Guidelines for bolstering resilience:

‘Running a business means thinking ahead’

Practical tools for entrepreneurs, businesses and trade associations to bolster their resilience

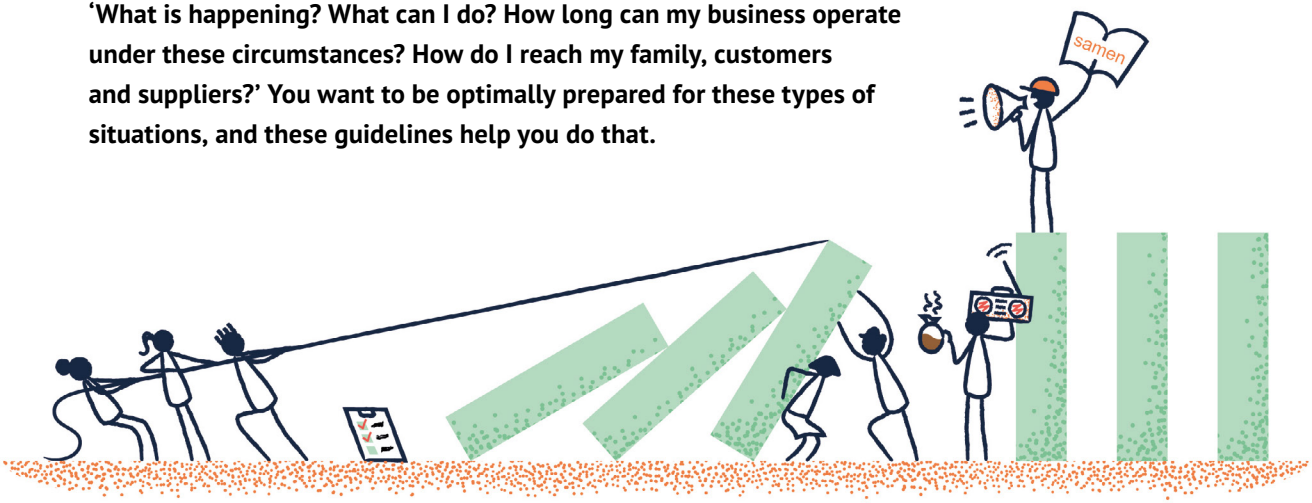
VNO NCW
CONFEDERATION OF NETHERLANDS INDUSTRY AND EMPLOYERS

MKB Nederland
ROYAL DUTCH ASSOCIATION OF SMALL AND MEDIUM SIZED ENTERPRISES

Contents

Introduction

‘Your business means everything to you, but all of a sudden nothing works anymore. You suddenly lose your internet connection, the lights are off, the ticket machine fails, you cannot reach suppliers and customers are confronted with a closed (digital) door.’ You wonder, ‘What is happening? What can I do? How long can my business operate under these circumstances? How do I reach my family, customers and suppliers?’ You want to be optimally prepared for these types of situations, and these guidelines help you do that.



Over recent years, international security has rapidly declined. In the Denk Vooruit [Think Ahead] campaign, the Netherlands National Coordinator for Counterterrorism and Security states: 'The question is not whether we will be faced with major societal disruptions, but when.'[1] Both the general public and businesses need to be resilient and prepared for emergency scenarios. For the business community, the government is focusing on the following three scenarios:

- Internet and telephone outage (72 hours or more),
- Power outage (72 hours or more), and
- A situation in which the Netherlands becomes involved in a military conflict.

Resilience is the ability of an organisation to prepare for disruption, to limit the impact of such a disruption, and to respond and recover effectively ('resiliently'). These guidelines help to bolster both your business's and your personal resilience.

In addition, you – as an entrepreneur – play a key role in improving societal resilience. Perhaps you provide basic necessities, perhaps you provide services to vital processes, and so on. In short: your preparation not only protects your own business, yourself and your staff, but it also supports customers, suppliers and society as a whole. Taking action now will enable you to rapidly respond to disruptions and make it easier to adapt to changing needs.

1 About the campaign | Denk Vooruit (https://english.denkvooruit.nl/service/about-the-campaign)

These guidelines are intended for entrepreneurs, businesses[2] and their trade associations. The document contains a strategy featuring practical sample measures to bolster businesses' resilience. Nothing is mandatory. We mainly provide examples and inspiration. Trade associations can adapt the sample measures to their own trade or sector as they see fit.

Following the guidelines step by step will enable you to ask and answer critical questions regarding your production and supply chains, and regarding the continuity of your operations. This will help you set priorities and take measures geared to your situation. Thus, you will also improve your business's resilience against other hazards and threats.

The guidelines have been compiled by the Confederation of Netherlands Industry and Employers (VNO-NCW) and entrepreneurs' association MKB-Nederland, in conjunction with the Ministry of Economic Affairs. Together, these parties strive to improve the resilience of the overall Dutch business community against the three emergency scenarios outlined.

2 Businesses that form part of the vital infrastructure are subject to statutory requirements that extend beyond these guidelines (in some cases, far beyond). Such requirements are set down in sector legislation, but also in the Bill on Weerbaarheid kritieke entiteiten [Resilience of critical entities] and the Bill on Cyberbeveiliging [Cyber security]. See: NIS2 and CER directives | National Coordinator for Counterterrorism and Security. (https://www.nctv.nl/onderwerpen/c/cer--en-nis2-richtlijnen)

Reading guide

In these guidelines, we start off with two key questions:

1. Which activities are really crucial to your business?
2. What is the minimum operational process required for the survival of your business?

The answers to these questions show which components of your organisation are indispensable to its survival. We call these components the *crown jewels* of your organisation. Subsequently, five steps are elaborated which compare to the links in the security chain.[3]

[3] The security chain organises crisis control and disaster management in five steps: being proactive, prevention, preparation, repression, and aftercare. For the purpose of these guidelines, these five steps have been adapted to: thinking ahead, prevention, preparation, responding, and recovery and continued development.

STEP 1.

‘Thinking ahead: how do I protect my crown jewels?’

You receive practical tools for (better) protecting your crown jewels (‘security principles’) and information on the appropriate actions to be taken.

STEP 2.

‘Prevention is better than cure: take precautionary measures.’

You identify additional precautionary measures that can be taken to (better) protect your crown jewels, and you set clear priorities in this respect.

STEP 3.

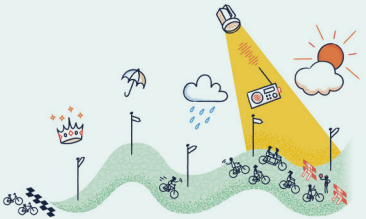
‘Be prepared: elaborate the main preparations, test and do drills.’

You draw up a practical emergency and recovery plan: an ‘emergency manual’. Regular testing and drilling will continuously improve your preparedness.

STEP 4.

‘Respond in a controlled and alert manner: know what you need to do.’

If things go wrong, you act effectively and in a targeted manner. You implement what you have prepared and improvise wherever necessary, with the emergency manual as a guide.



STEP 5.
'Recovery and continued development.'

After an incident, you restore operations in a structured and systematic manner. You map your experiences and use them to render your organisation even stronger and more resilient in the future.

Each step outlines a brief strategy comprising actions, sample measures and references to additional information. The sample measures can be implemented as they are by a wide range of businesses.

In addition, two appendices have been provided. Appendix 1 is an elaboration of the three key scenarios for businesses.[4] Appendix 2 is a brief case with questions. This case can be used to assess the preparations and, wherever necessary, take additional measures or make additional preparations.

4 These guidelines do not cover the national crisis structure, strategy, decisions, measures and communication involved in restoring failed internet, telecom and/or power services. Such matters are contained in national contingency plans, which can be found here: Landelijke Crisisplannen | National Coordinator for Counterterrorism and Security (https://www.nctv.nl/ onderwerpen/l/landelijke-crisisplannen).

The basis: What are your business's crown jewels?

To know what and whom you need if things go wrong, it is important to know exactly what you need to protect. To this end, you must identify the crown jewels of your business. Crown jewels are those individuals, processes, resources and products within your business that have absolute priority in terms of the continuity (uninterrupted progress) of operations. They are the most important components for which you wish optimum protection.[5]

To identify these crown jewels, you can examine the following four components of your operations:

1. **Staff and organisation:** You yourself as an entrepreneur, the management, employees and mutual cooperation.
2. **Chains and customers:** Your (most important) customers, suppliers and partners that buy or supply.
3. **Products and services:** Your unique offering, range of products, (knowledge) product and/or services.
4. **Ancillary processes and aids:** Procurement, logistics, administration/finances, IT, buildings, stock, means of payment and means of transport.

5 How do I map my interests to be protected? | What can you do yourself? | Nationaal Cyber Security Centrum. (https://www.ncsc.nl/risicomanagement/hoe-breng-ik-mijn-te-beschermen-belangen-kaart)

Four components that harbour crown jewels

The two key questions to be asked in this respect:

1. Which activities are really crucial to your business?
2. What is the minimum operational process required for the survival of your business?

A rule of thumb for the identification of your crown jewels is: If the loss of a component of your business will result in the (near) paralysis of the business, this component is considered a crown jewel.

Analyse what is of the essence for your business and elaborate this in an overview, in collaboration with staff and relevant partners. Regularly assess whether this overview is still up to date.

STEP 1.
Thinking ahead: how do I protect my crown jewels?

In this step, we provide you with practical tools for (better) protecting your crown jewels – what we term the 'security principles' – and the actions they require. Use the three emergency scenarios from the introduction as your point of departure.

The security principles and actions are structured around the four components of the operations (see page 13).

Security principles

Staff and organisation

- **Safety:** How do I ensure the safety of my staff and their families?
- **Continuity and availability:** Which staff members hold a crucial position within the business and how difficult is it to replace them?
- **Contactability:** What arrangements have I made in terms of contactability in the event that communication is no longer possible

Chains and customers

- **Continuity and availability:** On whom am I – as an entrepreneur – highly dependent? Consider, for example, collaboration with suppliers, service providers and customers. But also: is my business working with, or am I supplying to, businesses in a vital sector?[6]

[6] Overview of Vital Processes, National Coordinator for Counterterrorism and Security. (https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur/overzicht-vitale-processen)

- **Contactability:** How do I contact my suppliers and customers, and how can they contact me?
- **Financial damage:** Am I sufficiently aware of the financial risks for my business, and do I know what is covered or not covered by my insurance?
- **Reputation:** How do I prevent (unnecessary) damage to my reputation?

Products and services

- **Continuity and availability:** How do I still get my products and services produced (in a timely fashion)?
- **Deliverability:** How do I still transport my goods, and what do I do if that is (temporarily) no longer possible?
- **Availability of utilities:** Do I continue to operate if key utilities fail, and if so, how?
- **Protection:** How do I protect my products, data and intellectual property under crisis conditions or if certain security provisions are no longer available?

Ancillary processes and aids

- **Continuity and availability:** Which automated processes, such as procurement, administration (for example, invoicing or salary payments) or IT-driven transactions will stagnate or come to a standstill in the event of a power outage and/or internet/telecoms failure lasting 72 hours or more? And after how long will this start to jeopardise the continuity of my business?
- **Reliability:** How do I safeguard the quality of my production, if (IT) processes, transactions and utilities are no longer reliable and/or available?

Potential actions

The above questions can serve as a basis for you to set priorities and examine how the crown jewels identified can be (better) protected. The actions listed below can help in this respect. The order provides an indication of their priority; however, this may differ from one business to the next.

Staff and organisation

Safety:

- In some cases, a safe and controlled shutdown of the business will be better or even imperative. Set down clear parameters for when it is unsafe (or impossible) to (continue to) work or to come to the business, or for when the safety of those at home and next of kin prevails. Ensure that staff will be able to get home safely in such cases.
- Provide additional safety measures for continued operation under disrupted circumstances.

Continuity and availability:

- Ensure that replacements can be hired and/or that you have trained replacements if staff in crucial positions should drop out.
- Take into account that some staff in crucial positions may be engaged in additional duties (e.g. if they are reservists in the armed forces), have volunteer care duties, or liable to be called up for military service (in the Netherlands or in another country), which may result in their prolonged absence in emergency situations.

- If need be, provide alternative transport for collecting and taking home staff members whose presence in the business or in the branch is essential and justified.
- Consider using staff for other work in the event of a prolonged crisis.
- Coordinate with similar businesses or request advice from your trade association on dealing with the prolonged unavailability or absence of staff.

Contactability:

- Set down agreements regarding contactability, together with staff.
- Ensure that everyone is familiar with the agreements. Provide regular refreshers to ensure that the agreements are (automatically) set in motion in the event that communication is (temporarily) impossible.

Chains and customers

Continuity and availability:

- Approach businesses in vital sectors (see footnote 6) with which you collaborate as a customer. Discuss what additional agreements are needed and possible to safeguard the continuity of your deliveries or products. Determine how long your existing stock will last if your main suppliers are unable (or do not want) to deliver.
- Set down agreements with your main suppliers or subcontractors on how to cope with potential dependency issues. For example:
  - How to reduce the dependency on the physical delivery of components or products.

- How to continue to operate and deliver, even if suppliers or customers are spread over a wide geographic area.

- Consider maintaining additional stock of crucial raw materials and/or components.
- Seek coordination with businesses with which you are already collaborating or have formed a network, with a view to learning practical details regarding business continuity, sharing something or taking over something.
  - In this respect, extend your efforts to business connections outside your own sector.
  - As a small business, do not hesitate to approach larger businesses ('large helping small').

Contactability:

- In terms and conditions of delivery, contracts and project plans, set down who can be contacted in what manner under disrupted circumstances.

Financial damage:

- Check whether the terms and conditions of delivery, contracts and service agreements can be geared to exceptional circumstances (force majeure).
- Insure additional risks wherever possible or increase your current coverage.
- Set aside additional money and consult your bank regarding the possibilities.
- Check the availability of specific tax arrangements, such as extensions of payment. Consult your accountant.

Reputation:

- Be open and transparent if agreements, commitments and/or deliveries are or may be jeopardised, and seek solutions together with customers, suppliers and so on.
- Consider in advance how you will deal with complaints, notices of default and communication in order to limit damage to your reputation. For example, contact a good lawyer and/or communications specialist in your network who can assist you in such matters.

Products and services

Continuity and availability:

- Consider how your business can remain open, active and profitable in the event of a prolonged crisis situation, e.g. a situation in which the Netherlands becomes involved in a military conflict and is required to provide assistance to NATO.

Deliverability:

- Consider alternative transport options or other goods delivery methods. For example, explore the temporary feasibility of selling from home, pick-ups, your own delivery service or a central delivery locat.

Availability of utilities:

- Check whether and where you can reduce your dependency on utilities and key technical facilities (for example, IT) for your production and deliveries.
  - o Are there alternative ways to continue to operate, such as manual operation?

- Check the internal and external agreements on management and maintenance, and set down additional safeguards (wherever necessary).

Protection:

- If need be, provide additional (manual) physical security or surveillance.
- Under normal conditions, but especially in times of hybrid[7] and/or military threats, your unique services or products may be vulnerable to espionage, theft or sabotage. Alert staff to this. Identify the main risks and take protective measures.[8]

Ancillary processes and aids

Continuity and availability:

- Reduce your dependency on automated ancillary processes. For example: ensure that you have options for manually drawing up invoices or making bookings.
- Improve your security. For example, check whether building security and access is set up in a manner that allows safe (manual) operation.
- In terms of energy, reduce your dependency on a single type of fuel. For example, home batteries and emergency power systems will help you to continue to produce for a longer period of time in the event of a power outage.

7 Warfare between nations involving the integrated use of resources and actors, for the purpose of attaining certain strategic objectives. See: *Een duiding van het fenomeen 'hybride dreiging'* [An interpretation of the 'hybrid threat' phenomenon], National Coordinator for Counterterrorism and Security (https://www.nctv.nl/documenten/2019/04/18/duiding-fenomeen-hybride-dreiging).

8 Step 2 | Know the risks | Render your business resilient (https://www.maakjebedrijfweerbaar.nl/ken-de-risicos).

- See whether you can maintain an efficient balance between fuel-powered and electrical equipment.
- If you are located on a street, in a multi-tenant building or on an industrial estate, check how you can help one another during a crisis. For example, explore the advantages of collective procurement and use of items such as emergency power systems, home batteries or additional, alternative means of communication (for example, walkie-talkies or even radio transmission equipment[9]).

Reliability:

- Find out what is legally possible and allowed in the field of, for example, health and safety at work and fire safety, if you are installing additional technical (power) systems or storing additional fuel. If need be, contact the supervising authority or authorities to discuss possibilities, impossibilities or bottlenecks.
- Check where, under normal circumstances, the quality of products or services is monitored by automated procedures and systems. Develop additional manual procedures for such monitoring, so you can carry out additional manual and targeted quality control checks and quality inspections.

9 Certificates are required for the possession and use of transmission equipment. See: radiozendamateur worden | rijksinspectie digitale infrastructuur (rdi) [Becoming an amateur radio operator], Dutch Authority for Digital Infrastructure (RDI) (https://www.rdi.nl/onderwerpen/vergunningen-en-registraties/radiozendamateurs/opleiding-en-examens).

In conclusion

Furthermore, consider ways in which your business could support society and/or vital sectors during a (prolonged) crisis. Crisis situations can lead to disruptions in chains and to changes in the demand for products and services. Businesses that adapt to such disruptions and changes in a flexible and responsible manner can continue to serve their customers and help to sustain societal processes.

In this respect, ask yourself the following questions: What role can your business play if existing suppliers drop out? To what extent can a temporary scale-up enable you to support customers or chain partners?

Now that you have a better picture of where additional protection is needed and of the options to that effect, it is time for the next step: taking targeted additional precautionary measures to (better) protect your crown jewels.

STEP 2.
Prevention is better than cure: taking precautionary measures

Now it is time for (even) more action! Render your crown jewels (more) resilient, to ensure that you can continue to operate safely and for as long as possible in the event of disruption or in times of crisis. What additional measures or means do you need to this end?

For each component of the operations, the following figure presents potential sample measures for better protecting your crown jewels.[10]
The previous step has already pointed you in the right direction. This step helps you select and implement appropriate precautionary measures.

10 NCSC - *De bellijst, simpel maar effectief* [National Cyber Security Centre (NCSC) - The call list, simple yet effective] (https://www.ncsc.nl/preventieve-beveiligingsmaatregelen/de-bellijst-simpel-maar-effectief)

Staff and organisation

- Agreements on contactability and communication
- Arrangements for replacement of staff
- Paper lists of contact details
- Safe (additionally secured) working locations
- Agreed assembly point(s) / emergency location(s)
- Alternative means of transport, such as company (delivery) bicycles
- Alternative (additional) means of communication, such as a second telephone with a SIM card from another provider, satellite communication
- In-house emergency response (first aid) training
- On-site emergency kits
- Places to sleep, sanitary and kitchen facilities for essential staff
- Personal protection equipment
- ....

Chains and customers

- Specific agreements with the vital sectors
- Selected alternative or additional suppliers
- Paper list(s) of contact details for customers and suppliers
- Agreements on external contactability and communication
- Additional (buffer) stock / alternative stock locations
- Alternative delivery method(s)
- More stringent terms and conditions of delivery and contracts
- Supplementary insurance or coverage
- .....

Ancillary processes and aids

- Paper print-out of key administration / company data
- Paper notepads for invoices and receipts
- Back-up(s) (off-line systems)
- Paper catalogues, bookings, order lists, price lists, etc.
- Procedures for manual quality control
- Manually operable building (access) security (enabling safe closing)
- Alternative means of payment or (additional) cash
- Home office(s)
- Emergency power system (+ supply of diesel), home batteries, power banks
- Alternative means of communication (walkie-talkies, transmission equipment)
- Additional fuel in safe storage
- Solar or paraffin lamps, candles
- .....

Products and services

- Adapted products or services during a prolonged crisis
- Alternative transport facilities
- Alternative (manual) procedures
- Alternative business hours / selling from home
- On-site communication aids, such as paper notices/signs
- Additional IT and physical security measures
- .....

Points for attention

- **Emergency kit:** Provide emergency kit(s) both at home and in the office.[11] In emergency situations, a battery-powered radio will keep you informed of government news and recommendations. Also consider facilities and aids that allow you to remain at the business location for a prolonged period of time, in a safe and responsible manner.
- **Sanitation:** Bear in mind that toilets can no longer be used during prolonged power outages, because sewer systems or sewage purification plants will fail. Consider alternatives wherever necessary.[12]
- **Alternative means of payment:** Consider the use of cash, QR payments or offline card payments.[13]
- **Back-ups (copies of stored data):** Provide high-quality back-ups.[14]
- **Cyber hygiene:** Use the five basic principles of digital resilience to bring your business's cyber hygiene up to par and test it.[15] Many incidents still occur because organisations' cyber hygiene is sub-standard.

11 Stel je noodpakket samen | Denk vooruit [Prepare your emergency kit | Think ahead] (https://www.denkvooruit.nl/bereid-je-voor/stel-je-noodpakket-samen)
12 Voorbereiden voor 72 uur | Denk vooruit [Prepare for 72 hours | Think ahead] (https://www.denkvooruit.nl/vraag-en-antwoord-2/voorbereiden)
13 Adviezen MOB Denk vooruit, ook voor betalen [Recommendations of the National Forum on the Payment System, Think ahead, also with respect to payments] and Terugvalopties pinnen - PIN.NL [Fall-back options for card payments] (https://www.pin.nl/ondernemer/storingen/terugvalopties/)
14 NCSC - Maak in 3 stappen een goede back-up. [National Cyber Security Centre (NCSC) – 3 steps to make a good back-up] (https://www.ncsc.nl/back-up/maak-3-stappen-een-goede-back-up)
15 NCSC - De 5 basisprincipes van veilig digitaal ondernemen. [National Cyber Security Centre (NCSC) – The 5 basic principles of safe digital entrepreneurship] (https://www.ncsc.nl/basisprincipes/overzicht)

- **General:** Be aware that every new facility or alternative procedure needs to be legal, safe and secure. For that reason, initially it is wise to keep it simple and convenient. Consult experts, the trade association, fellow entrepreneurs or a supervisory body if need be. For example, pay close attention to (fire) safety and contactability, (emergency) lighting in rooms and near emergency exits during power outages, but also consider the risks of having additional cash in stock, such as theft or robberies.

The next step is to ensure that you – as a business – actually are and will remain prepared.

STEP 3.
Be prepared: elaborate the main preparations, test and do drills wherever possible

‘Things you seldom do, you seldom do well.’ Nobody knows whether or when a disruption or crisis will occur, or how long it will last. Perhaps the additional measures, agreements and alternative procedures developed for emergency situations will not be needed for a long time. This may be a reassuring thought, but it also means that you may not be able to implement them properly when the time comes.

For that reason, it is wise to set down all the aids, alternative procedures, emergency facilities and agreements in a plan, comprising clear directions and instructions. Thus, you will have a practical **emergency manual**. Appoint someone within the business to be responsible for the manual. They must ensure that the manual is regularly updated and remains to the point.

What can the emergency manual cover? Consider the following topics:

1. **(Crisis) decision-making lines.** Describe who will be in charge in an emergency situation, who makes the decisions, and who has authority over what.
2. **Agreements with staff about the home front** Provide your staff with information on what they can arrange in advance on the home front, such as an emergency kit, so they are prepared for an emergency situation.[16]
3. **(Emergency) communication plan.** Set down where and how you can contact each other if normal communication fails (for example, set down physical meeting locations). This extends to the home front, staff, customers and suppliers.

[16] Be prepared | Think ahead. (https://www.denkvooruit.nl/bereid-je-voor)

4. **Agreements with suppliers and service providers.** Describe how your cooperation will continue during a crisis, and that operational activities may possibly be scaled down to a purely emergency business level.
5. **Alternative payment and distribution methods.** Ensure that everyone is aware of the options available if the usual payment and/or distribution methods no longer work.
6. **Main principles of (alternative) procedures and recovery.** Describe how important processes or facilities can continue to function during a disruption, or how they can be restored as quickly as possible if they fail. Elaborate upon this in a recovery plan or checklist.[17]

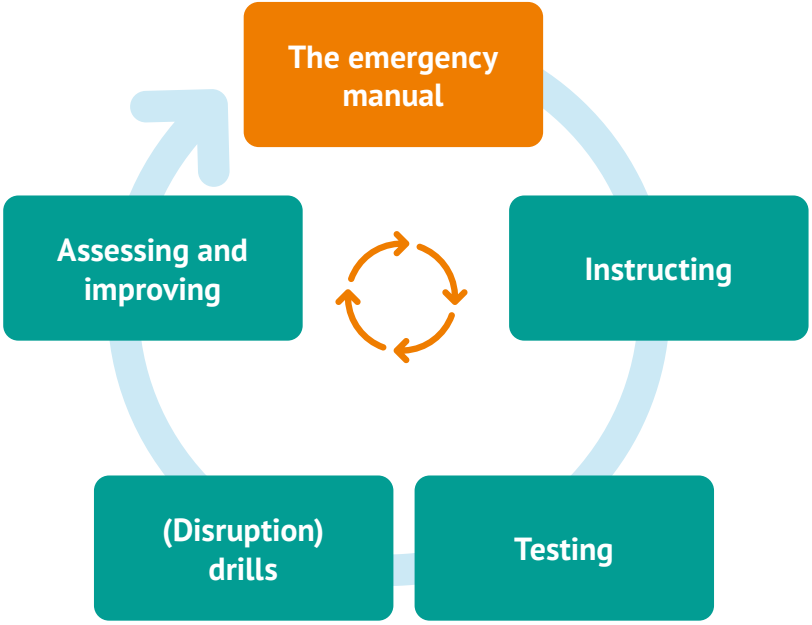
Experience shows that, in many cases, manuals are not used during a crisis. For that reason, it makes sense to draw up a brief checklist based on the manual and distribute it (for example, pocket-sized, on a plastic card). Such a checklist will be especially useful in the early, hectic hours of a crisis, as it helps you determine, step by step, what actions to prepare or carry out, in which order and when.

17 Tip: If you are highly dependent on IT, manage many IT systems or have outsourced many IT systems, it would be wise to draw up a separate Business Continuity Plan (BCP). See, for example: Business Continuity Plan: Well prepared for an emergency | KVK (https://www.kvk.nl/ en/secure-business/well-prepared-for-an-emergency/)

Points for attention

- Ensure that everyone is familiar with the manual (and knows where to find it). Provide paper printouts at multiple locations (at the office and at home).
- Regularly test technical (fall-back) facilities, including power and energy supplies, IT systems and back-up systems. Anything that does not work needs to be fixed or redesigned as quickly as possible.
- Distribute the (handy-sized) first response checklist to all those concerned.
- Conduct regular drills using the manual and the checklist, so that you, your staff and collaboration partners know what is expected of them in an emergency situation.
- Practicing (realistic) scenarios is essential. As a manager, you set a good example by visibly paying structural attention to such drills and emphasising their importance. This ensures that teams will remain motivated and be better prepared.
- Drills do not need to be complicated. Start with a simple paper exercise; that already makes a difference. Later on, you can expand to practical drills.
- Targeted training and practicing under pressure help to increase the mental resilience of individual staff and teams.
- Assess and improve. Regularly update the manual (and the checklist(s)), for example, after a drill.

The figure below summarises the actions and points for attention for this step:



The next step describes the specific challenges that can occur when your business is hit by a (prolonged) disruption or crisis situation. It explains how to respond in such situations and how to deal with the focus and improvisation required at such times.

STEP 4.
Respond in a controlled and alert manner: know what you need to do

‘And then it happens: unexpected, inconvenient and also different from what everyone had foreseen.’ In such cases, you need to step up, do what has been prepared and improvise where needed. The emergency manual outlined in the previous step now serves as your fall-back basis. However, you must take into account that under emergency conditions, stress and uncertainty may affect actions and collaboration.

A great deal depends on your information position and that of others: ‘Do you still have access to information on the threat or disruption? Can you still communicate? Or will you resort to alternative means of communication right away?’ That is why it would be wise to immediately use the checklist that you have developed for the first few hours (the first day).

Your primary concern is, obviously, safety: your own safety and the safety of your staff, visitors or customers on site, and the home front. This also includes securing communication and locations. Then comes the continuity of operations, deliveries, alternative procedures and emergency measures. In less urgent situations, the continuity of the operations may constitute your (main) priority.

The following table gives an example for the structure and contents of a (response) checklist:

(Own) safety (staff, visitors, family)	• Do I have access to (sufficient) emergency resources (the emergency kits), first of all drinking water? • Do I have my medication, first-aid kit etc.? • Does the (emergency) lighting and ventilation work? • Can I reach emergency services (possibly physically)?
(Emergency) communication	• Can my staff and our families be contacted? • Which of the agreements made apply now and are they feasible? • Which means of communication (still) work? • Are there any alternative means of communication available and do they work?
Information (position)	• Where can I get information on the threat / situation? • Do I have the necessary means (radio, physical contact) at my disposal? • What do the authorities say? What is the nature of the (imminent) events? • Who (else) do I need?

Location(s)

- Is/are my location(s) (sufficiently) safe vis-à-vis the threat?
- Is a safe stay on site (heating, fresh air, (emergency) lighting, alarms) still safeguarded?
- What are safe and reliable alternative means of transport?

Operations (alternative procedures and emergency measures)

- How do I secure the critical processes, goods and stock?
- Is crucial information available (on paper), as well as securities and means of payment (cash)?

Points for attention

- In the first (often hectic) hours, chaos (and sometimes even panic) can be prevented by falling back on the agreements that you have made with staff and the home front.
- Help one another, not only within the organisation, but also within neighbouring businesses and the chains and networks in which you normally operate.
- Show leadership. Demonstrate that you are there for your organisation and your staff. This is what the preparations were intended for. At all stages, make it clear when continuing the business is (still) possible or when activities need to stop.
- Also consider, for example, opening up your business site(s) to take care of or help others.

During the crisis, respond and act as decisively as possible, on the basis of the precautionary measures, preparations and improvisation. Once the circumstances improve and essential facilities have been (partially) restored, you can start your return to normal operations in a step-by-step manner. The last step will help you in this respect.

STEP 5.
Recovery and continued development

‘There is light at the end of every tunnel.’ Once the (partial) restoration of failed facilities comes into sight, it is time to re-open and restart the business, step by step. Here, too, it would be advisable to use a recovery plan (included in the emergency manual) or a checklist that you have drawn up beforehand. Two stages can be distinguished in the recovery process:

1. ‘Back to business’

The business is partially operational again. The main production, delivery and communication processes are already working, but some processes have not yet returned to normal or are still limited. Use the recovery plan and/or a checklist that contains, for example, the following components:

- Check how staff, their immediate environment, suppliers and customers are doing. Discuss expectations and indicate where disruptions or alternative operational agreements are still in place.
- Set priorities. Which processes can (safely) restart first and what communication does that require?
- Determine which additional (quality) control checks and manual procedures are required to this end.

2. ‘Back to normal’

Gradually, the situation will recover fully. Inform the staff about the recovery, monitor their well-being and provide additional support where needed. This is also the time for assessing damage, if any, and claim such with insurance companies or compensation funds.

As soon as is reasonably practical, bring together your staff and others with whom you have collaborated for a review:

- Discuss what went well and what could be improved;
- Incorporate the lessons learned in your emergency manual;
- Reflect on the efforts and commitment of staff.

Finally: It is important to pay and keep paying attention to staff requiring additional (mental) support during the recovery process.

In conclusion

Reading and implementing these guidelines step by step will better prepare you for difficult circumstances and enable you to act faster and more effectively.

If, after reading the guidelines, you need more support in their implementation, please contact your trade association.

If you have any questions or comments regarding the guidelines themselves, contact VNO-NCW and MKB-Nederland.

Contact

VNO-NCW and MKB-Nederland
Sabine Gielens
gielens@vnoncw-mkb.nl

Bibliography of sources consulted

- Federation of Finnish Entrepreneurs. (2025). SME Preparedness Guide. FFE.
- Kamer van Koophandel. Bedrijfscontinuïteitsplan: blijf overeind na een ramp. https://www.kvk.nl/veilig-zakendoen/goed-voorbereid-op-een-calamiteit/
- Parliamentary Document 5937426, p. 7. (6 December 2024). https://www.nctv.nl/document-en/2024/12/06/kamerbrief-weerbaarheid-tegen-militaire-en-hybride-dreigingen
- Maatschappelijk Overleg Betalingsverkeer. (20 May 2025). Denk vooruit, ook voor betalen. https://www.dnb.nl/media/vctdty4f/advies-mob-denk-vooruit-ook-voor-betalen.pdf
- Ministry of Economic Affairs. Maak je bedrijf weerbaar. Ken de risico's. https://www.maakjebedrijfweerbaar.nl/ken-de-risicos
- Nationaal Coördinator Terrorismebestrijding en Veiligheid [National Coordinator for Counterterrorism and Security] (NCTV). Over denk vooruit.
- NCTV. Landelijke Crisisplannen. https://www.nctv.nl/onderwerpen/l/landelijke-crisisplannen
- NCTV. NIS2- en CER-directives. https://www.nctv.nl/onderwerpen/c/cer--en-nis2-richtlijnen
- NCTV. Overview of vital processes. https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur/overzicht-vitale-processen

- NCTV. Een duiding van het fenomeen hybride dreiging. https://www.nctv.nl/documenten/2019/04/18/duiding-fenomeen-hybride-dreiging
- NCTV. (2025). Bereid je voor op een noodsituatie. https://www.denkvooruit.nl/informatieboekje; https://www.denkvooruit.nl/bereid-je-voor/stel-je-noodpakket-samen; https://www.denkvooruit.nl/vraag-en-antwoord-2/voorbereiden
- NCTV. (22 July 2025). Societal Resilience Communication Tool (light version). https://www.nctv.nl/documenten/2025/07/22/gesprekstool-maatschappelijke-weerbaarheid-light-versie
- Nationaal Cyber Security Centrum [National Cyber Security Centre] (NCSC). Hoe breng ik mijn te beschermen belangen in kaart. https://www.ncsc.nl/risicomanagement/hoe-breng-ik-mijn-te-beschermen-belangen-kaart
- NCSC. De bellijst, simpel maar effectief. https://www.ncsc.nl/preventieve-beveiligingsmaatregelen/de-bellijst-simpel-maar-effectief
- NCSC. Maak in 3 stappen een goede back-up. https://www.ncsc.nl/back-up/maak-3-stappen-een-goede-back-up
- NCSC. De 5 basisprincipes van veilig digitaal ondernemen. https://www.ncsc.nl/basisprincipes/overzicht
- Nederlands Instituut Bedrijfshulpverlening. (2025). Whitepaper Weerbaarheid. NIBHV. https://www.nibhv.nl/hulpmiddel/whitepaper-weerbaarheid/

- Rijksinspectie Digitale Infrastructuur. Radiozendamateur worden. https://www.rdi.nl/onderwerpen/vergunningen-en-registraties/radiozendamateurs/opleiding-en-examens
- Swedish Civil Defence and Resilience Agency (January 2026). Preparedness for businesses – In case of crisis or war
- Reports on resilience meetings organised by VNO-NCW, MKB-Nederland, the Ministry of Economic Affairs and the Netherlands Enterprise Agency (RVO) (2025)

Appendix 1 – Conceivable scenarios[18]

Internet and telephone outage

In several European countries, teams operating on behalf of a state actor sabotage digital infrastructure. They target strategic locations, such as fibre optic cables at data centres, internet hubs and telecom providers. In the Netherlands, such a team has hit a national mobile telecom provider.

The outage has an immediate major impact on daily life. In parts of the country, mobile networks and the landline network shut down, which means it is no longer possible to phone or use the internet. As more and more appliances are connected to the Internet ('Internet of Things'), such as lighting, solar panels and thermostats, they will not be available either. The over-the-counter payment system is disrupted; people can no longer pay in supermarkets and pharmacies, for example. Withdrawing cash is no longer possible as cash dispensers are also disrupted.

18 The three scenarios were drawn up in February 2025 by the Ministry of Economic Affairs (EZ) and the Ministry of Climate Policy and Green Growth (KGG), in coordination with the telecoms and electricity sectors. They are based on the umbrella scenario laid out in the Letter to Parliament dated 6 December 2024 (https://www.nctv.nl/documenten/2024/12/06/kamerbrief-weerbaarheid-tegen-militaire-en-hybride-dreigingen). The parameters were set down in consultation with VNO-NCW and MKB-Nederland; they are in line with the strategies pursued in various European countries. The aforementioned Ministries updated the scenarios in January 2026 for these guidelines.

Foreign trade is also affected. Travellers can hit the road, but their journeys will be hampered as Rijkswaterstaat – the government authority responsible for infrastructure in the Netherlands – has no way of digitally monitoring the roads, whilst regional train traffic is hampered due to the failure of internal networks. The telecom provider indicates that it is unclear how long it will take before telephone and data facilities can be restored. The restoration process is complicated as mechanics have no access to internal digital systems that are necessary for maintenance work.

In this scenario, our point of departure is that it will take 72 hours to reinstate the bulk of the network and telecom facilities in the affected area, on the basis of emergency solutions and provisional measures.

Power outage

The power fails in a region of the Netherlands, leaving the 2 million customers of a grid operator without electricity. It rapidly becomes clear that the power failure is the result of an attack by a state actor. The attack has destroyed distribution stations at several locations.
The grid operators are working on restoration. It is unclear how long it will take before the power supply is restored.

The outage has an immediate major impact on daily life. Battery-operated electrical appliances, such as mobile phones and laptops, medical home equipment and electric cars can continue to function for a few hours but will then also shut down. Within a few hours, telecommunication will largely fail as well. The over-the-counter payment system is disrupted; people can no

longer pay in supermarkets and pharmacies, for example.

Withdrawing cash is no longer possible, as cash dispensers are also disrupted. Train traffic breaks down, causing congestion at railway stations. Traffic jams arise due to the failure of matrix signs, traffic lights and remote-controlled infrastructure such as bridges. Schiphol Airport is situated outside of the area affected by the power outage but is nonetheless disrupted on account of the motorway and railway congestion.

Approximately one day after the outage, more utilities fail. Heating systems no longer work and taps in homes on the third storey or higher no longer produce water. Problems arise with emergency power facilities for vital objects, as not all fuel supplies are sufficient.

It takes 72 hours to reinstate the bulk of the power supply in the affected area, on the basis f emergency solutions, help from abroad and provisional measures.

The Netherlands involved in a military conflict

The Netherlands becomes involved in a military conflict in Eastern Europe and needs to fulfil its obligations under the NATO alliance. This is a prolonged situation featuring the following events:

- The transfer of large volumes of military equipment and personnel, disrupting the transport of other goods;
- Threats pertaining to seaports and transport connections, resulting in a large-scale and prolonged disruption to trade and the economy;
- European countries along the eastern border mobilise people of military age, to which many economic migrants respond;
- The Ministry of Defence has limited capacity for executing its third main task: supporting civil society in the event of disasters or crises, or securing objects;
- A stream of refugees heads for the Netherlands;
- Hospitals are crowded, as wounded soldiers and refugees take a maximum toll on the healthcare system in the Netherlands.

Appendix 2 - Test your resilience

Imagine:

It is Monday morning, and your shop or business is open. All of a sudden, the power fails. No light, it is getting cold fast, no card payments, no email, no contact with staff or your family at home. You don't know whether it will last three hours or three days. The clock is ticking.

Now consider the following questions:

- What is the first thing you do?
- Where is critical danger threatening now?
- Which operational processes will shut down immediately or quickly?
- What damage is irreversible or (too) extensive?
- What agreements have you made with staff, customers and suppliers to continue your operations for the time being?
- Who will you inform first and how?
- What arrangements have you made to cope with unexpected setbacks?
- How do you ensure that you will be operational again as soon as possible?

Answer the questions on the basis of the emergency manual and the checklist(s). Are your staff, you yourself and your main chain partners prepared for dealing with such a situation and for taking action? If not, what (additional) resources do you need to be better prepared?

Want to conduct more such tests? Vary the above case, for example, by changing the day or the time, or by introducing your own absence as the one bearing primary responsibility. Or use one of the other scenarios.[19]

19 Societal Resilience Communication Tool (light version) | National Coordinator for Counterterrorism and Security (https://www. nctv.nl/documenten/2025/07/22/gesprekstool-maatschappelijke-weerbaarheid-light-versie)

Imprint

Project leader:
Sabine Gielens, VNO-NCW and MKB-Nederland

Author:
Laurens van der Sluys Veer, International Safety Research Nederland

Illustrations:
Willemijn ten Wolde, Tante Willem

Design:
Anoeska Kruithof, VNO-NCW and MKB-Nederland

Cover photo: Erik van ’t Woud/ANP
Cover image text: ‘Power cut, yet still open!’

2500086

VNO NCW
CONFEDERATION OF NETHERLANDS INDUSTRY AND EMPLOYERS

MKB Nederland
ROYAL DUTCH ASSOCIATION OF SMALL AND MEDIUM SIZED ENTERPRISES