ISPT WHITEPAPER

FIVE STEPS TO RESILIENCE

Industrial IoT & Cyber Security

The Netherlands 2019

Institute for
Sustainable
Process Technology

Table of contents

Preface: Digitization

Within ISPT, the Institute for Sustainable Process Technology, we explore solutions for a sustainable future through cooperation between industry, universities and research institutes. With Industry 4.0 we entered a digital transformation, which is there to stay and will give us new possibilities in factories and across value chains. Connected factories exchanging data in interaction with each other. This transformation has huge potential but also obliges us to build new skills to be able to apply the new technology and to consider risks and new vulnerability. With this 5-step plan organizations can check their approach towards digital vulnerability. I am are very pleased that this booklet is now available and was introduced and applied in ISPT innovation projects. It is a good example of cooperation and information exchange to become frontrunners in the implementation of the Industry 4.0 topics.

Tjeerd Jongsma

director ISPT

The digital revolution is taking place in every sector. Also, in the energy sector. We do not achieve the goals of the energy transition just by using traditional energy technology. Digitization has to play an important role in the transition. It will realize large energy savings using automatic control. But this increasing automation also requires attention to the security of our energy infrastructure. That is the reason why approaches as described in this booklet can play an important role in maintaining security and taking advantage of the digital technologies at the same time.

John Post

Programmadirecteur digitalisering Topsector Energie

TOPSECTOR ENERGIE
Empowering the new economy

Introduction

The Ministry of Economic Affairs and Climate Policy started the program ICT resilience (Telekwetsbaarheid). The aim of this program is to make users of telecommunication services aware of their dependency to telecom and the risks thereby incurred. The program seeks to provide user-directed advice on how to diminish this risk.
Within the program research has been carried out with partners from various sectors such as ISPT & TSE. Whenever possible, already existing instruments have been employed or adapted. If no appropriate instruments were found, new ones have been created, e.g., the Raster method, assessment techniques and checklists.

All experiences, lessons, instruments and expertise have been brought together under one framework. This framework provides a coherent set of five steps that ensures organizational resilience against telecom failures. We refer to this framework as the Five-Step Plan.
By employing the Five-Step Plan, an organization can become aware of its dependencies to telecommunication, it can investigate the risks of failures or disruptions and it can choose appropriate administrative measures that are maintained during transitions (of telecom services or within organizations).
This document describes the Five-Step Plan for industry.

Reading guide

The document has three parts.

The Five-Step Plan: describes the framework of the Five-Step Plan and provides indications for its use in practice;
Instruments: describes each available instrument within the framework;
Appendices: examples, templates and other additional information.

THE FIVE-STEP PLAN

Overview of the plan

Introduction

Factories are dependent on various telecom services: Internet, cloud services, cloud-based services, GPS, camera surveillance, telemetry, remote controllers, fire alarm systems, radio relay systems, wireless microphones, satellite communication. The list is endless. Telecommunication is a basic need.

Telecom providers aim to deliver their services failure-free. They have an interest in providing failure-free services as disruptions can be expensive and be harmful to their image. However, failure cannot always be prevented. Something can always go wrong: power cuts, software errors, cables being damaged during excavation, individual mistakes or other deficiencies.

The effects of service failure will not only be visible in the infrastructure. They can lead to social problems and even serious disruptions. Public transportation stands still, production stops, emergency services are obstructed, logistical coordination fails, and communication becomes impossible.

Citizens and organizations therefore need to be prepared so that they are not alarmed by such incidents. Essential organizations and critical infrastructure providers need to be able to provide their services. Organizations need to be aware of their dependencies and vulnerabilities in order to take appropriate measures. All this starts with creating awareness. And since telecom and organization change, awareness must be constantly maintained.

In practice, it turns out to be difficult for organizations to achieve this. Knowledge of telecommunication and ICT dependencies is meagre and there are no ready-made measures that can be applied by laymen. The Five-Step Plan offers a solution in this regard.

Target group

The Five-Step Plan is primarily written for the process industry. But in general, it is useful both for commercial and non-commercial organizations, for businesses and non-profit institutions. It can be applied in both small and large institutions, irrespective of their telecom usage. Within an organization, the Five-Step Plan is particularly directed at policy-makers and managers that are in charge of continuity, crisis management, telecom and IT.

Framework

The Five-Step Plan is a framework. This means that it offers a structure within which different methods and tools are integrated in a logical manner. The Five-Step Plan thus consists of a structure ("What do you need to do and in what order?") and an implementation toolkit (a series of tools that can be applied).

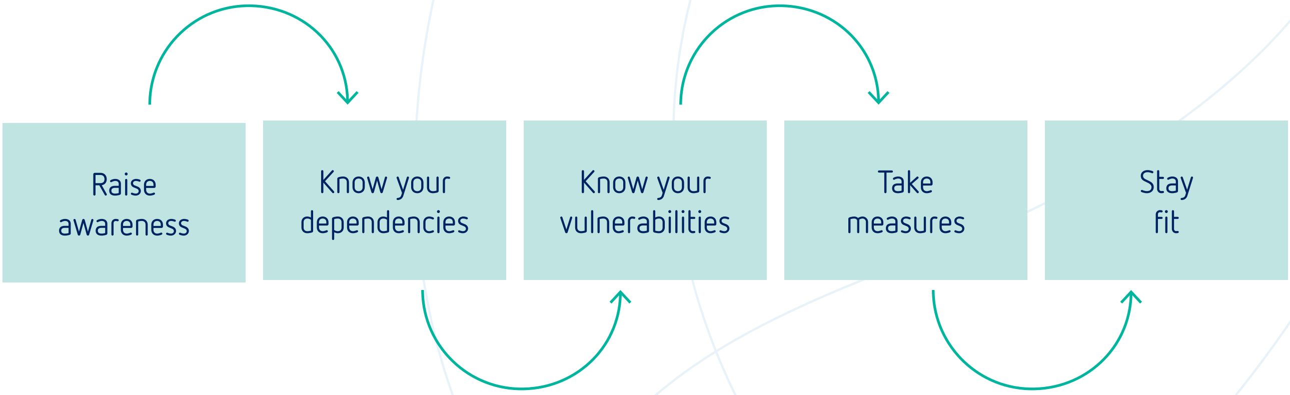


Figure 1: Overview of the five steps

The steps

How do I prepare for failure?

BE AWARE

Step 1: How do I raise awareness in my organization?

You must realize that your organization is dependent upon internal ICTs and telecom in a variety of ways. Even in processes and locations where you would not expect it. Discuss with colleagues to discover the necessary information.

- **What kind of ICT & telecommunication systems exists in my organization?**
  Telecommunication is very broad. Not only (mobile) telephones but also data connections between locations (VPN), Internet and inter-nal SCADA systems. Perhaps you make use of transceivers, intercom access or manage entrances from a distance. All of this is telecommunication.

- **What is the available information and where can I find it?**
  The website of the Radiocommunications Agency provides a lot of information. There you can find an introductory video about our daily dependence on telecommunication and the impact of malfunctions. Additionally, a PDF document provides information on the consequences of telecom disruptions failures for small businesses and contains advice on possible solutions.

- **How do I ensure that my organization sees the importance of preparing for telecom failures?**
  Discuss the risks of disruptions within your organization. Provide examples from the Radiocommunications Agency website. Were there any examples of previous incidents? Discuss these within your organization.

KNOW YOUR DEPENDENCIES

Step 2: What are dependencies within my organization?

Sometimes services can become ‘hidden’, meaning that it is not immediately clear in what way (if at all) they are dependent on telecom. Examples are the alarm within the lift or the fire alarm system. Search all telecom processes within your organization.

- **What are our organizational processes and which of these make use of telecom?**
  Answer this question with all departments. What are they doing? Who are their contact persons and how do they communicate with these persons?
  Create a matrix of processes and telecom services. Divide processes into three categories: 1) primary processes, 2) supporting processes (such as ordering goods), 3) building processes (access, fire alarm etc.).

- **Which processes are essential?**
  The disruption of essential processes can affect the organization financially or it can affect its image. Determine the importance of each processes by dividing them into three levels of importance (low, medium, high).

- **Which telecommunication services are essential?**
  Based on the previous steps you can determine the impact of communication services disruption.

KNOW YOUR VULNERABILITIES

Step 3: What are the vulnerabilities in my organization?

In this step, you investigate your organization's risks regarding telecom disruptions. Does more than one cable run through the same pipe? Can a disruption be endured long enough?

- **How can I limit the risks within my organization?**
  Determine your companies' risks using checklists, historic incidents and carry out training exercises.
- **Do you want to carry out an extensive analysis?**
  Apply the Raster method. Raster is a graphic tool with which your organization can gain insight into how telecommunication is physically built and where the disruption risks appear.
  More information on www.risicotools.nl.

TAKE MEASURES

Step 4: How do I diminish risks?

Risk management is always a matter of weighing options. Focus therefore on the most essential risks.

- **How can I reduce the risks?**
  Measures against risk can be technical, organizational or a combination of the two. Technical measures generally diminish the chance of a disruption; organizational measures generally diminish the negative effects of a disruption.

- **Which measures can I take?**
  Some measures are simple and inexpensive. Can employees for example fall back on traditional work processes? Other solutions are technical such as the pager or the satellite telephone. Take care that these technical solutions do not create new risks.

STAY FIT

Step 5: How do I recognize new risks?

Risk management is not a one-off activity. After all, through technological innovation, new risks can emerge. Make sure that the subject stays on the agenda.

- **Repeat:** telecommunication keeps innovating, your organization keeps changing. Repeat steps 2 to 4 above regularly, especially after changes in technical and organizational processes. Consider a factory that starts production of a new product or a health institution that incorporates a home care institution.

- **Practice:** Practice makes perfect. Practice leads to new knowledge, awareness and increase trust in your organization.

- **Learn:** Never waste a good crisis. Make use of past incidents in order to learn from them. What went well? What could be improved? Are the measures efficient? Do employees intervene properly? Evaluate the lessons you've learned!

Overview

The Five-Step Plan is similar to a cooking recipe: you have to start at the beginning, and you cannot skip steps. If your organization has carried out significant preparatory work (e.g. if an inventory of telecommunication services is already made), then you can reuse this work during the five-step process. In this case, the Five-Step Plan will not lead to significant additional workload. But do not to assume too easily that the necessary activities have already been carried out.

Be aware	• Film • Presentations • Quick scan • Monitoring incidents • Science Café
Know your dependencies	• Interviews • Brainstorm • Checklists
Know your vulnerabilities	• Raster • Checklists
Take measures	• Alternatives tool • Checklist • Interactive PDF
Stay fit	• Training and practice • Serious Game • BCM

Step 1: Raising awareness

'The program Televulnerability is an authority in The Netherlands within the field of (social) continuity during telecom disruptions. The program keeps developing and shares acquired knowledge and experience with the relevant target groups. The program conceives itself as one of the network players, meaning that the acquired knowledge is not only shared with target groups but also seeks to embed this knowledge within organizations. In order to achieve its goals, the program wishes to engage partners within specific sector organizations.' (Source: TKW Content Plan)

In the following steps, it is necessary that parties allocate time in working on their Televulnerability. Creating awareness is necessary for motivating people to become active in this regard and take their organizations along with them. In the content plan, five public groups are mentioned. Two of these are especially important:

- Managers and employees that are (or feel) responsible for telecom disruptions. They seek to increase the organization's resilience but are not yet aware of all vulnerabilities. They want general information on the program and want to distribute this within their organization.

- Managers and employees that deal with telecom and disruptions. These employees investigate vulnerabilities and are interested in applicable tools and methods.

Framing

A problem can be framed in a variety of ways depending on the context.

Main idea/approach	Sample text	Instrument/Efficiency
Formal authority/ competence.	The State Secretary of Economic Affairs proposes that The Netherlands has an infrastructural problem.	Useful for allocating assets.
Knowledge authority on televulnerability.	A Telecom Authority concludes that networks are stable, but users are insufficiently prepared for disruptions.	"Tele-vulnerability" section from the AT website, presentation.
Innovation but 'design for resilience' or preparation.	The Netherlands is a modern, well-organized society which innovates, but...	A positive frame in which the problem is introduced. See the movie.
Incidents occur and have consequences.	It is quiet in Rotterdam. The city awakes. The baker bakes. Birds chirp. But the trams are not running (the Waalhaven failure).	Incident monitoring/ Storytelling/ Complex dependencies become visible during malfunctions (leaking layers of abstraction).
Safety culture, with a focus on ICT. Branch-specific.	The chemical industry prioritizes safety for personnel, inhabitants, environment but also for business continuity.	Join dialogue within the sector. For example, with the Knowledge Café.
As a cybersecurity issue.	The phrase CIA ('Confidentiality, Integrity & Availability) is often used in the cybersecurity sector. Availability is an often-ignored issue.	Capitalize on global trend toward cybersecurity. You focus, however, on only one small part of the greater whole. An advantage of this is that resources are already reserved.
Penny wise? Pound foolish!	It doesn't have to be expensive. It can still prevent distress. It can be organizational.	The costs of failure to increase telecom resilience outweighs the costs of the action.

Instruments

	Effort	Complexity	Page
Film	*x – – – –*	*x – – – –*	*20*
Presentations	*– x – – –*	*– x – – –*	*21*
Incident monitoring	*– – – – x*	*– – x – –*	*22*
Science café	*– x – – –*	*– – – x –*	*23*
Quick scan	*x – – – –*	*– x – – –*	*24*

Appendix

- Appendix C: sample matrix for organizational processes and telecom services

Step 2: Dependencies

After creating awareness, the next logical step is to map out the organization’s dependence on telecommunication. In this regard, keep in mind that ‘telecommunication’ does not only stand for telephone. It includes for example internet, transceivers, emergency communication, etc. Telecommunication is sometimes hidden in processes and places one would not expect.

The outcome of this step is an analysis that shows work processes within the organization and these work processes’ dependence on telecommunication. The analysis constitutes the point of departure for the actual risk analysis.

This step also covers the important aspect of selecting work processes that are essential to the organization. These are processes that must continue at all times, as opposed to processes that may temporarily be stopped. The degree to which work processes are essential determines which telecommunication services are the most important. In the analysis one should investigate the vulnerability of these essential services. The more essential, the higher the priority.

Instruments

	Effort	Complexity	Page
Telecom-matrix	*– – x – –*	*– x – – –*	*25*
Inventory brainstorm, check-list	*x – – – –*	*– – x – –*	*26*

Appendices

- Appendix B: interview script for preparing interviews
- Appendix C: sample matrix for mapping out business processes and associated telecom services
- Appendix D: checklist for often-used telecom services.

Step 3: Vulnerabilities

Aim

The previous step has resulted in a list of telecommunication services that are essential to the organization. In this third step, you assess the vulnerability of these services. Therefore, you will need to answer the following questions:

- How are telecommunication services built? What are their components: devices, cables, wireless connections etc.?
- How susceptible are these components to power failure, incorrect settings or spontaneous defects?
- What are the biggest risks that need to be addressed?

A multidisciplinary team

Attention needs to be paid not only to the technical probability of failure but also to the effects on various processes in the factory or on the plant. Because of this, it is necessary to involve employees from different departments and levels of the organization. This diversity of members often leads to surprising insights, more so than when the team consists exclusively of IT/OT- and telecom-specialists.

Infrastructure: including yours

Infrastructure includes all hardware of telecom providers. Yet much infrastructure is also your property. Especially the latter creates numerous risks you can resolve yourself. The providers' infrastructure can of course also be exposed to risks: network overload or cloud disruptions are two examples. It is thus necessary to map out all telecom infrastructure: yours in detail, that of providers in broader strokes.

Diagram based on http://amela-po.com/

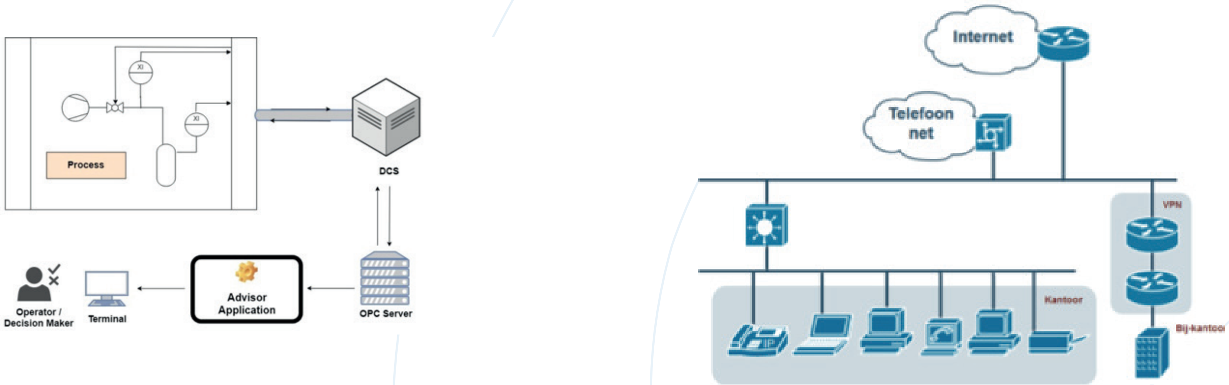


Figure 4: Example of a typical network diagram

The devil is in the details

It might be tempting to only roughly describe the infrastructure. More often than not drawing connections between devices is quite difficult. It is nonetheless necessary to attempt making such drawings as detailed as possible. The more details you leave aside, the more you are forced to merely assume. Assumptions can be mistaken and that's where risks crop up.

In Figure 4 you can see an example of a diagram as often used in IT organizations.
In the diagram, two spaces are represented: the stockroom and the office. In these spaces we find PCs, printers and telephones. Also, there is a room with servers and an internal network to connect all these devices. Through a VPN-network, a nearby office is connected. Telecom providers are connected via Internet and public telephone network. Such a diagram indicates the existing relationships between different parts of a network. Yet it does not provide enough details.

Figure 5 reproduces the current situation much more accurately. The different servers, for example, seem to run on only one device. Based on the diagram in Figure 5 it is clear that a malfunction on one Ethernet cable (letter f in the diagram) would affect the entire workspace. It is therefore necessary to provide enough detail when diagramming telecom services.

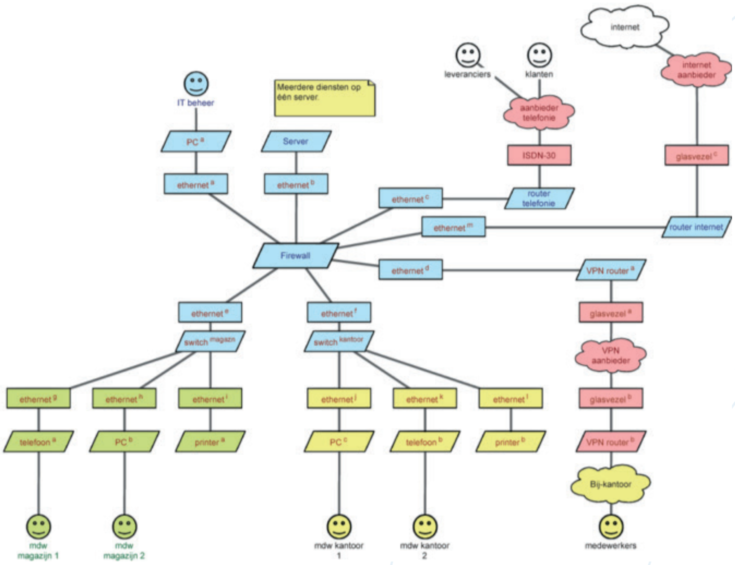


Figure 5: Detailed drawing of the same example

Instruments

	Effort	Complexity	Page
Raster	*− − − x −*	*− − − x −*	*27*
Checklist vulnerabilities	*x − − − −*	*− x − − −*	*28*

Appendix

- Appendix E: checklist with many frequent vulnerabilities and risks

Step 4: Measures

The previous step has resulted in a list of failure risks: the existing vulnerabilities, the possible effects and their probability. In this next step, several measures for dealing with serious risks (risks of great consequences and/or great probability) are discussed. Of course, one can always decide to accept the risk.

Organizational or technical

Control measures can be organizational or technical. An example of a technical measure is the instalment of an emergency line or the double-supply servers. Organizational measures are for example the establishment of emergency procedures, extra personnel, or extra training for personnel.

Costs and benefits

No measure is free: they require effort or even investments. The costs of such measures are known, predictable and transparent. You have to compare these costs to the cost of an incident. The costs of a serious incident are uncertain, but they can be very high. The costs of these measures are like insurance premiums: a small regular cost in order to avoid and survive calamity.

Falling back on manual procedures

Older organizations might have an advantage if they still know the traditional methods from before automation. Yet this approach presumes that the knowledge has remained within the organization. It is questionable whether this can be relied on, as personnel flow throughout the years will diminish the remaining 'old' knowledge.

Old is not always bad

The term 'old' has a negative connotation, but old equipment is not necessarily obsolete. If old devices are properly maintained, components are still available and the employees have the necessary knowledge to use them, there is no reason to reject them. Only when the system shows defects, maintenance becomes a problem, and usage knowledge is lost, old equipment becomes an issue.

Instruments

	Effort	Complexity	Page
Alternatives-tool	*x* − − − −	− *x* − − −	*29*
Checklist measures	*x* − − − −	− *x* − − −	*29*
Interactive PDF	*x* − − − −	− *x* − − −	*30*

Appendix

- Appendix F: checklist with frequently used measures

Step 5: Internalization - Staying fit

Taking measures for resilience is not a one-time activity. The telecom sector is subject to fast innovation and organizations themselves change rapidly, e.g., during reorganizations or when new services are provided. What is safe and reliable now, can be outdated in a few months. It is important to embed attention for televulnerabilities within the organization.

Instruments

	Effort	Complexity	Page
Serious Game	– – *x* – –	– *x* – – –	*31*

Applying the Five-Step Plan

The Five-Step Plan proposes a framework that has proven effective in various sectors such as chemical industry and healthcare. The plan is general enough to be applicable in various organizations, irrespective of size or branch. This chapter provides tips for the application of the plan in different circumstances.

Organizing resilience

For many organizations, telecom resilience adds yet another activity on top of already existing ones. It is therefore tempting to see telecom vulnerability as the problem of IT, crisis management or some other department. Although such departments can manage the issue, it is not strategic to leave televulnerability to only one department. Technical and facilities personnel are typically aware of available control measures and the probability of failures. However, they know little of the existing workflow, the informal workarounds and the possibility of disruptions from a practical point of view.

It is therefore important that employees from all layers of the organization and all departments are involved. The following need to be represented:

- A senior employee from each department.
- Employees from ICT and telecom management.
- Employees from building- and facilities management.
- Employees from quality control and crisis management.
- A member of the management team.

Skills

In order to carry out the Five-Step Plan a project leader is needed. Although the included activities are not per se technical, a leader is capable of maintaining an overview of the application of each tool. It is necessary that the person in question has a basic knowledge in organizational processes and the used telecom services. Additionally, the person needs experience in leading organization-wide projects.

All knowledge of the organization, telecom services and their technical realizations (including vulnerability and effects of disruptions) will come from the project team. Thus, as explained above, a broad team composition is needed.

The implementation of the Five-Step Plan is not particularly difficult. Still, most smaller organizations will choose to outsource the implementation to an organization with expertise in this area. Ask in your branch organizations if it is possible to contact such an expert.

Activating and preserving momentum

A frequent misconception is that televulnerability is the responsibility of someone else: the ICT department, facilities management, or some external provider. This might apply to daily maintenance, but not to the effects of incidents. In case of a disruption, everyone participates in managing the negative effects. It is thus everyone’s responsibility to make the organization resilient.

A necessary condition is continuous and visible attention from the management. Lacking management support, employees might ask themselves whether their contribution is indeed wanted.

A serious incident can be a wake-up call. That is, however, a harsh way of learning, one you would like to avoid. If you think that attention for televulnerability is expensive, compare the efforts with the recovery costs of a serious incident. Instead of learning from an incident in your own organization, you can also learn from branch colleagues. Incident-monitoring and other instruments in Creating Awareness (Step 1) are also useful later in the five-step trajectory. It can be useful to apply these instruments with regularity.

Road map

Depending on the available time resources, a subset of these instruments can be deployed.

	Short and sweet	Thorough and complete
Step 1	*Film* *Presentation* *Quick scan*	*Incidents monitoring* *Knowledge Café* *Quick scan*
Step 2	*Inventory brainstorm and checklist*	*Telecom-matrix*
Step 3	*Checklist vulnerabilities*	*Raster*
Step 4	*Checklist measures* *Alternatives-tool*	*Raster* *Alternatives-tool*
Step 5	*Serious Game*	*Serious Game*

Figure 6: Road map for the instruments

Instruments

	Effort	Complexity	Page
Step 1			
Film	x − − − −	x − − − −	20
Presentations	− x − − −	− x − − −	21
Incident monitoring	− − − − x	− − x − −	22
Science café	− x − − −	− − − x −	23
Quick scan	x − − − −	− x − − −	24
Step 2			
Telecom-matrix	− − x − −	− x − − −	25
Inventory brainstorm and checklist	x − − − −	− − x − −	26
Step 3			
Raster	− − − x −	− − − x −	27
Checklist vulnerabilities	x − − − −	− x − − −	28
Step 4			
Alternatives-tool	x − − − −	− x − − −	29
Checklist measures	x − − − −	− x − − −	29
Interactive PDF	x − − − −	− x − − −	30
Step 5			
Serious Game	− − x − −	− x − − −	31

Step 1: Film

Effort	*fast and cheap*	*x – – – –*	*length or duration*
Complexity	*simple*	*x – – – –*	*difficult*

What is it?	*A short, colourful and positive animation movie.*
What does it deliver?	*What is 'televulnerability' and why is it important?*
When to use?	*To provide an introduction to new employees.*
How does it work?	*Watch the movie, in a group or individually.*
Whom do I need?	*(does not apply).*
What do I need?	*(does not apply).*
Disadvantages:	*The movie is generic, not specified for certain branches.*
More information:	*Website Radiocommunications Agency.*

In 2016, the Radiocommunications Agency created a movie that explains, in less than 3 minutes, the problem of televulnerability. The movie is useful for communicating to a broad public. The movie is downloadable in Dutch and English, both with subtitles.

For the meeting with the National Coordinator Terrorism and Security (NCTV) a movie was developed together with partners from the Eemsmond Municipality and Chemie Park Delfzijl. This movie is not public but can be used by employees from telecom agencies for training purposes.

In 2019 a new film will be released by Radiocommunications Agency.

Figure 7: Snapshot from the movie.

Step 1: Presentations

Effort	*fast and cheap*	*– x – – –*	*length or duration*
Complexity	*simple*	*x – – – –*	*difficult*

What is it?	*Internal PowerPoint presentation.*
What does it deliver?	*Insight into televulnerability and its importance for an organization.*
When to use?	*To bring the subject to the attention of larger groups. For decision making or starting a large project.*
How does it work?	*Based on available templates, one can create a tailor-made presentation.*
Whom do I need?	*An experienced employee with knowledge of telecom or ICT and presentation skills.*
What do I need?	*PowerPoint Templates.*
Disadvantages:	*Answering questions from the public requires expertise.*
More information:	*Program Televulnerability.*

A classic approach to introduce the subject. Within the program, there is sufficient experience with this approach. The presentation is typically used in combination with the movie and some sample incidents. Upon request, illustrative presentations can be provided. These are generally also useful for partners to arrive at their own story.

Step 1: Incident monitoring

Effort	*fast and cheap*	– – – – *x*	*length or duration*
Complexity	*simple*	– – *x* – –	*difficult*

What is it?	*Keep track of incidents in the organization and branch.*
What does it deliver?	*Overview of risks that have materialized and their effects. Examples to show that risks are not imaginary.*
When to use?	*When there is a need to learn from mistakes and a wish to constantly improve.*
How does it work?	*Incidents are signalled through social media, traditional media, informal conversation and through the network.*
Whom do I need?	*Individuals that signal incidents. Experience with ICT in order to classify the incident.*
What do I need?	*Subscription to social media monitoring systems.*
Disadvantages:	*Very dependent on the level of detail used in monitoring. Requires monitoring over long periods.*
More information:	-

'Never waste a good crisis' or 'Disasters are good for policy-making'. Organizations learn from crises. This way of learning is possibly the most effective path to action. The closer one gets to personal experiences, the easier it gets to find the learning moment. The best examples are given from own experience. The monitoring is ideally carried out by individuals with sector-specific expertise.

In theory, imaginary examples can also be used if they are realistic and plausible. But real cases are more powerful. The Televulnerability program checks weekly for incidents of failures. The program uses the LexisNexis database of regional and national newspapers and makes use of the Coosto analyses of social media. Incidents are also gathered from hearsay.

In some cases, an incident is employed as a case study. One example of such a case study can be found at this address: https://www.inspectie-jenv.nl/Publicaties/rapporten/2012/07/16/storing-telecommunicationnetwerk-waalhaven-rotterdam

Step 1: Science Café

Effort	*fast and cheap*	*– x – – –*	*length or duration*
Complexity	*simple*	*– – – x –*	*difficult*

What is it?	*A workshop for 20-80 people led by experts.*
What does it deliver?	*New and shared insights on how to work on televulnerability.*
When to use?	*At a congress with participants with different backgrounds that do not know each other.*
How does it work?	*In a 1-1,5h session, three experts present their own perspective on televulnerability.* *After that, participants take up the subject and start a deeper discussion on the matter.* *Experts manage this discussion.*
Whom do I need?	*Experts that can present the subject from different perspectives. It is useful to have experts with a lot of practical experience on the subject.*
What do I need?	*A good preparation and a discussion leader. An informal setting to facilitate interaction with the participants.*
Disadvantages:	*Unpredictable outcomes (positive evaluation most of the time).*
More information:	*Background information on Science cafés: http://actioncatalogue.eu/method/7439* *An example in the Netherlands: http://sciencecafedeventer.nl/science_cafe/*

The approach is useful to explore the range of televulnerability within a sector. Experts and practitioners can exchange views on the matter and share examples. This can stimulate participants to further explore the subject on their own.

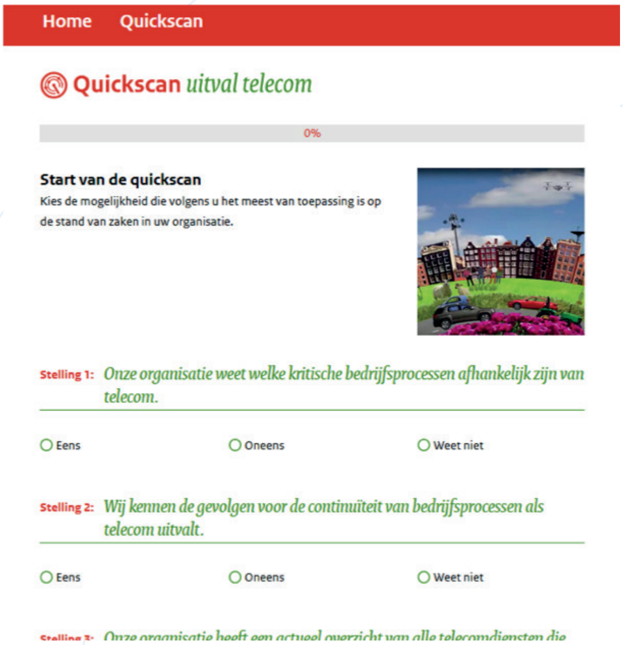
Appendices

- Appendix A: Example announcement of a Science café at a conference on ICT in healthcare

Step 1: Quick scan

Effort	*fast and cheap*	*x – – – –*	*length or duration*
Complexity	*simple*	*– x – – –*	*difficult*

What is it?	*A short anonymous online questionnaire.*
What does it deliver?	*A tailor-made advice on how to increase resilience within an organization.*
When to use?	*Come to grips with televulnerability and start working on it.*
How does it work?	*You fill in the questionnaire and receive tailor-made advice. The scan can be shared on social media.*
Whom do I need?	*The questionnaire is filled in by IT employees or managers (or advisers on management).*
What do I need?	*(not applicable).*
Disadvantages:	*No advice for technical facilities within the organization.*
More information:	-



Quickscan *uitval telecom*

Start van de quickscan

Kies de mogelijkheid die volgens u het meest van toepassing is op de stand van zaken in uw organisatie.

Stelling 1: *Onze organisatie weet welke kritische bedrijfsprocessen afhankelijk zijn van telecom.*

○ Eens ○ Oneens ○ Weet niet

Stelling 2: *Wij kennen de gevolgen voor de continuïteit van bedrijfsprocessen als telecom uitvalt.*

○ Eens ○ Oneens ○ Weet niet

Stelling 3: *Onze organisatie heeft een actueel overzicht van alle telecomdiensten die*

Figure 8: Screenshot of Quick scan.

Step 2: Telecom-matrix

Effort	*fast and cheap*	– – x – –	*length or duration*
Complexity	*simple*	– x – – –	*difficult*

What is it?	*Mapping out work processes and use telecom based on interviews with different employees within the organization.*
What does it deliver?	*Through the discussions with these employees, you create a justified list of (essential) telecom services. The result is a matrix of these vital processes and services.*
When to use?	*When there is no clear view of an organization's processes and used services. When there is enough time to map out these processes.*
How does it work?	*It is based on interviews. It is essential that all departments are targeted in order to get a comprehensive view of work processes. Based on this overview, one can decide which services are taken into consideration within the risk analysis.*
Whom do I need?	*A project leader and employees from your organization, with knowledge of telecom and IT. Employees that employ these services in their primary work.*
What do I need?	*No extra materials are needed for this step.*
Disadvantages:	*It results in a clear diagram of telecom services. It makes it easy to set up priorities in the risk analysis.*
More information:	-

Before taking the interviews, it is necessary to map out which employees have an accurate image of the work-processes within each department and the respective telecom services. A deep understanding of the technical aspects is not necessary.

In most organizations, a distinction can be made between production departments, staff departments and administrative departments. Employees from each of these departments need to be invited for the interviews. In this way, you obtain a complete image of the work processes and telecom services.

At least one person needs to have knowledge of how the ICT is deployed within the organization. Involving crisis teams is advisable as these employees are often aware of procedures during disasters and existing priorities. If during the interviews it appears that other employees have essential knowledge of (or experience with) telecom deployment within the organization, these employees need to be further invited in subsequent sessions.

Determining the level of importance is crucial for the risk analysis. The essential processes in an organization need to continue during a power failure, meaning that their shutdown can lead to immediate problems. Understanding the risks associated with these processes is therefore crucial.

The level of importance of processes differs in each organization. Emergency healthcare is different than a municipality building. Keep an eye on legal regulations concerning obligatory services. It is also important to categorize processes that can be halted for hours as opposed to those that can be halted for days.

During the risk analysis of the essential services, determine also the impact of the power failure on these processes.

In the Appendix, you can find an example of an interview script that can be send to interviewees beforehand. In addition, a series of sample interview questions are provided. These can be used during the group discussion.

Matrix

Based on the interviews, you can create a matrix consisting of: a) the level of importance for each process and b) the level of importance for telecom services relative to each process. An example of such a matrix is given in the Appendix.

One side of the matrix can contain processes; the other side can contain telecom services. By creating this matrix, a clear picture of the current situation can be obtained by crossing the relevant combinations and then indicating importance through colours. Through this marking, the relationship between work processes and telecom services is easily perceived.

Validation

After creating the matrix, the second phase can start. In order to make sure nothing is ignored or marked incorrectly, an interim presentation of results to stakeholders is advisable. During such a presentation, the team can explain the choices made. The future steps of the research can also be discussed with the involved stakeholders.

Appendices

- Appendix B: interviews
- Appendix C: sample matrix for organizational processes and telecom services

Step 2: Brainstorming and checklist

Effort	*fast and cheap*	*x – – – –*	*length or duration*
Complexity	*simple*	*– – x – –*	*difficult*

What is it?	*An inventory of all telecom services employed created through brainstorming and using a checklist of often-employed services.*
What does it deliver?	*A list of often-employed services.*
When to use?	*If you need a quick overview.*
How does it work?	*The group discusses the checklist and fills it in with concrete examples from their own organization. One person summarizes the outcomes by creating a list of the services mentioned.*
Whom do I need?	*Employees from the organization with knowledge of IT and telecom.* *Employees that make use of telecom services in primary processes, staff services and administration.*
What do I need?	*The checklist.*
Disadvantages:	*It is possible to miss services. Also, the list is not ordered according to priority. There needs to be a subjective appreciation of the importance of each service.*
More information:	-

The creation of a telecom matrix can take a lot of time, but the result is a trustworthy analysis that can constitute a basis for further risk analysis. If there is no possibility to do the interviews, there are other methods of mapping out telecom dependencies.

A brainstorm session in a multidisciplinary setting is a simple alternative. In a team where different departments are represented, a list can be made of all the organizational processes and the telecom services necessary for these processes. It is essential to have all the necessary competence participate in the brainstorm session. During the brainstorm, participants employ a checklist with frequently used telecom services.

Appendices

- Appendix D: checklist containing frequently used telecom services

Step 3: The Raster method

Effort	*fast and cheap*	– – – *x* –	*length or duration*
Complexity	*simple*	– – – *x* –	*difficult*

What is it?	*Raster is a method for plotting telecom services and the risk of their malfunction (specified per part).*
What does it deliver?	*The result is a list of the big risks. This can be used subsequently to decide upon the most urgent actions.*
When to use?	*When your telecom services are fairly extensive and there is enough time to map them out.*
How does it work?	*You draw services using a software. Based on a list, each component's risk of malfunction is approximated. An evaluation is also made concerning shared causes of error – these are situations in which more than one device or cable malfunction due to the same cause. Highest risks are selected and prioritized. Repoutational damage can be taken into consideration.*
Whom do I need?	*IT-knowledgeable project leader with experience regarding the Raster software.* *Employees with knowledge of IT, telecom and all organizational processes.*
What do I need?	*Software (free, see link below), data regarding your IT and telecom networks.* *Continuity plans, if available.*
Advantages:	*Creates useful diagrams. Discussions lead to awareness and better insight for all involved.* *Leads to improvements that are practical and efficient.*
Disadvantages:	*It can be difficult to gather all the necessary expertise. A project leader with experience is necessary.*
More information:	*More information: website https://risicotools.nl*

Incidents regarding the availability of telecom services often take place because of malfunctioning components. An underground cable might be damaged, a power cut creates a failure. To avoid these situations, you must first be aware of the existence of those cables and devices. An important component of the Raster method is thus the drawing of a diagram in which all components are visible.

Incidents can also take place when one event leads to the simultaneous failure of two or more components. For example, two cables within the same pipe can be cut during the same accident; a software update can cause servers to stop working. Such situations are known as 'shared causes' and they are dangerous because of their increased impact.

Important steps in the Raster method are the drawing of the services and the evaluation of the probability of impact of individual and shared causes of error. Unlike other methods, Raster does not use a limited, numeric approach to risk. Risks with low probability and significant effect are especially important. These infrequent but catastrophic events are called 'black swans'. Raster helps to expose black swans.

Risk analyses are always partly subjective as information is seldom complete. Raster encourages critical reflection. Uncertainty is normal and evaluations can be tagged as 'unknown' or 'contradictory' if no better judgment can be made. Raster can even be applied when much of the needed information is missing as incoming information can be gradually added.

In order to avoid an incomplete evaluation, the Raster method is applied by a team of experts in which each stakeholder has their own expertise. Raster simplifies the collaboration between experts with different backgrounds. It also simplifies the production of recommendations by using a tested methodical analysis. The recommendations are based on both technical and social aspects (e.g., consequences of failures to external stakeholders).

A full manual for using the Raster method as well as the downloadable software can be found at:
https://risicotools.nl

Step 3: Checklist vulnerabilities

Effort	*fast and cheap*	*x – – – –*	*length or duration*
Complexity	*simple*	*– x – – –*	*difficult*

What is it?	*The checklist is an easy way of getting acquainted with the six most frequent vulnerabilities.*
What does it deliver?	*Depending on the time employed, an evaluation of those risks.*
When to use?	*For smaller organizations or when there is no time or external help to minimize the risks.*
How does it work?	*Each risk on the checklist is discussed with the participants. For each risk, describe the possibility of the risk, its effects and the probability of occurrence. The results are written down and are employed when choosing maintenance measures.*
Whom do I need?	*Senior employees with knowledge of work processes, IT and telecom.*
What do I need?	*The checklist. Technical documentation of the employed IT and telecom services.*
Disadvantages:	*It does not provide a full overview of risks. Some risks can be missed.*

Appendices

- Appendix E: checklist with frequently encountered power-failure risks

Step 4: Alternatives-tool

Effort	*fast and cheap*	*x – – – –*	*length or duration*
Complexity	*simple*	*– x – – –*	*difficult*

What is it?	*An easily searchable tool for all telecom services.*
What does it deliver?	*An adapted list for the chosen application.*
When to use?	*When considering the replacement of a service or when you fall back on alternative services.*
How does it work?	*Filters the list with telecom services based on target group (assistants, consumers etc.), application (safety, business communication, social communication) and content (speech, data, video, etc.). The tool visualizes all telecom services that satisfy the criteria.*
Whom do I need?	*(Not applicable).*
What do I need?	*(Not applicable).*
Advantages:	*Quick and complete overview.*
More information:	*More information: website https://risicotools.nl/en/*

Step 4: Checklist measures

Effort	*fast and cheap*	*x – – – –*	*length or duration*
Complexity	*simple*	*– x – – –*	*difficult*

What is it?	*The checklist contains tips for frequently used measures.*
What does it deliver?	*Ideas and choices for decreasing risk and increasing resilience.*
When to use?	*For smaller organizations or when there is no time or external help to minimize the risks.*
How does it work?	*The measures are discussed with one or two employees. Measures that are useful, acceptable and achievable are then carried out under the supervision of the management team.*
Whom do I need?	*One or more senior employees from the organization with knowledge of work processes, IT and telecom.*
What do I need?	*The checklist. Budget to carry out measures.*
Disadvantages:	*No customization. Control measures for specific risks are not on the list.*

Appendices

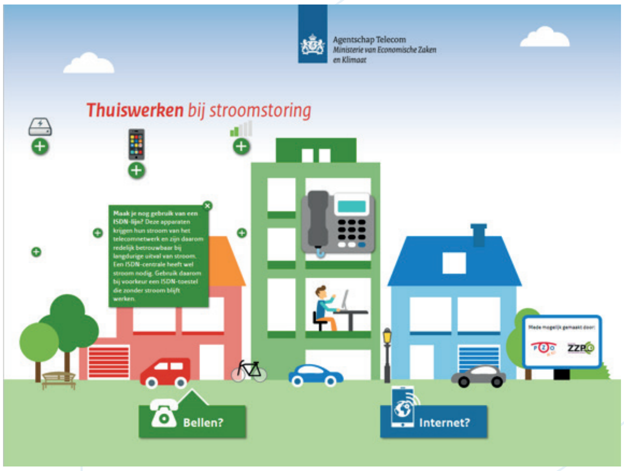
- Appendix F: checklist with frequently used measures

Step 4: Interactive PDF

Effort	*fast and cheap*	*x – – – –*	*length or duration*
Complexity	*simple*	*– x – – –*	*difficult*

What is it?	*A PDF document with tips for freelancers and homeworkers.*
What does it deliver?	*Measures to help minimize the effects of failures.*
When to use?	*Freelancers that work from home. Homeworkers.*
How does it work?	*You can click on items in the PDF in order to get suggestions.*
Whom do I need?	*(Nobody).*
What do I need?	*A laptop or computer to use the PDF.*
Disadvantages:	*Only the most common tips are given.*
More information:	*https://www.agentschaptelecom.nl/onderwerpen/telekwetsbaarheid/thuiswerken-bij-stroomuitval*

The instrument is developed by branch organizations PZO and ZZP Nederland


Agentschap Telecom
Ministerie van Economische Zaken en Klimaat
Thuiswerken bij stroomstoring
Made mogelijk gemaakt door:
Bellen?
Internet?

Maak je nog gebruik van een ISDN-lijn? Deze apparaten krijgen hun stroom van het telecomnetwerk en zijn daarom redelijk betrouwbaar bij langdurige uitval van stroom. Een ISDN-centrale heeft wel stroom nodig. Gebruik daarom bij voorkeur een ISDN-toestel die zonder stroom blijft werken.

Figure 9: Screenshot from interactive PDF.

Step 5: Serious Game

Effort	*fast and cheap*	*– – x – –*	*length or duration*
Complexity	*simple*	*– x – – –*	*difficult*

What is it?	*A work-form in which a group of employees experience the effects of televulnerability based on a simulation.*
What does it deliver?	*Awareness within a large group of employees. Support for measures against vulnerability.*
When to use?	*If the core group has already been acquainted with the subject and wishes to discover more control measures.*
How does it work?	*The Serious Game is in developmental phase.*
Whom do I need?	*(To be determined).*
What do I need?	*(To be determined).*
Disadvantages:	*(To be determined).*
More information:	*(To be determined).*

A Serious Game is particularly appropriate for the creation and maintenance of awareness within an organization. A Serious Game has a serious goal — for example, education or the creation of insight – and combines the achievement of this goal with enjoyable activities. Pleasure makes experience more intense and thus facilitates the sharing of information. There are different variants of such games, from board games and card games to computer games.

Aims

An important aim of the Televulnerability game is the provision of insight to less-experienced employees regarding the seriousness of threats for telecom infrastructure. In addition, all participants acquire knowledge on infrastructure vulnerability and are provided a perspective on how to act upon this.
By gamifying the interaction, the knowledge transfer is more intense than during the presentation of a report. This also ensures that participants remember what is being learned.

The following learning goals need to be achieved:

- Participants acquired more insights regarding telecom risks.
- Participants have more knowledge on the effects of failure on primary work processes.
- Participants have acquired knowledge on how to deal with risks.
- Participants know the tasks and responsibilities of different employees during an incident.

A possible additional result is that existing plans for crisis management can be made more specific based on the insights of the participants from administrative departments.

Form

The game will expectedly run as follows: The game leader discusses the aims and the participants with the commissioner. The participants are invited through internal communication. Participants are assigned roles – either their daily roles in the organization or other roles depending on the learning aims. Then the participants simulate a failure. The choices that the participants make have an influence on the course of events and on the options left to other participants. The game ends with a de-briefing session in which the lessons learned are discussed. The game leader and the commissioner then discuss the game.

The definitive form and the game tools need to be determined.

APPENDICES

Appendix A - Example Science café

In April 2018 a three-day conference was organized on the theme: safe and reliable exchange of data in healthcare. This was organized together with the platform for societal information ECP.

The announcement of the program:

Continuity in healthcare: even if the connection drops

Availability is one of the aspects of cybersecurity (the well-known trio 'Confidentiality, Integrity and Availability' or CIA). Digital exchange of information increases dependence on telecom infrastructure. Reliable as these may be, infrastructures are not free from incidents. Why are some institutions prepared, and some not, to deal with power disruptions? What measures can be taken within a healthcare facility in order to diminish the effects of a failure? Is it possible (or desirable) to fall back on 'old' systems? And what processes are dependent on telecom?

Three experts share their experiences with telecom disruptions and answer questions from the room. The session will be led by Jako Jellema, researcher in the program Televulnerabiltiy from Radiocommunications Agency.

During the session, various 'good practices' will be discussed ("What can I do, specifically?"), thus providing information on what may and may not be done during disruptions.

Speakers

Marijke Terpstra, Regional Manager Stichting Brentano and partner at Vrada. Marijke is an expert on televulnerability. Due to a digging incident, healthcare in one of the Bretano locations could not access ICT and she has experienced a major failure in which mobile services were not available.

Eelco Vriezekolk, Program Manager Televulnerabiltiy at Radiocommunications Agency. Eelco has obtained a doctoral degree on methods for countering network failures. He developed a five-step plan based on which organizationscan diminish their vulnerabilities regarding power failures. Within the Televulnerability program from the Radiocommunications Agency, of which Eelco is a program manager, a series of pilot projects are deployed for testing the five-step plan. One of the projects takes place in the healthcare sector.

Bart Koopmans, Integral Safety Expert/Adviser, GHOR at GGD GHOR Nederland and Safety Region Gelderland. Bart is for GGD GHOR Nederland portfolio holder on healthcare continuity and self-managed continuity in regional and national networks. He would like to discuss with you the importance of a good risk preparation at healthcare institutions where care-dependent patients are located. He will also discuss the ins and outs of the organization of crisis and disaster management in The Netherlands.

Appendix B - Interview script

This interview script assumes that the inventory is created in collaboration with the branch organization, a knowledge institute, consultants and other external experts.

Introduction

<Department> and <external partner> carry out a project together. The goal is to catalogue the risks of telecom disruptions at the <organization>. Together with the <commissioner> there is an approach set out for this project.

In the first phase of this project, a series of interviews will be held with representatives of different departments within <organization>. The aim of the interviews is to obtain a good image of communication systems that are used within <organization>.

De interviews are being taken by <names interviewers>. All interviews will have the character of an open discussion. All information will be managed confidentially: external communication about the project will only take place with the approval of <department> and <external partner>.

Process of the interview

The interview will be based on the questions shown below. During the interviews, we will be taking notes. The interview will be transcribed and within one week sent back to the interviewee for corrections. All transcripts will be used by the project leaders.

Interview questions

The interview will be based on these questions.

1. What is your role within the organization?
2. What ICT-processes do you use? Think of:
   - How are you informed?
   - Which data do you need? How does that data reach you?
   - What are your contacts within the organization and how do you communicate with them?
3. What alternatives do you have for when standard communication systems do not work?

Preparation

To keep the discussion efficient and minimize your work, we would like to prepare in advance. All information that you might send is more than welcome. For example: plans, handbooks, diagrams for crisis response and management. This information can of course also be provided after the interview. No extra effort is needed on your part.

Thank you in advance for your collaboration!

Appendix C - Example telecom-matrix

Example of a matrix of work-processes and telecom services for a fictional healthcare institution.

X : the telecom-technique is necessary for this process

(X) : the telecom-technique is sometimes used in this process

		Primary processes					Supporting processes			Building processes		Importance telecom-Technique
Work Process		Send/receive notifications through personal alarms to residents	Camera surveillance for residents during the night	Access to Electronic Client Files for medical data	Prescribe or change medication in medication systems	Access doctor on duty	Order food	Order devices and tools	Find contacts through the intranet	Intercom gates and doors	Fire alarm system: send alarms to fire department	
Importance		Medium	Low	High	Medium	High	Medium	Low	Low	Medium	High	
Telecom-Technique	Office LAN		X	X	X		X	X	X			high
	Internal phone	X				X						high
	Landline	X				X						high
	Mobile phone and data	(X)				X						high
	Connection OMS										X	high
	E-mail							X				low
	VPN to IT Provider			X	X				X			high
	IT provider data Centre	X							X			medium
	Internet Access	X					X	X				medium

Appendix D - Checklist telecom services

Primary processes

□ SCADA

□ Mobile telephony

□ Landline telephony

□ Call systems, Personal Alarms

□ Internet Access

□ Cloud-services

□ Office network/ LAN (including WIFI) / Wide Area Network (WAN)

□ Porto phones (TETRA, analog or digital, with or without licence)

□ Telemetry, process management, SCADA, ICS

□ GPS, Galileo (time-synchronization, location determination, navigation)

□ LoRa, Zigbee (Internet of Things-applications)

Supporting processes

□ Access to financial systems, ordering systems, ERP

□ Telephony and social media for client services and reception

□ Satellite telephones, transceivers, and NCV-devices for crisis management

Building processes

□ Transceivers for administrative assistance

□ Public fire alarm system

□ Management and surveillance of warming

□ Electric access system

□ Alarm systems for lifts

Appendix D - Checklist telecom services

□ **Knowledge remains with one person.** Personnel expertise is of course something to be proud of – but what if that person leaves or is sick? To what extent is that a single point of failure?

□ **Electricity black out.** Important devices need to be connected to emergency sources. Is that the case for you? Are there servers that are not connected to an emergency source?

□ **Old devices?** Old does not mean more exposed to risk but be careful about maintenance. Make sure reparations are done properly and that components are still available.

□ **Failures by third parties.** You are dependent on your communication on third parties. Are the agreements with these parties sufficient? Can you follow up if these agreements are not respected? Activities can be outsourced but not the responsibility if things go bad.

□ **Vulnerable cables.** Is your location connected to Internet via one cable? One incident can then lead to your organization being isolated.

□ **Quality of mobile signal.** The mobile networks in the Netherlands are very good. But there are places where the signal is less so. For example, in remote places, in some building or in cellars. Failure of the mobile network must not be excluded. If assistance makes use of mobile phones, then safety can become an issue.

Appendix F - Checklist measures

□ **Collaboration.** Ask your branch organization if they recommend supplementary measures. Discuss telecom vulnerability with other organizations within your sector.

□ **Agree upon activities during black out.** In order to avoid that only one person knows the way, important processes and activities need to be written down. For example, who needs to inform about a cable malfunction?

□ **Train and practice.** If you don't do it often, you often don't do it well. Train regularly with incidents. Test emergency power sources on their functionality during blackouts. Maintain a paper version of the agreements in emergency situations: Who does what? How do you reach each other? Don't just make back-ups, practice their implementation as well.

□ **Cloud and data-centre.** Storing data and services externally makes you less vulnerable when you are not accessible. For example, during fire or floods. Make sure that your data is available from this alternative location (for example while working from home or a shared office location).

□ **Keep track of incidents.** You can address your providers regarding incidents only when you have an overview of these incidents. Your insight into the matter will also be improved if you have an accurate image of malfunctions and their solutions.

□ **Double connection.** Investigate whether it is possible to have double connections: for example, one cable through the west wing the other through the east wing. In this way is your organization less vulnerable to damage due to digging.

□ **Dependence on one provider.** If not all your employees use the same network, then the malfunctioning of one network becomes less of a problem. Consider double-sim phones that can switch between providers.

□ **Essential devices.** Some devices cannot be replaced. Malfunctioning can have important consequences. Make sure you have good agreements with the providers of these devices and make sure that necessary manual instructions are up to date.

□ **Old work processes.** Do not throw away old shoes! You can fall back on how things went in the past when newer technologies malfunction. Make sure that these older devices and work processes are maintained – not only in the head of old employees, but also in written instructions.

Appendix G - Example Science Café Acronyms

GPS	– Global Positioning System
IT	– Information Technology
IoT	– The Internet of Things
IIoT	– Industrial IoT
OT	– Operational Technology
LAN	– Local Area Network
WAN	– Wide Area Network

Colophon

Authors and contributions

Mirjam van Burgel
Jako Jellema
Liesbeth Kruizinga
Jessica Overweg
Eelco Vriezekolk
Frans van den Akker
Anne van der Zwaan
Meine Koeslag

Translation

Eugen Popa

Image & diagram credits

Enexis diagram
The noun project - IoT by Krisztián Mátyás from the Noun Project
Sowande Boksteen diagram & raster

Credits

This document was based on a Dutch publication in 2018 by the Dutch National Radiocommunications Agency (Agentschap Telecom).
This project is co-funded by TKI E&I with the supplementary grant ‘TKI-Toeslag’ for Topconsortia for Knowledge and Innovation (TKIs) of the Ministry of Economic Affairs and Climate Policy.

Copyright & licensing

Institute for
Sustainable
Process Technology