Guide to Risk Assessment for Communication Systems

How can you ensure that you do not miss anything when evaluating your critical communications environment?

Guide to Risk Assessment for Communication Systems

How can you ensure that you do not miss anything when evaluating your critical communications environment?

The short answer, unfortunately, is that you cannot. But by carrying out a thorough and carefully considered current-state analysis, you can minimise false confidence and maximise the resilience of your communications in order to prepare the organisation as effectively as possible.

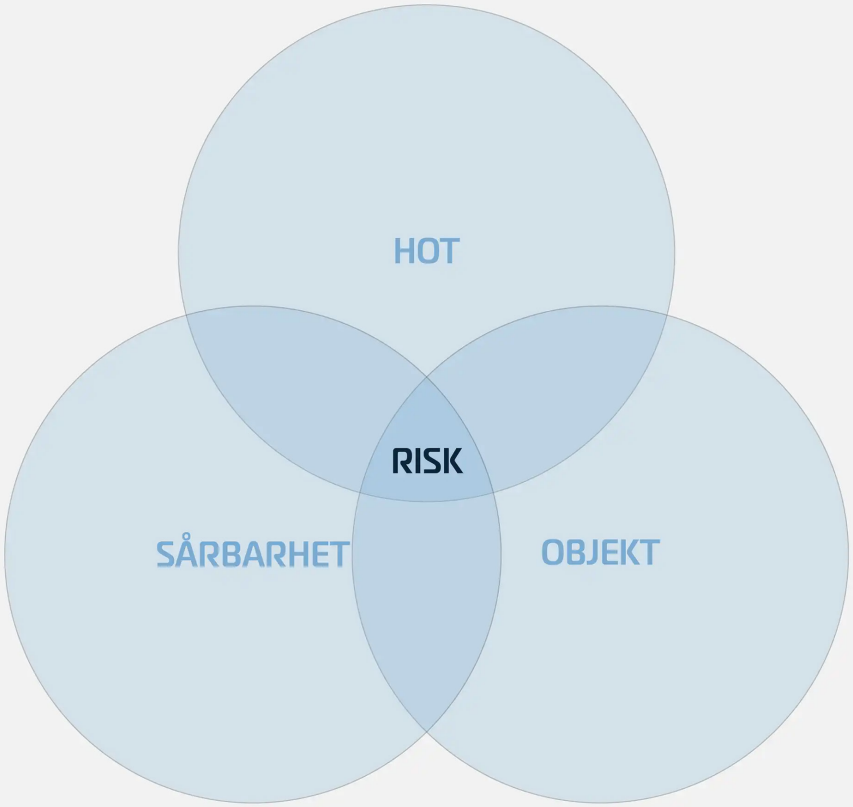
This article is part of a series intended to help you "bulletproof" your mission- or business-critical communications environment. We recommend reading the articles in the following order:

- Introduction to Preparedness Communications — Why prepare?
- Guide to Risk Analysis for Communication Systems — What can go wrong? (this article)
- 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?

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.

Risk and Vulnerability Analysis

As with all risk analyses, this part of the process is intended to identify and assess risks and threats — but with a specific focus on your communications environment.
We cannot provide the answers for you, but with this "checklist" we hope to help you design a risk analysis and methodology that suits your organisation and your communications environment.



Hot	Potentiell incident utanför objektet som kan medföra påverkan.
Sårbarhet	Brist i det analyserade objektet som möjliggör ett hot.
Konsekvens	Påföljden om hotet realiseras.
Objekt	Systemet som granskas.
Risk	Variabel som utgör resultatet av bedömningen.

HOT → utnyttjar en → SÅRBARHET → som leder till → KONSEKVENS → vilket utgör en → RISK

Define the Object

Initially, you need to limit the scope of your analysis by deciding which system, or systems, should be reviewed. This means defining the system, its components and its boundaries — for example, "the TETRA system" or "the private mobile network".
It becomes much easier to focus on threats that are relevant to the object in question if all objects and their components are clearly documented.

Identify Threats

You need to identify and list all potential events that could limit or eliminate your ability to use the object in question — both large and small.

This includes all potential hazards, regardless of whether they arise from accident, negligence or malicious intent. It also does not matter whether they are caused by internal or external circumstances. "Everything" may be relevant and should be evaluated and documented.

Method

Map the object

Describe the object, its process, function and constituent parts.

Brainstorm threats

Assemble a group with different areas of expertise to identify what could go wrong.

Available data

Is there relevant statistics or documentation?

Seek support

Can you get help from internal experts, industry organisations, authorities, consultants or suppliers?

Threat Landscape Matrix

Category / Cause	Examples	Accident	Negligence	Intentional act
Availability / Outage	Power outage, no internet, locked system	Storm, lightning strike, bug	Cable damage, disconnected server, incorrect handling	Sabotage, ransomware
Performance / Disruption	Poor reception, congestion, buffering	Interference from other systems, hardware deficiencies	Underdimensioned capacity and/or component	Jamming, overload attack
Confidentiality / Integrity / Leakage	Exposed information, manipulated data	System fault, bug	Insufficient procedures, insufficient access management	Espionage, MiTM, intrusion, phishing, insider

In the matrix, potential threats are broadly grouped according to the type of problem that may occur, shown on the Y-axis, and the underlying cause, shown on the X-axis.

Depending on your specific conditions, the different threats will be more or less relevant.

Evaluate Vulnerabilities

This step is about evaluating the object's current weaknesses — specifically in relation to the threats already identified.

For each individual threat, one or more vulnerabilities need to be linked. In other words, deficiencies that the selected threats can exploit in order to materialise.

Method

Map the object

Review specifications, drawings, system descriptions, and so on.

Available data

Is there information, templates, best practices, etc. available?

Seek support

Can you get help from security experts, authorities or suppliers?

Assessment Matrix for Vulnerabilities

Area / Significance	Negligible	Significant	Acute
Technical	Acceptable emergency power	Insufficient emergency power, outdated firmware, expired antivirus, insufficient encryption	Single points of failure, zero-day
Physical	Acceptable perimeter protection	Insufficient perimeter protection	No perimeter protection
Organisational	Acceptable password management	Insufficient access management	No access management
Human		Social engineering	Weak passwords

The matrix can be expanded with more levels to make it more granular.

Assess Consequences

Now it is time to determine the consequences if the threats you have identified actually materialise.

Here too, the consequences must be investigated, evaluated and documented for each individual risk. Since the severity of consequences can differ significantly depending on how long they last, it is important to include a time perspective.

For power outages, it may even be useful to treat them as different threats depending on duration.

Another time-related perspective to consider is how long you need to be able to manage on your own before external support can be expected.

Assessment Matrix for Consequences

What / Severity	None	Limited	Moderate	Serious	Critical
Availability / Outage	-	Momentary power outage	Short-term power outage	Long-term power outage	"Permanent" power outage
Performance / Disruption	-	Intermittent disruptions	Insufficient reception or bandwidth	Deficient reception or bandwidth	No reception, coverage or bandwidth
Integrity / Confidentiality / Leakage	-	-	Loss of sensitive information	Loss of confidential information	Loss of secret information

The matrix can be adapted with more or fewer levels and groups.

"Those who conduct essential services must — individually and in collaboration — strengthen their ability to maintain the most important societal functions primarily using their own resources for at least two weeks."

from Preparedness for businesses — If crisis or war comes, a guideline from the Swedish Civil Defence and Resilience Agency

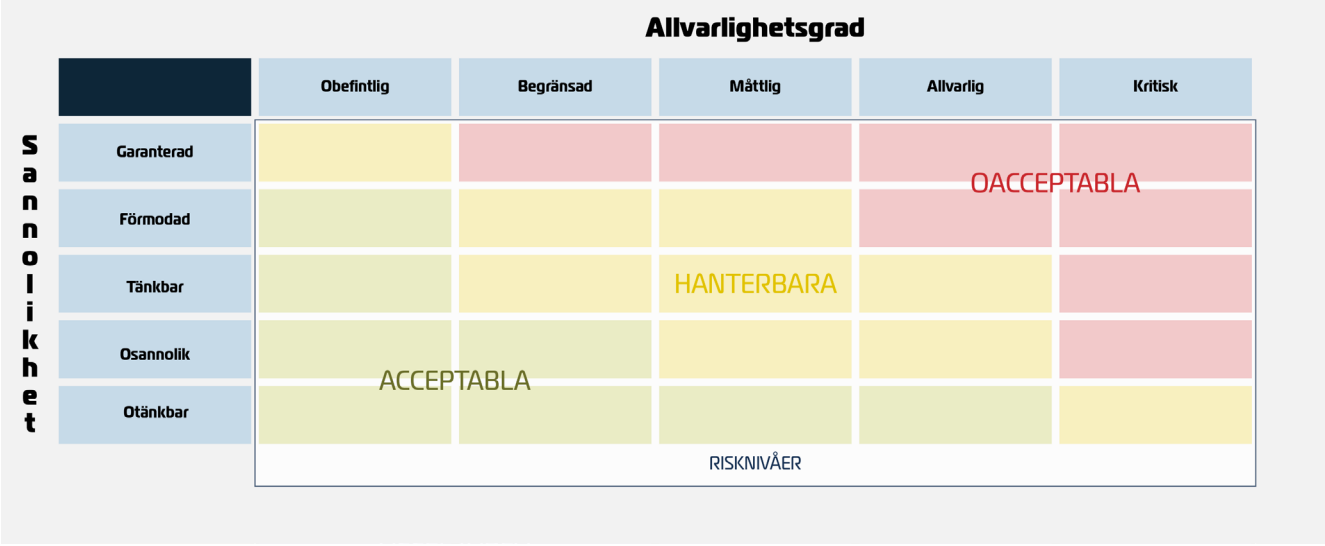
Evaluate and Prioritise Risks

Once you know which threats you face, which vulnerabilities you have and which potential consequences you risk, you can finally determine the risk levels and thereby obtain a priority list to work from.

This can be done by weighing the probability of each individual threat occurring against the "severity" that the specific threat represents.

Probability can be estimated by comparing the threat and the vulnerability, while severity is linked to the consequence.

Assessment Matrix for Risk Levels



The matrix can be adapted with more or fewer levels of severity and probability.

If you assign a value to the different steps on each axis, the figures can be multiplied to create a simple way to prioritise your measures.

Conclusion

Blind Spots

It is "easy" to prepare for scenarios that you or someone else in the organisation has experienced, but it is at least as important to prepare for those you have never faced.

There are three types of risk awareness:

- **The risks you know about and have under control.**
- **The risks you know about but do not control.**
- **The risks you neither know about nor control.**

To cover all categories, we likely need to think outside the box and maintain a dialogue with external parties.

Next Steps

Once you have compiled all the data, you will likely have a very good picture of your situation, your needs and the measures required.

If your analysis shows that:

All risk levels are acceptable

No further action is necessary.

Unacceptable risk levels remain despite implemented measures

Acquire or improve a backup communications system.

- **See our Guide to Reliable Backup Communications.**

Risks need to be managed or eliminated

Improve the existing, regular communications system.

- **See our Guide to Robust Communication Systems.**

Certain risk levels cannot be reduced

Acquire a new regular and/or backup communications system.

- **Contact us for a review and needs analysis.**

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