalone radio system such as DMR or HF radio, infrastructure-free solution
Standalone radio system	Other radio system such as DMR or HF radio, infrastructure-free solution

Finding the right backup system requires a structured review of your specific situation, and this checklist is intended to help you along the way.

1. Risk and Vulnerability Assessment

Strictly speaking, backup communications are only necessary when your primary communications environment cannot eliminate or manage the risks you face.

A suitable way to evaluate this is to carry out a risk and vulnerability assessment of your current communication system, or systems — something we cover in article 2 of this series.

If the review shows that your systems, and by extension your organisation, cannot meet internal requirements and/or external expectations, you are in the right place.

2. Needs Assessment

A backup communication system does not need to do everything, but you must determine what is essential and what is unnecessary in precarious situations.

In short, you need to decide:

- **what the system must be able to do**
- **under which circumstances the system must be able to do it**
- **in which way, or ways, the system must be able to do it**

Below is a non-exhaustive list of aspects and questions to consider in order to design backup communication systems that work when they are needed.

2.1 Scenarios

First and foremost, you need to determine under which circumstances the backup communication system will be used. This defines the external boundaries for the questions and decisions that follow.

- **What conditions apply when the backup communication system is to be used?**
- **Which triggers are relevant — what needs to happen for the backup system to be activated?**
- **How long is the backup system expected to be used once it has been put into operation?**

Do not forget to identify and assess any external expectations from customers, citizens, authorities or other important stakeholders. These directly and indirectly influence the scenarios you need to consider.

2.2 Participants

Under this heading, you should identify and list all entities that need to use the system during the scenarios that have been defined.

People

- **Which internal individuals — or roles — need to communicate with each other?**
- **Who needs to lead, speak and listen, respectively?**
- **How do they need to be able to reach each other in practical or organisational terms? Not technically.**
- **Do they need to be able to send messages or data to each other?**

Applications and Equipment

- Do you have command-and-control support systems, camera systems or other equipment that need to remain available during the listed scenarios?
- How does this equipment need to be available in practical terms? Not technically.
- What performance is required in order to use the application or equipment?

Collaboration

- Do we need to keep channels open to external parties such as authorities, suppliers or customers?
- Can we use their systems, can we provide ours, or do they need to be integrated?
- Which external individuals or equipment may be affected?

2.3 Functions and Features

You now need to determine which communication methods and features need to work, or must work, in order to satisfy the needs above in the relevant scenarios.

Voice Communication

- Emergency calls
- Group calls
- Individual calls / telephone calls
- Prioritisation

Messages

- SMS / SDS
- Status

Connections

- Alerting?
- Case management?
- Database?
- Intranet?
- Internet?

2.4 Availability

Here, you need to determine when, where and how the system must provide its function during the defined scenarios.

Access

- How and when does the system need to be available?
- Do different participants need different permissions and/or priorities?

Coverage and Capacity

- Where does the system need to be available?
- What needs to be available at each location?
- Can the need change, and if so, how might that happen?

3. System Selection

Once you have compiled the needs that must be covered and the risks that must be avoided, this must be translated into a requirements list in order to evaluate and identify suitable systems.

This is not only about identifying the right technical platform. It is also about avoiding bottlenecks, single points of failure and other potential vulnerabilities before implementation. Poor system design, components and installations can have major consequences that may not be discovered until it is too late.

- **A classic pitfall is that the "backup solution" shares vulnerabilities with the primary system. These bottlenecks may be obvious, but they may also be hidden. The systems may share a fibre connection, a server or a fuse.**

The task, therefore, is to choose a supplier that not only understands the technologies, but also has relevant experience of delivering a robust business-critical installation.

Once a system proposal has been produced, it may be appropriate to carry out a "simulated" risk and vulnerability assessment before ordering, in order to identify potential issues before they materialise. This review can preferably be carried out together with the supplier to ensure that you have a shared understanding of the challenges.

4. Preparations

Backup communications are not only about technology. They are about the ability to lead, make decisions and collaborate when everything else fails.

This means that the work is not complete once a needs-based system has been installed. In order to be prepared for the scenarios in which the system will be used, there are additional questions to consider to ensure that the system actually delivers the assurance it is intended to provide.

4.1 Logistics

By "logistics", we mean ensuring that all relevant backup communication equipment is operational and available without delay when needed.

Fixed Installed Equipment

- How do you ensure that it works at all locations once it is activated?
- Is there a plan for preventive maintenance?
- Are there routines for regular function checks?
- How do you ensure that configurations remain correct over time?

Portable Equipment

- How do you ensure that user devices, peripheral equipment and accessories are available where they are needed — when they are needed?
- Is there a plan for preventive maintenance, such as battery maintenance charging?
- Are there routines for regular function checks?
- How do you ensure that configurations remain correct over time?

4.2 Methodology

In this section, you should clarify how you ensure that all affected parties know what to do when backup communications are activated.

Responsibility

- Is there someone responsible for preparedness communications?
- Is the issue anchored in management?
- Are backup communications included in crisis and continuity plans?

Procedures

- Is the system documented in detail?
- Are there checklists for commissioning?
- Are there quick-reference guides for use?
- Are there troubleshooting flowcharts?
- Are there manuals for maintenance and repair?

Exercises

- Do you plan for regular training?
- Can the system be used during live operational exercises?
- Does the exercise plan include the possibility to train for different scenarios?

5. Conclusion

We mentioned this already in the first article in this series, but it is worth repeating:

"Since threat landscapes, needs, requirements and technical possibilities are constantly changing, the need for appropriate measures also evolves."

Maintaining resilience and preparedness over time requires continuous work.

This article series and its content may also become irrelevant over time, even though we have tried to keep it as general as possible.

Do Not Forget Primary Communications

Even if you have a backup system designed according to best practice, do not neglect your primary communication systems. Make sure to strengthen them and make them resilient to identified risks and threats.

The longer you can keep primary communications operational, the easier it will reasonably be to keep the organisation running during incidents, crises and war.

Plan C

As we mentioned at the very beginning, no system is one hundred percent reliable — not even backup systems. In other words, it may be worth designing procedures and working methods for scenarios in which no technology is available.

About Celab

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

Celab Communications AB is a Swedish company within the Tången Group that, since its founding in 1978, has achieved significant success in mission- and business critical communications.

By this, we mean solutions for organizations where reliable communication is essential to operational success and/or employee safety.

The company's foundational concept is to provide communication systems based on world-leading equipment, which, through our unique expertise, are developed, refined, and optimized specifically for our customers and their unique operations.

Celab COMMUNICATIONS

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