EENA Operations Document

Contingency Plans

Title:	Contingency Plans		
Version:	1.0		
Code:	3.2.2 Contingency Plans		
Revision Date:	02-12-2013		
Status of the document:	Draft	For comments	**Approved**

EENA asbl
info@eena.org - www.eena.org

Contributors to this document

This document was written by members of the EENA Operations Committee:

Members	Country / Organisation
Andy Heward	London Ambulance Service NHS Trust / Chair EENA Operations Committee
Tony O'Brien	EENA
Alexander Bousema	Consultant / Vice-chair EENA Operations Committee (author)
Uberto Delprato	IES / Vice-chair EENA Operations Committee
Mladen Vratonjic	Vice-chair EENA Operations Committee
Cristina Lumbreras	EENA (author)
Joke Bonte	Ministry of Internal affairs, BE
David Lane	IAEM

Legal Disclaimer

This document is authored by EENA staff members with contributions from individual members of EENA and represents the views of EENA. This document does not represent the views of individual members of EENA, or any other parties.

This document is published for information purposes only and it does not declare to be a statement or interpretation of EU law or the national law of EU Member States. This document is entirely without prejudice to the views of relevant national statutory authorities and their legal functions and powers, whether under EU law or the national law of their Member State. Accordingly, under no circumstances may reliance be placed upon this document by any parties in compliance or otherwise with any applicable laws. Neither may reliance be placed upon this document in relation to the suitability or functionality of any technical specifications, or any other matters discussed in it. Legal advice, technical advice and other advice as relevant, may be sought as necessary.

EENA asbl
info@eena.org - www.eena.org

Table of contents

EENA asbl
info@eena.org - www.eena.org

1 Introduction

All public safety answering points (PSAPs) have to be available or reachable 24 hours a day, all year long. However, they may become partially or totally unavailable due to all kind of different reasons such as technical failures, epidemics or natural disasters. Emergency services need to be prepared to react when situations like this occur. Consequently, PSAPs have to ensure that people who are in life-threatening situations and need urgent assistance are able to contact emergency services, calls can be handled and first responders can be dispatched. This can mean the difference between life and death for someone in an emergency.

This document will give an introduction to measures that can be taken to respond to potential disruptions and to recover from these business disruptions and system failures. Also it will give examples in the different areas where these threats can occur. This document is not meant to give a complete implementation guide and give all the in depth possibilities but it tries to give a clear overview of potential measures such as the relocation of staff, use of information technology systems on secondary locations and even fall back to the use of manual procedures when automated systems fail.

Contingency management is not a stand-alone process. It is a process that derives from risk management and should be embedded to standard operations procedures. This document starts introducing how contingency management is related to the risk management process.

Most European emergency services create contingency plans using different approaches. The scope of this document is to gather information on this issue and outline some of the 'best practice' approaches and lessons learned from the authorities' perspective of implementations already executed in the various environments in Europe. The description of practices was obtained through information sent by EENA members. As a conclusion, recommendations and EENA requirements are described.

2 Abbreviations and Glossary

All definitions of terms and acronyms related to 112 are available in the 112 Terminology EENA Operations Document.[1]

[1] www.eena.org/view/en/Committees/112operations/index/generalframework.html

3 Methodology

3.1.1 Risk management

To be able to create a contingency plan there is a need for a risk assessment which is the basis for all situations and occurrences that might appear and could have an impact on normal operations within the PSAP. In this document we will focus on downside risks, i.e. occurrences that are considered threats and have a negative impact on the functioning of the emergency services.

Risk management should cover all different levels: from individual PSAP to nation-wide risk plans. In some cases, collaboration between different countries in case of unavailability of PSAPs should also be planned.

We can establish two levels of contingency plans:

- Individual PSAP's internal risk management
- Cooperation between PSAPs in case of unavailability

A risk assessment can be done in various ways. There are two methods that commonly used: The Kinley method and the Prince II (methodology which is mainly used in project environments).

The first step would be to establish a list of potential risks that could have an impact on the service. After this, a probability of occurrence should be given to each of the elements on the list. This is the only way to decide if measures for this potential risk should be taken or not.

Kinley method
RISK = CHANCE x IMPACT x EXPOSURE

Prince II
RISK = PROBABILITY x IMPACT x PROXIMITY

The two methods take almost the same approach of scoring risks. Prince II is more looking at the potential moment that the risk can occur (proximity) and Kinley is looking at the exposure of the organisation when the risk occurs.

The first step is to make inventory of all elements contributing to the functioning of the PSAP environment. When an organisation has configuration management in place, for example conform IT-Service management approach ITIL[2], it is already much easier to make a list of these elements. Besides the IT components there are numerous other elements that can have an impact on the functioning of emergency services. To be sure that no elements are missed the organisation should be looked at from different perspectives.

To make a usable list of elements commonly the risks can be split up in the following categories;

- Human resources
- Purchasing
- Organisation
- Finance
- ICT (information and communication technology) /Automation
- Communication
- Building and facilities

Although all these aspects will not be covered in this document, it is important to take them into account when writing the list of potential risks. This document will focus on human resources, organisation, ICT, communication, building and facilities.

[2]http://www.itil-officialsite.com/

EENA asbl
info@eena.org - www.eena.org

Once all risk elements are listed the elements can be assessed. What is the chance/probability of a specific element to malfunction/fail/be unavailable and what is the impact on the emergency process when this element malfunctions/fails/is unavailable.

As example we can look at the building of the PSAP. The chance of total unavailability of the building is very low, but if it would happen the impact would be very high (high impact). Consequently the total score for this risk will be high.

After this, the element time (proximity) should be considered. Some elements will only fail and risks only happen at certain moments in time or will only happen when a certain number of events will follow each other. Therefore, the advice is to always include the time element in the assessments especially in a complex environment as the PSAP to stimulate looking not only at the elements but also at the combination of elements and to find "what if" scenarios.

A clear example of an occurrence that will only happen at a certain time is New Year's Eve where there is a spike in the usage of mobile networks around midnight which could result in a temporary disruption of the mobile network. Usually, the risk of massive usage of the mobile network by all citizens would be categorised as low. But in the special date of the 31st of December this risk should be considered as high.

An example of an occurrence that will only happen when multiple elements come together is a rural area where "nothing ever happens" until there is a large festival organised where a storm could result in a dangerous situation. A lot of people suddenly want to use the mobile network to alert the emergency services and to call home. This could result in a breakdown of the mobile network.

Besides the impact a risk can have on emergency services, there are also other aspects to be considered in an active management of a certain risk: social, technological, economics and political aspects (STEP). Especially in emergency services, social and political aspects could be very important and these risks need to be actively managed.

Also there can be situations where handling a risk is so expensive that it is not possible to completely exclude a risk from happening (for example increasing the availability of the infrastructure from 99,999% to 100%).

When all the risks are listed and scored the next step is to find the appropriate way to manage them: accept, avoid, reduce, fall-back or transfer. For the risks that are not acceptable, cannot be avoided, cannot be further reduced and could not be transferred there is a need to be handled when they occur with a fall-back plan (contingency plan).

EENA asbl
info@eena.org - www.eena.org

3.1.2 Contingency management

As described in the risk management methodology, contingency management is only a part of preventing unavailability of an emergency service. The active risk management prevents further damages in case a risk occurs. It makes the service available as quickly as possible using pre-defined (temporary) means and eventually returns it to normal operations.

There is a thin line between risks that are managed by reducing the risk and the ones handled with a contingency plan. A good example could be a secure internet connection being used as back-up for a dedicated network connection between two systems. In case the dedicated network connection fails, the internet connection will automatically take over. It can be considered that this risk has already been managed with this solution because the chance that both connections fail at the same time could be scored very low. But other aspects should be taken into account: the internet connection can be considered as a security risk. Therefore it may be needed that the take over is made with clearance from security officers. The internet connection is then considered as a temporary measure to have the emergency service functionalities available. Consequently, it is considered as a contingency management action.

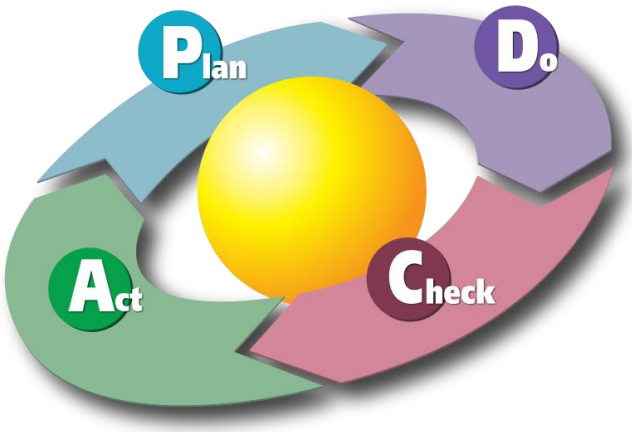
Contingency management is an active process that consists of six steps to be managed and be continuously improved. It is also worth mentioning that contingency management can be only successful when the measures are tested.

Plan
- Fall-back plan

Do
- Implement
- Communicate
- Activate
- Return to normal operations

Check
- Evaluate

Act
- Improve fall-back plan



EENA asbl
info@eena.org - www.eena.org

Fall-back plan

With the risk assessment it was established which elements in the PSAP were critical such as infrastructure, communication connections, building and facilities and personnel. After this, notification procedures and chain of management when a partial or total unavailability situation occurs should be written down in order to get a rapid and comprehensive overview of the damage suffered.

During this phase, the risk management team should constantly evaluate how already identified key assets can be affected, to what extent and if it would not be better to reconsider measures to avoid or reduce the risk or if there are new possibilities to avoid or reduce the risk. Important is to always keep in mind that a contingency plan should always be the last possibility because it disrupts normal operation and could create other risks.

In the fall-back plans the procedure to return to normal operations should not be underestimated. A contingency plan is brought into place because "regular" measures were not good enough to prevent the risk from occurring. So this type of situation could disrupt a lot of normal procedures and ways of working. So besides making sure that the availability of the emergency services is guaranteed the situation should be kept to period as short as possible.

Implementation

After the implementation, the PSAP has to activate its contingency plan and decide on the actions to be carried out following the procedures. Activation of the contingency plan is not starting with a fall-back procedure but being ready to act when it is needed.

Communicate

The implementation needs to be followed by communication of the contingency plans and education, dry runs and fall-back tests need to be performed to be sure that in case of the risk occurring everybody knows what to do.

Activate (temporary) measures

Then when a fall-back plan goes into effect it should be clear who, how and when to act to implement the temporary measures to keep the threatened/failing emergency service functionality up and running.

Return to normal operations

After the situation is under control (for example the failed components are restored or the people are healthy again after a flu epidemic) the temporary measures should be reversed and normal operations should be restored. After this it is very important to see if the fall-back procedures and fall-back components are also brought back into a state that they can be re-used again when needed.

After restoring the normal operations it is good practice to do a complete test cycle of all functionalities to assure that the situation is really back to normal and all functionality, people and infrastructure is working properly again.

Evaluate

After a fall-back plan was used or tested it should be evaluated. Here it is very important to revisit the other possibilities to manage the risks. For example, looking at new technologies that can prevent the risk and even vaccination against diseases of key personnel could be considered to prevent the emergency services to be unavailable when an epidemic occurs.

4 Individual PSAPs internal contingency plan

This chapter is intended to review the main causes that may affect partially or totally the availability of an individual PSAP. Additionally, preventive measures are also described. Examples of how corrective measures should be described in the contingency plan have been added.

4.1 Infrastructure failures

4.1.1 Description

We consider all essential supplies to be part of the infrastructure necessary for the operation of the PSAP. The most common and potentially problematic failures are listed below:

- Power failure: this results into an immediate disruption of the PSAPs operations.
- Heating/air conditioning failure: depending on the building, the climate and the season, this kind of failure can affect significantly the ability of the PSAPs staff to carry out its tasks.

  It is also worth mentioning that servers and other machines need a stable temperature to function. A disruption in the cooling system of these appliances can be equally prejudicial to the PSAP.
- Water supply failure: such a problem can also have an impact on the staff's well being, and can become a major difficulty if it lasts for many hours or even days.
- Telecommunication networks: for a PSAP it is crucial to be reachable through the telecommunication network. If it completely fails, calls shall be routed to another PSAP (see Cooperation between PSAPs contingency plans chapter).

4.1.2 Preventive measures

The ideal way to prevent infrastructure failures is to take them into account when designing or choosing the PSAP building.

Furthermore, many additional issues can be avoided with proper maintenance and operation of the PSAPs electricity, heating, air conditioning and water appliances. This includes periodic revisions of the whole installation.

The maintenance staff (whether part of the PSAP or outside contractors) should be readily available when a problem occurs. If the PSAP decides to outsource maintenance, the contract should include clauses specifying typical intervention times or availability statistics.

In all cases, a plan should be prepared to cater for all possible failures. For each of these failures, the plan should appoint a responsible member of staff and include necessary information to act (for example the contact number of the maintenance person or company or other useful data).

To avoid power failures, the most commonly available solution is the installation of thermal electricity generators. This will also prevent that the heating and air conditioning fails. An alternative could be a different electricity supply (e.g. connection to the mid or high voltage network instead of the local low voltage network).

Regarding heating and air conditioning problems, a temporary answer can be given by electricity powered radiators or fans. Furthermore, for water supply, water containers or chemical toilets should enhance temporarily the situation.

For telephone networks, the effect of failures can be mitigated or even cancelled if the PSAP contracts several operators and if it has more than one point of interconnection with the network.

4.1.3 Example of procedure in the contingency plan

In the contingency plan, a procedure for each case has to be defined. A person has to be responsible to follow the predefined plan. Below you will find a simplified example.

Type of failure	Responsible member of staff	Steps to be taken
Power supply	Office hours: security officer Rest of hours: supervisor	Call the electricity supplier on telephone XXX (this is an already agreed telephone number)

4.2 Software and functionality

An information technology (IT) failure is normally independent from a telecommunications failure. The voice communication is established between the caller and the operator, but the operator is unable to properly handle the call because the IT system is partially or totally unavailable (for example caller location, geographic information system or databases).

4.2.1 Preventive measures

For IT infrastructure and software, it is essential that PSAPs have redundant systems and services. Many issues can be avoided with proper administration. The maintenance staff (be it part of the PSAP or outside contractors) should be either present or quickly available when an IT crash occurs. If the PSAP decides to outsource maintenance, the contract should include clauses specifying typical intervention times. A plan including all possible incidents should be drafted. The plan should describe who is responsible amongst the staff and include any necessary information to act.

It is of the utmost importance that operators answering calls are trained to use conventional tools (paper and pen) if the IT infrastructure happens to fail. This means that they need to have in mind a clear idea of the key questions to ask to the caller, the protocols to follow and the ability to locate the caller (with physical maps for instance).

4.2.2 Example of procedure in the contingency plan

As an example, we show how the IT contingency plan may be described:

Type of incident	Responsible member of staff	Actions to be carried out
Geographic Information System failure	Supervisor	Inform operators and tell them to use physical maps, inform IT maintenance team.

EENA asbl
info@eena.org - www.eena.org

4.3 Human resources

Human Resources are the PSAP´s most valuable asset. If the workers are exposed to an epidemic, the PSAP has to be able to respond appropriately to maintain its quality of service to the citizens.

4.3.1 Preventive measures

Additional staff has to be on standby duty to be alerted in case of need. An internal procedure describing the steps to be taken in case of complete or partial unavailability of calls has to be available for PSAP's staff.

4.3.2 Example of procedure in the contingency plan

The HR contingency plan may be presented as follows:

Type of incident	Responsible member of staff	Actions to be carried out
40% of operators on sick leave	HR Director	Call standby staff
>50% of operators on sick leave	Operations officer	Initiate "re-routing of calls to buddy" procedure

4.4 Need of evacuation of the building

It may result necessary under some circumstances such as bomb threats, fire or flooding to evacuate the PSAP building. In these cases, the main objectives are to protect staff and minimise the disruption in the emergency call taking.

4.4.1 Preventive measures

In any event, an evacuation plan should be devised, including for instance a clear marking of exits and exit paths as well as sound or visual alarms. In parallel, there should regular evacuation trials involving the whole staff to make sure that they evacuate the building as quickly as possible if the need arises.

The PSAP should ensure that incoming emergency calls can be rerouted to another as subsequently described in the document.

Ideally, a backup centre should be available where all operators could be redeployed and continue operating normally.

4.4.2 Example of procedure in the contingency plan

The evacuation plan may be presented as follows:

Type of incident	Responsible member of staff	Actions to be carried out
Fire alarm	Supervisor	Evacuate building, alert fire brigade, inform other PSAPs

5 Cooperation between PSAPs contingency plans

As described in the previous chapter, many circumstances occurring in an individual PSAP, may have the total unavailability of an individual PSAP. Consequently, calls needs to be rerouted to another PSAP to ensure the service. A policy of rerouting emergency calls to another PSAP in case of unavailability or overload has to be established. For this, a minimum interconnection of centres is needed. These policies should, if possible, be automated in the telephony network and be implemented without human involvement. In addition, catastrophic situations, e.g. weather events, may have a devastating impact on communications infrastructure. Telecommunication operators and public authorities have to concentrate efforts to assure the access to emergency services even in force majeure situations.

6 EENA recommendations

As a summary of this document EENA would like to make recommendations about how to manage contingency plans and inform the stakeholders that are involved. It is not intended that all measures are to be taken in all cases. Each emergency service needs to develop its own contingency plans that fit that agencies unique environment. Not all the above recommendations are a good fit for all agencies.

Stakeholders	Actions
European Authorities	Enforce compliance with the Universal Service Directive
National telecommunication regulator Network operators	Enforce compliance with laws about access to emergency services
Telecommunication operators	Ensure access to emergency services Ensure rerouting to another PSAP in case of unavailability as planned by the national/regional authorities
National / Regional Authorities	Create general contingency plans to ensure rerouting of calls in case of unavailability of PSAPs
Emergency services	Create its particular detailed contingency plan(s) for all risks that can disrupt the service Assure optimal maintenance of the PSAPs' infrastructure and software components

7 EENA Requirements

Requirements	
Detailed contingency plan with actions and responsible staff	Compulsory
High level plan to reroute calls to other PSAPs in case of total unavailability of a PSAP	Compulsory

EENA asbl
info@eena.org - www.eena.org