European Commission

JRC TECHNICAL REPORTS

Guidance on the production of a water security plan for drinking water supply

ERNCIP Chemical and Biological (CB) Risks to Drinking Water Thematic Group

Teixeira, R.
Carmi, O.
Raich, J.
Gattinesi, P.
Hohenblum, P.

Theocharidou, M. (Ed.)
Giannopoulos, G. (Ed.)

2019

The research leading to these results has received funding from the European Union as part of the European Reference Network for Critical Infrastructure Protection project.

Joint Research Centre

EUR 29846 EN

Contact information
Name: Georgios GIANNOPOULOS
Address: via E. Fermi 2749, 21027, Ispra (VA), Italy
Email: georgios.giannopouls@ec.europa.eu
Tel. +39 0332786211

JRC Science Hub
https://ec.europa.eu/jrc

JRC116548

EUR 29846 EN

PDF ISBN 978-92-76-10967-9 ISSN 1831-9424 doi:10.2760/415051

Luxembourg: Publications Office of the European Union, 2019

How to cite this report: Teixeira et al., *Guidance for the production of a water security plan for drinking water supply*, EUR 29846, Publications Office of the European Union, 2019, Luxembourg, 2019, ISBN 978-92-76-10967-9, doi:10.2760/415051, JRC116548.

Contents

Acknowledgements

This work received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 775989, as part of the European Reference Network for Critical Infrastructure Protection project. The authors would like to express their sincere gratitude to the Portuguese security and intelligence service, the Directorate-General for Migration and Home Affairs, and EurEau (the European Federation of National Associations of Water Services) for providing feedback on and insights into the document and the issues covered.

Authors

Rui TEIXEIRA, Municipality of Barreiro (Waters of Barreiro), Portugal

Ofer CARMI, Hagihon, Israel

Jordi RAICH MONTIU, s::can, Spain

Peter GATTINESI, United Kingdom

Philipp HOHENBLUM, Environment Agency Austria, Austria

Contributors

Montserrat BATLLE RIBAS, Adasa, Spain

Thomas BERNARD, Fraunhofer IOSB, Germany

Eric CHAUVEHEID, Vivaqua, Belgium

Jean Francois RENARD, Suez Eau France SAS, France

Vaclav JIRKOVSKY, Czech Technical University in Prague, Czechia

Kálmán KONCZ, AQUASERV SA, Romania

Miquel PARAIRA, Aigües de Barcelona, Spain

Maria ROSARIO COELHO, Águas do Algarve, Portugal

Luís SIMAS, ERSAR, Portugal

Andreas WEINGARTNER, s::can, Austria

Editor

Marianthi THEOCHARIDOU, European Commission, Joint Research Centre, Italy

Georgios GIANNOPOULOS, European Commission, Joint Research Centre, Italy

Abstract

Although European Directive 2008/114/EC on the protection of critical infrastructures (Council of the European Union, 2008) does not designate the water supply sector as a critical infrastructure, all governments recognise that their water supply is vital to national security. Water systems are vulnerable to unintentional and intentional threats, which can include physical acts of sabotage, cyberattack on information systems or supervisory control and data acquisition systems, and contamination.

In the event of the anomalous situation of the contamination of drinking water, it is essential that the impacts of potential health risks are minimised during and after the emergency. This document provides guidance to water utility operators on assessing the risks they face and on the factors to consider if they want to improve their detection capabilities. Guidance is also provided on the preparation of response and recovery plans in the event of a contamination event.

Water security planning will help to identify security vulnerabilities and establish security measures to detect the intentional contamination of water supply systems, including a communication strategy to facilitate a fast and effective response. Where a water safety plan already exists, water security planning should be integrated into the safety planning approach.

The first step in water security planning is for the water utility operator to assess the risks of threats of the deliberate contamination of drinking water, with the risk assessment providing the basis for the design and implementation of the water security plan. Through this risk assessment process, a target protection level could be set, with utility operators identifying the benefits of installing sensors in the network together with event detection software and/or an event detection procedure. Criteria such as time taken to detect contamination and the volume of contaminated water supplied will help to establish sensor deployment options.

It is recommended that the process for the creation and maintenance of a water security plan comprise four phases:

1. phase 1 —planning and preparation;
2. phase 2 —protection (event detection and confirmation);
3. phase 3 — response (planning and management of the event);
4. phase 4 — remediation and recovery.

Planning and preparation will include creating and maintaining the water security plan, allocating roles and responsibilities, undertaking risk assessments to identify mitigation and security measures, and performing the relevant training and practical exercises. When an emergency occurs, it is vital not to waste time deciding how to act and debating what information to communicate to consumers. Advance planning for an emergency will help to mitigate its impacts by ensuring timely communication and the rapid implementation of mitigation measures.

Event detection involves the monitoring of indicators and allows an immediate response in the case of potential contamination, followed by confirmation of the nature of the event. For the identification of possible emergency situations, water utility operators rely on information from monitoring and control systems, which can quickly identify an anomalous situation, and on information from various external sources.

Online contamination warning systems are one focus of water security planning, along with customer complaint monitoring, public health surveillance and enhanced security.

Online contamination monitoring is most likely to minimise the consequences of intentional contamination, although, to ensure the timely detection of contamination, such monitoring must be integrated into routine operational monitoring.

An immediate response in the event that contamination is confirmed is critical, involving communication with the public and with local/national emergency authorities, to ensure that the public has access to a safe drinking water supply. This response phase is followed by the remedial activities that lead to a full return to the normal provision of uncontaminated drinking water. The remediation and rehabilitation phase forms the final step in the water security plan and will need to be developed after the contamination incident has been confirmed and the full extent determined.

Regular revision of the water security plan is an essential part of its life cycle.

All drinking water systems are vulnerable to some degree to contamination, with experience indicating that the threat of deliberate contamination is real. While steps can be taken to prevent intentional contamination, it is impossible to completely eliminate this risk; therefore, water utility operators need to consider developing and implementing water security plans.

1. Introduction

1.1. Context

Managers of water supply systems are becoming increasingly aware of the importance of a water security plan for responding to emergency situations, as there are now many factors that can negatively influence the quality of the water supplied to populations through the introduction of microbiological, chemical or radiological hazards.

An emergency situation is generally defined as something that arises unexpectedly and can have significant negative consequences if quick and effective corrective action is not taken. Emergencies may result from water supply interruptions or damage to infrastructural components, but other situations may also arise that may cause water contamination and pose a risk to the health of consumers.

In the event of the anomalous situation of the contamination of drinking water, intentionally or accidentally, a water security plan is essential to ensure the most effective response and communication. Such a plan can minimise the impacts of potential health risks during and after the emergency and also help to establish measures to prevent such situations from occurring.

The aim of a water security plan is to support water utility operators to improve the security of their water supply systems.

As any deliberate contamination of drinking water is likely to be perceived as an act of terrorism, the security plan should be developed in the context of the relevant national and European counterterrorism initiatives. For example, as part of the EU's counterterrorism strategy, the European Commission maintains a chemical, biological, radiological and nuclear (CBRN) action plan to enhance preparedness against CBRN security risks. The 2017 CBRN action plan details a number of measures at national and European levels, including measures aimed at ensuring more robust preparedness for and responses to CBRN security incidents (European Commission, 2017).

These proposals for a water security plan were developed by the European Reference Network for Critical Infrastructure Protection (ERNCIP) Chemical and Biological (CB) Risks to Drinking Water Thematic Group ([1]). Earlier proposals for this guidance include those by Weingartner and Raich-Montiu (2015) and Hohenblum et al. (2016).

1.2. Purpose of this document

The purpose of this document is to assist water utility operators with the establishment of a water security plan within their organisation. A water security plan should be seen as a tool to be prepared and used when the security of a drinking water supply is pursued within an organisation, and it should provide clarity on what to do in the event of an unexpected water security emergency.

This document provides guidance to water utility operators on assessing the risks they face and on the factors to consider if they want to improve their detection capabilities.

([1]) The ERNCIP was established as one of the specific measures under the 2017 CBRN action plan (European Commission, 2017), which aims to enhance the EU's knowledge of CBRN risks (Gattinesi, 2018).

Guidance is also provided on the preparation of response and recovery plans to be used in case of a contamination event.

The decision to establish a water security plan should not require a large investment or be very time consuming. On the contrary, water utility operators should be able to assess the feasibility of implementing the desired level of protection using existing resources within the organisation.

1.3. Purpose of a water security plan

A water security plan should be established before an unexpected emergency event happens, to mitigate intentional contamination (e.g. terrorist attacks) of drinking water. It should increase awareness of potential threats and enable the timely detection of anomalous situations. A water security plan will help to identify security vulnerabilities and establish measures to protect the security of water supply systems by detecting intentional contamination. In particular, it should identify measures to respond to verified contamination events, to mitigate or eliminate their impacts, including a communication strategy that will facilitate a fast and effective response. A water security plan should aim to (ERSAR, 2018; Teixeira and Cabanas, 2018):

- establish a preventive and awareness-raising plan, protection and response measures, and a remediation and recovery plan, as well as emergency drills and training exercises to assess and correct vulnerabilities in the system;
- identify internal and external communication channels, especially with the public, to be used in the event of an emergency situation that may influence the operation of the supply of water for human consumption, defining communication responsibilities (e.g. who reports the event, who coordinates the operations to respond as necessary and who makes the decisions);
- define the communication actions necessary during the process of returning to the normal operation of the water supply system;
- provide for the review of the plan on a regular basis and after an event or emergency drill, or whenever justified.

EVENT
Anomalous or unexpected situation, which jeopardises the normal functioning of the system for supplying water for human consumption.

For the preparation and implementation of this plan, a multidisciplinary team should be established, drawn from the relevant departments of the water utility operator, such as operations and management, with representatives from the various external entities involved in security, water supply and civil contingencies.

Ideally, a water security plan will align fully with conventional approaches to consumer protection established by good practice in standard operating procedures, general drinking water standards and any other plans already implemented, such as a water

safety plan [2] or any local/national emergency plans. This guidance supports the development of a separate stand-alone water security plan in cases where a water safety plan is not yet in place and encourages a complementary approach in cases where there are existing water safety plans, including the consideration of an integrated approach where relevant.

When in place in an organisation, a water security plan is expected to:

- decrease the probability of a contamination event not being detected;
- facilitate a more effective and adequate response to any emergency situation, reducing the risk to the public;
- allow the quicker restoration of normality;
- define clear responsibilities and roles within the organisation and for all authorities, agencies and other entities involved in the event of an emergency;
- allow a move from corrective to preventive maintenance;
- enable the better use of online systems/real-time data, giving improved water quality though:
    - the more cost-effective provision of near real-time data, for the detection and management of events;
    - providing information on water quality that is linked with other data from flowmeters, valves, etc.;
- improve the security culture in the organisation;
- improve the continuity of the organisation's operations in the face of any eventuality;
- better define internal, external and public communication procedures;
- facilitate better cooperation between the organisation and authorities, agencies, external entities, users and the population in general.

1.4. Scope of a water security plan

In defining the scope of a water security plan, potential emergency scenarios could be identified at the various stages of the water supply system that may result in water contamination or impede supply. So, while a water security plan mainly focuses on mitigating the intentional contamination of the water supply system, other situations may also be considered, such as those discussed by Weingartner and Raich-Montiu (2015), ERSAR (2018), and Teixeira and Cabanas (2018):

- accidents in the water supply system;
- outbreaks caused by waterborne diseases;
- natural disasters.

Low-probability, high-impact contamination is typically anthropogenic and characterised by a fast increase in the level and concentration of the contaminant, requiring a fast, as close as possible to real-time, detection and response from the water utility operator. To address this risk of intentional or accidental contamination of the drinking water supply, a water security plan should be prepared. Where a safety

[2] In 2004, the World Health Organization (WHO) issued *Guidelines for drinking-water quality*, which recommended that water suppliers develop and implement 'Water Safety Plans' (WHO, 2004). The scope and purpose of these plans are described in WHO, 2009. The use of water safety plans is also encouraged by the EU's Drinking Water Directive (Council Directive 98/83/EC).

plan already exists, the security plan should be an extension of the existing water safety plan and integrated into the water safety plan.
Deliberate contamination that is deemed to constitute a terrorist situation will be considered a serious tactical-police incident. While the designation may vary between countries, the overall management of the incident will probably rest with the national counterterrorism authorities, including the role of coordinating the various security forces and services.

It is therefore imperative to evaluate the application of a water security plan in conjunction with local and national emergency plans — which define the management approaches and procedures to be adopted (response measures) in emergency situations that put the health and safety of people at risk — the preservation of material and technical infrastructure assets, and the continuity of service of water supply systems.

The physical protection of infrastructure assets is an integral part of security planning. However, detailed guidance on physical protection is outside the scope of these guidelines, as such guidance requires different expertise. Readers are advised to consult the relevant guidelines and standards for physical security.

The cybersecurity of control systems is another integral part of security planning, as the causes of intentional water contamination could include cyber-related components. Under the directive on the security of network and information systems (NIS directive) (European Parliament and Council of the European Union, 2016), operators of essential services (including the operators of water supplies) have to take appropriate security measures and notify the relevant national authority of serious cyber-related incidents. Such measures include preventing cyber-related risks, ensuring the security of network and information systems, and handling cyber-related incidents. Detailed guidance on cybersecurity ([3]) is outside the scope of these guidelines. Readers are advised to consult relevant standards, such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 family of information security management systems standards.

Finally, guidance on radiological contamination is also outside the scope of these guidelines. This document will therefore make only general references to these aspects where relevant.

([3]) The NIS directive (Directive (EU) 2016/1148) is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

2. Water security plan design

2.1. Introduction to water security planning

The purpose of this section is to outline the potential contents of a water security plan and to give guidance to water utility operators on assessing their need for water security planning to mitigate potential deliberate chemical or biological contamination of the water supply.

In deciding on whether or not to undertake water security planning, water utility operators will need to prepare by ensuring that the relevant information and personnel are available. As described by ERSAR (2018) and Teixeira and Cabanas (2018), this would typically include:

— a full physical description of their water supply infrastructure, including details of any existing water safety plans, and any relevant local/national emergency plans (see subsection 2.2);
— an awareness of potential threats in their region and sector, including threats arising from terrorism (see subsection 2.3);
— the identification of the roles and responsibilities in relation to security planning within their organisation (see subsection 2.4).

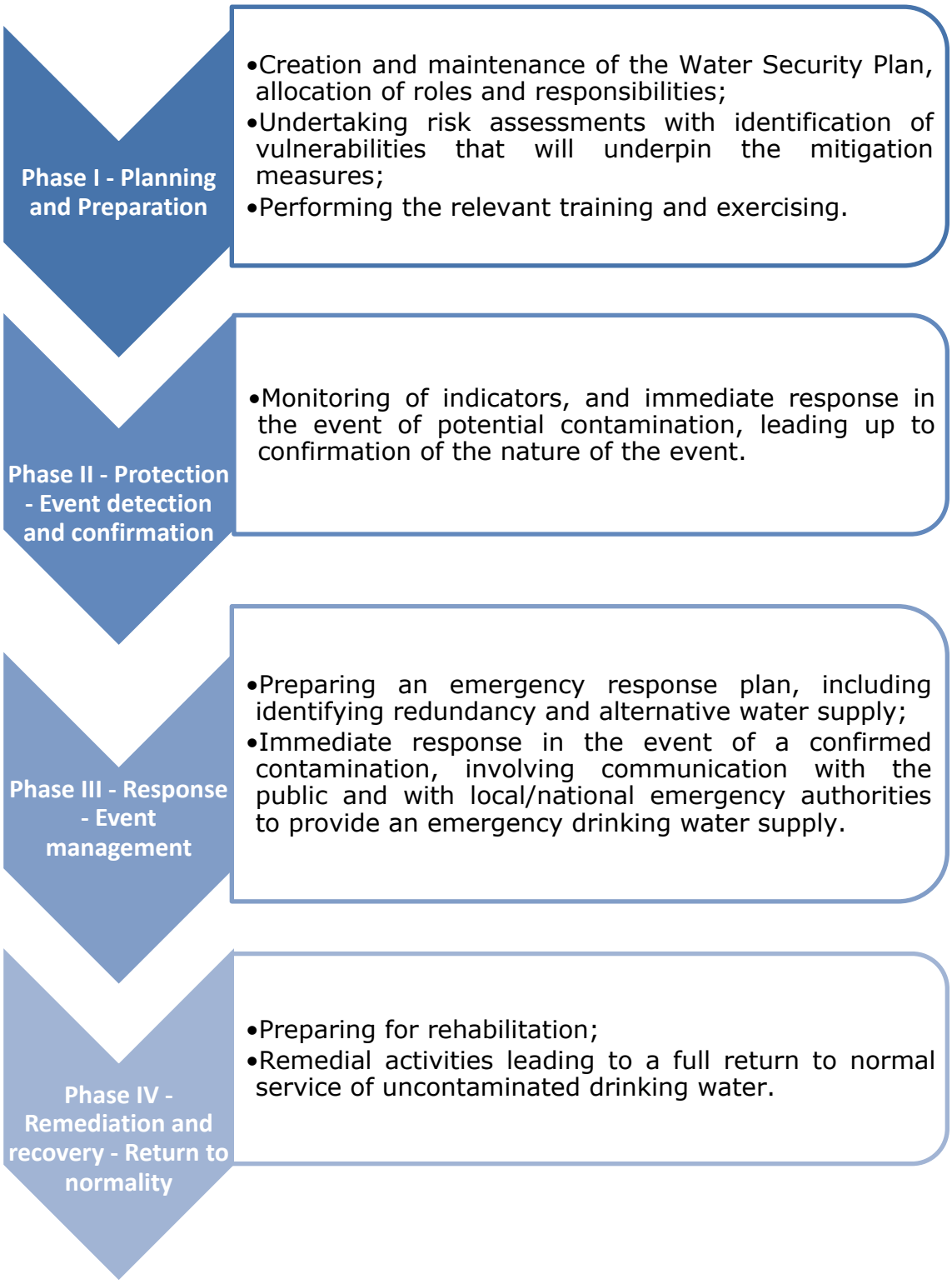
To initiate water security planning, the available preparatory information needs to be assessed by the water utility operator, to identify risks in relation to threats of the deliberate contamination of drinking water. This risk assessment (see subsection 2.5) will also provide the basis for the design and implementation of the water security plan.

If, as a result of the initial assessment by the water utility operator, the need for a water security plan is confirmed, this guidance document could be used to provide recommendations in terms of creating and maintaining a water security plan. This process is structured into the following four phases, corresponding to the timeline of the development of a potential contamination emergency (adapted from Council of the European Union, 2005):

1. phase 1 — planning and preparation;
2. phase 2 — protection (event detection and confirmation);
3. phase 3 — response (planning and management of the event);
4. phase 4 — remediation and recovery.

These phases are outlined in Figure 1 and will be discussed in detail in Section 3.

Figure 1. Outline of the phases of a water security plan



Source: JRC, 2019

2.2. General characterisation of a water supply system

To undertake water security planning, the water utility operator will need a detailed description of the entire water supply system, from water sources and the facilities for the treatment, storage and distribution of water to the tap of the consumer (ERSAR, 2018; Teixeira and Cabanas, 2018). The description of the system should be complemented by location maps for the various types of infrastructure, maps indicating the location of sensitive customers served by the supply system and the identification of alternative supply systems and redundancies in the system, which will be necessary for the definition of response measures and the evaluation of their extent.

For example, the description of the supply system could refer to documents from the water utility operator's maintenance department, to a water safety plan or to the general emergency plan, if this information is kept up to date.

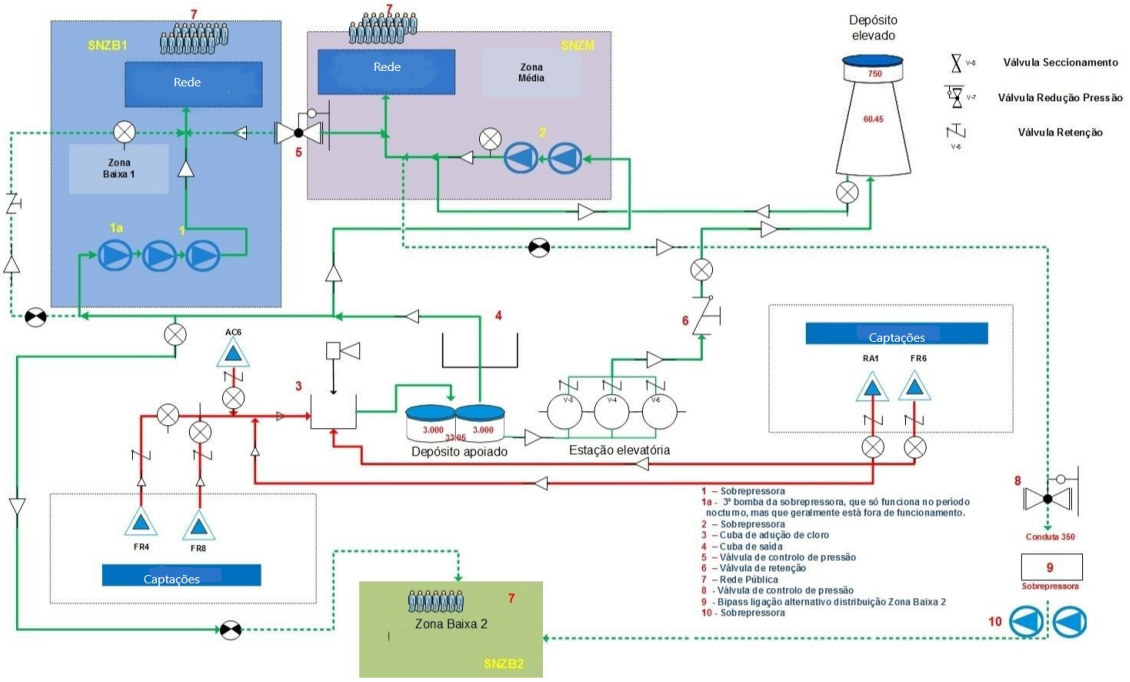
Table 1 provides a summary of the infrastructure types of an example water supply system. Figure 2 shows the general architecture of a subsystem of this water supply system.

Table 1. Summary of the infrastructure types of an example water supply system

Stage	Infrastructure type	Quantities
Sources	Abstractions/water treatment stations	12
Supply system and reservoirs	Pumping stations	3
	Supply system pipes	16 km
	Reservoirs	7
	Treatment facilities	5
Distribution network	Blowers/pumping stations	5
	Distribution network	310 km

Source: Teixeira and Cabanas, 2018

Figure 2. General architecture of a subsystem of a water supply system



Source: Teixeira and Cabanas, 2018

2.3. Threat identification guidance

The primary purpose of a water security plan is to enable a better response to incidents affecting a water supply system (Janke et al., 2014; ERSAR, 2018; Teixeira and Cabanas, 2018), such as:

- deliberate contamination with hazardous chemicals (terrorism) or biological agents (bioterrorism);
- contamination resulting from cyberterrorism;
- sabotage;
- vandalism.

INCIDENT

Any event resulting from intentional human action with the objective of affecting the quality and/or quantity of water for consumption.

The perpetrators of these incidents can generally be categorised as either **internal** or **external** to the water utility operator or its community.

Internal threats may be from disgruntled employees currently or previously employed by the organisation, or service providers or external suppliers that have access to the organisation. A 'disgruntled trusted insider' poses the greatest threat, because of the combination of intent, knowledge and capability. **External threats** range from mindless vandalism to state-sponsored terrorism.

Critical infrastructure is an attractive target for terrorists because of the potential consequences and ripple effects of a successful attack. The distribution components of a water system are especially at risk because of the potentially large number of people

who could be affected by an attack. The potential sources of such terrorism are not limited to conventional terrorist organisations such as al-Qaida and Islamic State/Daesh. Lone-wolf actors are known to have conspired to use chemical or biological weapons to attack a water system (Aldersley, 2018), and state-sponsored actors also have the means to undertake such attacks, as demonstrated at Salisbury, UK, in 2018.

The availability of information about the threats posed by terrorism varies across Member States. Some countries have proactive agencies monitoring the threats from terrorism, while other countries may include consideration of these threats in national risk assessments.

Water utility operators will need to refer to their relevant national/local security authorities or security intelligence services to obtain whatever relevant threat information is available to them.

2.4. Allocation of responsibilities and the constitution of teams (internal team and external entities)

When an emergency occurs, it is vital not to waste time deciding how to act and what information to communicate to consumers. Planning for an emergency will help to mitigate its impacts by ensuring timely communication and the rapid implementation of mitigation measures.

It is therefore fundamental to identify who will be involved in communicating information regarding the emergency situation and implementing the response measures, internally and externally, that is, to establish the water security plan's coordination team and define the rules of operation, the communication channels and the responsibilities of each team member (EPA, 2018; ERSAR, 2018; Teixeira and Cabanas, 2018). Senior management support is crucial to ensure that the necessary priorities for implementing the water security plan are defined, and to facilitate any changes in working practices.

Examples of how these roles and responsibilities might be defined are found in Annex 1 — Examples of roles and responsibilities in water security planning. A key role will be the emergency event manager, who will be supported by a multidisciplinary coordination team, which should involve top-level management and also the various operational areas that are directly involved in the water supply system.

2.5. Risk assessment and water security

As discussed in subsection 2.1, the first step in security planning should be risk assessment, whereby any potential threats of malicious activities identified are considered in conjunction with the vulnerabilities of the water system infrastructure to identify the potential impact from an incident, in terms of casualties and numbers of people affected by loss of access to drinking water. From this assessment, the risks to the operator and its customers, particularly hospitals, military, administrative or government buildings, stadiums, hotels and other places of tourist accommodation, and commercial centres, where the contamination of drinking water could have serious consequences, can be assessed.

The following are common elements of security risk assessments and any evaluation method should incorporate these points (Janke et al., 2014; Silva, 2015):

- the characterisation of the water system, including its mission and objectives;
- an assessment of the threats to the water system;
- an assessment of the probability of each of these threats materialising (based on past incidents or information from national authorities, security intelligence services, etc.);
- a consideration of how the most likely threats could materialise (since they should be addressed first), i.e. a consideration of potential modi operandi;
- a consideration of what security issues are likely to be exploited by threat agents to materialise threats;
- an assessment of the potential impacts of exploiting each of these vulnerabilities;
- a definition of and the implementation of security measures (protection) with a view to reducing or eliminating the vulnerabilities identified;
- a definition of and the implementation of measures to reduce the impacts arising from the exploitation of vulnerabilities by threat agents (crisis management, resilience, redundancies, recovery, business continuity).

The risk assessment will provide the basis for the design and implementation of the water security plan. It will also provide a basis for future reviews of the plan, by enabling the identification of any changes to the risks as a result of updates to the infrastructure or based on new intelligence on threats of deliberate contamination.

Because the risk assessment produced by a water utility operator will inevitably highlight weaknesses and the security measures to be taken, the assessment will be extremely sensitive and will need to be carefully managed by the utility operator. This may apply particularly to certain sections of the utility operator's security plan, and therefore the utility operator will need to apply appropriate measures to the water security plan it produces, such as making sensitive parts available to only trusted individuals within the organisation on a 'need to know' basis. It is also recommended that care be taken with any electronic storage or communication of such sensitive sections, even within the utility operator's own systems.

However, some elements of the security plan will need to be widely available to the staff of the utility operator and to key external stakeholders. Therefore, it is recommended that a security plan have two parts: a main part that is available to all relevant staff within the utility organisation and external partners, and a separate annex for the sensitive sections, the availability of which should be tightly controlled. Advice on protecting the security of sensitive information should be available through local law enforcement agencies, security authorities or security intelligence services.

Threats must be analysed 'in perspective'. The utility operator will need to assess its weakest points and consider what actions a potential attacker might employ against these points. From this, the water utility operator will be able to identify its level of exposure. The probability associated with a potential threat could be estimated for a determined period of time related to a long-term relative occurrence frequency or to a degree of confidence that an event will occur. For example, a probability scale could be adopted that identifies a low, moderate or high probability of the threat materialising in the short, medium and long terms.

Through this risk assessment process, a protection level should be set as a target. By analysing consequences, utility operators could identify critical components, harden or secure those that could reasonably be better protected and develop plans on how to respond in the event of a successful attack.

The risk assessment will also inform the water utility operator of the benefits of installing sensors in the network together with implementing event detection software and/or an event detection procedure. Criteria such as the shortest possible time to detect the event and also minimising the volume of contaminated water supplied will help to identify sensor deployment options.

In summary, a risk assessment is essential because it will allow the system's security vulnerabilities to be identified, which serves as the basis for the design and implementation of the water security plan.

2.6. Conclusion

A water security plan should be considered complementary to verifying compliance with legal drinking water quality requirements and any existing water safety plan. The aim of implementing a water security plan is to detect any intentional contamination of drinking water in the shortest possible time and to minimise or eliminate hazards to consumers. The incorporation of security-driven measures into the daily operations of a water utility organisation could also help to detect other safety issues, in particular the following accidents (ERSAR, 2018; Teixeira and Cabanas, 2018):

— electric power failures;
— failures in electromechanical equipment;
— bursts in water mains;
— bursts in collectors adjacent to water pipes;
— the accidental contamination of water treated by clandestine connections to the network;
— the contamination of water by chemicals used in water treatment;
— fires in facilities;
— civil construction accidents;
— exposed pipelines;
— the existence of wells and holes in the vicinity of the public supply system, as well as the existence of unsealed holes or inadequately sealed holes;
— road accidents in the vicinity of water sources or reservoirs;
— the extravasation of chemicals from the retention basin resulting from accidents at Seveso companies and/or other dangerous industries;
— mechanical effects resulting from explosions at companies covered by the Seveso Directive and/or other dangerous industries.

ACCIDENT
Any event resulting from natural causes or involuntary or negligent human actions that affects the quality and/or quantity of water for human consumption.

Likewise, the implementation of water security plan measures could also result in the detection of outbreaks of waterborne diseases, such as:

— disease due to *Legionella*;
— disease due to *Cryptosporidium*;
— disease caused by another microbiological agent;
— disease caused by a chemical contaminant.

The effectiveness of any water security plan will depend on the following factors:

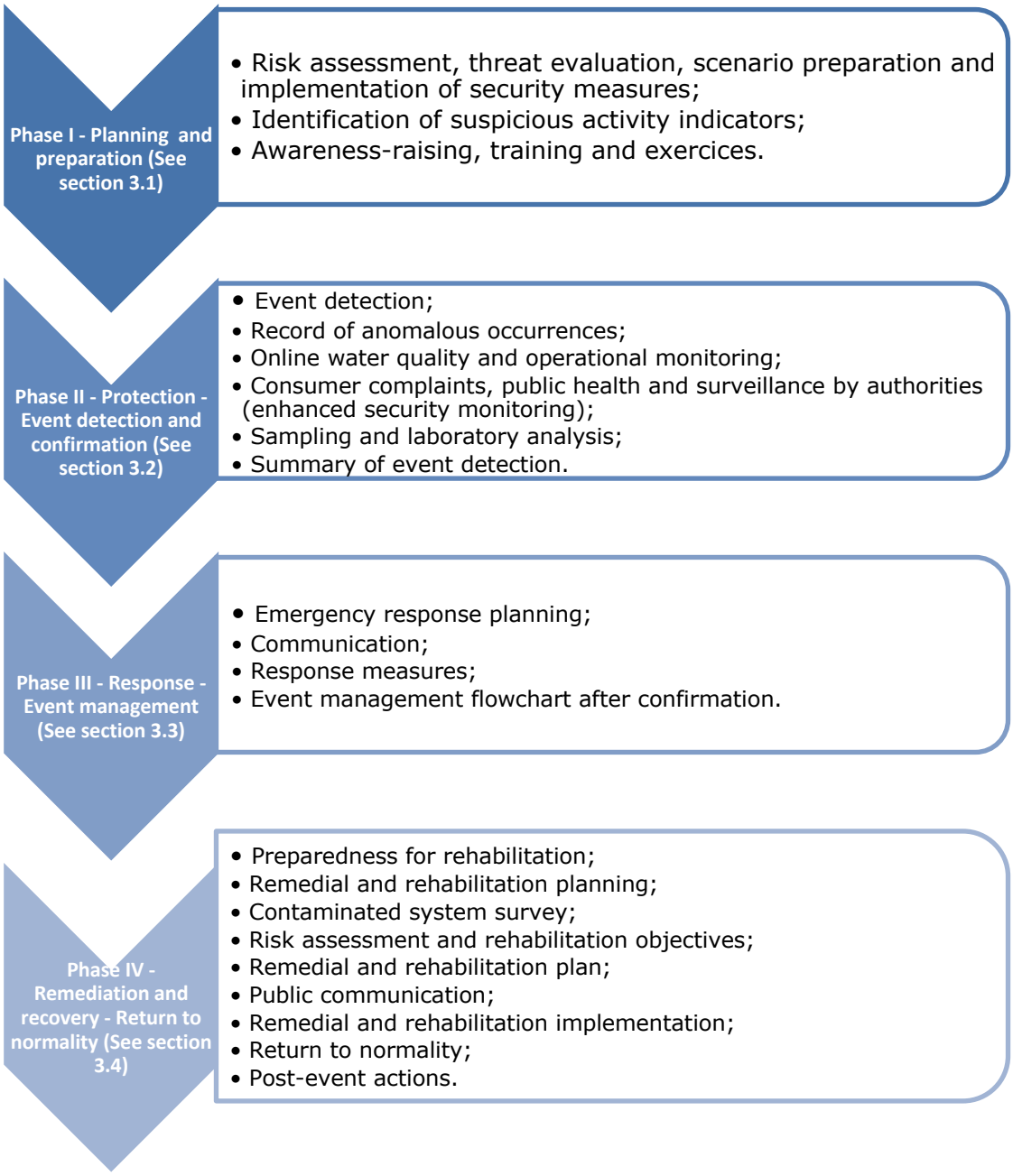
— the collation and analysis of the latest information available on the water supply system;
— the analysis and understanding of the potential hazards resulting from the contamination of water;
— an assessment of the risks to be mitigated (and how to reduce risks to an acceptable level);
— a determination of the measures necessary to ensure that risks are reduced and controlled;
— the effective and adequate planning of how to communicate with the public and the relevant emergency authorities.

3. Water security plan implementation

This section provides detailed guidance to operators on the creation and implementation of a water security plan aimed at reducing the risk of the chemical or biological contamination of drinking water. It is based on the following documents: Council of the European Union (2005), Janke et al. (2014), EPA (2015, 2018), ERSAR (2018) and Teixeira and Cabanas (2018).

The four phases of water security planning are shown in Figure 3 and described in the following subsections.

Figure 3. Phases of a water security plan in detail



Source: JRC, 2019

3.1. Phase 1 — planning and preparation

The planning and preparation phase will include creating and maintaining the water security plan, allocating roles and responsibilities, undertaking risk assessments to identify vulnerabilities and that will underpin the mitigation measures and new security measures employed, and performing the relevant training and practical exercises (Council of the European Union, 2005; Janke et al., 2014; EPA, 2018).

3.1.1. Risk assessment, threat evaluation, scenario preparation and implementation of security measures

As outlined in Section 2.5, a risk assessment should form part of the process of establishing the need for and required scope of a water security plan (Janke et al., 2014). The first step in creating the plan is to elaborate on this risk assessment with the involvement of all the actors identified as having a role in the water utility operator's security planning, including the consideration of the threats of intentional chemical or biological contamination of drinking water.

In this preparatory phase, entities that may add value to the security of water supply systems need to be engaged, in addition to the management of the water utility operator. These entities will include, but not be limited to, the security intelligence services and law enforcement agencies, as described in Annex 1 — Examples of roles and responsibilities in water security planning. The relevant national authorities will be the primary source of information on threats, which will be based partly on historical events and partly on intelligence on the aspirations and capabilities of terrorists.

The characteristics of contamination threats are explored further in Annex 2 — Characterisation and evaluation of the threats. This considers three perspectives of contamination threats:

— the type of contaminant;
— the introduction of the contaminant into the water system (quantities, and method and location of release);
— the potential consequences.

The risk assessment process should identify those threats that are most relevant to the specific water utility operator, involving an assessment of the likelihood of the threat, coupled with an estimate of the impact to the water utility operator and its customers should the threat be realised. One very useful way of articulating the most likely contamination threats as part of the security planning process is to produce scenarios, describing the most likely threat(s) identified for the water utility operator, taking into account its size and location. Some example scenarios are included in Annex 3 — Potential contamination scenarios.

In many Member States, advice on assessing the risks from terrorism is provided through the local police or security authorities or intelligence services. Some suggestions on grading the impact of contamination are contained in Annex 4 — Establishment of contamination impact and event severity.

The risk assessment should conclude with an identification of the key vulnerabilities in terms of deliberate contamination, which will provide the basis for the implementation of improvements in detection measures and also new security measures, including online monitoring. Annex 5 — Implementation of security measures in the various infrastructure types of the water supply system — provides further guidance to operators on the implementation of online monitoring.

3.1.2. Identification of suspicious activity indicators

Another essential output of the security planning process is the identification of a set of indicators to more quickly identify a deliberate attempt to contaminate drinking water. The following is a list of candidate indicators that water utility operators could consider (Janke et al., 2014):

— consumer feedback:
  - complaints from users of unusual smells and/or tastes of water;
  - reports from health authorities of an abnormal level of sudden illness;

— the online monitoring of water:
  - operational control plan (remote management);
  - quick kits and operator analysis;
  - laboratory results;
  - sudden unexplained changes detected by sensors;
  - anomalous data changed by cyberattack and detected by the event detection system (EDS) software of a continuous water quality monitoring (CWQM) system;
  - water supply incidents: reflux indicated by a water meter or a water meter being removed without being authorised by personnel;
  - the dumping or discharge of materials in water catchment areas;

— physical access security incidents:
  - persons raising and/or cutting the fence of an installation;
  - the opening, accessing or suspect handling of sewage closure covers, equipment or installations;
  - people climbing to the top of water reservoirs;
  - the unauthorised collection of images of facilities, structures and/or equipment;
  - unauthorised access at entrance gates and/or access to property including tampering with locks;
  - vehicles being connected to hydrants (except fire service vehicles and management service vehicles);
  - suspicious acquisitions of high-pressure pumps and accessories, as notified by the security agencies;
  - suspected acquisitions of significant amounts of industrial chemicals, herbicides, rodenticides or pesticides, as notified by the security agencies;
  - suspicious object being abandoned near or inside facilities of the water supply system;
  - the suspicion and/or discovery of hidden camera use;
  - anonymous threats;

- the unauthorised parking of vehicles in reserved areas or near sensitive areas;
- unusual or prolonged interest in security measures or security or maintenance personnel, security cameras, places of entry and access controls, and physical barriers;
- the access or attempted unjustified access of an external official or supplier contracted to locations or information that are outside the scope of their functions;
- disappearance or attempt to obtain official vehicles, uniforms, badges, access cards or credentials of access to sensitive and critical places;
- nervous or dissimulated behaviour, avoiding visual contact with safety or security elements;
- the unauthorised use of a drone near water utility infrastructure;

— cybersecurity incidents:

- unauthorised access to the control software system, whether it be human access or changes induced intentionally or unintentionally by virus infections and other software threats residing on the control system's host machine;
- packet access to the network segments hosting supervisory control and data acquisition (SCADA) devices and the ability to control or interrupt critical facility operations.

Typically, a combination of indicators would be used to assess a potential contamination threat. This will require the clear identification of roles and responsibilities within all departments of the water utility organisation. It is therefore essential that all departments of the organisation are involved in the security planning process, so that their contributions to all phases of the water security plan can be identified.

It should be noted that details of the specific indicators produced by a water utility operator for its water security plan will be extremely sensitive and will need to be managed by the utility operator accordingly. Such details should be contained in a document separate from the main part of the security plan, along with any other sensitive sections, and made available to only trusted individuals within the organisation on a 'need to know' basis. It is recommended that care also be taken with any electronic storage or communication of such sensitive items, even within the utility operator's own system.

3.1.3. Awareness raising, training and exercises

It is very important during this stage that an appropriate security culture is encouraged, not only among the staff of the water utility operator, but also in the surrounding community, by promoting their fundamental collaboration and awareness of the need to be alert, without causing alarm. All parties could provide useful relevant indicators of potential contamination threats. To facilitate this, the notification process needs to be easy to implement (Janke et al., 2014; EPA, 2018).

Management entities and civic municipalities may need to reassess the dissemination of information on a community's water supply. The need to comply with the rules of transparency and access of citizens to administrative information must be balanced

against the risk of facilitating the hostile actions of any agents wishing to contaminate a water supply system. This issue of excessive information should be considered when deciding on physical security measures.

Some measures that may assist with the implementation of a security culture among the personnel of organisation are suggested in Annex 6 — Guidance on awareness raising, training and exercises.

The ability to effectively implement the concepts, guidance and procedures of an effective and adequate response requires that the personnel responsible for responding be trained in the response and supporting procedures. Exercises allow utility personnel and response partners to practise procedures and tasks that fall outside the typical duties of their roles, enabling them to meet the challenges associated with a contamination incident. In addition, effective training and exercise programmes are useful for integrating utility response procedures with those of external partners.

Training and practical exercises have three main purposes:

— to enable the regular review and update of all procedures, contact pilot experience lists and other materials;
— to practise carrying out procedures of an effective and adequate response with the multiple parties that may be involved in an incident response;
— to capture problems in the implementation of partners and maintained familiarity procedures during exercises in order to continually improve and compensate for changes.

Ultimately, training and practical exercises will allow a utility operator to learn from mistakes in a no-fault environment, thereby recognising opportunities to improve the execution of plans and procedures, and modify them when necessary. Further guidance on how to plan and conduct appropriate exercises and training for an effective and adequate response is provided in Annex 6 — Guidance on awareness raising, training and exercises.

3.2. Phase 2 — protection: event detection and confirmation

This phase involves the monitoring of indicators and the immediate response in the case of potential contamination, followed by confirmation of the nature of the event. For the identification of possible emergency situations, water utility operators rely on information from monitoring and control systems, which can quickly identify an anomalous situation, and on information from various external sources. This subsection was based on the following sources: EPA (2003b, 2004a, 2015, 2018), Council of the European Union (2005), Herrick (2006), Ministry of Health Israel (2009, 2016), Janke et al. (2014), Carmi (2018), ERSAR (2018) and Teixeira and Cabanas (2018).

3.2.1. Event detection

The detection of a potential contamination event may arise from monitoring the indicators identified in phase 1 (see Section 3.1.2), where four types of indicator sources were identified:

— feedback from consumers and relevant authorities;

— the online monitoring of water;
— physical access security incidents;
— cybersecurity incidents.

The confirmation of a contamination incident, and its extent, will then be required to ensure that an appropriate response is implemented. To reduce any uncertainty associated with the diagnosis, further data will need to be collected and evaluated, both internally and externally (EPA, 2015, 2018; Hohenblum et al., 2016; ERSAR, 2018; Teixeira and Cabanas, 2018).

During the investigation of a suspected contamination event, a water utility operator must evaluate its confidence in any information that indicates that the system may be contaminated. A combination of indicators could be used to assess any potential contamination. Comprehensive guidance on the methods that could be considered by a water utility operator is provided in Annex 4 — Establishment of contamination impact and event severity. This guidance details how utility operators can apply metrics to the different types of indicators and use these metrics to decide whether there is contamination or not, by considering the following:

— confidence of information: possible, credible or verified;

— impact of information: low, medium or high;

— certainty level of event: caution, suspicious or confirmed;

— severity level of event: minor, major or catastrophic.

3.2.2. Record of anomalous occurrences

Whenever any data indicating a potential contamination event are received by a water utility operator, it is essential that this anomalous occurrence is recorded and reported, according to the responsibilities established in the water security plan (ERSAR, 2018; Teixeira and Cabanas, 2018).

This is important for ensuring that all relevant information is collected and communicated to the event coordination team in a timely manner. Information on any potential contamination events will also be useful during periodic reviews of the water security plan and of the data source indicators being monitored, so that realistic trigger points can be established, avoiding false alarms. An example of how to record anomalous notifications is provided in Table 2. The event manager would normally be the person responsible for maintaining these records.

Table 2. Example of how to record anomalous occurrences in the water supply system

Potential event indicator (anomalous situation)	Who identified the potential event	What caused the potential event	What was done	By whom	Perception of the level of certainty

Source: Teixeira and Cabanas, 2018

3.2.3. Online water quality and operational monitoring

Online monitoring and sensors are central to the timely detection of contamination and should be an integrated part of daily operations (Janke et al., 2014; Carmi, 2018). Where to locate sensors needs to be decided not only on the basis of security considerations but also on the basis of other operational aspects such as ease of maintenance.

The water security plan should clearly link the detection of events in real time by online monitoring systems with interfaces used by the laboratory that performs identification and confirmation testing. The installation of online monitoring technology along the network, at points identified as critical or key, is recommended.

The report *Practical guidelines on the requirements of a continuous online water-quality monitoring system in drinking-water-supply systems* (Carmi, 2018) emphasises the importance of hydraulic models and the application of a geographic information system (GIS), sensor placement optimisation, the type of sensors and number of monitoring stations needed, data communication and EDSs to manage big data and false alarms, a contamination dissemination look-ahead simulation (CDLAS) model and an event management system.

Online contaminant monitoring systems and simple contamination warning systems (CWSs) have been available for some time as tools to reduce the consequences of attacks involving the deliberate contamination of water by either chemical or biological intrusions.

A CWS should be designed to detect contamination events and provide information on the location of the contaminants within the system, including an estimation of the characteristics of the contamination (i.e. contaminant type, injection time and duration, concentration and injected mass flow rate). Once the type and characteristics of the contamination are identified, a containment strategy can be implemented to minimise the spread of contamination throughout the system and to determine which parts of the system need to be contained and/or flushed.

CWSs have been envisaged to include multiple approaches to monitoring. For instance, water quality sensors located throughout the distribution system combined with a public health surveillance system and a customer complaint monitoring program are believed to be capable of detecting a wide range of contaminants in water systems.

3.2.4. Consumer complaints, public health and surveillance by authorities (enhanced security monitoring)

Another important step in the protection phase is collecting feedback from consumers (Janke et al., 2014), the health authority and other entities involved in water supply process, such as the regulator of water services, civil protection agencies, local government, the environmental agency and police authorities. Some consumers, such as hospitals, health centres and dialysis clinics, are particularly sensitive and of particular importance, since they have very stringent requirements in terms of water quality for obvious reasons and therefore their feedback can be very valuable for detecting abnormalities.

Another important point to consider is any sudden increase in the number of people entering hospitals and health centres with symptoms that may be linked to the consumption of contaminated water.

Water utility operators should track consumer complaints regarding unusual tastes, odours or appearances of water, and record what steps they took to address these water quality problems. The development of a process to automate the compilation and tracking of information provided by consumers would be very useful. Such a system, coupled with anomaly detection software, might enable the rapid identification of unusual trends, which may indicate a contamination incident.

Syndromic surveillance conducted by public health authorities might identify any potential drinking water contamination incidents. This surveillance includes collecting information on, for instance, unusual trends in over-the-counter sales of medication and reports from emergency medical service logs, 112 call centres and poison control hotlines. Information from these sources can be integrated into a CWS by developing a reliable and automated method of linking the public health sector and drinking water utility operators.

A protocol should be established in collaboration with the health authorities, so that reports of the results of this surveillance reach the operators of water supply systems; this could be daily or weekly, for example, depending on the region, country and protocol established.

Security breaches can be monitored and documented through enhanced security practices that detect anomalous conditions. A tampering event could potentially be detected in progress and thus possibly prevent the introduction of a harmful contaminant into the drinking water system.

3.2.5. Sampling and laboratory analysis

To determine and confirm if potential contamination detected by the online water quality monitoring system is a credible threat, sampling field and laboratory analyses of water samples should be completed (EPA, 2003a,b, 2004c, 2018; Herrick, 2006; Ministry of Health Israel, 2009, 2016; Janke et al., 2014). Detailed guidance can be found in the report *Analytical Best Practices* ([4]). The utility operator will need to determine the level of threat and therefore will require evidence concerning the type of contaminant and how serious the contamination may be in terms of public health.

Sampling and analysis are also performed to support remediation and recovery activities and ensure full recovery and the return of the water supply to normal.

Little may be known about the identity of suspected water contaminants. In such a case, the sampling approach may need to be more comprehensive, including all types of analyses, and be carried out by specialised personnel. According to some national legislation regarding the management of serious incidents of deliberate contamination, sample collections may be done by the competent law enforcement authority.

For this reason, field analyses and/or rapid analysis technologies should be considered, as, despite inaccuracies, these could help in many cases:

([4]) Full reference to the ERNCIP document to be published.

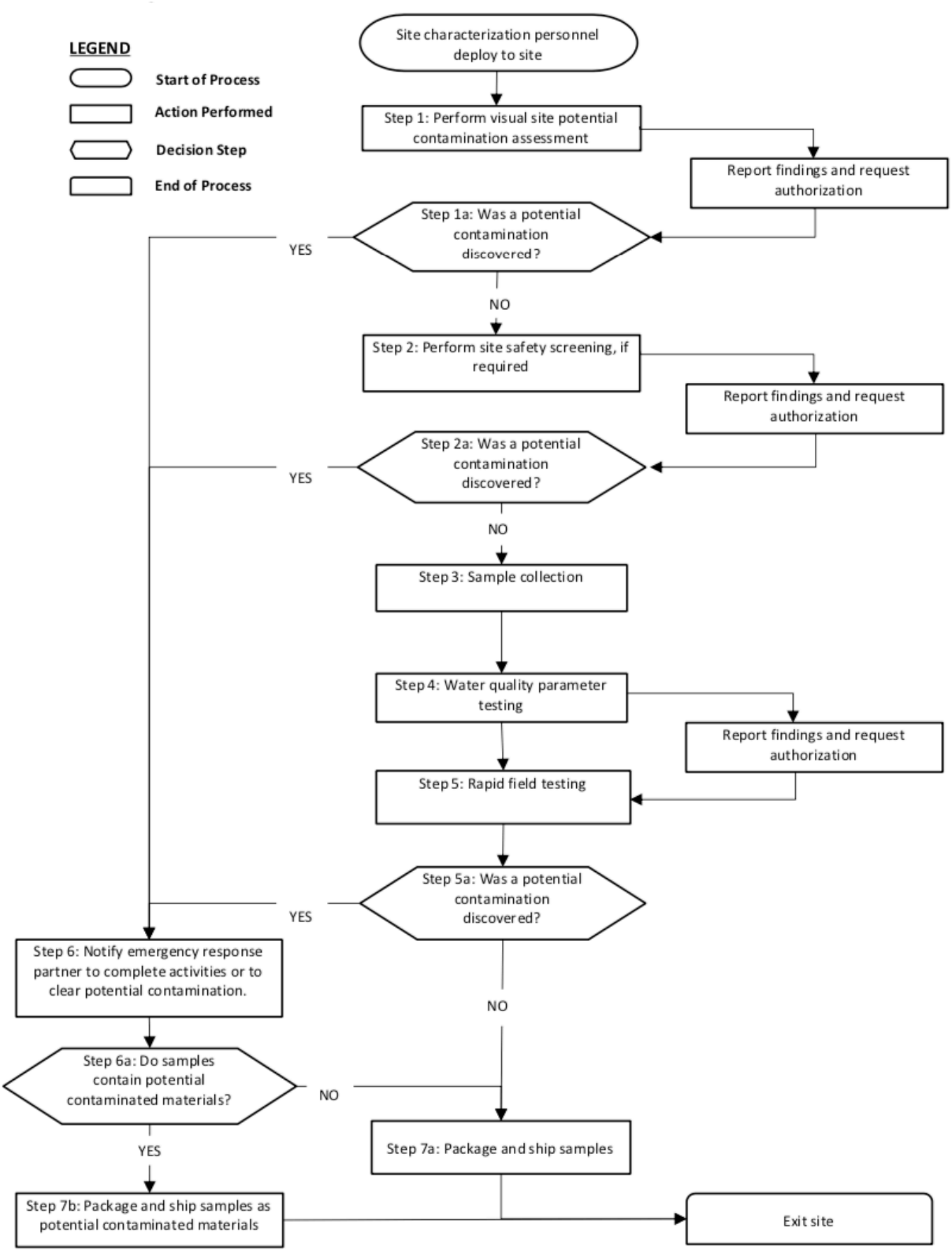
1. to determine very quickly whether water is toxic or not, even if the toxin cannot be identified;
2. by limiting the number of samples that need to be collected or the number of parameters that need to be fully analysed, which is helpful for avoiding unnecessary work in the laboratory and obtaining results more quickly.

A detailed sampling plan should include some information regarding the following:

— how the approach to sampling has been based on the results of the sensor monitoring system, on an initial site hazard assessment and an evaluation of site conditions;
— the time and location of sample collection — details of different sampling sites within the water distribution system;
— the type of samples collected (grab, composite);
— procedures for collecting samples for detecting chemicals and pathogens;
— special laboratory requirements regarding sample collection and transport to ensure sample security and integrity (e.g. container types, holding times and conditions, preservation requirements);
— how to properly label samples with identification details, for packaging and transport as quickly as possible with all critical information documented;
— specialised sampling techniques for personnel in health, safety and protection to manage the risk of accidental exposure during sampling, sample transport or sample receipt at a laboratory;
— laboratory communication with samplers regarding the number of samples required, the prioritisation of samples and how to alert the laboratories involved;
— development and training of effective and responsive sampling teams;
— chain of custody.

Figure 4 shows the steps to be followed in this phase of site characterisation and the sampling process.

Figure 4. Flow chart outlining the steps of an example site characterisation and sampling process



Source: EPA, 2004c — DSCRP template

Laboratories contribute to the water security plan by providing water utility operators with analytical capabilities and capacity, thus supporting the monitoring and surveillance of, response to and remediation of intentional and unintentional water contamination events involving chemical, biological or radiological contaminants.

The national laboratories authority/agency ensures a consistent and coordinated laboratory response to water contamination events.

During a natural disaster, terrorist event or accident affecting the water sector, a large number of environmental samples will be generated, most likely overwhelming the capacity and/or capability of any individual laboratory to provide sufficient analytical support. The water security plan should not obligate laboratories to provide support in such an event, but rather should set out a consistent approach that defines how water sector authorities and local and national authorities/agencies should work together to meet the need for analytical support.

The water security plan should therefore not supplant or subordinate existing plans of legal authorities, but rather should be used when needed to coordinate laboratory support for water contamination incidents.

The laboratories addresses water contamination incidents that, because of their suspected cause or size, may require additional analytical support and a broader response than they can provide and the response needed should be at another level, regional or national, that will provide procedures for a coordinated response to water contamination incidents that threaten public health and safety. As part of this approach, samples will be analysed to identify unknown contaminants and determine the extent of contamination, the success of remediation efforts and when the system can be returned to normal service.

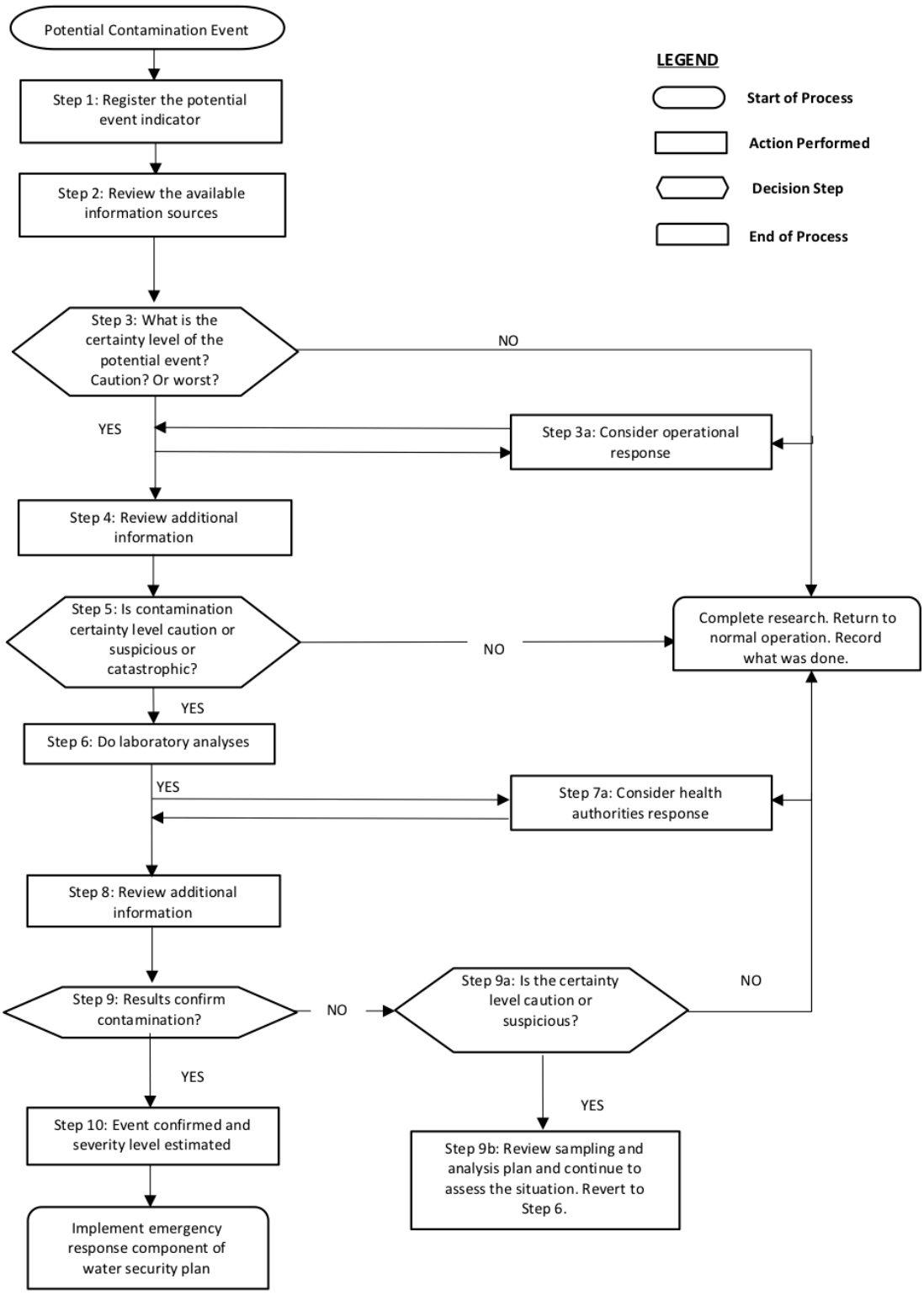
Samples may also be collected and analysed as part of a criminal investigation. In such a case, a water security plan can facilitate, for example, the following type of support:

— analyses;
— consulting;
— data review, reporting, transmission and exchange;
— reagent exchange;
— sample storage and brokerage;
— training;
— coordination and communication with other entities;
— assumption of other support laboratories' normal workloads;
— staff exchange (laboratories should be aware that legal issues, such as overtime and liability regulations, may limit this support).

3.2.6. Summary of event detection

Figure 5 shows the steps to be followed in the event detection phase (EPA, 2015; ERSAR, 2018; Teixeira and Cabanas, 2018).

Figure 5. Flow chart outlining the steps of an example event detection process



Source: Teixeira and Cabanas, 2018

3.3. Phase 3 —response: management of the event

This phase deals with the immediate response in the event of confirmed water contamination, involving communication with the public and coordination with local/national emergency authorities to ensure that the drinking water supply is safe. The planning of the immediate response, including the identification of redundancy and an alternative water supply, must be undertaken when the water security plan is first established.

During the event, the emergency event manager will need to make decisions based on the available information. This will involve the convening the event coordination team, if this had not been done during the event detection phase, based on the nature and severity of the event.

For an event classified as catastrophic, external consultants/specialists may be needed to assist the multidisciplinary coordination team in obtaining a fuller assessment of the situation, as should be defined in the water security plan.

This subsection is based on the following sources: Oregon Health Authority (2002), Council of the European Union (2005), Janke et al. (2014), WaterISAC (2014), EPA (2015, 2018, n.d.), ERSAR (2018), Serafinelli et al. (2018) and Teixeira and Cabanas (2018).

3.3.1. Emergency response planning

In parallel with installing a CWQM system, it is vital that a utility operator develop an emergency response plan with the aim of eliminating or lessening further public exposure once a contaminant has been detected in the system (EPA, 2018; ERSAR, 2018; Teixeira and Cabanas, 2018). This response plan should be prepared when the water security plan is initially established, and should list all the immediate actions needed to respond quickly and reduce the amount of damage caused. The 'response time' is a realistic estimate of the total time it would take the utility operator to respond effectively to a confirmed detection of contamination, to eliminate or lessen further public exposure. The plan should aim to minimise the response time.

Immediate actions could include effectively warning endangered customers not to drink the water, cutting off the water supply in the affected area, stopping pumps and closing main valves.

Minimising the response time is important in the optimisation process described above because, as response time increases, monitoring becomes less relevant even with a larger number of monitoring stations. Investing heavily in a CWQM system is of little use if the utility operator does not know how to respond effectively to any system alerts.

The response plan should prepare the water system operator for all kinds of emergencies — natural disasters, anthropogenic events and terrorist activities — and should contain specific instructions about who to call if there is an emergency situation that may affect the water system. It should facilitate the development of procedures for responding to events that affect the drinking water, such as a contaminated water source or reservoir.

The emergency response plan should include the organisation of any important management and operations procedures into one document.

It is vital that the people who will be involved in communicating information on the emergency situation and implementing the necessary and adequate response measures are clearly identified, as emphasised above. Further guidance is detailed in Annex 1 — Examples of roles and responsibilities in water security planning.

3.3.2. Communication

A key part of managing an emergency is clear and consistent communication with all relevant stakeholders (WaterISAC, 2014; EPA, 2015, 2018; ERSAR, 2018; Serafinelli et al., 2018; Teixeira and Cabanas, 2018). It is therefore essential that a water security plan incorporates a communication strategy, outlining the communication procedures, including a regularly updated list of preferred media contacts. Once a contamination event has been confirmed, this communications strategy should be instigated.

In the event of a general breakdown of communication, the members of the internal team should have the ability to maintain contact through alternative means, e.g. radio, walkie-talkie or meeting at a designated place within the facilities of the water utility operator. Detailed guidance on communication strategy options are provided in Annex 7 — Communication options. Whenever communication with external entities and/or with the public is necessary, responsibilities should be identified in the water security plan. A recommended approach is set out in the contact list defined in Table 3 in Annex 1 — Examples of roles and responsibilities in water security planning.

3.3.3. Response measures

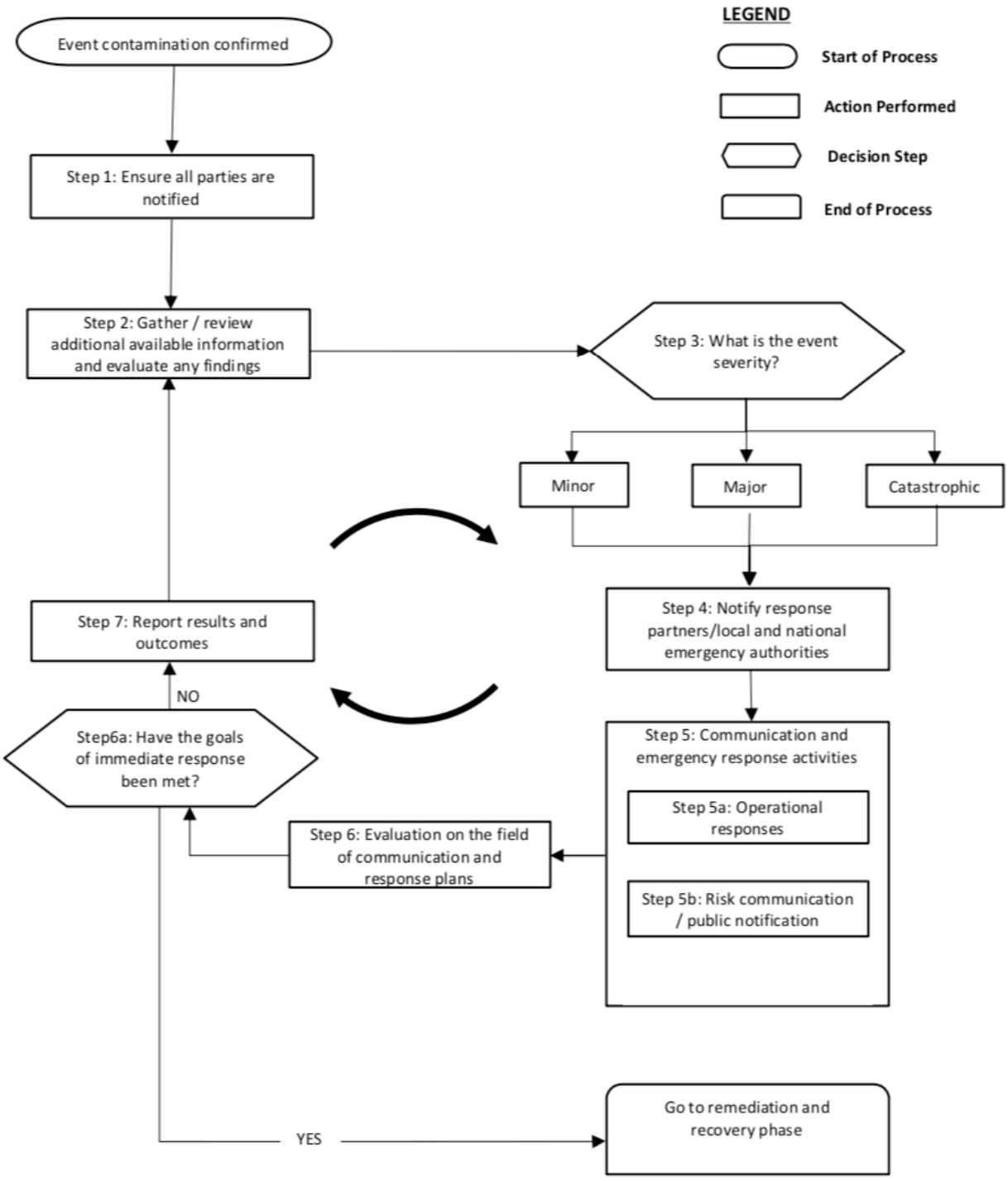
The first 3 hours following confirmation of a contamination event constitute the immediate response phase. The goals of this phase are to limit the number of people exposed to contaminated water by stopping the contaminant's movement in the water system, to inform the public of the danger and to take steps to isolate the contaminated areas of the system from any non-contaminated areas using the contamination dissemination model of the CWQM system. The utility operator should have a well-planned and rehearsed standard operating procedure for this immediate response phase (Oregon Health Authority, 2002; Janke, et al., 2014; EPA, n.d.).

As it is likely that an emergency event will be unpredictable in terms of what actually occurs, it is very difficult to pre-determine response actions. Instead, it is recommended that potential response measures be pre-identified in the water security plan, in the form of an emergency response plan, based on the most likely scenarios. The priorities of the immediate response measures will be to prevent any further contamination reaching the public and to ensure that adequate drinking water is provided to the community. It is recommended that developing specified response measures form an integral part of practical exercises, and also reviews of real incidents, whether or not any contamination actually occurred. Some potential response measures are outlined in Annex 8 — Response measures.

3.3.4. Event management after confirmation of contamination

Figure 6 summarises the procedures that should be performed in the different phases of the event after an emergency situation has been confirmed.

Figure 6. Flow chart outlining the steps in an example investigation and response phase



Source: EPA, 2015 — DSCRP template

3.4. Phase 4 — remediation and recovery

This phase covers all remedial activities leading to the full return to the normal provision of uncontaminated drinking water. The remediation and rehabilitation plan forms the final phase of the water security plan, and provides guidelines for the water operator for returning to normal operations after the occurrence of a water contamination incident.

The remediation and rehabilitation process will come after the immediate response steps defined in the emergency response plan, which aim to minimise the potential for the exposure of the public to the potentially contaminated water, and will be determined after the contamination incident has been confirmed.

This subsection is based on the following sources: EPA (2003a,b, 2004a,b,c, 2015), Council of the European Union (2005), Herrick (2006), Ministry of Health Israel (2009, 2016) and State Water Resources Control Board (2015).

3.4.1. Preparedness for rehabilitation

The water utility operator will play a key role in the rehabilitation process following contamination (EPA, 2004a,c; Herrick, 2006; Ministry of Health Israel, 2009, 2016; State Water Resources Control Board, 2015). The utility operator staff will possess detailed knowledge and technical expertise regarding the configuration and operation of the water source, water storage, water treatment and the water distribution systems, and will need to enable rapid access to the site of contamination, as well as providing records of operations, drawings, etc.

It is therefore vital that the utility operator be prepared in advance for the rehabilitation of a contaminated water supply network. This preparedness will enable the utility operator to return as quickly as possible to normal operation following a contamination event, and provide safe, reliable drinking water to the public.

The initial preparation, undertaken when the water security plan is first established, should include the nomination of a rehabilitation advisory committee, specifying individual roles and responsibilities, the relevant government external authorities and agencies, and all the means needed for the process.

The utility operator should prepare in advance a file detailing relevant procedures and containing all documents necessary for rehabilitation. The file should be accessible to all staff involved/authorised. The utility operator should appoint a specific person who is responsible for periodically updating the file. Further guidance on how to prepare for rehabilitation is provided in Annex 9 — Remediation and rehabilitation plan: roles, responsibilities and processes.

In the case of small utility operators, it is recommended that a regional body be formed with responsibility for dealing with the preparation and the rehabilitation process.

The planning should include identifying the locations of alternative water sources and alternative short- and long-term water supplies for customers, based on an analysis of the redundancies of the water supply system.

3.4.2. Remediation and rehabilitation planning

The rehabilitation process will be significantly enhanced by the water utility operator's preparedness, including by defining roles and responsibilities, the options, and the external authorities and stakeholders involved (EPA, 2004a,c; Herrick, 2006; Ministry of Health Israel, 2009, 2016; State Water Resources Control Board, 2015).

Following the immediate response after the confirmation of contamination of a water system, the utility operator will need to fully evaluate the situation, convene the rehabilitation advisory committee and act according to the water security plan. The utility operator should rapidly survey the situation, including by identifying the contaminant, obtaining detailed mapping of the pipes affected and investigating the means to flush and/or neutralise the contaminant. When the information is available, the objectives of the remedial action can be defined, alternative approaches can be analysed and an optimal remedial action can be selected. The utility operator should then develop and execute a remediation and rehabilitation plan, tailored specifically to respond to the contamination event confirmed, including post-remediation monitoring to verify the complete removal of the contaminant. The monitoring activities should continue well after return to normal operations to confirm that all rehabilitation goals have been met.

Depending on the nature and severity of the contamination incident, alternative short- and/or long-term water supplies may be required.

During the entire rehabilitation process, the utility operator and/or public health authority should keep the public informed about the details of the process: how it could affect human health, what the utility operator and other authorities are doing to restore the supply of safe water, what alternative water supply is available and when the water supply system is expected to return to normal, supplying safe drinking water.

3.4.3. Contaminated system survey

The utility operator should rapidly survey the situation (within 3 hours of the immediate response phase), using professional and experienced water system and water quality personnel, in collaboration with the rehabilitation advisory committee (EPA, 2004a,c; Herrick, 2006; Ministry of Health Israel, 2009, 2016; State Water Resources Control Board, 2015).

The basic preliminary investigation of the contamination event should provide:

- information regarding water quality and operational data relevant to the event (from the EDS);
- any information known regarding the contamination, including the results of any field/laboratory tests already done;
- details of the locations of relevant sampling points for further field/laboratory tests;
- details of any special operational events, such as burst pipes, maintenance work (in treatment plants, reservoirs, the network) or water outages, that preceded the contamination event;
- an inquiry of possible environmental issues caused by the contamination;
- details of the water supply system, including the source of the water, hydraulic information (rate and direction of flow, pressure, reservoir levels, etc.), backflow devices, etc.

An additional, deeper investigation could include:

— collecting additional water samples from a wider area, according to the sampling and analysis plan;
— performing more field/laboratory tests and types of tests, according to the sampling and analysis plan;
— checking for possible sewage, flooding or unusual industrial or agricultural activity that may have influenced water quality, etc.;
— collecting morbidity information.

The survey should determine:

— the nature of the contamination: type, concentration, toxicity, infectivity, health and environmental aspects, and the contaminant's persistence/stability in the water system, degradation characteristics, solubility, volatility and aerosol production potential;
— the water composition, especially parameters that may affect the treatment efficiency such as turbidity and alkalinity;
— protection and safety measures for the water utility operator's remediation teams;
— the boundaries of the contamination area, the volume of water contaminated and the flow direction as determined by the CDLAS model and verified by tested water samples to define the extent of remedial action needed;
— the physical characteristics of the part of the system contaminated (e.g. the water source, treatment plant, distribution network); if it is the distribution network, for example, the characteristics to determine would be water demand, population size, pipe diameters and types, hydraulic water devices, pressures, flow rates, sediments, public and important buildings, etc.;
— the public health impact;
— the environmental impact of flushing the contaminated water into the sewage or drainage system.

3.4.4. Risk assessment and rehabilitation objectives

On the basis of the results of the survey and the system characterisation, a risk assessment should be done, in collaboration with the rehabilitation advisory committee. The risk assessment should evaluate the risks posed by the contamination (EPA, 2004a,c; Herrick, 2006; Ministry of Health Israel, 2009, 2016; State Water Resources Control Board, 2015). During the remediation actions, an additional risk assessment may be necessary to evaluate risk reduction resulting from the response actions.

Such a risk assessment should evaluate the following:

— the potential human health and sanitation risks;
— environmental risks;
— how urgent it is to restore different levels of decontaminated water for various purposes (e.g. sanitation only);
— the danger level to water consumers as a function of the disinfection/neutralisation level of the contaminant;
— the risks posed to the water utility operator's remediation teams;
— the location of weak points in the supply system.

The results of the risk assessment should in turn be used to determine whether or not any further field investigations are needed and to define the main and intermediate goals of the rehabilitation process, permitting a range of remedial options to be considered. The final remediation goals should be based on achieving exposure levels that are acceptable in terms of protecting human health and the environment. The objectives of remedial action depend on the exposure pathway, for example whether the contaminated water will be treated to allow its consumption as drinking water or whether it will be treated to allow its safe discharge to the drainage or sewage system.

In conjunction with the rehabilitation advisory committee and any relevant government authorities, the water utility operator should conduct a systematic and detailed evaluation of rehabilitation alternatives based on the objectives of the remedial action and the means available, with emphasis on protecting public health and expediting the restoration of a normal water supply, while keeping in mind environmental issues. It should also be kept in mind that the lack of a (safe) piped water supply is in itself an acute health hazard.

Guidance on remediation alternatives can be found in Annex 10 — Remediation and rehabilitation plan: analysis of alternatives and selection of remedies.

Comparative analysis should be conducted, not only by the utility operator in collaboration with the rehabilitation advisory committee, but also by other authorities involved in the process, to evaluate the suitability of each alternative relative to one another and relative to each criterion.

The advantages and disadvantages of each alternative should be identified, and the protection of human health and the environment and compliance with applicable regulations should serve as thresholds for determining these advantages and disadvantages.

The remedial action selected should satisfy the objectives of a remedial action and should be documented in the remediation and rehabilitation plan.

3.4.5. Remediation and rehabilitation plan

Once the preferred option has been selected, the rehabilitation plan can be developed by the utility operator and approved by the rehabilitation advisory committee (EPA, 2003b, 2004a,b, 2015; Herrick, 2006; State Water Resources Control Board, 2015; Ministry of Health Israel, 2016).

The remediation method should be tailored to the type and concentration of the contaminant, the relevant standards, the cleansing and the physical characterisation of the system.

If necessary, any lack of information or equipment should be specified in the plan.

It is recommended that a small-scale pilot application of the technology to be used be performed. This will verify whether or not the chosen technology meets the criteria in terms of the sufficient removal of the contaminant and the cost, and will allow operating parameters to be optimised.

The rehabilitation plan should include all the specifications, documents and drawings (process flow diagrams, piping and instrumentation diagrams, vicinity map, etc.), and

detail the steps to be taken during all stages of the remedial action. It is recommended that the process be organised in accordance with a plan approval form for the rehabilitation of a contaminated water system, which should also be approved by the advisory committee. The plan should include the following components:

- remediation goals;
- the rehabilitation plan stages, schedule and milestones, and the duration of cleaning and target level of cleanliness for each stage;
- a description of each task and deliverable at each stage;
- details of any toxic neutralisation materials, apparatus and system disinfection methods to be used:
    - the type and concentration of the neutralising materials, their effectiveness and their potential impacts on human health and the environment;
    - the by-products of the neutralised contaminant;
    - the volume of contaminated water to be neutralised or drained;
    - the equipment and method used for applying the neutralisation materials;
    - residuals of decontamination and remediation wastes:
    - decontamination fluids such as detergents and wash water;
    - residuals of water treatment such as bio-solids and filter cake;
    - contaminated soil or sediments;
    - contaminated consumer, public building and institute, business and industry equipment such as home filters, ice makers, water heaters, sprinklers, garden hoses, swimming pools and spas;
    - the estimated time for the cleaning, the direction of washing, washing the consumer house connection and blind pipes;
    - plans for sampling to check the efficiency of cleaning;
    - contaminated pipes that cannot be drained or neutralised;
- details of relevant teams and personnel;
- the total volume of water to be treated, the contaminant type and concentration, contact time, etc.;
- the system volume, maximum flow rates, possible working pressures and possible flow directions;
- the time that the neutralising materials will be in contact with the surface area of the water accessories for optimal cleaning;
- the influence of the by-products of cleaning on the water accessories;
- the estimated time for the final washing and prevention of backflow;
- plans for sampling to check the efficiency of washing;
- details of areas that require clarification, problems anticipated and site preparation;
- the availability of and mobilisation time in relation to equipment/supplies;
- proposed use of subcontractors;
- sampling and tests to be performed — site security, health and safety sampling, test and analysis procedures, and quality assurance plan to ensure that the final product meets the design specifications;
- alternative water supplies;
- proposed costs.

During the remediation and rehabilitation process, it will be necessary to take samples and perform various tests to evaluate the efficacy of the treatment process and determine whether or not the remediation objectives were attained. The hydraulic

model and the water quality CDLAS model will support the sampling activity. The sampling and test schedule should include details on:

— sample location and frequency:
    - the location and sampling frequency and the constituents to be analysed should be defined for each sample to be collected;
    - a table may be used to clearly show the number of samples to be collected, along with the appropriate number of replicates, blanks and other control samples;
    - a water distribution map should be included to show the locations of existing or proposed sample points;
— sample identification:
    - for each sample, an identification number, the event stage, the date and time of collection, the type of analysis needed and its code, and the name of the sample collector should be given;
— sampling equipment, procedures and handling:
    - sampling procedures should be clearly written out and should provide detailed instructions for each type of sample, to enable the field team to meet the quality objectives;
    - a list of the equipment to be used, such as field quality meters and test kits, various sample containers for different chemical and microbiological analyses, reagents and safety supplies, should be included;
    - a detailed table should describe the container types, sample preservation materials, shipping requirements and holding times for each kind of analysis.

3.4.6. Public communication

The rehabilitation procedure is a long and complicated process and therefore notifications for and communication with the public are necessary to prevent panic and reduce the impact on daily life. Public cooperation is needed with regard to draining and treating building pipes, changing contaminated consumer equipment, etc.

Throughout the event, the coordination of the various agencies and authorities is vital to prevent contradictory messages being communicated to the public. Only one single channel of/entity for communication with the public is recommended.

Various methods of communication with the public (internet, telephone, advertisements, radio/television, etc.) are appropriate for providing information during the remediation, recovery and return to normal operations phase.

Hotline telephone numbers for 24/7 call centres should be provided to consumers so that they can obtain additional information and have questions answered if needed. The call centre should be provided with continuously updated information regarding the water network.

Information about the following should be communicated to consumers:

— the rehabilitation activities that are occurring;
— the time estimated for the restoration of normal operations;
— continued monitoring, analysis and results;

— the water quality expected for different uses during the process;
— consumers' private systems and equipment: whether or not equipment is usable, how the equipment can be cleaned (by the consumer or a professional) and the logistics in relation to the collection and disposal of non-usable equipment;
— cooperation needed from the public with regard to the drainage of water from building pipes;
— alternative water supplies and water distribution stations.

3.4.7. Implementation of the remediation and rehabilitation plan

During the remediation and recovery phase, the rehabilitation advisory committee, health authorities, regulator, water samplers, laboratories, suppliers, the environmental agency, civil protection agencies, military authorities and local governments are the most relevant partners involved in facilitating a return to normality as quickly as possible and without further problems. During this phase, communication with the public remains essential (EPA, 2004a,b,c, 2015; Herrick, 2006; Ministry of Health Israel, 2016).

After approval of the remediation and rehabilitation plan by the rehabilitation advisory committee and the relevant government authorities, the plan should be executed accordingly. At each stage, the actions taken and the sampling test results should be reported to the advisory committee and, accordingly, a decision on whether or not to progress to the next stage should be taken. If problems arise and changes to the plan are needed, further approval by the advisory committee will be required.

The rehabilitation process will involve a designated team without interruption to continuous work.

All activities should be documented in a report, which will be the basis for determining whether or not the remediation goals have been met. The report should include:

— a description of the event;
— the results of pre- and post-remediation risk assessment surveys;
— details of the decisions taken by the rehabilitation advisory committee;
— details of the remedial actions taken;
— results of sampling tests carried out during the remediation process.

Post-remediation monitoring should be done to provide long-term assurance that the system can maintain normal operations. Monitoring activities may include periodic sampling and tests, the periodic inspection and maintenance of water distribution system components and treatment equipment if these remain on site, and communication of information of monitoring activities and results to the public.

A final investigation and risk assessment should be carried out by the advisory committee after the end of the remediation process and the final washing step, and should involve:

— collecting additional water samples from previously contaminated areas, as well as from adjoining non-contaminated areas, in line with the sampling and analysis plan;
— performing the field/laboratory tests and types specified in the sampling and analysis plan;

— a consideration of the safety of the water network in terms of human health and the environment at the end of the process;
— a consideration of the suitability of the water for various purposes:
    - agricultural use, such as agricultural or garden irrigation and for livestock;
    - industrial/institutional/commercial use, such as cooling towers, steam systems, food, drugs and cosmetics preparation, medical and dentist operations, dialysis and recreational water;
    - home use, such as sanitation, laundering, cleaning, dish washing, washing, food preparation and drinking.

3.4.8. Returning to normality

The exit from an emergency situation will be the responsibility of the emergency event manager (EPA, 2018; ERSAR, 2018; Teixeira and Cabanas, 2018).

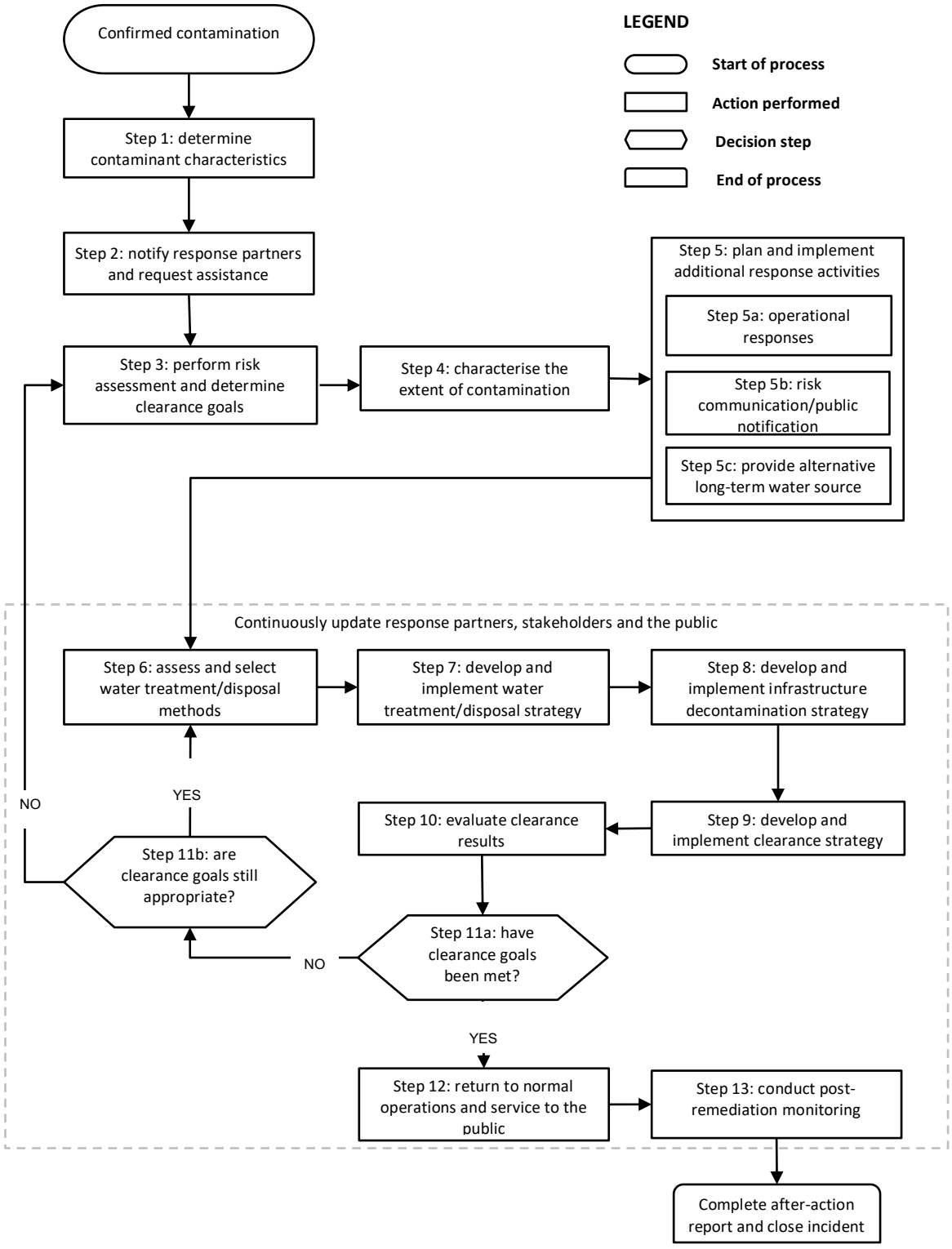
The emergency event manager should decide, based on the information available, when to deactivate the emergency plan, as well as when normal operation of the water supply system has been restored.

The emergency event manager is also responsible for ensuring the transfer of the coordination of all the actions developed during the event, or in development, to the respective functional areas, passing in this phase to the implementation of the measures to return to normality, after which the final report should be prepared, which should allow a clear evaluation of the causes that gave rise to the event, the actions taken, the control measures implemented, the indication of when and on what basis the return to normality was assumed and what lessons were learned during the event.

The water supply system must go through a clearance process before it can return to normal operation. This clearance process involves the additional sampling and analysis of the contaminated areas of the distribution system to verify that clearance goals have been met. Water regulators and public health agencies play a lead role in assessing if these goals have been met and providing final clearance, but the decision could also be based on input from other stakeholders and experts, such as those on the advisory rehabilitation committee. If the goals are not been met, adjustments to the risk assessment may be necessary or additional decontamination activities may be required. If the goals are met, the system can return to normal service. As part of returning to normal service, the water regulators and public health agencies may require that the utility operator implement a long-term monitoring programme to demonstrate that the contaminant concentration remains below the remediation threshold. Depending on the specifics of the incident, different sections of the system may be cleared at different times or clearance may occur gradually, clearing the use of the water for different things (e.g. toilet flushing, bathing, consumption) at different stages in the clearance process. Laboratories and real-time online monitoring through sensors are very important to help dealing with this process, because the operators to control the process constantly on a daily basis operations and then request the necessary analysis to confirm the results, which makes the process of returning to normality quicker and more efficient.

Figure 7 shows an example of the steps of the remediation and recovery phase to follow to return to normality.

Figure 7. Flow chart outlining the steps of an example remediation and recovery phase



Source: EPA, 2015 — DSCRP template

3.4.9. Post-event actions

Following a confirmed contamination event, a number of actions will be required after the remedial and recovery activities have been successfully completed.

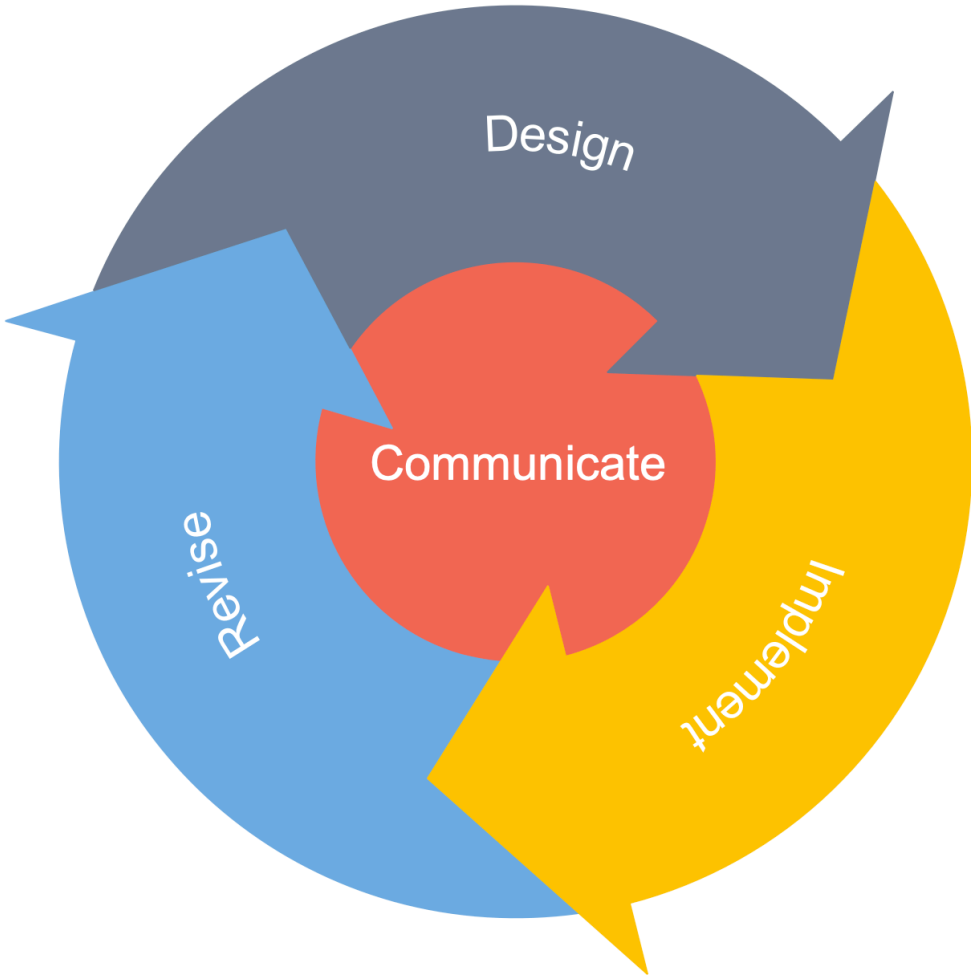
These actions may include fulfilling the reporting requirements of external bodies such as water regulatory authorities, police authorities and civil contingency agencies.

In addition, debriefing internally within the organisation will be essential so that all areas of the organisation are fully aware of the facts. A key part of this should be a review of the water security plan, so that all lessons learned can be assimilated as quickly as possible into a revised version of the plan.

4. Water security plan revision

The revision of a water security plan is an essential part of its life cycle, as shown in Figure 8 (WaterISAC, 2014; ERSAR, 2018; Teixeira and Cabanas, 2018). Fortunately, the likelihood of a terrorist attack on water infrastructure remains comparatively low, albeit the consequences could be very severe. It is therefore essential that the security plan is constantly reviewed and updated so that the planned security and response measures can be validated against actual events wherever possible.

Figure 8. Water security plan life cycle



Source: JRC, 2019

It is recommended that the water security plan be reviewed by the coordination team when:

— any emergency event occurs, particularly to evaluate the lessons learned from terrorist events:
  - conduct an evaluation:
    - collect data and information related to the advisory;
    - perform and evaluation;
    - analyse and synthetize the data;
  - modify standard operating procedures:

        - incorporate changes to standard operating procedures;
    - update approaches to public outreach:
        - identify additional communication steps;
        - follow up with the public;

— there is a significant change to the water supply system;
— there is a significant change to the CWQM system or field/laboratory tests and methods;
— there is a possibility that the plan could be improved;

The security programme should be annually reviewed and its effectiveness tested by:

— doing an annual water system security assessment;
— using mock tampering or terrorist events, computer system security challenges, etc.;
— using a third-party expert to periodically evaluate it.

The programme should be revised as needed.

5. Water security plan disclosure

The coordination team should ensure that the water security plan is disseminated among all parties involved, namely internal collaborators, external entities and/or others that may be involved (ERSAR, 2018; Teixeira and Cabanas, 2018).

This process is related to the training and awareness-raising actions mentioned above, namely as part of the prevention phase.

The water security plan should contain some criteria related to its dissemination to new employees, for instance that new employees must be evaluated and vetted before being given access to the plan.

Disclosure by external entities should also be subject to evaluation, namely which entities should be contemplated for disclosure and to what degree should be defined.

It must be emphasised that water security plans, which will probably identify vulnerabilities in the water supply system, contain sensitive information and therefore must only be disseminated in a secure manner to trusted parties.

6. Final considerations

Although the EU directive on the protection of critical European infrastructures (Council of the European Union, 2008) does not designate the water supply sector as a critical infrastructure, all governments recognise that their water supply is vital to national security. Despite this, a strategic analysis of security measures that protect against contamination has not been undertaken at national or European level. To date, security activities in relation to water supply have largely centred on implementing physical security measures (e.g. security guards and fences).

Water systems are vulnerable to unintentional and intentional threats. Unintentional threats can occur from natural causes (e.g. droughts, floods and earthquakes), accidents or equipment failures, e.g. pipe breakages. Accidents or equipment failures can lead to utility disruptions and loss of service to customers or even water contamination causing public health risks, illness, disease or even death. Intentional threats can include threats of physical acts of sabotage, cyberattack on information or SCADA systems, or contamination (Allgeier and Magnuson, 2009).

With regard to intentional threats, the 'intent' and 'capability' of the perpetrators must be considered, as must whether the threats are internal or external. Utility operators must pay special attention to intentional contamination threats in terms of the possible approach taken by a perpetrator, the type of contaminant and the magnitude of the possible consequences, as well as possible countermeasures (i.e. physical security measures, CWSs and cyber-related countermeasures). Such countermeasures could be implemented by the utility operator or the community to protect and respond to physical and contamination threats to the water supply.

Because of the magnitude of the public health and economic consequences that could result from a contamination event, the consideration of online CWSs is a key focus of water security planning. Customer complaint monitoring, public health surveillance and enhanced security should be important components of any water security plan.

With regard to the architecture of the CWS in terms of the earliest possible detection and concomitant response, online contamination monitoring offers the best opportunity for minimising the consequences of intentional contamination. This is not an easy process for many reasons, e.g. technical difficulties, immature technologies, lack of resources and institutional constraints; however, a CWS that incorporates online contamination monitoring is the best way of achieving the highest possible level of security. Effective online contamination monitoring (i.e. that ensures timely detection of contamination) must be integrated into routine monitoring approaches, and routine monitoring must be integrated into normal system operations.

Online contamination monitoring that is integrated into real-time operational control offers the possibility of early detection and an effective response. An effective response is, however, dependent on the timely identification of the location of the contamination source.

All drinking water systems have some degree of vulnerability to contamination, and analysis shows that it is possible to contaminate drinking water at levels that cause varying degrees of harm. Furthermore, experience indicates that the threat of contamination, overt or circumstantial, is real. Thus, there is a clear need to address the contamination threat. While certain steps may be taken to reduce vulnerabilities and prevent intentional contamination, it is impossible to completely eliminate vulnerabilities and therefore it is necessary to plan

how to respond to contamination threats that do arise, through developing and implementing a water security plan (Hohenblum et al., 2016).

References

Aldersley, M. (2018), 'ISIS suspect "who plotted to carry out mass poisoning attack in Italy" is arrested in Sardinia', *Mail Online*, 28 November 2018 (https://www.dailymail.co.uk/news/article-6439159/ISIS-suspect-plotted-carry-mass-poisoning-attack-Italy-arrested-Sardinia.html).

Allgeier, S. C. and Magnuson, M. L. (2009), 'Responding to threats and incidents of intentional drinking water contamination', *Journal of Contemporary Water Research & Education*, Vol. 129, No 1, pp. 13-17, doi:10.1111/j.1936-704X.2004.mp129001004.x.

Carmi, O. (2018), *Practical guidelines on the requirements of a continuous online water-quality monitoring system in drinking-water-supply systems*, Theocharidou, M. (ed.), ERNCIP Chemical and Biological (CB) Risks to Drinking Water Thematic Group, Publications Office of the European Union, Luxembourg, doi:10.2760/033873.

Council of the European Union (2005), 'Counter-terrorism strategy' (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33275) (accessed 16 April 2019).

Council of the European Union (2008), Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

EPA (United States Environmental Protection Agency) (2003a), *Response Protocol Toolbox: Planning for and responding to drinking water contamination threats and incidents. Module 2: Contamination threat management guide* (https://www.epa.gov/sites/production/files/2015-06/documents/module_2.pdf) (accessed 16 April 2019).

EPA (2003b), *Response Protocol Toolbox: Planning for and responding to drinking water contamination threats and incidents. Module 3: Site characterization and sampling guide* (https://www.epa.gov/sites/production/files/2015-06/documents/module_3.pdf) (accessed 16 April 2019).

EPA (2004a), *Emergency response plan guidance for small and medium community water systems to comply with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002* (https://www.epa.gov/sites/production/files/2015-04/documents/2004_04_27_watersecurity_pubs_small_medium_erp_guidance040704.pdf).

EPA (2004b), *Response Protocol Toolbox: Planning for and responding to drinking water contamination threats and incidents. Module 6: Remediation and recovery guide* (https://www.epa.gov/sites/production/files/2015-06/documents/module_6.pdf) (accessed 16 April 2019).

EPA (2004c), *Response Protocol Toolbox: Planning for and responding to drinking water contamination threats and incidents. Response guidelines* (https://www.epa.gov/sites/production/files/2015-05/documents/drinking_water_response_protocol_toolbox.pdf) (accessed 16 April 2019).

EPA (2011), *Planning for an emergency drinking water supply*, Office of Research and Development, EPA, Washington, DC (https://www.epa.gov/sites/production/files/2015-03/documents/planning_for_an_emergency_drinking_water_supply.pdf) (accessed 16 April 2019).

EPA (2015), *A water security handbook: Planning for and responding to drinking water contamination threats and incidents*, Office of Ground Water and Drinking Water, EPA, Washington, DC (https://www.epa.gov/sites/production/files/2015-06/documents/watersecurity_water_security_handbook_rptb_1.pdf).

EPA (2018), *Guidance for responding to drinking water contamination incidents* (https://www.epa.gov/sites/production/files/2018-12/documents/responding_to_dw_contamination_incidents.pdf) (accessed 16 April 2019).

EPA (n.d.), *Guarding against terrorist and security threats: Suggested measures for drinking water and wastewater utilities (water utilities)* (https://www.waterboards.ca.gov/drinking_water/certlic/drinkingwater/documents/security/AppendixI_%20USEPAthreatlevelguide_march_%2031.pdf) (accessed 30 August 2019).

ERSAR (Water and Waste Services Regulation Authority) (2018), *Communication plan for emergencies in water quality for human consumption, Technical Guide 25*, Lisbon.

European Commission (2017), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — Action plan to enhance preparedness against chemical, biological, radiological and nuclear security risks (COM(2017) 610 final) (https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52017DC0610) (accessed 16 April 2019).

European Parliament and Council of the European Union (2016), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1) (http://data.europa.eu/eli/dir/2016/1148/oj).

Gattinesi, P. (2018), *European Reference Network for Critical Infrastructure Protection: ERNCIP handbook 2018 edition*, Publications Office of the European Union, Luxembourg, doi:10.2760/245080.

Herrick, C. (2006), *Emergency response and recovery planning for water systems: A kit of tools*, Water Research Foundation Report Series, AwwaRF Report 91097F, IWA Publishing, London.

Hohenblum, P., Pitchers, R., Raich, J., Tanchou, V., van der Gaag, B. and Weingartner, A. (2016), *Proposals for a guidance related to a water security plan to protect drinking water*, ERNCIP Thematic Group Chemical and Biological (CB) Risks to Drinking Water, Publications Office of the European Union, Luxembourg, doi:10.2760/258130.

Janke, R., Tryby, M. E. and Clark, R. M. (2014), 'Protecting water supply critical infrastructure: An overview', in Clark, R. M. and Hakim, S. (eds), *Securing water and wastewater systems*, Springer International Publishing, Cham, pp. 29-85, doi:10.1007/978-3-319-01092-2_2.

Ministry of Health Israel (2009), *Guidelines for performance and submission of engineering sanitary survey — Hebrew*, Ministry of Health, Jerusalem (https://www.health.gov.il/hozer/bsv_10812b.pdf) (accessed 16 April 2019).

Ministry of Health Israel (2016), *Guidelines for rehabilitation of damage water network system — Hebrew* (https://www.health.gov.il/hozer/bsv_water_system.pdf) (accessed 16 April 2019).

Oregon Health Authority (2002), *Public water system emergency response plan: Introduction to the model plan*

(https://www.oregon.gov/oha/PH/HEALTHYENVIRONMENTS/DRINKINGWATER/PREPAREDNESS/Documents/ERP-StateModel.pdf) (accessed 16 April 2019).

Serafinelli, E., Reilly, P., Stevenson, R., Peterson, Fallou, L. and Carreira, E. (2018), *A communication strategy to build critical infrastructure resilience*, Improver, Deliverable No D4.5, European Commission (https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bba3be40&appId=PPGMS).

Silva, T. M. G. da (2015), *A ameaça terrorista em Portugal*, Faculdade de Ciências Sociais e Humanas, Universidade Nova de Lisboa, Lisbon (https://run.unl.pt/handle/10362/16264) (accessed 16 April 2019).

State Water Resources Control Board (2015), *State Water Resources Control Board Division of Drinking Water emergency response plan guidance for public drinking water systems serving a population of 3,300 or more (approximately 1,000 SC or more)*, State Water Resources Control Board, Division of Drinking Water (https://www.waterboards.ca.gov/drinking_water/certlic/drinkingwater/documents/security/ddw_emergency_guidelines_0215.pdf).

Teixeira, R. and Cabanas, D. (2018), *Communication plan for emergencies in water quality for human consumption in municipality of Barreiro.*

WaterISAC (2014), 'July 9 and 10, 2014 public notification in water contamination events and outages (two-part webinar)' (https://www.waterisac.org/portal/webcasts/july-9-10-2014-public-notification-in-water-contamination-events-and-outages) (accessed 16 April 2019).

Weingartner, A. and Raich-Montiu, J. (2015), *Proposal for a water security plan to improve the detection of threats in the distribution network affecting drinking water quality*, ERNCIP Thematic Group Chemical and Biological Risks to Drinking Water task 2, deliverable 2.2, Publications Office of the European Union, Luxembourg, doi:10.2788/63373.

WHO (World Health Organization) (2004), *Guidelines for drinking-water quality*, 3rd edition, WHO, Geneva (https://www.who.int/) (accessed 16 April 2019).

WHO (2009), *Water safety plan manual: Step-by-step risk management for drinking-water suppliers*, WHO, Geneva.

WHO (2011), *Guidelines for drinking-water quality*, 4th edition, WHO, Geneva (http://www.who.int) (accessed 16 April 2019).

List of abbreviations

CBRN	chemical, biological, radiological and nuclear
CDLAS	contamination dissemination look-ahead simulation
CWQM	continuous water quality monitoring
CWS	contamination warning system
EDS	event detection system
ERNCIP	European Reference Network for Critical Infrastructure Protection
GIS	geographic information system
PV	permitted value
SCADA	supervisory control and data acquisition
WHO	World Health Organization

List of figures

List of tables

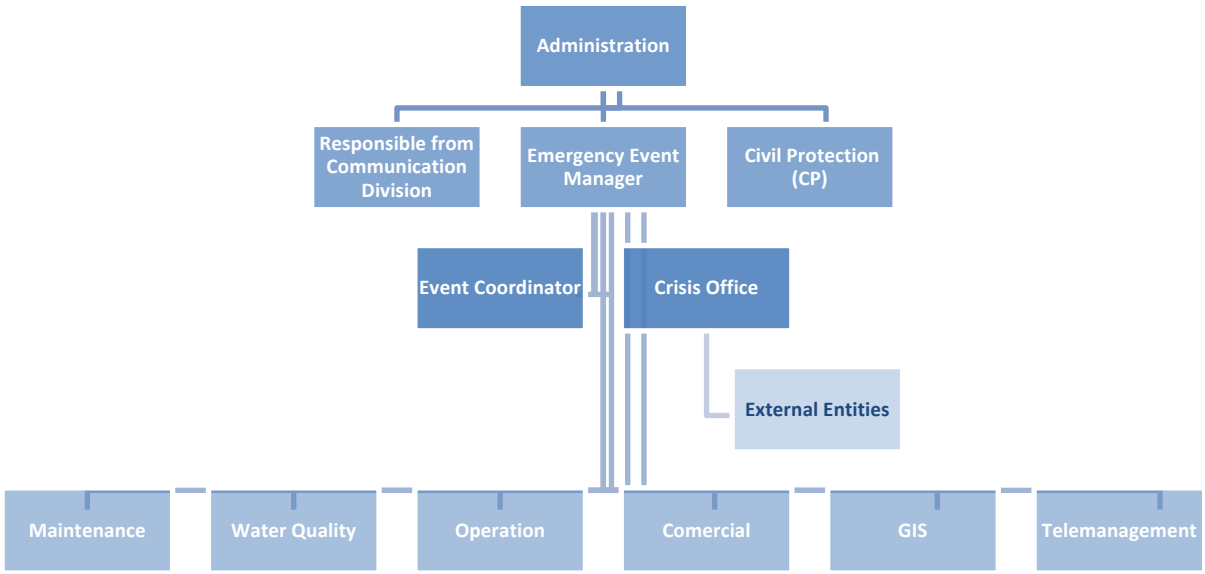
Annexes

Annex 1 — Examples of roles and responsibilities in water security planning

The responsibility for producing and owning the water security plan, including the responsibility for maintaining/updating the plan and its necessary revisions, should be allocated by the senior management of the water utility operator. Normally, this responsibility would be allocated to the operations director, who would delegate the role of water security plan manager, which could, but not necessarily, be the person nominated to be the emergency event manager.

The multidisciplinary coordination team, which is the internal team responsible for coordinating the plan, should support the emergency event manager in the proper assessment of a situation and associated decision-making. This coordination team should involve the top-level management and also representatives of the various operational areas with direct involvement in the water supply system (EPA, 2018; ERSAR, 2018; Teixeira and Cabanas, 2018), as shown in Figure 9.

Figure 9. Organisation chart of an example event coordination team



Source: Teixeira and Cabanas, 2018

The members of this team should have clear definitions of their roles, and the persons responsible for collecting data in all operational areas, as well as the person responsible for the classification of the severity level of the event, depending on the data received, should be clearly identified.

The constitution of the multidisciplinary coordination team may vary according to the degree of severity of the event, based on the level of responsibility of the team and the tasks to be performed, as well as how the continuity of the service has been affected. The roles of managing and/or coordinating the event can also be defined according to the level of severity (minor, major or catastrophic), to ensure effective organisation and the effective management of the emergency, including through the support of external entities, as needed.

Table 3 shows the constitution of example coordination teams, depending on event severity.

Table 3. The constitution of example coordination teams depending on event severity

Coordination team		
Event severity	**Emergency event manager**	**Event coordinator**
Minor event	Head of operations division of water utility operator	Head of water quality division of water utility operator
	Substitute: Head of water production division of water utility operator	Substitute: Head of information system division of water utility operator
Major event	Director of operations of water utility operator	Director of water quality of water utility operator
	Substitute: Director of water production of water utility operator	Substitute: Director of information system of water utility operator
Catastrophic event	President or chief executive officer of the utility operator/board and rehabilitation advisory committee	Civil protection or security authorities/security intelligence services and utility operator
	Substitute: Vice president or chief operating officer of the utility operator/board and rehabilitation advisory committee	Substitute: Civil protection or security authorities/security intelligence services and utility operator

Source: Teixeira and Cabanas, 2018

With regard to external entities, all partner stakeholders should be considered, in particular the water regulator, public health authorities, firefighter associations, hospitals, local government, the most-exposed consumers, the police authorities, the national environment agency, industrial sites, the intelligence services, military authorities, civil protection agencies and other entities with any interest or influence in relation to this issue, such as laboratories and specific suppliers.

Table 4 shows some of the external entities that could be considered and how their details should be recorded.

Table 4. Example of recording contact details of external entities

External entities				
Entity	**Name**	**Function**	**Telephone**	**Email**
Regulator				
Environment agency				
Hospital				
Firefighter association				
Health authorities				
Intelligence services				
Civil protection agencies				
Local government				
Water samplers				
Military authorities				
Police authorities				
University community				
Main users/sensitive users				
Suppliers				
Other				

Source: Teixeira and Cabanas, 2018

With regard to a catastrophic event, management could be undertaken by the senior management of the water utility operator and the coordination of the event could be the responsibility of the security authorities and the utility operator, which, according to the guidelines provided by the emergency event manager, must implement mitigation measures. A crisis office should be created in the meantime. It must be remembered that deliberate contamination that is deemed to constitute a terrorist situation will be considered a serious tactical-police incident. While the designation may vary between countries, the overall management of such an incident would probably rest with the national counterterrorism authorities, including the role of coordinating the various security forces and services.

The functional entities must manage any catastrophic event in the most appropriate way, accepting the coordinator's guidelines, bypassing any constraints of the situation and always

focusing on ensuring that the service can be returned to its normal functioning as soon as possible. Logistics services (warehousing, purchasing, suppliers, etc.) as well as the allocation of external service entities are decisive for managers to carry out its activity in emergency situations.

Table 5 shows an example of how responsibilities are assigned during an event classified as catastrophic.

Table 5. Example of how responsibilities are assigned during a catastrophic event

Role	Responsible for the assignment	Functions to be performed
Emergency event manager	Senior management	Responsible for making decisions during the event and, eventually, for communicating with the public
Event coordinator	Civil protection or security authorities/intelligence services and utility	Responsible for the organisation, treatment and validation of information received, continuous reassessment of impacts to update the nature and severity of the event, presenting solutions and implementing guidelines for mitigation measures
Crisis office coordinator	To be appointed by the president or chief executive officer of the utility operator/board and rehabilitation advisory committee	Responsible for the management and coordination of the crisis office, the convening of service leaders and communication with the different external entities, service users and media

Source: Teixeira and Cabanas, 2018

Table 6 provides a general overview of the possible roles and responsibilities of the utility operator and response partners in implementing an effective and adequate response to an emergency situation. Note that this is an example only and not a comprehensive list, since response partner organisations and roles may vary between localities, regions and/or countries.

Table 6. General overview of potential roles and responsibilities of the utility operator and its response partners

Partner	Typical responsibilities
Drinking water utility operator incident command	Coordinates and implements overall incident response activities including the investigation, operational responses, risk communication and planning for remediation. Provides appropriate notifications to response partners
Local health authorities	Support development of public notifications and serve as a conduit to national health authorities. Serve as a technical resource during the investigation. Provide information about health risks associated with suspected contaminants
Local fire departments	Coordinate with the utility operator in the event that the water service in a specific response area should be shut down. They can notify affected neighbourhoods and assist in the distribution of an alternative drinking water supply. They may also be able to assist with flushing operations, provide input regarding fire suppression requirements and communicate safety considerations related to the use of contaminated water for firefighting
Water sampler teams	Support site characterisation and sampling activities. Take responsibility for a location where contamination has occurred or a hazard may exist until the level of the hazard has been determined
Police authorities	Support investigation activities by controlling access to a suspected contamination site. May serve as a conduit to local and/or national law enforcement and intelligence services. May assist in distribution of an alternative drinking water supply. May assume, according to national legislations, incident command and take charge of the activities under certain circumstances, such as intentional contamination, in coordination with the utility operator
Environmental and public health laboratories	Provide or coordinate laboratory support for the analysis of water samples during investigation and remediation efforts. National public health laboratories provide access to the Centers for Disease Control and Prevention's laboratory response network
National or regional drinking water and national wastewater agencies	Provide resources and technical expertise during investigation, response and remediation, and advise the utility operator regarding regulatory requirements for treating contaminated water, public notification, environmental concerns about discharged water and the provision/quality of alternative drinking water supplies
National agencies and authorities (environmental agencies, security authorities/security intelligence services, civil protection agencies)	Provide resources, technical expertise and support to the utility operator with regard to investigating and responding to a contamination incident. May assume incident command and take charge of the activities under certain circumstances, such as intentional contamination, in cooperation with the utility operator
Military authorities	Provide resources and support for a wide range of incident activities. Act as a 'force multiplier', bringing personnel trained in a formal command structure who can perform a wide range of tasks (e.g. distributing bottled water, collecting samples, staffing call centres and analysing samples)
Local government	Communicates with constituencies regarding the impact of the incident on the community, actions taken to protect the public and the progression of the response and recovery efforts

Source: EPA, 2018

Annex 2 — Characterisation and evaluation of the threats

The characterisation and evaluation of threats to the water supply system (Janke et al., 2014; EPA, 2015, 2018) should be based on historical data and the sharing of existing information held by national authorities, including intelligence services, and also on, inter alia, the existing communication and cooperation between countries and particularly at EU level.

Water utility operators are encouraged to consider the following aspects of contamination:

— the water distribution system: contaminant quantity, method and location within the water system of contaminant injection or release, etc.;
— contaminant: type, concentration, toxicity, etc.;
— magnitude of potential consequences: on public health, on water network rehabilitation, etc.

The contamination of a distribution system could occur through contaminant release (e.g. dumping chemicals or pesticides into a water tank) or injection. Fire hydrants, tanks, reservoirs and pump stations could be vulnerable to both contaminant release and contaminant injection.

Three aspects of contamination threats need to be considered:

— the type and quantity of the contaminant released, as well as the behaviour of the contaminant once released into the system;
— the location or locations in the water system where the contaminant is introduced;
— the type and distribution of the population downstream of contaminant introduction and this population's behaviour as the contamination progresses through the water system.

Large amounts of material are generally needed to deliberately contaminate water sources, making it difficult for terrorists to acquire, produce or transport sufficient quantities of potential contaminants. Nonetheless, water utility operators should consider the specific vulnerabilities of their water distribution systems. For example, the risk assessment process should identify any key vulnerability points where the introduction of contaminants, whether by chance or with the help of insider knowledge, could have an adverse impact, through low dilution, diminishing the effects of disinfectants, chemical decomposition or oxidation.

The magnitude of any adverse consequences following the release of a contaminant into a water distribution system is a function of the contaminant's characteristics:

— its toxicity;
— the quantity released;
— its behaviour in water distribution system.

The behaviour of the contaminant is dependent on its interaction with any available disinfectant and naturally occurring biological materials present in water distribution systems. Adverse health effects are dependent on contaminant solubility and organoleptic properties, which influence exposure and dose.

The consequences of a water contamination event can be significant. The contamination of a water system can adversely affect the people, businesses and community it serves as a result of causing fear among the population, the loss of the water service, significant economic costs for decontamination and recovery, and adverse public health effects, which could be significant in magnitude. Public health consequences can be described and estimated in terms of:

— exposures (i.e. people in their places of residence and business witness contamination in their tap water);
— doses (i.e. people in the community served by the water system ingest contaminated water or somehow accumulate some measurable quantity of the contaminant or contaminants in their bodies);
— health effects (i.e. a health effect can be estimated as a result of the ingestion of a certain amount of contaminant): health effects can occur in the short term, i.e. within days or weeks of exposure, or in the long term, i.e. within months or years.

In the short term, health effects could include sickness, incapacitation or death. In the long term (i.e. months or years), health effects could include increased cancer risk, although such health effects may be difficult to link to water distribution system contamination.

Moreover, in addition to the potential threats to health, there could be other types of threat, which should be considered during this stage of characterisation and evaluation, e.g. the introduction of hydrocarbons, solvents, very odorant products or other substances that, without being directly toxic to people, could prevent water from being used for hygiene purposes, such as hand washing and showers, with high levels of disturbance possible in hospitals, schools, and other public and administrative buildings.

Indirect threats that should also be considered by water utility operators include the introduction of contaminants that force the closure of network valves, thereby stopping water distribution, with consequences for firefighting services and risks for high buildings, commercial areas, railway stations, and other public and administrative buildings.

Annex 3 — Potential contamination scenarios

Water utility operators may find it useful to consider potential contamination scenarios when assessing potential threats to their systems. This annex sets out four types of scenario. Information about the feasibility of these scenarios should be established by the water utility operator with the support of local police authorities and intelligence services, at the level of the country and/or the region depending on the territorial context in which they are located.

Scenario type 1 — deliberate chemical, biological or radiological contamination of the water supply system

In this scenario, it is recommended that the various potential methods of deliberate contamination of the infrastructures of the water supply system be considered:

— direct contamination by adding chemical/biological/radiological materials to the water infrastructure; this could involve the use of insider knowledge;
— adulteration of the chemical parameters used in the treatment plant and/or chlorination point facilities; this could result from intrusion, an internal agent or contracted supplier or cyberattack;
— direct contamination with chemical/biological/radiological materials at any point connected to the water supply network.

Scenario type 2 — threats to attack (by deliberate chemical, biological and/or radiological contamination) the water supply system

This scenario considers messages containing threats that the system for supplying water for human consumption will be attacked. These messages may be in the form of letters, telephone calls or emails, or through social networks or other routes, such as a threat written on the wall of a water supply system building. In this scenario, the risks, not those arising from an actual attack, but that an attack will actually occur or has just occurred will need to be considered.

When considering this scenario, the processes for evaluating the credibility of a threat will need to be set out, as will those for checking the integrity of critical points in the system. In such a scenario, threats are likely to be made publicly, so any risks arising from the public's reaction to the threats must also be considered in terms of planning the response. The response measures must include effective and proportionate communication with the public, without creating fear, which is the goal of terrorists.

Scenario type 3 — attack of water supply infrastructures with improvised explosive devices

Water utility operators need to consider the risks from attacks against the water supply infrastructure with any kind of improvised explosive device, whether or not such attacks could lead to contamination. While this is outside the scope of this guidance, it should be considered by water utility operators in the development and implementation of their water security plans.

Scenario type 4 — armed attack against critical assets of the water supply system

This scenario considers an armed attack on any critical infrastructure asset of the water supply system, with the aim of taking control of it, by internal agents present on the premises of the water supply system, who, on the basis of their knowledge of the system, are capable of forcibly contaminating the water and disrupting service. While specific guidance on this

scenario is outside the scope of this document, it should be considered by water utility operators in the development and implementation of their water security plans.

Access to information on contamination scenarios

It is important to emphasise that details of the contamination scenarios produced by a water utility operator for its water security plan will be extremely sensitive, and access to these details will need to be managed by the utility operator accordingly. They should be contained in a document separate from the main part of the security plan, along with any other sensitive information, and made available to only trusted individuals within the organisation on a 'need to know' basis. It is recommended that care also be taken with any electronic storage or communication of such sensitive information, even within the utility operator's own systems.

Annex 4 — Establishment of contamination impact and event severity

During the investigation of a suspected contamination event, a utility operator will need to evaluate its confidence in any information that indicates that the system may be contaminated. Consideration should also be given to the potential impact of the suspected incident on the system and its customers. Together, this confidence level and the potential impact will help to determine the potential severity of the event and hence inform the utility operator's decisions with regard to a response.

Confidence in data

A utility operator should evaluate how certain it is that contamination has occurred based on the available information. The level of confidence in the data can be expressed using descriptive terms or by numbers in a tier system that have a clearly defined meaning for the utility operator's personnel and response partners.

For instance, the terms 'possible', 'credible' and 'verified' could be used to express three levels of confidence in information from a particular data source indicating that contamination is present. Expressing the confidence level in a standard format helps to efficiently convey the current state of the incident to the response team.

Criteria will need to be established by the water utility operator for different types of indicator to help the response team assign a confidence level. Potential suspicious activity indicators are suggested in Section 3.1.2. Factors to consider when establishing confidence criteria include:

— the type and source of the information indicating contamination: for example, an anonymous vague verbal threat would be assigned only a low level of confidence (i.e. 'possible'); a more specific threat detailing the type of contaminant and its location might be considered more credible; and an anomaly in water quality identified by online monitoring systems would be more credible still, with the confidence level depending on the extent of the anomalous measurement;
— information from other utility departments and partners (e.g. treatment status, work orders);
— any corroborating evidence (e.g. additional indicators, evidence of tampering);
— site characterisation and sampling (e.g. sampling results, presence of site hazards).

Table 7. Example of a table of indicators used to evaluate confidence in data and the certainty of a contamination event

Data source	Confidence	Grade
Verbal threat	Possible	1
Physical breach of infrastructure asset notified within the past 48 hours	Possible	1
Water quality anomaly detected by one sensor — turbidity	Possible	1
Information from other utility operator/agency	Possible	1
Presence of site hazards — pesticide package	Credible	2
Activation of a security system alarm	Credible	2
Positive laboratory results — 100 *E. coli*/100 ml	Verified	3

Note: *E. coli*, *Escherichia coli*.
Source: JRC, 2019

Impact

A utility operator should also evaluate the potential impact of contamination, that is, the potential consequences for its system and customers based on the indicator(s) of suspicious activity.

Determining the severity of an incident will have a significant influence on when and how response activities are implemented. As for confidence level, a tier/level system could be used to express the potential impact of contamination, for instance as 'low', 'moderate' or 'high'.

Factors to consider when establishing impact criteria include:

- the potential impact on public health (e.g. no effect: 'low'; non-serious effects: 'moderate'; illness/fatalities: 'high');
- the number of customers potentially affected (e.g. none: 'low'; a single block: 'moderate'; an entire pressure zone: 'high');
- the potential impact of use restrictions on customers (e.g. boil warning, do-not-drink, do-not-use);
- the potential impact on critical customers (e.g. hospitals);
- the potential impact on the system/geographical extent (e.g. single storage tank, entire system);
- the regulatory impacts (e.g. potential for non-compliance with regulations, reporting requirements);
- the potential impact on non-critical measures (e.g. the aesthetics of the water, customer confidence).

Table 8. Example of a table of indicators used to evaluate the level of impact of the event

Data source	Impact level	Grade
No effect on public health	Low	1
Illness	Moderate	2
Fatalities	High	3
Number of customers potentially affected — pressure zone	Moderate	2

Source: JRC, 2019

Confidence and impact levels should be evaluated immediately after any indication of contamination has been observed and throughout the investigation as new information is gathered. At the highest level, the evaluation should determine whether to rule out contamination, to begin/continue the investigation or to confirm that contamination has occurred. The evaluation of confidence and impact levels is also useful for decision-making when planning the various investigation and response activities.

As an example, an indicator of contamination with a verified confidence level, such as the detection of residual potassium permanganate in water in the distribution system, may pose little risk to public health (and be assigned an impact level of 'low') and would lead to the notification of the public but no use restriction. On the other hand, a verbal, unspecific threat of contamination with a 'toxin' may be assigned a confidence level of only 'possible' but a 'high' potential impact level (i.e. it would have severe consequences for public health), and therefore would warrant urgent investigation and preliminary responses (e.g. isolation) pending further investigation.

The confidence and impact levels should be simple and easy to understand so that they convey their meanings clearly, particularly to response partners. In this guidance, confidence and impact levels are described for reference; however, these should be customised as needed so that they are meaningful and have the most value for the utility operator and its response partners.

While confidence and impact ratings are useful tools, it is important to use an evaluation process that allows those leading the incident response the flexibility to adapt the response to the situation. The evaluation of confidence and impact levels should help guide response decisions, but not constrain or limit the selection of response activities.

The investigation of an indicator of contamination could assign one of three confidence levels ('possible', 'credible' or 'verified') and one of three impact levels ('low', 'moderate' or and 'high'), for example; however other scales could also be used. The confidence levels guide the overall investigation and response, while the impact levels guide the implementation and urgency of specific activities as the utility operator's confidence in the source of information progresses.

Criteria for assessing the level of certainty (based on internal sources)

All information regarding an alleged event must be taken seriously, until any indication of contamination is either confirmed or explained.

An initial determination of the level of certainty of an event is essential for decision-making. This determination consists of defining the elements to be investigated, according to the classification of the anomalous situation, and obtaining information and concrete data, with the aim of adequately characterising the situation.

Information from external sources must be supported by information from internal sources. Similarly, some internal sources, such as alarms raised by sensors, will need to be verified by sampling and field and/or laboratory tests.

LEVEL OF CERTAINTY

The level of certainty of the event should be classified as **'caution', 'suspicious'** or **'confirmed'.**

All information, even if subject to confirmation, that may affect the level of service provided and compromise the quality and continuity of the water supply, whether obtained from an internal or an external source, must be recorded and available for consultation whenever warranted or requested.

Table 9 shows an example of the evaluation criteria used to determine the level of certainty of an event, taking into account information from operational sensors and online monitoring.

Table 9. Example of criteria for assessing the level of certainty of the event (based on internal sources)

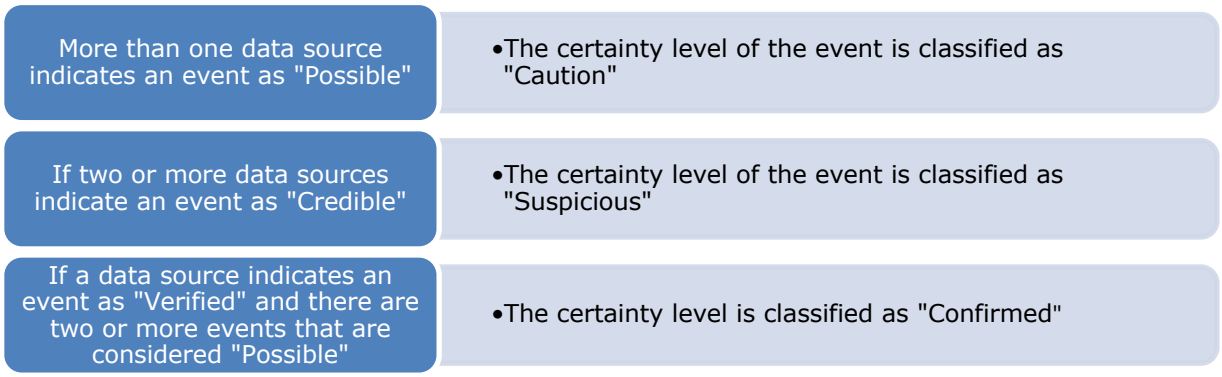
Certainty level of contamination event:	Caution	Suspicious	Confirmed
Potential information sources: • Ultraviolet-visible spectroscopy • Temperature • Residual disinfectant • pH • Conductivity • Turbidity • Other parameters	Alarm from an online sensor or meter observed within a pre-determined period of time	Alarms from two different sensors or meters, observed over a certain period of time	(1) An online sensor alarm confirmed by laboratory results; (2) three or more alarms from independent online sensors

Source: Teixeira and Cabanas, 2018

Criteria for assessing the level of certainty (based on external sources)

In cases in which external sources of data indicate contamination, as listed in Section 3.1.2, a more complex criteria model, as set out in Figure 10, could be considered to assess the level of certainty of the event. The exact determination of the combination of indicator type and confidence leading to the confirmation of a contamination event should be determined by each water utility operator, and must be regularly reviewed in light of experience, especially if false alarms have been triggered.

Figure 10. Examples of criteria for assessing the level of certainty of the event (based on external sources)



Source: Teixeira and Cabanas, 2018

Classification of event severity

The severity of an emergency situation is dynamic and can be classified as more or less severe according to the information available at the time and the development of events.

Establishing appropriate response measures depends significantly on the ability to predict the potential consequences of the contamination of the water distribution system.

To evaluate the severity of an event, an evaluation process can be used, combining certainty and impact levels in a severity matrix, on the basis of both qualitative and quantitative criteria. This evaluation process will establish what severity level should be assigned to an event, e.g. 'minor', 'major' or 'catastrophic'. Tables 7 and 8 provide examples of indicators used to evaluate confidence in the available data and the potential impact level of an event, and Table 12 provides an example of the type of matrix that can be used to estimate the severity of an event. These evaluations are the basis of the overall evaluation process aimed at determining the severity of an event.

Investigation activities involve the collection of information about the incident in an attempt to either rule out or confirm contamination and to classify the severity of the incident once it has been confirmed. These activities include gathering and reviewing available information from a variety of sources and collecting new information from the field through site characterisation and sample collection and analysis.

Criteria used to evaluate the severity level of an event

Examples of qualitative criteria used to evaluate the severity of an event are described in Table 10.

Table 10. Examples of qualitative criteria used to evaluate the severity level of an event

Severity level	Classification	Description
1	**Minor**	Anomalous or unexpected situation that by its magnitude or confinement is not a threat beyond the area in which it was produced An event that has repercussions for and impacts on a small area and where the resolution of the event is likely to lead to possible interactions with external entities
2	**Major**	An event that develop would into an emergency situation if immediate corrective action is not taken and water distribution is maintained An event that has repercussions for and impacts on a supply area. For the resolution of such an event, intervention by external entities at the local level may be justified. The severity and scope of the event may also justify involving the media, as well as sensitive users
3	**Catastrophic**	An uncontrolled or difficult-to-control event that has caused or may cause personal, material or environmental damage. It requires immediate action to recover control and minimise the consequences. Water distribution is interrupted An event with implications throughout the supply system. To resolve this type of event, intervention by external entities at the national level may be justified. The seriousness and scope of the event may justify the systematic use of the media, as well as direct contact with affected users

Source: Teixeira and Cabanas, 2018

Examples of quantitative criteria used to evaluate the severity of an event are described in Table 11.

Table 11. Examples of quantitative criteria used to evaluate the severity level of an event

Information	Source of information	Level of severity		
		Minor	Major	Catastrophic
Coliforms (ufc/100 ml)	Lab n	1-50	51-200	> 200
***E. coli* (ufc/10 ml)**	Lab n	1-10	11-50	> 50
Enterococci (ufc/100 ml)	Lab n	1-30	31-100	> 100
***Clostridium perfringens* (ufc/100 ml)**	Lab n	1-10	11-50	> 50
***Salmonella* or *Shigella* — presence/absence (100/5 000 ml)**	Lab n	Absence	Absence	Presence
Cryptosporidium giardia	Lab n	Between 1 and 2 times the guideline value	Between 2 and 10 times the guideline value	Greater than 10 times the guideline value
Other pathogenic microorganisms (*Legionella* and *Pseudomonas aeruginosa*)	Lab n	Between 1 and 10	Between 11 and 99	Greater than 99
Inorganic chemical parameters of Annex I to Directive 98/83/EC, radiological material, aluminium, ammonia	Lab n/operations	Between 1 and 2 times the PV	Between 2 and 4 times the PV	Greater than 4 times the PV
Organic chemical parameters	Lab n	Between 1 and 2 times the PV	Between 2 and 4 times the PV	Greater than 4 times the PV
Activation of security system alarm	Security manager	No	Possible	Confirmed
Water treatment system or manoeuvres of the affected system	Operations	No	Partially closed	Totally closed
Water flow rate in the zone affected by the event	Operations	< 100 m^3/day	100-1 000 m^3/day	> 1 000 m^3/day
Unscheduled cut in supply	Operations	< 12h	12-24	> 24h
Confirmed incident history	Operations	No	At least one incident confirmed in the past year	At least one incident confirmed in the past 6 months
Several default parameters at various stages of the supply system	Lab n/operations	Only at one stage	At two stages	At more than two stages
Number of complaints received in the past 24 hours	Utility help desk	1-5	5-10	> 10
Sensitivity level for affected users	Security plan	Sensitive	Very sensitive	Hypersensitive

Information	Source of information	Level of severity Minor	Major	Catastrophic
Cases of illness reported by health authorities	Health authorities	Not reported	Reported in one zone	Reported in various zones
Media involvement	Communication department	No	Local journals	Social networks, television and radio

Note: *E. coli*, *Escherichia coli*; PV, parametric value.
Source: Teixeira and Cabanas, 2018

After analysing all available information, the internal team can classify the severity of the event using qualitative and quantitative criteria (see Table 12).

Table 12. Example of a matrix used to evaluate the severity of an event

Event severity matrix	Event certainty level (value assigned)	Caution (1)	Suspicious (2)	Confirmed (3)
Impact level (value assigned)				3
High (3)		3	6	9
Medium (2)		2	4	6
Low (1)		1	2	3

Key:

Minor	Major	Catastrophic

Source: JRC, 2019

Process of gathering and reviewing available information

To begin the investigation into possible contamination, a utility operator should gather and review all the information available from internal resources and external response partners. This information should include any data that are routinely collected by the utility operator or response partner and that may have some relevance to the current incident. Examples include information on customer calls, online water quality monitoring data, compliance sampling data, data on treatment irregularities, information on maintenance and repair work orders, and public health trend data. These sources of information can provide context and may support decision-making with regard to the direction of the investigation and the responses, especially during the initial stages of the incident when very little information is known. These sources should continue to be checked for updates to information periodically throughout the investigation, particularly those sources that gather data frequently or continuously (e.g. online monitoring stations, customer complaint calls).

Thus, criteria that contribute to the determination of the level of severity of the emergency situation should be defined by considering the following:

— the impact of the event on the level or quality of service (area of supply and/or supply affected, reliability of supply, restrictions in terms of water quantity, problems with the quality of water for supply);
— the length of time estimated to be required to resolve the event, that is, to return the level of service provided to the various types of users to normal;

— any complaints from users regarding the water supply and/or the water supply service and whether or not future complaints are expected (preferably validated information);
— whether or not involvement of the media (information to be validated internally) is required and if so what communication channels to use (e.g. newspaper or local radio, social networks, television);
— confirmation of terrorist attack alert to the competent authorities (civil protection, security forces, intelligence services and/or security information services).

Site characterisation, sampling and analysis

Characterising the site at which there has been an indication of contamination and collecting samples for field or laboratory analysis are important activities that support the investigation of suspected contamination. Characterising the site may provide further evidence of contamination and samples collected from the site can be analysed for water quality parameters and contaminants of concern. Coupled with other available information, the results from these activities can answer many questions about an incident. Other sites of interest may also require investigation, such as any locations where contamination is suspected to have been introduced.

Site characterisation and sampling should be completed for each site to provide instructions to the teams performing field activities. A brief checklist that can be completed during an incident and distributed to field personnel trained to implement the activities, including key response partners, should be prepared in advance and describe:

— the site of interest along with any known information about the site and indicator of contamination;
— the field activities to be performed;
— the water quality parameters to be analysed at the site;
— the samples that should be collected for analysis off site;
— the personnel and response partners that will be deployed to the site;
— what will happen to samples after field activities (e.g. whether they will be sent to a laboratory or given to a response partner);
— the method and frequency of communicating and reporting results;
— the health and safety requirements;
— any approvals/authorisations required (e.g. from the security intelligence services, law enforcement, health and safety authorities).

Which field activities should be performed at a site should be determined by the specifics of the incident and the site, the capabilities of the utility operator and its response partners and the results of the evaluation of confidence and impact levels. Field activities fall into five general categories:

— visual hazard assessment of site: performed upon approach and while accessing the site to screen for the presence of hazards;
— site safety screening: performed to ensure the site is safe for entry;
— water quality parameter testing: performed to collect general water quality data in the field;
— rapid field testing: performed to collect specific contaminant or contaminant class (volatile materials, metals, etc.) data in the field;
— sample collection for laboratory analysis: performed to collect samples for detailed or targeted analysis in a laboratory.
—

Post confirmation of a contamination event

In addition to the above information, information should also be collected on the following during an event related to water contamination (confirmed by laboratory results):

— the part of the water supply system that has been damaged/affected and the level of contamination of water for human consumption;
— where the contamination was discovered and whether it was discovered at a single point of sampling or at several points;
— whether the results of laboratory tests are initial or confirmed, and an estimation of the volume of contaminated water that has been supplied;
— the number of users likely to be affected;
— whether or not repairs have been carried out in the area where water is suspected to be contaminated;
— whether or not there is any situation in which a water contamination event would be expected;
— whether or not any pollution discovered is relevant to the characteristics of the event;
— if the event is occurring in a consumer home networks.

The level of severity assigned to an event should be immediately communicated to the person in charge of event management, that is, the person who defines the responsibilities and functions to be performed by the water security plan team before the event.

Annex 5 — Implementation of security measures in the various infrastructure types of the water supply system

This annex provides guidance on the implementation of security measures for the drinking water infrastructure to prevent or hinder the materialisation of the most probable scenarios of a terrorist threat (Janke et al., 2014; EPA, 2015, n.d.; Carmi, 2018).

The first step should be to correct the most serious security deficiencies identified by the security system risk assessment as soon as possible. This should be prioritised, with immediate investment in the most obvious and cost-effective improvements to the security system, and funds allocated to completing other improvements subsequently.

Some measures could be implemented immediately without cost or with no significant or time-consuming costs, while others may involve significant costs, depending on the level of security desired, e.g. patrolling to verify the integrity of security at locations identified as critical within the water supply system network or the installation of an online monitoring system and sensors and complementary data analysis software.

Online monitoring

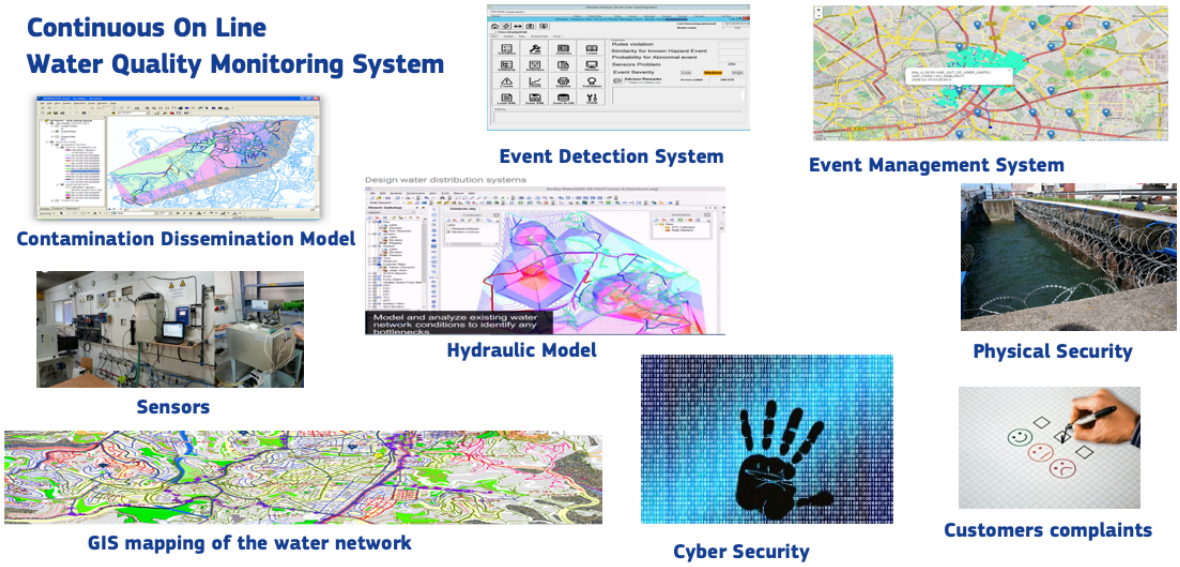
The detection of contamination could be facilitated by the installation of an online monitoring system and sensors and complementary data analysis software, so that any change to the normal standard of water quality would be detected as soon as possible and any intentional (or unintentional) contamination of drinking water would be detected.

CWQM is a proactive approach to monitoring water quality and potential contamination. It involves the use of advanced technologies and enhanced surveillance to collect, integrate, analyse and communicate information, and should be a fundamental element of a water security plan.

A CWQM system comprises a suite of tools that constitute a decision support system, providing event managers with the information necessary to make good decisions, assisting in the evaluation of multiple response actions, and thereby minimising human exposure to contaminants and maximising the effectiveness of intervention strategies.

Figure 11 shows examples of online monitoring systems and event detection and management software. These include links to external sources of information that may be very important and should be cross-referenced, such as information on customer complaints, data from public health or security authorities or security intelligences services, and results of laboratory analysis.

Figure 11. Examples of CWQM systems included in a decision support system



A CWQM system is one component needed in a surveillance system to enable the timely detection of incidents that affect water quality in drinking water distribution systems. Additional requirements are physical and cybersecurity monitoring, customer complaints and public health surveillance, and laboratory analysis.

Once integrated into the daily operations of a water utility operator, a CWQM system will detect deliberate acts of contamination such as terrorist attacks or sabotage, as well as natural disasters, accidents and mishaps or operational mistakes. Such a system can also be used to further understanding of the operation of the water distribution system.

A CWQM system is a vital management tool for monitoring the water network and an important component of a decision support system for detecting anomalies. A CWQM system enables timely event detection, thus allowing actions to be carried out quickly to minimise the dissemination of any contaminant, limit the impact on the health of residents and restrict damage to the water network. In turn, this enables faster rehabilitation of the network and the effective mitigation of economic impacts.

The basis of a CWQM system is a network of water quality monitoring stations at strategic locations throughout a drinking water distribution system. Each station should contain a suite of sensors that measure water quality and operational parameters. Real-time and near-real-time water quality data collected from sensors are continuously analysed by an EDS allowing the utility operator to rapidly detect water quality anomalies.

The installation, implementation and operation of a CWQM system requires the input of the utility operator's hydraulic engineers, i.e. those who are familiar with the water network, water quality experts, electronics and communications experts, IT (information technology) security experts and skilled technicians.

These guidelines briefly explain the CWQM approach so that users are familiar with how to implement such a system in a utility organisation.

Online monitoring security measures could include:

— monitoring the quality of the source water, that is, the water leaving the plant, and the water in distribution and storage systems to establish baseline results, followed by reviewing operational and analytical data to detect unusual variations;
— maintaining disinfectant residuals as required by regulations;
— to the extent possible, increasing the frequency and extent of monitoring activities and reviewing the results against baseline;
— increasing the frequency of reviewing operational and analytical data (including customer complaints) with the aim of detecting unusual variation (as an indicator of unexpected changes in the product); variations due to natural or routine operational variability should be considered first.

Other measures to consider are outlined below:

— Physical security measures:
    - installation of backflow preventers at key connection points;
    - increase in the frequency of the collection of water samples for analysis under the operational control plan during special and temporary events;
    - raising awareness among the population, without causing public alarm, of the need to be attentive to points identified as critical, giving instructions on the procedure to be adopted in the event of an anomalous event being detected, namely providing a description of the individuals involved and the registration number of any vehicle;
    - permanent security presence at critical points in the supply system, particularly during special and temporary events;
    - report to entities and authorities involved in the plan in cases of incidents or possible incidents;
    - follow up on customer complaints concerning water quality and/or suspicious behaviour within water supply facilities;
    - confirm communication protocol with public health officials concerning potential waterborne illnesses;
    - with regard to chemical deliveries, check for driver identification and verify load;
    - maintain vigilance and be alert to suspicious activity;
    - inspect buildings in regular use for suspicious packages and evidence of unauthorised entry;
    - report any suspicious activity to appropriate authorities;
    - prosecute intruders, trespassers and those detained for tampering to the fullest extent possible under applicable laws with the collaboration of police authorities;
    - review requests for tours of water supply facilities and identify protocols for managing tours;
    - implement controls for construction activities at critical sites;
    - implement best management practices for optimising drinking water treatment;
    - test security alarms and systems for reliability with frequency;
    - increase surveillance activities in areas of source and finished water;
    - verify the identity of all personnel entering the water utility; make the visible use of identification badges mandatory; randomly check identification badges and cards of those on the premises;
    - establish a system of identification — photo identification badges, etc.;

- at the discretion of the facility manager or security director, remove all vehicles and objects (e.g. refuse containers) located near mission critical security perimeters of the facility and other sensitive areas;
- consider the steps needed to control access to all areas under the jurisdiction of the water utility operator;
- ensure that the list of sensitive customers (e.g. hospitals, nursing homes, daycare centres, schools) within the service area is accurate and shared with appropriate public health officials;
- reconfirm that county and state health officials are on high alert and will inform water utility operators of any potential waterborne illnesses;
- ensure that existing security policies, procedures and equipment are effectively used;
- re-check the security of all on-site chemical storage and utilisation areas and limit access to authorised personnel only;
- keep track of hazardous chemicals;
- use only known, properly labelled chemicals;
- inspect incoming chemicals for signs of tampering or counterfeiting;
- implement frequent and staggered inspections of the exterior of buildings (including roof areas) and parking areas;
- consider placing staff at remote (unmanned) facilities;
- protect wells, intake structures, reservoirs, etc., with fencing;
- secure doors, windows, hatches, etc., using locks, seals, alarms, motion sensors or other appropriate means (remember to consult federal, state and local fire and occupational safety codes before making any changes);
- account for all keys to all areas of the system;
- use video surveillance and security guards where appropriate;
- provide adequate interior and exterior security lighting;
- implement a system of controlling vehicles authorised to park on the premises (e.g. using placards, decals, etc.).

— Personnel monitoring measures (guarding against the threat of an insider, e.g. a disgruntled/radicalised employee):

- control access to mission critical facilities;
- screen prospective employees (references, background checks, etc.): measures for the prevention of internal threats are well established for civil aviation security and other key areas (see Implementing Regulation (EU) 2019/103 of the 23 January 2019), and water utility operators should consider a system of checks for employees — whether internal or external (e.g. suppliers if they are unaccompanied) — similar to that of or inspired by the abovementioned Implementing Regulation, namely a scheme that differentiates between normal and enhanced security checks, depending on the nature of the job; for example, the aforementioned regulation distinguishes between two procedures:
  - A — normal processes, which confirm the applicant's identity, criminal records of the past 5 years in all countries of residence, employment record, including education and work breaks (i.e. periods where no occupation is mentioned); checks should be completed before the beginning of the specific job training, and then repeated after, say, 3 years;

        - B — reinforced processes for employees with access to mission critical facilities that are performed before the beginning of functions and repeated, for example, every 12 months, where possible liaising with national intelligence and other relevant authorities;
    - restrict personal items allowed in facility and establish a policy for inspecting employee lockers and other storage spaces for personal items;
    - collect identification badges, keys and other security items when employment is terminated;
    - monitor employee activity through daily work assignments.
- Cybersecurity measures:
    - verify the security of critical information systems (e.g. SCADA), the online monitoring system and data transmission, the internet, email) and review safe computer and internet access procedures with employees to prevent cyber intrusion;
    - re-check the security of critical information systems (e.g. SCADA, the online monitoring system and data transmission, the internet, email) and ensure staff change computer passwords regularly;
    - restrict access to computer process control and data systems to those with appropriate clearance;
    - eliminate computer access immediately when employment is terminated (deleting passwords, etc.);
    - establish a system to trace individuals' computer activity;
    - develop and maintain adequate critical computer-based data systems;
    - acquire and maintain a virus protection program for all computers that have internet access or can be accessed off site;
    - implement automatic logging out of the system when the operator is not present at the workstation, thereby rendering the authentication process useful;
    - restrict and protect physical access to SCADA equipment;
    - protect SCADA network access from remote locations via digital subscriber lines (DSL) and/or dial-up modem lines;
    - implement secure wireless access points in the network;
    - verify that all SCADA networks are not connected directly or indirectly to the internet;
    - install firewalls with a strong and verified firewall configuration;
    - monitor system event logs;
    - use intrusion detection systems;
    - routinely apply operating and SCADA system software patches;
    - implement secure network and/or router configuration;
    - change passwords from those provided by the manufacturer as default.

Annex 6 — Guidance on awareness raising, training and exercises

Raising awareness of the characterisation of the threat

It is very important that a security culture is implemented not only among the employees of the water supply management entity, policy authorities and others that are involved in this sector but also in the surrounding community, promoting their fundamental collaboration through raising awareness of the importance of being alert, without causing alarm. It is important that attention is paid to a set of indicators, particularly in the most sensitive and critical parts of the system and if something unusual or suspicious happens, and that the managing body and/or competent authorities are immediately notified of any anomalies so that they can check them out.

To implement a security culture among the personnel of an organisation, various measures can be implemented, for example (Janke et al., 2014; EPA, 2015, 2018):

- awareness training from entities that have a better understanding of security issues regarding the water supply sector ([5]);
- train staff in security procedures, such as handling hazardous materials and maintaining and using self-contained breathing apparatus;
- secure equipment such as vehicles and spare parts;
- monitor requests for potentially sensitive information;
- secure buildings, rooms and storage areas not in regular use;
- maintain a list of secured areas or facilities and monitor activity in these areas;
- carefully review all facility tour requests before approving; if allowed, implement security measures including a list of names prior to the tour, request identification for each attendee prior to the tour, prohibit backpacks/duffle bags and cameras, and establish parking restrictions;
- on a daily basis, inspect the interior and exterior of buildings in regular use for suspicious activity or packages, signs of tampering or indications of unauthorised entry;
- implement mailroom security procedures following guidance provided by the postal services;
- discontinue tours and prohibit public access to all operational facilities;
- consider requesting increased law enforcement surveillance, particularly of critical assets and otherwise unprotected areas;
- assign security responsibilities to qualified individuals;
- encourage staff to be alert to any signs of suspicious activity;
- immediately investigate all information about suspicious activity and alert intelligence services and police authorities when appropriate;
- conduct a daily check of the water system for signs of tampering or other unusual activity;
- establish procedures for restricting entry to authorised personnel, contractors, vendors and visitors only by making proof of identity and check-in and check-out procedures mandatory;
- restrict access to areas of the water system and accompany visitors if access is needed;
- raise awareness of the importance of security and authentication in the design, deployment and operation of SCADA networks.

Training and exercises — implementation through training and exercises

([5]) In some Member States, security intelligence services provide such awareness training.

To ensure an effective and adequate incident response, training should be conducted to familiarise the utility operator's personnel and response partners with the response procedures and their corresponding tasks.

Training should include providing information on how the response plan is organised (e.g. investigation activities, response utilities with an interactive program to activities, planning for remediation), as well as on the roles and responsibilities of personnel and response partners. Moreover, training activities associated with specific response activities (e.g. field sampling, site characterisation) should be conducted.

Training should also stress the importance of coordination between utility operator personnel and external response partners for establishing a consistent, shared understanding of roles and capabilities during the investigation of and response to a contamination incident. The roles of all parties during an incident should be clearly understood, including the process of working together during an incident.

Several resources can be used to assist with training development. Many authorities, agencies, and public or private entities have created resources for developing training programmes for utility operators and periodically conduct general training and large-scale exercises. Local emergency planning committees may also offer local training opportunities that allow water utility operators to practise response functions with local emergency partners.

The training strategy for an effective and adequate response should include a suite of core courses, augmented by a training programme based on the discussion and operations exercises.

This training programme should begin with 'discussion-based' exercises (seminars, workshops and tabletop exercises) to introduce and teach new concepts and assess the plans and procedures of various contamination scenarios. Following the discussion-based exercises, 'operations-based' exercises (drills, functional exercises and full-scale exercises) can be used to test and evaluate procedures and programme effectiveness under more advanced simulated or real-world 'what if' scenarios.

Utility operators with an existing emergency preparedness training programme should incorporate specific training and exercises. The training programme should include internal exercises to maintain knowledge of and ability in implementing the response and its supporting procedures, such as site characterisation and public notifications, as well as to maintain the competency of personnel in their procedural roles.

It is recommended that discussion-based exercises be conducted annually or after routine updates. Operations-based exercises should be conducted in a 2 to 3 year cycle or after any significant modifications or changes to personnel.

Training and exercises — discussion-based exercises

Discussion-based exercises are normally used as a starting point in a progressive building-block approach leading up to operations-based exercises. They include:

- **Seminars:** these are used to orient participants to, or provide an overview of, authorities, strategies, plans, policies, procedures, protocols, resources, concepts and ideas.
- **Workshops:** similar to seminars, workshops are typically used to test new ideas, processes or procedures; train groups in coordinated activities; and build processes such

as a contamination response procedure/plan. Workshops often require more active participation than seminars, and may use breakout sessions to allow smaller groups to explore certain aspects of an issue.

— **Tabletop exercises:** these are used to assess plans, policies and procedures or to assess the types of systems needed to guide the prevention of, response to or recovery from a defined/simulated incident. Tabletop exercises are typically aimed at facilitating an understanding of concepts/plans, identifying strengths and areas for improvement, and/or achieving changes in perception.

Discussion-based exercises are appropriate tools for the development of procedures and for familiarising utility operator personnel and response partners with their roles and responsibilities in implementing these procedures.

Table 13 provides examples of discussion-based exercises that can be conducted to support the implementation of a contamination response. They can be used and modified to train utility operator personnel and external response partners.

Table 13. Examples of discussion-based exercises to support the implementation of a contamination response

Title	Exercise type	Description
Raising awareness	Seminar	Introduces contamination response procedures/plans and introduction of subject for utility personnel
Development workshop	Workshop	Discusses development of the contamination response including confidence/impact assessments, phase decision trees and response partner involvement. This may include both utilities and response partner personnel
Orientation training	Seminar	Provides training to utility personnel on roles/responsibilities as outlined in the contamination response
Tabletop exercise	Tabletop exercise	Presents contamination scenarios to utility and response partner personnel, allowing them to discuss procedures in the contamination response during a simulated incident

Source: EPA, 2018

Training and exercises — operations-based exercises

Once the contamination response has been drafted and personnel are trained and prepared, the overall response should be tested to identify necessary corrections and opportunities for improvement. This can be done through the implementation of operations-based exercises.

Operations-based exercises are characterised by the actual mobilisation of personnel and resources, and usually held over longer periods of time than discussion-based exercises, from several hours to a couple of days. Operations-based exercises can be used to validate plans,

procedures, policies and agreements, clarify roles and responsibilities, and identify resource gaps. They include:

- **Drills:** these are used to test a specific operation or function in a response plan through a coordinated/supervised activity (e.g. to practise using equipment, to develop/test new policies or procedures, to practise and maintain current skills).
- **Functional exercises:** these are single- or multi-agency/authority activities designed to evaluate capabilities and multiple functions using a simulated response. Functional exercises typically focus on practising and evaluating plans, policies and procedures. They often engage personnel involved in management, direction, command and control functions. They are conducted in a realistic, real-time environment; however, the movement of personnel and equipment is usually simulated.
- **Full-scale exercises:** these are multi-authority/agency, multi-jurisdictional activities involving the actual deployment of resources in a coordinated response as if a real incident had occurred. This facilitates the evaluation of field procedures concurrently with the management processes that guide implementation of the contamination response. A full-scale exercise is typically used to assess plans, procedures and coordinated responses under crisis conditions.

These exercises often follow discussion-based exercises, which provide basic training on procedures. Overall, operations-based exercises are more complex and detailed than discussion-based exercises and require more time to coordinate, assemble and conduct.

Table 14 provides examples of operations-based exercises that can be conducted for a contamination response.

Table 14.Examples of operations-based exercises to support implementation of a contamination response

Title	Exercise type	Description
Online monitoring and EDS software	Drill	Tests and practical implementation of online monitoring and event detection through EDS software, namely in how to operate the system, and how to interpret the data and alarms so that false positives can be identified and distinguished from real events
Site characterisation and sampling	Drill	Tests and practical implementation of site characterisation and triggered sampling procedures/equipment for field response personnel
Laboratory analysis	Drill	Testing and practising the collection, transport and analysis of samples and the reporting of results for field and laboratory personnel
Remediation and rehabilitation plan implementation	Drill	Building and testing several methods and technologies for the remediation and rehabilitation of the system (or part of), because this knowledge (time taken to implement, costs, risks, etc.) informs decision-making in the early stages of a crisis on the actions needed in terms of water restriction and response measures, and the estimation of how much time it will take to return to normality
Public notification	Drill	Practical implementation of procedures for assessing when it is necessary to notify the public, coordinating with primacy/public health agencies, and creating/issuing notifications
Utility operator functional exercise	Functional exercise	Exercises related to the roles of utility operator personnel and/or response partners, to test all procedures in a simulated environment (no movement of personnel or equipment) and identify improvements
Utility operator and response partner full-scale exercise	Full-scale exercise	Exercises related to the roles of utility operator personnel and response partners in a field environment (full deployment and mobilisation of personnel and equipment), to test the full implementation of the contamination response, involving the majority of procedures, and identify improvements

Source: EPA, 2018

Annex 7 — Communication options

This annex is based on the following sources: Oregon Health Authority (2002), WaterISAC (2014), EPA (2015, n.d.), ERSAR (2018) and Teixeira and Cabanas (2018).

Communication equipment and methods

A variety of equipment and methods can be used to communicate information about a drinking water contamination incident to personnel and response partners as well as to stakeholders and the public. Most utility operators probably already have standard equipment and methods for other response procedures and/or contamination responses. Planning for communication during an emergency response should consider how to coordinate the activities of multiple field teams and communicate directly with response partners.

Communication equipment and methods can include the following:

— television/radio;
— landline telephones;
— mobile phones;
— satellite phones;
— auto-dialler or reverse 112 voice recording systems;
— handheld or 800 MHz radios;
— audio-visual systems (including intercoms and closed-circuit television monitors);
— written bulletins or newsletters;
— email;
— social media;
— web portals or file-sharing platforms (e.g. SharePoint sites);
— physical loudspeakers for ensuring announcements reach old people, restricted areas, etc.

Regardless of the equipment and methods used to disseminate the information, utility operators should ensure that the public and response partners both receive and understand the information, particularly members of the public who may have limited access to the various means of communication used or who may require accessibility assistance.

Internal communication

Internal communication between the representatives of the different operational areas defined in Figure 3, involved in the management and resolution of the event, should be, in particular, through mobile phones, walkie-talkies and email and in person to ensure that all teams are called on to participate, depending on the nature and severity of the event.

External communication

The nature and level of severity of the event determine the scope, organisational structure, action plan and contacts with external entities, as well as the potential involvement of external entities and stakeholders in event resolution.

According to the relevance, applicable legal requirements and the type of entities to inform, the internal team must configure the information to be transmitted about the event, so that, in case of need, joint action plans are established with those entities.

Table 15 provides examples of the entities with which the internal team may need to establish communication channels, depending on the severity of the event.

Table 15. Examples of external entities to contact depending on the severity of the event

Event severity	Authorities	Other entities	Users	Social communication
Minor	Regulator, local health authority, district relief operations command, security forces (if it is an accident)		Only sensitive users affected by the event	As a reactive response
Major	Regulator, regional health authority, district relief operations command, security forces and security information services	Suppliers and external service providers involved in mitigation and resolution actions	The entire population affected by the event	As a preventive response
Catastrophic	Regulator, national health authority, national relief operations command, security forces and security information services, ministry of internal administration, ministry of environmental protection or public environmental authorities	Suppliers and external service entities involved in mitigation and resolution actions	The entire population supplied by the water distribution system	As a preventive response; the media should be involved in communicating event information and mitigation measures

Source: Teixeira and Cabanas, 2018

Effective communication between water supply entities and members of the public during crisis situations

An effective and adequate strategy for communicating with the public should include a steps for water supply entities (operators) to follow so that important information is communicated to members of the public during a major incident or disaster. These steps are to:

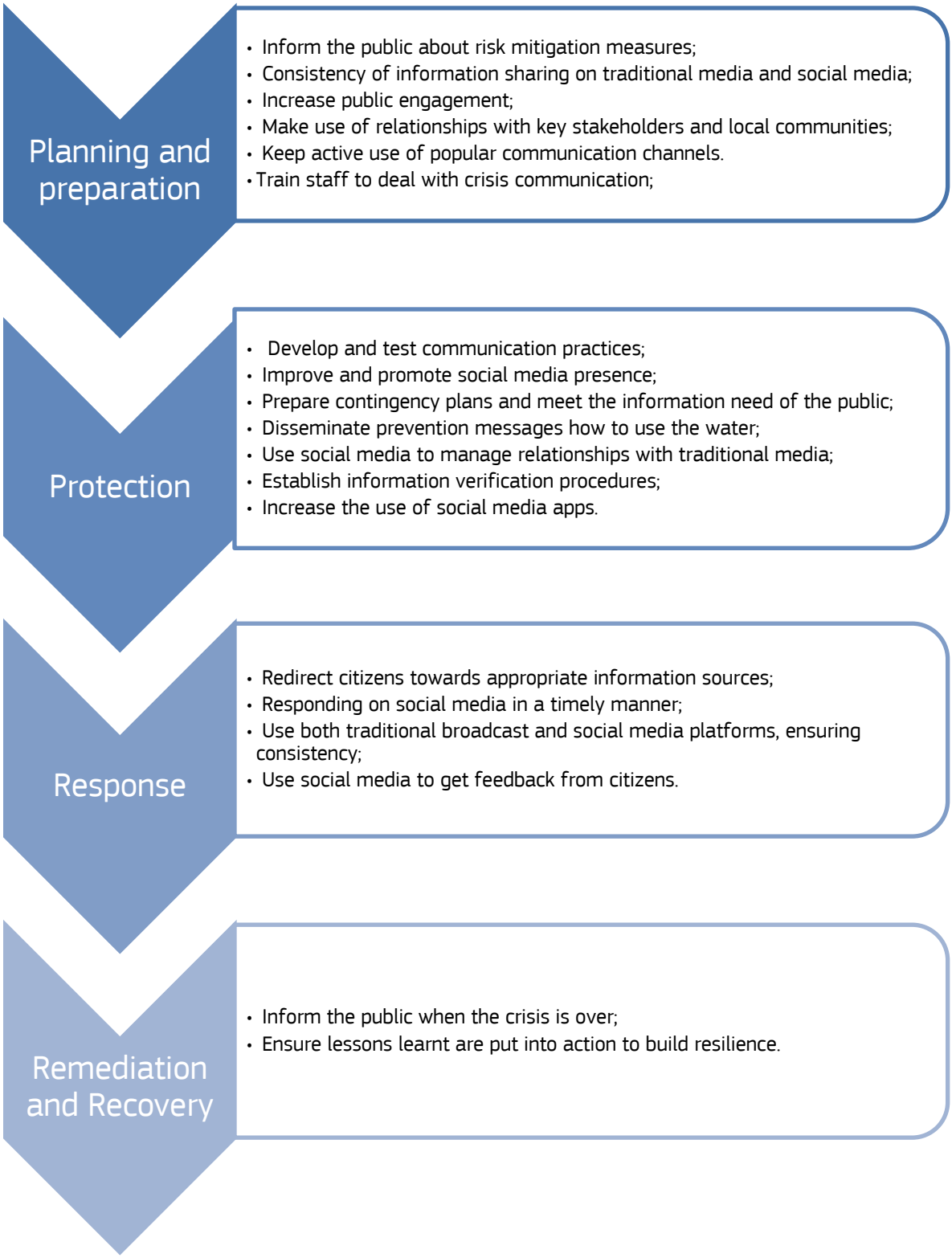
- analyse the information-seeking behaviours of local populations before deciding which media channels to deploy during disasters;
- engage key stakeholders to ensure a consistent message is transmitted across traditional and social media platforms;
- use social media to provide real-time updates to citizens about ongoing efforts to restore services;
- observe and adhere to context-specific regulatory frameworks for emergency management and resilience;
- employ post-disaster learning to enhance and develop future communication strategies.

These steps should inform the communication practices of operators at each stage of a disaster (mitigation/prevention, preparedness, response, recovery), and reflect best practice in the field of crisis and risk communication, with a view to establishing the most appropriate channels of communication to use before and during such incidents. A particular focus of this approach is how information shared via traditional media and social media can help build resilience in critical infrastructures, as well as in the communities they serve. In that regard, some key recommendations relate to:

— frequency of information: water supply operators should frequently share information with the public about ongoing efforts to restore critical services and make the public aware when no updates are available;
— clarity in crisis communication: simple, easy-to-understand messages should be used in all communications to build critical infrastructure resilience and manage the expectations of disaster-affected populations;
— consistency of communication across different channels (both traditional media and social media): using a combination of media allows critical infrastructure operators to reach a wider audience making sure that the same crisis information is available to the various target populations;
— working with key stakeholders to ensure that the information shared between critical infrastructure operators and emergency management organisations is accurate;
— water supply operators creating and maintaining active communication with emergency management organisations, news media operators and the general public to ensure the efficacy of crisis information flow.

The communication strategy flow chart shown in Figure 12 explores the steps that are applicable during each phase of a disaster (mitigation/prevention, preparedness, response and recovery). This is an example of a strategy used to build resilience and an effective and adequate response in terms of communicating with the public.

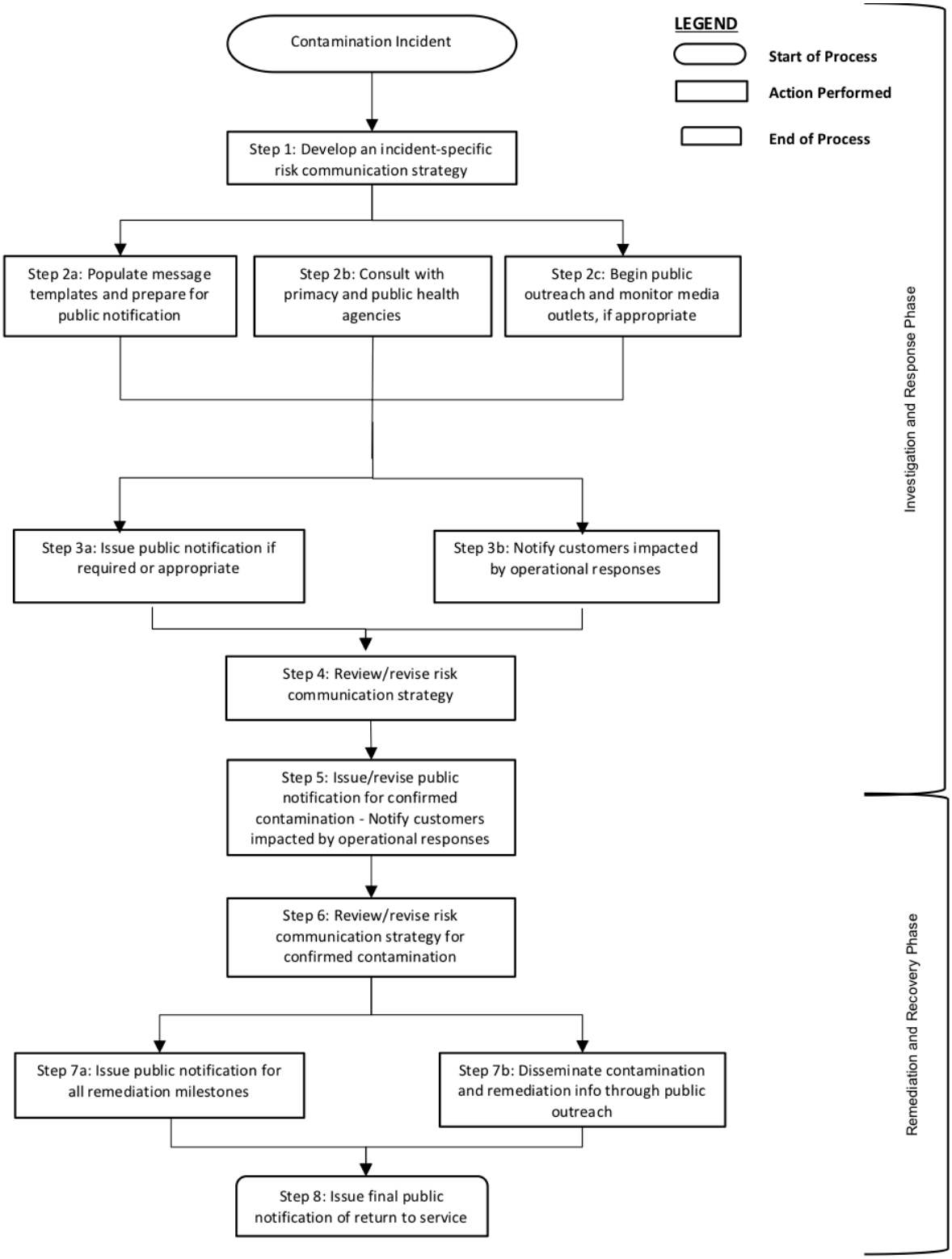
Figure 12. Example of a flow chart outlining a strategy for communicating with the public



Source: Serafinelli et al., 201

Figure 13 shows an example of a flow chart with the steps to be followed in a risk communication strategy.

Figure 13. Example of a risk communication overview flow chart



Source: EPA, 2015 — DSCRP template

The communication strategy also includes some measures that should be taken by the water supply operators before and during an emergency situation.

Before an event, operators should:

— organise drinking water advisories:
    - conduct an assessment of the assets needed to issue a drinking water advisory;
    - review regulations and guidance on public notification;
    - take into account the organisation's communication plan;
    - plan for media activities;
    - integrate communication into the standard operating procedures of the emergency response;
— collaborate with partners and stakeholders:
    - identify partners and critical and wholesale customers;
    - record and regularly update contact information;
    - develop a communication network with public authorities and agencies and also with public and private entities for collaboration in issuing an advisory;
    - meet authority and agency partners and community organisations and discuss protocols and resources for drinking water advisories;
    - plan and conduct regular communication actions with partner authorities and agencies and public and private organisations;
— develop a message:
    - collaborate with communication network to develop messages for various advisories and specific audiences;
    - translate and format messages for special populations (e.g. non-native-language speakers, those with visual impairments);
— conduct exercises:
    - plan exercises;
    - conduct exercises;
    - debrief after exercises and incorporate appropriate changes into protocols.

During an event, operators should:

— initiate an advisory:
    - identify the situation and collect facts;
    - notify drinking water regulator or primacy agency;
    - decide to issue an advisory;
    - identify the boundaries;
    - notify internal staff and external partners;
    - notify official authorities;
— prepare an advisory:
    - develop, format and translate the message;
    - approve the advisory;
    - identify the spokesperson;
    - assign communication responsibilities;
— distribute an advisory:
    - implement distribution methods;
    - use network to distribute messages;

    - work with the media;
— end an advisory:
    - issue end-of-advisory notice;
    - debrief;
    - modify authorities' and agencies' protocols as needed.

The communication strategy should include details on what to say and when to say it, because in the water sector, as in other sectors, in emergency situations the following are extremely important:

— essential information check list;
— coordination;
— focusing on essential information;
— planning on staging;
— not making assumptions about other agencies' knowledge of the water sector;
— boss' boss method;
— using the same source of information on contaminants in all communications.

The following essential information should be included in the message communicated:

— who is communicating the information;
— what action customers should take;
— what has occurred and a description of the event;
— where it occurred;
— when it occurred;
— the expected duration;
— why it happened;
— who is affected;
— basic information on the water system;
— current actions;
— where to get more information;
— details of alternative water supply and distribution points.

Deciding on operational responses can be difficult, because there could be unforeseen consequences of any action taken. For example, restricting water use or water delivery could result in portions of the service area, including hospitals and schools, being deprived of water. This could lead to poor sanitation or other effects, such as lack of water for firefighting systems, or risks from storage of drinking water in bottles exposed to heat and sun for several days. The consequences of possible actions must be studied from a preventive point of view, and potential problems must be considered, so that they can be eliminated or minimised.

To deal with the potential knock-on effects of response actions, advance planning for a contamination threat or incident is essential.

One way of minimising public exposure to contaminated water is to issue a public notice advising people to avoid drinking or using the water. Once a decision has been made to notify the public, the type of notification needs to be selected, based on the threat or incident and the contaminant potentially involved.

Examples of public notices about drinking water are described in Table 16.

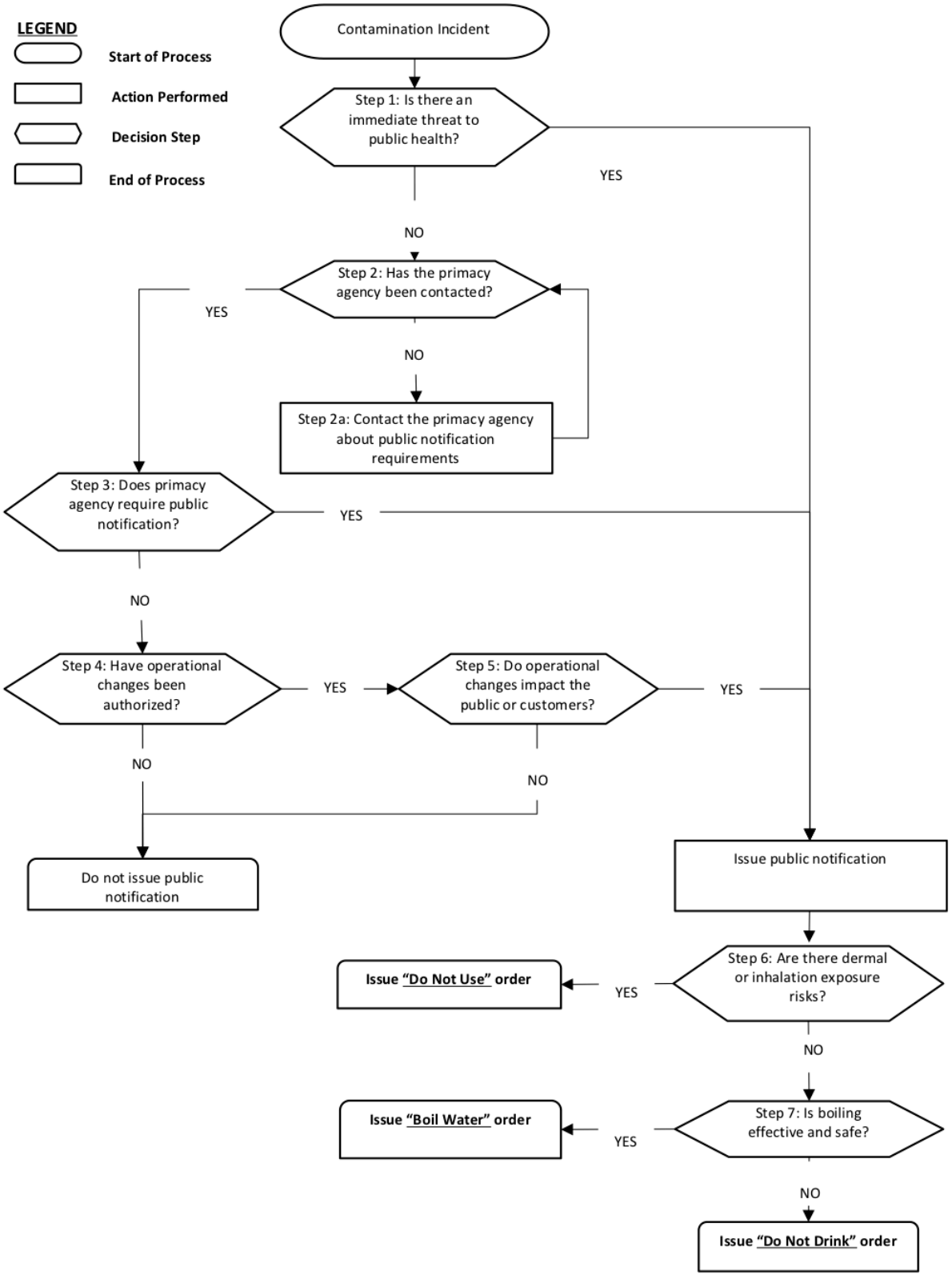
Table 16. Examples of types of public notices about drinking water

Type of notice	When to use this notice	Relative burden on public
Boil water before use	Use if boiling will make the water safe to drink and boiling does not create other health problems, particularly through routes of exposure other than drinking (e.g. inhalation or skin contact with water vapour)	Least burden — facilities that use large amounts of water for drinking or food preparation will be most affected
Do not drink water	Use if boiling is not an option and if water vapour and skin contact do not pose risks	More burden — an alternative water supply for drinking and food preparation will be needed
Do not use water	Use if the contaminant is unknown, if treatment is not possible at the time or if the contaminant poses a health risk through inhalation of water vapour or through skin contact with affected water	Greatest burden — an alternative water supply for all uses, including firefighting and flushing toilets, will be needed

Source: EPA, 2015

Figure 14 shows an example of a flow chart with the steps to be followed when deciding regarding the type of advisory to issue in the event water contamination.

Figure 14. Example of a flow chart to use when selecting contaminant warning advisory type



Source: EPA, 2018 — DSCRP template

Annex 8 — Response measures

Response measures need to be prepared in advance of an incident, based on scenarios identified as most relevant by the water utility operator, as described in Annex 3.

The most likely measures to be considered for this purpose, without prejudice to others, are those described in Janke et al. (2014) and EPA (2015, n.d.).

Preparation of response

- Post-emergency evacuation plans should be in an accessible, but secure, location near the entrance to the facility so they are immediately accessible by law enforcement or fire officers, or other first responders.
- An inventory of spare parts and on-hand chemicals should be regularly maintained, and any redundancy should be reviewed, especially for critical parts or chemicals.
- Sensitive populations should be identified within the service area (e.g. hospitals, dialysis clinics, nursing homes, daycare centres, schools) so they can be notified, as appropriate, in the event of a specific threat against the water utility. Processes to maintain this information regularly must be established.
- Critical files containing, for instance, as-built plans and drawings, sampling results, billing information and other critical information should be backed up.
- Appropriate background investigations should be conducted for staff, contractors, operators and others with access to the facility.
- Vulnerability assessments should be prepared and revised to incorporate any changes (e.g. assets added/replaced or new countermeasures implemented).
- It important to ensure that employees understand appropriate emergency notification procedures.
- Communication and coordination protocols (embedded in the utility's emergency response plan) should be reaffirmed with local authorities, such as police and fire departments, other first responders and hospitals, and regular tests of these protocols should be performed.
- Emergency response plans and associated communication protocols should be prepared and/or revised, with input from appropriate local officials concerned with law enforcement, emergency responses and public health.
- Employees should be reminded, on a regular basis, about events that constitute security violations and it is important to ensure that employees understand the notification protocol to be used in the event of a security breach.
- Draft press releases, public notices and other communications materials should be prepared for a variety of incidents. These should be routed through the appropriate channels for review to ensure that the messages are clear and consistent.
- Emergency response procedures and communication protocols should be reviewed and updated.
- Unannounced security spot checks (e.g. verification of personal identification and door security) at the access control points of critical facilities should be established.
- The frequency with which employee reminders of the threat situation and events that constitute security violations are posted should be increased.
- Ensure employees understand notification protocol in the event of a security breach.
- A security audit of physical security assets, such as fencing and lights, should be conducted, and missing/broken assets should be repaired or replaced. Debris that could be stacked to facilitate scaling should be removed from along fence lines.

— The physical security controls for all equipment and vehicles should be maximised so they are inoperable when not in use (e.g. lock steering wheels, secure keys, chain and padlock front-end loaders).
— Draft communications on potential incidents should be reviewed and media relations personnel should be briefed on the potential for press contact and/or issuance of release.
— Neighbouring water utility operators should be contacted to review coordinated response plans and mutual aid during emergencies.
— It should be confirmed that the emergency response and laboratory analytical support network are ready for deployment 24 hours per day, 7 days a week.
— Liaison with local police, and intelligence and security agencies should be reaffirmed to determine the likelihood of an attack on water utility personnel or facilities, and appropriate protective measures (e.g. road closures, extra surveillance) should be considered.
— Reminders for staff and contractors of the threat level should be posted frequently, along with reminders of what types of events constitute security violations.
— It should be ensured that employees are fully aware of emergency response communication protocols and have access to contact information for relevant law enforcement, public health, environmental protection and emergency response organisations.
— Inspect and practice activation of available emergency interconnections with neighbouring water agencies.
— A plan for an alternative water supply plan should be ready to implement (e.g. bottled water delivery).
— Threats should be assessed and regularly reassessed.
— There should be a permanent presence at critical points of the supply system for the duration of any emergency situation.
— Prior sensitisation, under the pretext of safety, for consumers to have survival kits, which include extra water reserves.

Response measures

Recommended response measures include the following:

— secure public supply points where water quality is not guaranteed;
— reinforce patrolling of critical points in the system;
— isolate the incident site for inspection by police authorities and determination of measures to implement;
— check the online monitoring system for further alarm locations;
— use the CDLAS model to define the contaminated area and isolate it by closing valves;
— collect water samples and ship to appropriate laboratory according to the severity of the incident;
— identify and evaluate the potential infrastructures of the affected supply system;
— assess options for immediate alternative supplies, the extent of the damage, if possible, and the potential for immediate repair;
— identify means available for an alternative supply;
— define an alternative fuelling system such as tank trucks;
— define alternative supply procedures until the final resolution of the situation;
— support quality control in relation to alternative supplies at the point of delivery to auto tanks and eventually within the tanks;
— adequately communicate with the public in accordance with other existing security plans;

— replenish supplies after the relevant indication by the competent authorities and those in charge of the situation;
— manage the whole event using the event management system ([6]).

([6]) For more information on event management systems , consult Carmi, 2018.

Annex 9 — Remediation and rehabilitation plan: roles, responsibilities and processes

This annex is based on EPA (2003a,b, 2004a,b,c, 2015), Council of the European Union (2005), Herrick (2006), Ministry of Health Israel (2009, 2016) and State Water Resources Control Board (2015).

The rehabilitation advisory committee

A rehabilitation advisory committee should be established in advance to provide professional support to the utility operator for the planning and managing of contamination events in the water network. It is particularly important at the beginning of the process to characterise the expected events and choose the most-suited remediation option. In the case of a large and widespread event, it may be that government authorities will take charge of the rehabilitation process.

The committee should include representatives of public health authorities, the water utility operator, environmental protection authorities, the regulator, the regional water company (if appropriate), intelligence services, police and/or military authorities, local government and the academic community. The committee will assemble periodically and will be updated with relevant information regarding contamination threats, water quality and rehabilitation technologies.

Defining roles and responsibilities

The following roles and responsibilities should be defined:

— the lead authority that will manage the rehabilitation process;
— the utility operator rehabilitation manager;
— the persons responsible for the water and sewage systems, who should provide expertise regarding the configuration and operation of the systems, and operating records, engineering drawings, etc.;
— various task teams (e.g. cleaning, repairs) and the person(s) responsible for their operation;
— a water quality expert responsible for a sampling and analysis plan and communicating with laboratories and the public health authority;
— utility operator personnel trained and certified for taking water samples or a list of external authorised personnel that sampling can be outsourced to and that will conduct the sampling according to the plan;
— a spokesperson responsible for communicating with external authorities and providing the public with information on the situation.

The utility operator should train all personnel involved in water network rehabilitation. The preparedness of the utility operator will be periodically checked by the relevant authorities.

The following external authorities and agencies (as applicable for each utility operator) may play a role:

— public health authorities;
— the water utility operator;
— security intelligence services;
— the regulator;
— environmental protection authorities;
— local government;

— police and/or military authorities;
— the regional water company (if different from the utility operator);
— laboratories;
— water samplers;
— professional cleaning and disinfection contractors;
— neighbouring utility operators and contractors that are able to help;
— disinfection material suppliers.

The means of implementation

The information and materials needed to support the implementation of the remediation and rehabilitation plan are outlined below:

— technical details of the water network from the hydraulic model and GIS application (physical properties of the system, storage volumes, rate and directions of flows, pressures, valves, hydrants, CWQM stations and system sampling points, chemical and microbiological characteristics of normal water, inputs for risk assessment, etc.);
— engineering analysis of the influence of reservoirs and pressure zones on the network;
— the list and locations of valves needed for isolation, so the utility operator's water demand zones (other zones) can be isolated;
— details of water sources and the volumetric flow rate in each water demand zone;
— detailed information on the sewage and drainage systems that may be necessary for flushing pipes or on an alternative solution for emptying water from the pipelines;
— a detailed public communication strategy;
— a plan for receiving and treating the water that was flushed from contaminated pipes (if the nature of the contamination prohibits the water from being flushed into the drainage or sewage systems);
— a stock of standard disinfection materials or details of who to contact to obtain such materials in an emergency;
— equipment for the disinfection of the network (e.g. mobile chlorination or steam apparatus) or a list of professional contractors available to provide disinfection services;
— a list of alternative clean water sources (also those external to the utility operator) for cleaning and flushing the network;
— equipment and materials for the repair and replacement of contaminated elements of the system (valves, pipelines and storage tanks);
— plans for the emptying and draining of water mains and reservoirs;
— a safety plan and equipment for field workers.

Documents and forms should contain the following:

— the procedure for the rehabilitation of the contaminated water system, guidelines for conducting a contaminated system survey and site characterisation, and documentation for all data collection;
— flow charts depicting the guidelines for the rehabilitation process;
— a plan approval form for the rehabilitation of the contaminated water system (including all the details needed for each stage of the rehabilitation process);
— appropriate procedures for sampling and analysis methods and forms for recording the results;
— a chart of the materials and methods used for cleaning and neutralising contaminants;
— specifications, drawings, schematics and detailed up-to-date network maps of the water system.

Annex 10 — Remediation and rehabilitation plan: analysis of alternatives and selection of options for remediation

This annex is based on EPA (2003a,b, 2004a,b,c, 2015), Council of the European Union (2005), Herrick (2006), Ministry of Health Israel (2009, 2016) and State Water Resources Control Board (2015).

The various alternatives for remediation are the combinations of technologies that could be used and how they should be applied. A detailed analysis of alternatives for remediation should be performed. Most of the alternatives for remediation include one of the following technology categories:

— containment;
— extraction/removal;
— treatment;
— natural attenuation;
— no further action.

It may be appropriate to use a combination of technologies.

Contaminated water may be present throughout the distribution system or may be limited to specific areas such as the water source, part of the distribution system or a storage reservoir.

The location of the contaminated water may influence the decision of whether to treat or remove the water and accordingly the method and equipment to use. The issue of whether to drain the water before any treatment or treat (neutralise) the contaminant in the water system should also be considered. If it is decided to remove the contaminated water first, whether to use the drainage or sewage system or remove the water to surface water (if neutralised) must be considered, as must the flow rates that are needed.

Other issues to be considered are:

— how to dispose of contaminated water from industry, farms, hospitals, etc.;
— how to initially drain and treat the main trunk lines, working downwards to supply mains and then minor pipes, so as to allow the upstream pipes to serve as clean water sources for the treatment of other pipes.

The goal of treatment could be to make the water acceptable for drinking or for sanitation only, or to pre-treat the water prior to disposal.

Environmental concerns associated with flushing contaminated and/or treated water should be considered.

Alternatives for the treatment of contaminated water

Traditional treatment technologies for the removal of typical drinking water contaminants may also be applicable when dealing with intentional water contamination.

Examples of treatment technologies for organic and inorganic, volatile and non-volatile chemicals, microbes and radionuclides include activated alumina, activated carbon, chlorination, ozonisation, filtration, ultraviolet disinfection and advanced oxidation.

Alternatives for the rehabilitation of system components

The remediation of water system components includes the rehabilitation of the physical components (e.g. decontamination, repair or replacement of water pipes, treatment or storage equipment, lining the interior of host pipes).

Examples of rehabilitation technologies for the treatment/disinfection of system components include chlorination, chlorine dioxide, washing with large volumes of water, washing with pressurised steam, air stripping, washing with highly alkaline solutions or detergent, mechanical cleaning with sand, 'pigs' or swabs, air scouring, and lining and coating with cement, epoxy resins or tubing.

In extreme cases, the contamination could prove irreversible, necessitating the total replacement of the water system with the attendant costs and delays in resuming service. In this case, an alternative water supply must be ensured in the interim. Should the water source itself be irreversibly contaminated, an alternative water source will also be needed.

Remedial action evaluation criteria and selection

Potential remedial actions should be evaluated by considering the following:

— the protection of human health and the environment;
— compliance with applicable regulations;
— the size of the population affected;
— the long-term effectiveness and permanence in maintaining the protection of human health and the environment;
— the time estimated for rehabilitation;
— the reduction in toxicity/infectivity and contaminant mobility resulting from the remedial action employed and the materials being treated;
— the generation of air, water or solid residuals from the remedial action;
— the impact of the neutralisation materials and by-products of the remedial treatment on human health and the environment;
— the influence of the neutralisation materials and by-products on the water network and water accessories;
— the short-term effectiveness in protecting human health and the environment;
— how easy the action is to implement technically and administratively, and the availability of an alternative technology, including a consideration of technical difficulties, the ability to monitor effectiveness, hazardous waste treatment and the availability of necessary equipment, materials, services and specialists, etc.;
— alternative water source and how the water will be supplied;
— cost.

A comparative analysis should be conducted by the utility operator, advisory committee and other authorities, to evaluate the performance of each remedial action being considered relative to one another and relative to the considerations listed above.

The advantages and disadvantages of each alternative should be identified, and the protection of human health and the environment and compliance with applicable regulations should serve as threshold criteria on which to base a final decision.

The remedial action selected should satisfy the objectives of a remedial action and should be documented in the remediation and rehabilitation plan.

KJ-NA-29846-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office of the European Union

doi:10.2760/415051
ISBN 978-92-76-10967-9