Business Resilience - An introduction to protecting your business

CFPA-E Guideline No 2:20XX21 N - DRAFT

© A. Rahman, Zurich Resilience Solutions

CFPAEUROPE®

Fire Safety | Security | Natural Hazards

insurance europe
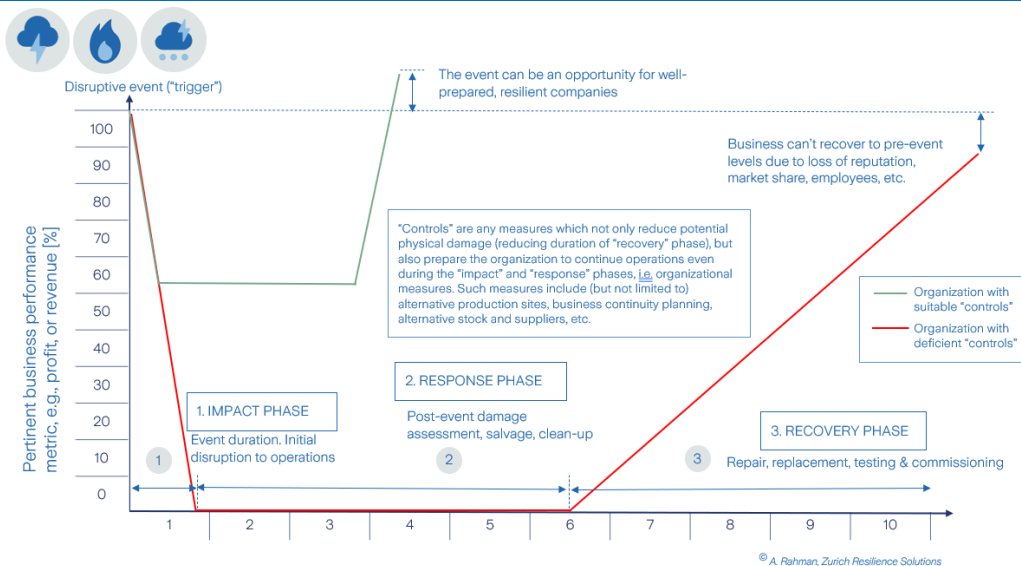
The CFPA Europe develops and publishes common guidelines about fire safety, security, and natural hazards with the aim to achieve similar interpretation and to give examples of acceptable solutions, concepts, and models. The aim is to facilitate and support fire protection, security, and protection against natural hazards across Europe, and the whole world.

Today fire safety, security and protection against natural hazards form an integral part of a modern strategy for survival, sustainability, and competitiveness. Therefore, the market imposes new demands for quality.

These Guidelines are intended for all interested parties and the public. Interested parties includes plant owners, insurers, rescue services, consultants, safety companies and the like so that, in the course of their work, they may be able to help manage risk in society.

The Guidelines reflect best practice developed by the national members of CFPA Europe. Where these Guidelines and national requirements conflict, national requirements shall apply.

This Guideline has been compiled by the Natural Hazards Group and is adopted by the members of CFPA Europe.

More information: www.cfpa-e.eu

Copenhagen, xxxxx 2022
CFPA Europe

Jesper Ditlev
Chairman

Berlin, xxxxx 2022
Natural hazard group

Dr. Mingyi Wang
Chairman

CFPAEUROPE®

Contents

Key words: business resilience, continuity management, emergency response plan

1   Introduction

Business resilience is an essential objective of any risk management strategy. Besides the commonly accepted objectives of protecting the workforce and restoring operations as quickly as possible after an event and limiting the impact on operations, analyzing the performance of the organizational and physical protection systems to the event is a vital feature of resilient organizations. In fact, a resilient organization will use these learnings to improve its response, not only to similar events but to any future shocks.

2   Scope

This document introduces the organizational measures, which will help a business mitigate the effects of a significant and potentially ~~damaging~~ disrupting event, whether natural or man-made, on its operations. This approach to business resilience delivers a framework on which a company can build, whatever its size and whatever the nature of its business.

3   Definitions

Business resilience is the ability of an organization to monitor, respond and learn from a disruptive ~~an~~ event. An organization with a sound business resilience strategy is one that has a higher likelihood of adapting, and even improving through learning, after an event, as it can absorb the shocks without disruption to its operations.

4   Business resilience management and planning

To increase the business resilience of an organization and to ensure a minimum required level for this, hazards and risks must first be identified and assessed, when operational processes of an organization exposed to them and can therefore be affected by them. Fire, natural hazards, burglary and theft and their linked risks are described in existing CFPA-E guidelines with recommendations for loss prevention (see section 11).

In addition, and based on the in-depth understanding about business resilience (see also section 6), the objectives and other elements of organization preparations (see also section 5) and strategy (see also section 7) for achieving them should be defined. Accordingly, the organizational structure including continuity management should be aligned to ensure the implementation of the defined objectives and strategy (see also section 8).

Furthermore, business resilience objectives and their achievement should be regularly reviewed in order to learn from relevant events, if necessary, and to adapt the strategy to the possible changed conditions (section 9).
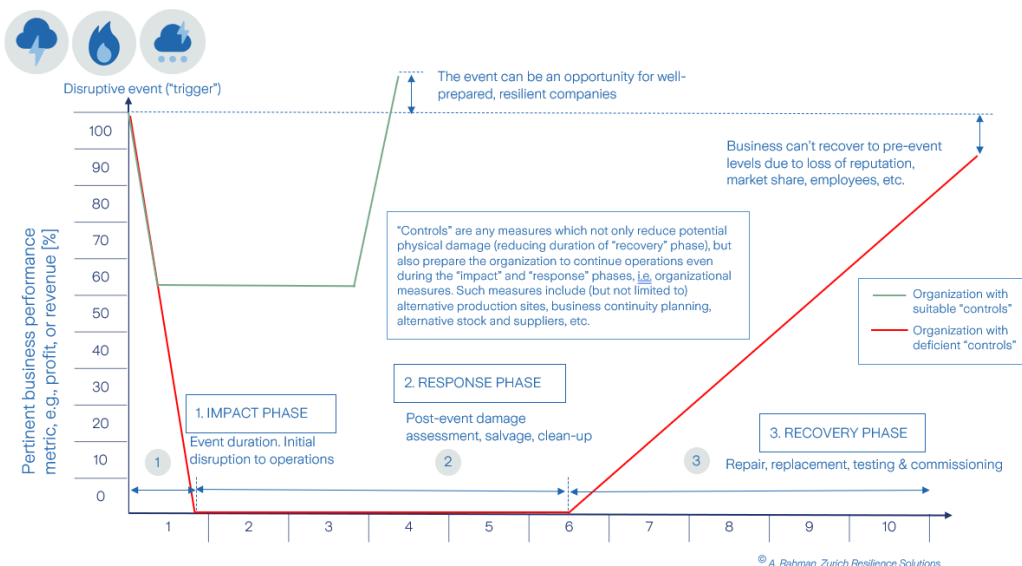
Figure 1: Schematic of recovery of resilient, compared to poorly prepared organizations

5 ~~What is business resilience? (~~New title: Objectives and elements of business resilience plans?)

The goal of a business resilience plan is to reduce the recovery time, and to restore operations to a level at least equal to that prior to the event or, ideally, improve them, based on the lessons learned from the response to the event. Business resilience is not a single measure but a range of measures, physical, organizational, risk transfer, and so on. As an example, organizational measures related to business resilience planning are emergency response plans, business continuity plans, supply chain planning, maintenance plans, and so on.

Generally speaking, a ~~A~~ business continuity plan (BCP) also contains the same elements as an emergency response plan (ERP) in terms of preparation, response, and monitoring. However, a BCP plan is focused on medium- to long-term measures to ensure minimal disruption to operations. The focus of an emergency response plan, on the other hand, is the immediate response to an event.

Business continuity and emergency response plans are key organizational components (amongst others) of a sound business resilience strategy and complement the physical and risk transfer components of business resilience.

6 Understanding the business

As part of a business resilience study the first step is a comprehensive understanding of all aspects of operations is necessary. Depending on the complexity of the type of business, two levels of analysis may be necessary, at group level, in which all locations comprising the organization are

included, and at single location level. For the analysis to be most effective the participation of as many stakeholders as possible is recommended.

Whether a multi- or single location is performed, the following steps are recommended:

1. The term „critical" must be agreed upon. For example, „critical" may include the location(s) (or for single locations, processes, stock, or equipment) which meet one or more of the following criteria:

   - High concentration of value at one location
   - Long replacement times for equipment and/or stock (limited number of suppliers, long delivery route, etc.)
   - Processes that are sensitive to loss of utilities, e.g., require long time for safe shut-down
   - The location is a significant contributor to the group value chain (interdependency) or revenue
   - Large concentration of occupants or population in the immediate vicinity, which could potentially be impacted by an adverse event, e.g., fire, or chemical leakage.
   - Sensitive area around the site that could be impacted environmentally
   - Multiple locations that could be affected by a single event
   - Location relies on workers living in highly exposed and vulnerable neighborhoods, not necessarily adjacent to the location of interest
   - Location relies on public utility and infrastructure services that are highly exposed and vulnerable

2. Perform a value chain analysis at each location, i.e., identify products and associated suppliers, processes, equipment, infrastructure, utilities, population, and so on, which are critical to operations.
3. Identify the hazards associated with each component of the value chain. These hazards may be associated with the location-specific processes (operational risks) or from factors outside the site (non-operational risks), e.g., 3rd party exposures (fuel tank farms), or natural hazard exposures to name a couple. Such hazards may trigger issues such as loss of power supply, denial of access, etc. which could potentially impact operations. Although locations may not be directly impacted, supplier locations may be impacted by an event, which disrupts one's own operations. In addition, employee absence, e. g. denial of access to the place of work due to a natural catastrophe, epidemic or a pandemic, can significantly impact operations.

While hazards that may threaten a business can't be totally eliminated, the likelihood of such an event can be proactively identified and its potential impact can be reduced by incorporating Business Continuity Management System (BCMS).

The BCMS is an important tool to identify and assess hazards and to prepare for (interconnected) risks of any kind, which can interfere with business operations. It creates awareness and a basic structure for more stability and the ability to proactively manage business-critical processes to a predefined level. BCMS is therefore a supplementary management system and serves as a holistic management process that improves business resistance systematically. Such systems are usually developed at group level and would thus require modification and refinement at each location within the group to account for local conditions, e.g., regulatory requirements, supply chain, value chain, and so on.

7   Continuity management structure

Business continuity management system should be integrated into general management of company and organization, linked with its risk management including the interaction to business interruption insurance.

Involvement of all stakeholders essential to operation of the organization will increase likelihood of effectiveness of the BCP.

~~Planning for business resilience is a fundamental requirement of sound risk management practice. The business continuity plan is one potential solution that is the product of the business continuity planning exercise. Other business resilience measures include (but are not limited to) emergency response planning, physical and organizational response measures, transition risk planning, and so on.~~

Figure 2:   Flooding can have a serious and prolonged impact on both small and large business operations

Scenario-based business resilience planning is a very effective risk management tool. Scenario planning not only allows management of complex risk landscapes, which depends on the type of operations of the organization, but also provides a mechanism to assess „emerging" risks, or risks for which no effective tools currently exist or are still in development (climate change, cyber risks, liability, or transition risks related to climate change).

Broadly speaking, such an approach entails identifying the potential hazards and associated vulnerabilities of the operations-critical exposures (see Sec 3). The loss severity is expressed in terms of the loss estimate, with the pertinent probability of occurrence. The probability refers either to the quality of the controls or, e.g., in the case of natural hazards, to the probability of hazard occurrence (expressed sometimes as a „return period", „recurrence interval", etc.), which is in fact a proxy for the design level of the protection systems.

The complexity of the risk landscape is to be considered in the analysis, specifically the fact that the exposure is of a multi-peril nature. As an example, if a site is exposed to fire (operational), flood, windstorm, and EQ (non-operational) then relocating the operations-critical equipment from the basement to the roof (reduce flood risk) will increase windstorm and EQ risks.

8   Develop Your Strategy

In the context of business continuity management, solution may be developed for the short-, medium- or long-term. Ideally, the business continuity plan contains instructions at all three levels, as the duration of the adverse event is difficult to predict, varies according to the type of event, and the duration of the associated consequences may extend much longer than the event itself.

As with any risk management strategy, the business continuity plan should ideally contain not only actions related to the response to an event, but any actions which could potentially mitigate the risk. A resilient organization will also adapt quickly to the risk landscape, which could change during unfolding of events.

The response to any event should be carefully documented to allow the organization to learn, adapt and be better prepared, not only to a future similar event, but to any potential loss trigger (disruptive event).

Actions related to alternative suppliers, relocation of some activities to other locations within the organization or 3rd party sites, alternative sources of utilities and site access routes, communication list of suppliers and customers, notifying them of disruption to operations, and other activities, may be included in the business continuity plan.

Long-term planning may include measures related to risk transfer (insurance), development of alternative locations through acquisitions, greenfield projects, strategic partnerships, etc.
The plan should include all critical exposures yet simple enough that it may be used at all locations or units within the organization.

Regular implementation of the plan is necessary to ensure familiarity as well as its effectiveness and reliability. Changes in markets, suppliers, processes, personnel (especially levels of management responsible for implementation of the plan), and so on may necessitate revision of the BCP. This can only be determined by regular implementation of the plan.

An important component of the BCP is communications both, within the organization as well as externally, e.g., suppliers, customers, and other stakeholders. Internal communications include staff and their families, upper management at Group level, other locations (especially where interdependencies are involved), and so on. A clear communication strategy will avoid distractions related to constant requests from internal stakeholders on status updates. External communications should be managed and implemented by a single, specially trained member of staff. This will avoid confusion and reassure the community, investors, and other stakeholders. All employees should be made aware of the communication policy and communication channels.

9   Lesson learned

Due to the general principles of management systems and in addition to regular review, the recovery management team should also analyze and assess all incidents, related to their cause,

mechanism of extension and efficiency of implemented plan and measures. If necessary, the strategy and recovery plan should be adapted. Such a process contributes significantly to site resilience.

10 Summary

Business Continuity Management is an essential component of the organizational risk management strategy.

As a first step in the development of a business continuity plan (BCP) the „critical" exposures of the organizational processes must be defined both, at Group as well as individual locations levels. Such an assessment should include factors such as processes, infrastructure and utilities, suppliers, equipment and stock, population potentially impacted, and so on. For each of these critical exposures the potential hazards are identified, and the corresponding vulnerabilities (quality of controls in place) assessed. A scenario-based approach is then implemented to determine the severity of the events (in terms of population impacted, and/or financial repercussions) and their probability of occurrence.

The BCP is a list of measures to be implemented for each of these events. The scenario-based approach should also identify the risk mitigation or adaptation measures to be implemented (risk transfer, physical protection measures, organizational measures, etc.) to manage the risk.

Learnings from historical events are essential in developing a resilient organization. Such learnings will support the organization not only in reducing the recovery time, but also in improving operations post-event and possibly even increasing competitive advantage.

11 European guidelines

Fire
Guideline No   1:2015 F -Internal fire protection control
Guideline No   2:2018 F -Panic & emergency exit devices
Guideline No   3:2011 F -Certification of thermographers
Guideline No   4:2010 F -Introduction to qualitative fire risk assessment
Guideline No   5:2016 F -Guidance signs, emergency lighting and general lighting
Guideline No   6:2021 F -Fire safety in care homes
Guideline No   7:2011 F -Safety distance between waste containers and buildings
Guideline No   8:2004 F -Preventing arson – information to young people
Guideline No   9:2012 F -Fire safety in restaurants
Guideline No   10:2008 F -Smoke alarms in the home
Guideline No   11:2015 F -Recommended numbers of fire protection trained staff
Guideline No   12:2012 F -Fire safety basics for hot work operatives
Guideline No   13:2006 F -Fire protection documentation
Guideline No   14:2019 F -Fire protection in information technology facilities
Guideline No   15:2012 F -Fire safety in guest harbours and marinas
Guideline No   16:2016 F -Fire protection in offices
Guideline No   17:2014 F -Fire safety in farm buildings
Guideline No   18:2013 F -Fire protection on chemical manufacturing sites
Guideline No   19:2009 F -Fire safety engineering concerning evacuation from buildings
Guideline No   20:2012 F -Fire safety in camping sites
Guideline No   21:2012 F -Fire prevention on construction sites

Guideline No 22:2012 F -Wind turbines – Fire protection guideline
Guideline No 23:2010 F -Securing the operational readiness of fire control system
Guideline No 24:2016 F -Fire safe homes
Guideline No 25:2010 F -Emergency plan
Guideline No 26:2010 F -Fire protection of temporary buildings on construction sites
Guideline No 27:2011 F -Fire safety in apartment buildings
Guideline No 28:2012 F -Fire safety in laboratories
Guideline No 29:2019 F -Protection of paintings: transports, exhibition and storage
Guideline No 30:2013 F -Managing fire safety in historic buildings
Guideline No 31:2013 F -Protection against self-ignition end explosions in handling and storage
                          -of silage and fodder in farms
Guideline No 32:2014 F -Treatment and storage of waste and combustible secondary raw
                          -materials
Guideline No 33:2015 F -Evacuation of people with disabilities
Guideline No 34:2015 F -Fire safety measures with emergency power supply
Guideline No 35:2015 F -Fire safety in warehouses
Guideline No 36:2017 F -Fire prevention in large tents
Guideline No 37:2018 F -Photovoltaic systems: recommendations on loss prevention

Natural hazards
Guideline No   1:2012 N -Protection against flood
Guideline No   2:2013 N -Business resilience – An introduction to protecting your business
Guideline No   3:2013 N -Protection of buildings against wind damage
Guideline No   4:2013 N -Lighting protection
Guideline No   5:2014 N -Managing heavy snow loads on roofs
Guideline No   6:2016 N -Forest fires
Guideline No   7:2018 N -Demountable / Mobile flood protection systems

Security
Guideline No   1:2010 S -Arson document
Guideline No   2:2010 S -Protection of empty buildings
Guideline No   3:2010 S -Security systems for empty buildings
Guideline No   4:2010 S -Guidance on keyholder selections and duties
Guideline No   5:2012 S -Security guidelines for museums and showrooms
Guideline No   6:2014 S -Security guidelines emergency exit doors in non-residential premises
Guideline No   7:2016 S -Developing evacuation and salvage plans for works of art and
                          -heritage buildings
Guideline No   8:2016 S -Security in schools
Guideline No   9:2016 S -Recommendation for the control of metal theft
Guideline No 10:2016 S -Protection of business intelligence
Guideline No 11:2018 S -Cyber security for small and medium-sized enterprises

Annex 1: Plans

Training plan

A plan for training, exercise and control should be created to get an overview of the information and training needs and that mandatory training and drills are performed with the correct regularity.

The plan should contain requirements and objectives, how the tasks will be monitored and by whom.

Emergency Response Plan

(This should comply with ISO 14001 requirements on emergency preparedness and response) An emergency plan should be drawn up within each activity in order to work through, organise, communicate, and document the organization, and resources necessary to take measures during and after an incident. The emergency plan should be communicated to everyone within the business.

Below is the proposed structure and content of an emergency response plan:

Preparation:
- Define the hazards and associated triggers.
- Identify the resources available
- Identify operations-critical equipment, stock, utilities, etc.
- Develop damage scenarios
- Identify alternative suppliers
- Develop a communication strategy for customers and suppliers
- Define an internal communication and action plan, which defines the emergency response organization (team) and responsibilities, communication strategy within the team and to employees.
- Prepare control measures, corresponding to the identified risks.
- Prepare monitoring and alert (warning) processes
- Prepare a list of suppliers for essential recovery services (repair, restoration of services, material and workmanship) and enter into contractual arrangements
- List of specialist expertise to take care of expected damage (including mental and physical health of personnel).
- Emergency routine for priority salvage.
- Schematic plans with symbols and comments about evacuation routines such as evacuation routes, assembly points, alarm management and emergency response equipment, e.g. fire extinguishing, flood protection, etc.

Response:
- Define the actions corresponding to each alert (warning) level
- Maintain a log (diary) of the incident with photographs. This will support management not only in analyzing the response post-event (lessons learned) but also in the claims handling process with the insurance carrier.
-

Recovery:
- Do not restore services and utilities before these have been checked by qualified personnel.
- Contact the insurance carrier and provide corroborating information related to the loss, e.g., event log (diary)

CFPA EUROPE®
Fire Safety | Security | Natural Hazards

www.cfpa-e.eu