INTERNATIONAL UNION OF RAILWAYS

UITP

COLPOFER

Recommendations for Crisis Management

April 2017

2016 UIC Additional Global Security Programme

Recommendations for Crisis Management
Coordinator: Jochen Grimmelt
Editor: Security Division, security@uic.org
Layout and production: Marina Grzanka, graphic designer, marina.grzanka@gmail.com
ISBN: 978-2-7461-2602-2

Definitions and Acronyms

Crisis

A crisis is a sudden event or set of circumstances that could significantly affect an organization's ability to carry out its business, that damages an organization's reputation and/or threatens the environment, the health, safety, and well-being of employees, customers, or the public at large. If not handled in an appropriate and timely manner (or if not handled at all), a crisis may turn into a disaster or catastrophe. Crises are deemed to be negative changes in the security, economic, political, societal, or environmental affairs, especially when they occur abruptly, with little or no warning.

Crisis Management

Crisis Management (CM) is the overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate and often involves the need to make quick decisions on the basis of uncertain or incomplete information.

CM includes the development of plans, based upon an integral approach with internal and external organizations, to reduce the risk of a crisis occurring and to deal with any crises that do arise, and the implementation of these plans so as to minimize the impact of crises and assist the organization to recover from them and restart its normal activities as quickly as possible.

List of abbreviations

CM: Crisis Management
CMT: Crisis Management Team
HR: Human Resources
CEO: Chief Executive Officer
BU: Business Unit
CSO: Chief Security Officer

Contents

1. Introduction

During the 11th Security Congress in New Delhi, UIC was asked by its members to provide a benchmark study about the Crisis Management efforts within the railway community.

This request was embedded in an additional security program[1] and was completed from March 2016 to October 2016, in cooperation with UIC and its members. During a workshop on Crisis Management that took place during the Security Week, hosted by UIC from 21.06.2016 to 24.06.2016, UIC was asked by its members to provide additional recommendations for Crisis Management efforts and requirements.

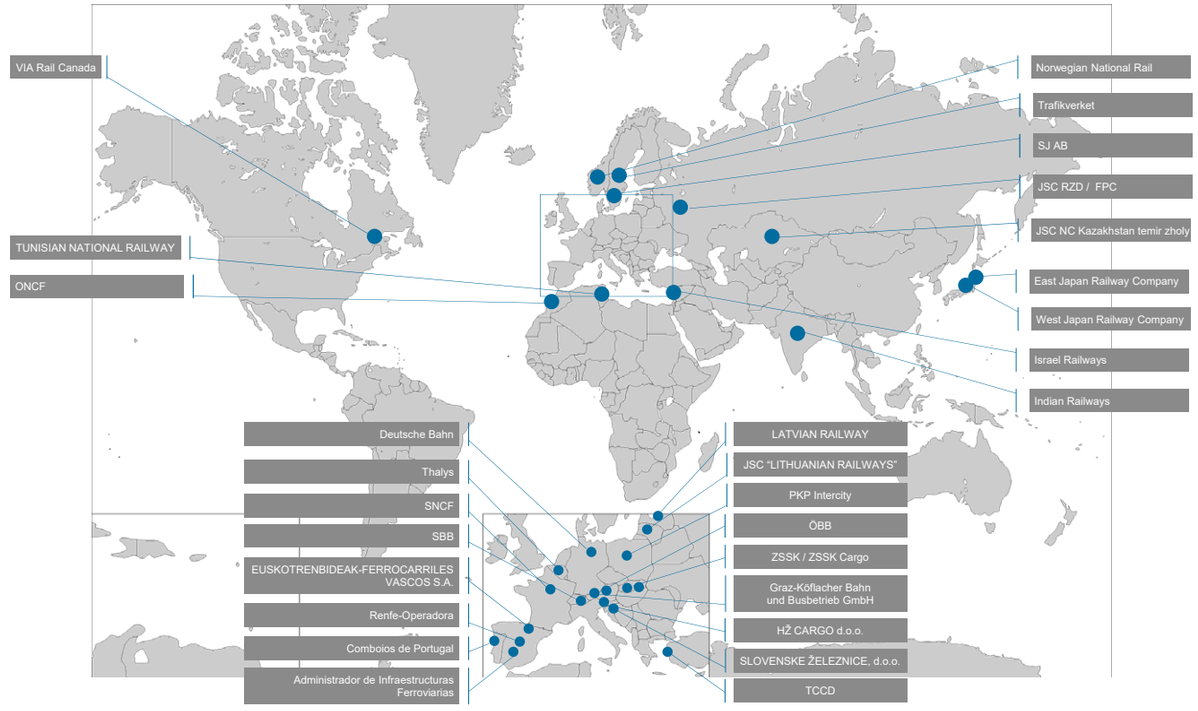
The results and the required documentation were ready by October 2016 and introduced during the Security Congress in Helsinki.

UIC thanks all members who participated in the Study, in the interviews and review, and who contributed to the completion.

Additionally, we would like to thank COLPOFER and UITP for participating and co-authoring this document.

[1] Together with a) information exchange on international trains and b) training of security and non-security staff

Recommendations for Crisis Management



2. Method

Transport operators must be aware that “if you operate – things will happen”. So better be prepared.

The following Chapters should assist rail operators in developing a Crisis Management Plan, or to check their existing plans for completeness. These recommendations are based on

- the questionnaires provided by the members,
- additional interviews with selected members,
- information and material on Crisis Management efforts provided by members,
- literature and internet research on good practices and the state of the art and
- the review of these recommendations by selected members.

In consideration of the close interaction and the multiple interfaces between rail operators, infrastructure operators, public transport operators, and police authorities, UITP and Colpofer were also invited to review and co-author the document, rendering it into a guideline for all types of operators.

Accordingly, within this document, the term “Operators” encompasses all types of rail, infrastructure and public-transport operators, represented by UIC, Colpofer, and UITP.

This is not intended as just another document about Crisis Management, but as a practical approach, giving rail operators as much concrete and practical advice as possible. The recommendations take into account the different sizes and abilities of rail operators, aiming at a level that should be considered as the minimum efforts.

3. Crisis Management Plan

A Crisis Management Plan should be considered as a superordinated document with underlying emergency plans. It provides overall organizational and general procedural guidelines for the management of information, activities, operations, and communications during an escalating emergency. It is the basis for the decision-making process of the rail operator.

3.1 Risk Analysis

The development of a Crisis Management Plan should start with an assessment of the potential vulnerabilities, risks, and threats facing a rail operator and the evaluation of the crisis preparedness at the corporate, regional or local level.

At least, the risks of incidents arising from:

- operations (accidents, collisions, derailments, fire, dangerous goods spillage),
- the environment (weather (snow, flooding, storm, ice), earthquakes),
- actions by third parties (strikes, damage to infrastructure, rolling stock),
- attacks by third parties (arson, sabotage, bomb threats, violence against customers and employees, cyber-attacks)

should be considered[2].

[2] Refer to Chapter 3.4.1 Experiences in Crisis Management

3.2 Priorities in Crisis Management

One of the most important issues of a Crisis Management Plan is the operator's philosophy for handling the crises. Specifically, what does the operator regard as its top priority during a crisis? All decisions made and actions taken should be checked against this philosophy. These priorities could be:

1. Saving lives and preventing serious injuries
2. Minimizing damage to the environment, property and assets
3. Protecting the operator's reputation/image
4. Business continuity/returning to normal operations

"Saving lives and preventing serious injuries" should always be the top priority and not negotiable.

Important or core business processes should be backed up by alternate technologies, processes or other means (Business Continuity). Since this is highly dependent on the type, structure, and abilities of the rail operator, this should be addressed separately. It is important to note that Crisis Management and Business Continuity Management are integral for the resilience of an operator (Business Resilience).

Figure 1: *Crisis Management and Business Continuity Management are essential for the operator's ability to resist disturbances, reduce the business impact, and to return to normal operation.*

3.3 Structure and Content of a Crisis Management Plan

When a Crisis Management Plan is being developed, the following items/topics should be addressed, based on the vulnerability, risk, and threat assessment. If a Crisis Management Plan is already in place, it should be evaluated and checked if additional topics can be addressed. The following structure is a suggestion only, which can be adapted and adjusted as needed.

Item	Description/Keywords
Area of Validity Period of Validity	• For which part of your company is this plan valid? For all? Are there (regional/ organizational) exceptions? Do you require local or regional specifications (these could be amended, using the same structure)?
Distribution	• Who has to receive the plan? Consider also external distribution to authorities, selected key contractors or important stakeholders.
Priorities, Purpose or Objectives of the CM Plan	• What do you want to achieve? • What are your prerogatives/priorities?
Crisis Definition/Crisis Level Early Warning Criteria	• Definition of your crisis level/alert level/escalation level/early warning system. • When do you want to activate your Crisis Management Plan? • What incidents at what scale are the triggers?
Activation of Crisis Management Plan	• Who confirms that there is a crisis? • What are the first procedures and the first steps taken?
Alerting/ Notification of CMT	• How do you alert? • What are the communication channels to use to activate the CMT? • How is the Crisis Management Team summoned?
Crisis Organization	• List the relevant entities for CM (e.g. the core or central crisis management team, regional crisis teams, working groups/staff of business units, corporate security, etc.) and their tasks/roles/competences/responsibilities, before, during, and after the crisis.
Crisis Management Team (CMT)	• State the composition (position/title) of the central crisis management team and at least one substitute. • State position/title and substitutes for additional members and experts. • Name list should be part of an Annex or checklist.

Item	Description/Keywords
Crisis Management Infrastructure	• Where does the Crisis Management Team meet? • If affordable: What would be the alternate location if primary location is not available? • What infrastructures and equipment should be ready? • Who is responsible for preparation?
Information Handling	• How do you want to collect, evaluate, and report incidents, monitoring of (social) media, prepare reports, support decision making, internally, towards stakeholders? • Who is responsible? In what form is the information distributed? • Are there considerations or procedures for handling classified information?
Crisis Communication	• How do you want to handle the media? Who are the spokespersons? How do you observe media reception and social networks? Location for press conferences? Who can help (communication advisors, call centers)? Appearance of internet presence (black site, creation of FAQ)? • Since communication is a key element in Crisis Management, a separate Crisis Communication Plan addressing these issues should be developed.
Liaison	• Do you have to liaise with police authorities or send rail personnel/specialists in external teams or CM teams? From where do these personnel come? • What are the requirements? • What is the required equipment (mobile phones, computer, access to company network, etc.)?
Return to Normal Operations	• How do you prepare, what plans are in place, who checks decisions and incidents during the crisis for the effects on your plans? What is your after-incident management? • What is the involvement in authorities in decision-making, especially to restart operations? • How do you take care of employees, customers (e.g. medical and/or psychological support)?
Training and Exercises	• How do you want to train for crisis management? How often? • Who is responsible for the preparation and the execution?

Item	Description/Keywords
Evaluating and Updating your Crisis Management Plan	AFTER • Organizational changes, introduction of new processes or technologies, change of responsibilities, etc. • experiences gained during emergencies, actual crisis situations (also by others!) • New evolving threats • Exercises • Your CM plan (as well as underlying emergency or contingency plans) should be evaluated and adjusted.
ATTACHMENTS	
Terminology and Definitions	• Define what you mean, and ensure that you have a common understanding
Contact Lists	• Names, contact data of relevant personnel and stakeholders
Map	• Location of Crisis Management Infrastructures, parking facilities, entry requirements, etc.
Checklists/ Forms	• As required
Special Plans (e.g. Contingency Plans, Evacuation Plans)	• E.g. for handling of pandemic, storm, strike, dangerous goods incidents, etc.

Table 1: *Structure and content of a Crisis Management Plan for Rail Operators*

3.4 Alert Levels

It is important to initiate Crisis Management at the right time. Better to start early and have everything in place, in case the situation deteriorates. To achieve this, the implementation of a warning or alert system is recommended. This chapter shows an example of a four-level model (Level 1-4) that leads from normal operation to the recognition of a crisis, thus activating the Crisis Management Plan.

The definition of the crisis level should be the task of the Crisis Management Team, unless otherwise clearly stated. The lists below are not complete and must be adapted for each company.

Level 0	Green	Normal Operation
Possible Characteristics	• Normal operations	
Media	• If at all, inquiries to general topics	
Measures	• None	
Resources	• No additional resources required	

Level 1	Brown	Limited Incident	Minor Incident	Striking
Possible Characteristics	• Incident, potential or actual, which is not seriously affecting the overall operations • While some damage and/or interruption may occur, the conditions are localized			
Media	• No, low or local media attention			
Measures	• On-duty employees can handle the situation on their own			
Resources	• Additional resources may be required on a local or low scale			

Level 2	Yellow	Crisis Watch	Potentially Critical	...
Possible Characteristics	• Incident does not cause major interruption of operations or services • Incident is a localized one with limited impact • Incidents that are isolated, minor but are repeating (danger of “smoldering crisis”)			
Media	• Situation is attracting slow media response • Little, but steady online media coverage • Little or no public attention			
Measures	• Observe development (be aware of “smoldering crisis”) • Notify superiors, inform internally • Crisis Management Plan is not activated, but working groups may be summoned • On-duty employees/operations centers can still handle the situation on their own			
Resources	• Additional resources may be required on a regional or larger scale • Efforts are becoming visible externally • External support is required			

Level 3	Orange	Crisis Warning	Crisis Alert	Critical
Possible Characteristics	• A major emergency that disrupts the normal operations and has knock-on effects to other business units or regions • Outside emergency resources are required, as well as a major effort from internal resources • A serious event that disrupts one or more operations/relations • Circumstances of the incident/issue are known outside the corporate office or operation • Incident is posing a major risk to personnel, customers, clients, reputation or resources • Decisions are required urgently			
Media	• Media Crisis causes growing attention from local media, and online media sites post reports			
Measures	• Observe development closely • Start regular information updates, and protocol of developments and decisions • Working groups are summoned • Crisis Management organization is partially activated, or the activation should be considered (e.g. working groups of business units are in place, communication starts explicit monitoring of social media, etc.)			
Resources	• Additional resources and external support of numerous entities may be required • Efforts are highly visible • Resources and support from other regions, areas is required			

Level 4	Red	Major Crisis	Crisis	Acute Crisis
Possible Characteristics	• A severe emergency. Operator must request mutual assistance from outside (e.g. civil aid services, armed forces, etc.) • A serious event that severely impairs or halts the operations of the operator and/ or has an impact on other stakeholders • Incident has caused fatalities or injuries to personnel, customers, clients, and/or major damage to operator's reputation or resources • External organization and entities are massively affected • Operations are severely disrupted			
Media	• Media have immediate and urgent need for information about the crisis, fatalities, injured or missing persons • Broad coverage in social and online media • Broadcast, TV and/or print media appear on-site for live coverage • Communications are increasingly difficult to manage			
Measures	• Crisis Management Plan organization is activated			
Resources	• External support and aid of authorities and other organizations is required on a large scale • The efforts are highly visible and require a large amount of coordination with other organizations			

Table 2: *Alert levels and escalatory steps in a crisis*

Additional Remarks

- The characteristics that define the different levels can be adjusted or can contain additional criteria (e.g. level of damage, number of fatalities, local or regional limitations, etc.) to allow an easier assessment of the actual situation.
- When reaching LEVEL 1 (Yellow), this should be clearly communicated to your staff.
- Every change of level should also be communicated.
- Use these levels to control the communication process to other internal and external stakeholders (e.g. when reaching LEVEL X, who has to be informed?) in accordance with "Table 7: Information and communication priorities" and "Table 8: Information requirements".
- There are models containing only three levels or models with five and more. A three-level model might have the disadvantage that the crisis level is reached very soon; a larger model requires a very fine and distinctive separation of the criteria.

This model is considered to be an example and should be adjusted according to your needs.

3.5 Composition of the Crisis Management Team

3.5.1 Central Crisis Management Team

In a crisis that is affecting the operator, the Crisis Management Team [CMT] should be placed on the top level of the organization, e.g. on corporate or holding level. It could be referred as the Core, Central or Corporate Crisis Management Team.

The main tasks of the Central Crisis Management Team should include at least the:

- Evaluation of the situation,
- Decision of the crisis level,
- Activation of the crisis organization,
- Identification of the required expertise,
- Determination of the required measures,
- Coordination of required decisions,
- Promulgation and documentation of decisions,
- Coordination with authorities (on a high level),
- Decision on the internal and external communication policy.

The actual composition of a CMT is highly dependent on the size of the company and the availability of qualified and experienced management staff.

A Central CMT should be small in size. Ideally it could consist of the following functions:

Function		Description/Task
Chair	Decision making body	**Pre-crisis, responsible for:** • the development and implementation of the crisis management plan/ strategy. **During crisis, responsible for:** • managing the CMT, • classification of crisis and its communication to the organization, • managing the company's overall crisis response and for keeping the CEO and other key executives fully informed of all developments, • calling meetings of the crisis management team and determining its composition, • obtaining additional resources, • communicating with key stakeholders (e.g. police authorities), release of information (confidentiality considerations) **After crisis, responsible for:** • debriefing and followup measures • recording "Lessons Learned"
Crisis Coordinator	Decision making body	**Pre-crisis, responsible for:** • development, review, training, and distribution of the crisis plan to the CMT members and others as appropriate, • readiness of CM infrastructure, • preparation of alert processes, • keeping documentation/checklist, etc. complete and up to date, • preparing/conducting exercises, incident reporting, information handling for early warning **During crisis, responsible for:** • managing/overseeing the support team, • information handling for the crisis team and others as appropriate, establishing and updating of the situation picture • situation reports/briefing, documentation/protocol, • close support/cooperation with Chair **After crisis, responsible for:** • debriefing and follow up measures

Communications Coordinator Spokesperson	Decision making body	**Pre-crisis, responsible for:** • development and implementation of a Crisis Communication Plan[3] **During crisis, responsible for:** • preparing and delivering press briefings, • internal information within company, • acting according to Crisis Communication Plan, giving interviews/ speeches/statements to media, and briefing and preparing spokesperson(s) for media interviews, In certain crises, it may be required that the role of the spokesperson must be taken by the CEO or President. A thorough briefing and preparation must be provided by the Communications Coordinator. **After crisis, responsible for:** • Background information, follow-up information, etc.
Legal Counsel	Decision making body	**During crisis, responsible for:** • provision of legal counsel to the team and arrangements for external legal support as necessary, • evaluation of decisions with regard to legal consequences, • participating in communication preparation, and advising on other crisis-specific issues, such as ex-gratia payments, • contact to special lawyers **After crisis, responsible for:** • Legal affairs, lawsuits, etc.
Human Resources Coordinator	Decision making body or extende CMT	**Pre-crisis, responsible for:** • Keeping database/records of personnel and contact information, • clearing of Crisis Management requirements (e.g. working hours, shifts, etc.) with unions/employee representatives **During crisis, responsible for:** • briefing/consultation of the CMT in HR matters, • evaluation of CMT decision under HR aspects and consequences, • point of contact with unions and employee representatives, • care for employees and their families, • coordination with grief counselors/psychologists **After crisis, responsible for:** • Further contact to employees, unions, relatives, • overtime compensation, etc.

3 Refer to Chapter 3.7

Support Staff	**Pre-crisis, responsible for:** • preparation of documents/checklists, etc. • readiness of crisis management infrastructure, etc. **During crisis, responsible for:** • information handling, situation reports, briefing preparation, • establishing and updating the situation picture • protocol/log of incidents and decisions, documentation, • logistics, support in administering the crisis team, logistics **After crisis, responsible for:** • support of debriefing, followup reports, keeping up information handling

Table 3: *Functions and tasks within the Central Crisis Management Team*

The Crisis Management Team should be accountable to the Chief Executive Officer, President or Managing Director ("CEO"). The CEO should not be directly involved in managing the crisis. His primary responsibility is to continue the effective management of the operator and to continue reporting the situation to the operator's external stakeholders (e.g. Board of Directors, relatives of victims, others).

Under special circumstances and depending on the severity of the crisis, it might be advisable that the CEO has to speak on behalf of the company, giving important public announcements.

In smaller organizations, it might be necessary for the CEO also to take the position of the Chair.

Human Resources are not necessarily part of the decision-making body. This should be decided with regard to the operator's structure and business, but should be clearly defined.

The tasks of documentation, logging (protocol), and establishing and updating the situation picture should be clearly addressed.

3.5.2 Extended Crisis Management Team

Depending on the type of the crisis, additional functions should be integrated, e.g.:

Function	Description/Task
Safety	Safety expertise, fire/work protection issues
IT	CIO or IT representative, assessment of impact of situation on IT, advising Crisis Management Team, point of contact on all IT issues
Finance	Assessment of financial impact, contact to insurance companies/banks, coordination of necessary financial transactions
Business Units	Representatives of affected business units (e.g. the Freight division in the event of large dangerous goods spillage)
Impact Analysis Team	Evaluation of the consequence of decisions of Crisis Management Team on future operations/events
Other Internal or External Advisors	Depending on the type of business and type of crisis. These could be environmental specialists, special lawyers, psychologists, etc. They should be preselected and included in the contact lists.
Liaison	It may be required to deploy specialists or advisors of the rail operator (=rail personnel!) in external teams or working groups. It is likely that representatives of the police, fire department or other public entities have to be present in the CMT as well.

Table 4: *Additional functions within the Crisis Management Team*

This list is not conclusive and is highly dependent on the type of operations and the size of the company.

3.5.3 Regional, Local or Business-Related Crisis Teams

If an operator has a regional substructure or is organized in separate business units, the crisis organization should also operate on that level. A crisis that only affects a region or a single part of the operator's undertakings (e.g. business unit) may be handled and decided within the regional organization or within that branch.

This should also be reflected in a regional crisis organization which should include all the required competences and resources.

However, to minimize the risk of a rapid escalation or a smoldering crisis, the crisis coordinator (or its organization) should be integrally involved in all the related information, decisions, and actions.

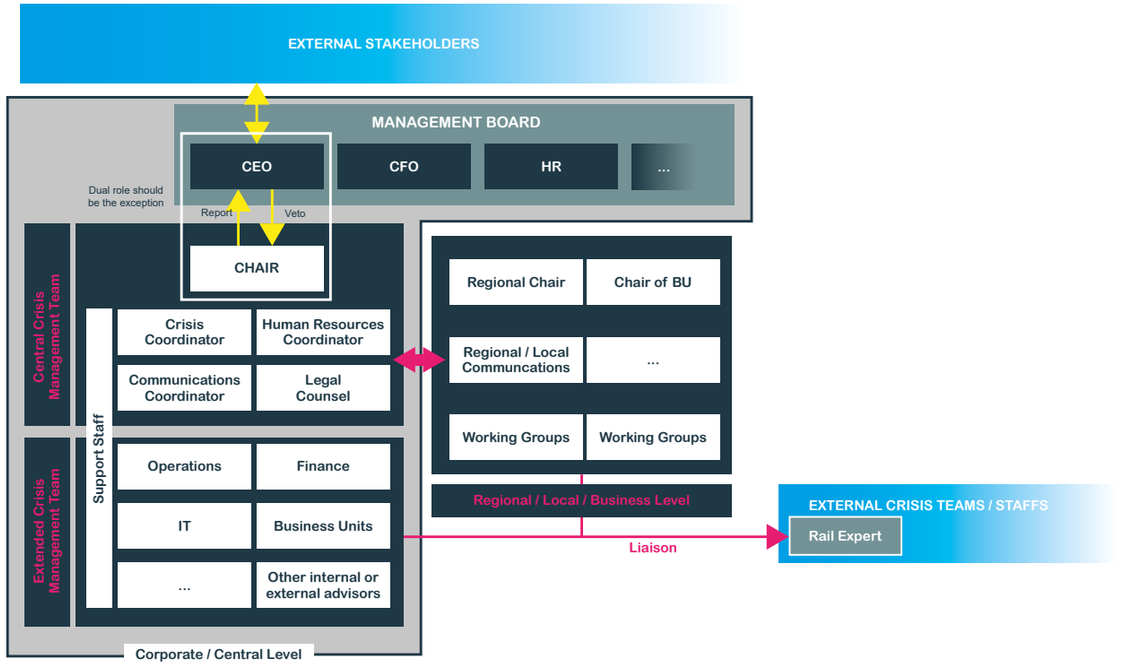


Figure 2: *Exemplary Crisis Management structure with involvement of the Central and Regional Crisis Teams*

3.5.4 Working Groups

To support the crisis management efforts on a regional or central scale, it may be required to implement working groups within business units/divisions (e.g. if a crisis is only affecting the Freight branch) or for special topics (e.g. pandemic, traffic reduction). These working groups should be nominated and available at very short notice. They should contribute to the decision-making and crisis communication process and have access to the required resources.

3.5.5 Endurance

The hot phase of a crisis may be over within a couple of hours. It is possible that it will last longer. Find solutions to keep up your crisis management organization for three days minimum, to cover the hot phase. However, since this may not be sufficient, seek possibilities of external help, such as the outsourcing of logistics or certain topics to special advisors. Consider the training of additional personnel to assist in the support staff or in the working groups.

Be aware that it requires logistics and other preparations (e.g. shift plans, sleeping, eating, drinking, etc.) to extend the endurance of your Crisis Management Teams or working groups.

3.6 Crisis Management Infrastructure

It is suggested that every operator should have a designated Crisis Management Infrastructure available. The purpose is to provide the required:

- space, logistics,
- communication links and communication coordination,
- meeting and briefing facilities,
- information collection, evaluation, and distribution,

for the Crisis Management Team.

Ideally, it is located near to the operator's office or alternatively near to existing operation centers. Larger companies, or those who operate 24/7 on a larger scale, should operate this continuously and it should be managed by the Corporate Crisis Coordinator.

A backup location could be defined if the preferred location is not accessible or has to be evacuated.

The recommended available documentation to gather for managing the crisis situation should be available in printed and electronic form.

DOCUMENTATION	Minimum	Should	Could
Crisis Management Plan, underlying emergency plans, and protocols, etc.	X		
Communication lists (CMT, corporate, stakeholders)	X		
Maps (digital and paper versions)	X		
Checklists	X		
Contact lists	X		

Table 5: *Recommended documentation for a Crisis Management Infrastructure*

A certain level of equipment is recommended for a Crisis Management Infrastructure.

EQUIPMENTS AND RESOURCES	Minimum	Should	Could
Working space for support staff/Information Cell	X		
Meeting room (“War Room”) sufficient for CMT plus additional members	X		
Additional meeting capabilities (e.g. for working groups)		X	
Alternative (backup) War Room/Information Cell at a different location			X
Computers with e-mail and internet access	X		
Printers, flipchart, whiteboards, marker boards	X		
Secured WiFi access			X
Connectivity for mobile computers (network access, internet access, cables, WiFi)		X	
Telephones for support staff	X		
Fax machine(s)	X		
Telephones for CMT members	X		
Telephone conference capability	X		
GSM availability (cellphones are working, e.g. by use of repeaters when building structure is blocking signals)		X	
Video conference capability			X
Video projection capability (screens, beamer, etc.)	X		
Television with newsfeed	X		
Alternative communications capability (e.g. radio, SatCom, GSM-R, etc.)		X	
Secure communication capabilities			X
Document shredder	X		
Emergency power generation			X
Spare cellphone batteries, batteries, and chargers	X		
Paper, pencils, markers, etc.	X		
Humanitarian logistics (food, drink, rest, etc.)	X		

Table 6: *Recommended equipment and resources for a Crisis Management Infrastructure*

The equipment and the documentation must be checked, maintained, and kept up to date at regular intervals.

3.7 Crisis Communication

3.7.1 Incident and Situation Reporting

It is paramount that an information flow is organized that allows – after an incident is detected – a fast evaluation of the:

Character of that incident

What happened? Who did it? When did it take place? Where did it take place? Why (How) did it happen?

Consequences

Could this (potentially) lead to a crisis?

This applies to all types of incidents, regardless of whether they have a security, safety or other background, e.g.

- incidents where persons are killed or severely hurt (quantify),
- incidents with severe damage to infrastructure or rolling stock (own or other),
- incidents leading to interruption of business processes (derailments, due to weather, etc.),
- spillage of dangerous goods (specify amount, damage),
- criminal actions (sabotage, theft, blackmail, cyber-attacks),
- acts of violence (against customers, employees, on operator’s infrastructure, in cars, etc.),
- recurrent incidents that are of no concern individually but might have a special media or management focus.

This list is not complete and must be adapted to the specific requirements and type of operations.

3.7.2 Exemplary Information Matrix – Communication Priorities

During an escalating situation or a developing crisis, the timely information of the internal organization, the authorities, and the public is essential.

As a rule of thumb:

- the more serious the situation, the larger the circle of those requiring information and
- for the initial internal information, speed is more essential than precision.

It is helpful to have some guidelines of when and how information about incidents is distributed internally and externally. Pay careful attention to the order in which different groups should receive information. For example, front-line staff should receive information before it is made public.

Table 7 shows a simple example of the internal and external information process, in reference to the crisis level. This should be adapted to your needs.

Who	When	What	How
Division heads		Full extent of incidents, areas affected, what is being done, possible cause, impact (what, where, whither, when)	Proactive contact, regular briefings and updates
Situation Center		Full extent of incidents, areas affected, what is being done, possible cause, impact (what, where, whither, when)	Proactive contact, regular briefings and updates
CSO		Full extent of incidents, areas affected, what is being done, possible cause, impact (what, where, whither, when)	Proactive contact, regular briefings and updates
CEO		Full extent of incidents, areas affected, what is being done, possible cause, impact (what, where, whither, when)	Proactive contact, regular briefings and updates
Employees		(Full) extent of incidents, areas affected, what is being done, (possible cause), impact (what, where, (whither), when)	Briefing by superiors, intranet, proactive contact, website
Authorities		(Full) extent of incidents, areas affected, what is being done, (possible cause), impact (what, where, (whither), when)	Proactive contact, phone call, email, fax visit
Press		According to crisis communication plan	
Clients		Likely resumption of business as usual, impact on current business ans safety/ security, measures taken	Website, press, call centre, social media

Table 7: *Information and communication priorities*

3.7.3 Information Policy and Requirements

Table 8 is a more advanced model. It distinguishes between certain types of incident, allowing a finer consideration.

	To Whom	Internally					Externally			
Type of incident (About / What)	When	Division Heads	Situation Centre	CSO	CEO	Central Crisis Team Member	...	Authorities	...	Ministries
Accident with fatalities										
Environmental damages										
Damages to infrastructure										
Violence / attacks on customers										
Violence / attacks on customers										

Level 0 | Level 1 | Level 2 | Level 3 | Level 4

Table 8: *Information requirements*

Both models are to be used in combination with an alert levels model (Chapter 3.4).

3.7.4 Codewords

It might prove helpful to develop and to promulgate codewords for certain types of incidents. E.g. if a train conductor/train service personnel discover(s) someone with a weapon in the train, it should be reported to the control center in a disguised way to avoid a panic. These codewords should be known by the operative personnel, at the control centers, and by the police authorities.

3.7.5 Terminology

Especially in large towns or metropolitan areas, numerous rail and urban transport operators are using the same infrastructure (multi-modal stations) or tracks. Additionally, several different police organizations may be responsible. To ensure a common understanding of incidents, procedures, and organization, a joint terminology should be developed to ensure that the same terms and phrases have the same meaning for every stakeholder.

3.7.6 Public Communication

The intensity and the outcome of a crisis can be heavily influenced by the handling of the press and the media. Therefore, it is recommended that the public communication is taken into account in the Crisis Management Plan.

It may be advisable to prepare a separate Crisis Communication Plan that covers (for example) the following:

- establishment of media and social media monitoring capabilities,
- spokesperson, space for press conferences and statements,
- communication to the key stakeholders,
- feeding of information into the social media,
- kind of information that should be released and how often,
- approval process and the authority for the release of information,
- information process to your employees,
- handling of questions/requests from media, families, victims, etc. (amount!),
- preparation of key media contact sheets and telephone/stakeholder log sheets,
- preparation of black/dark websites or splash sites for crisis communication,
- preparation of pre-draft messages,
- preparation and publishing process of FAQ,
- (external) assistance by using Call Centers, Communication Advisors.

The responsibility for the crisis – and public communication – should be an integral part of the Central Crisis Management Team[4].

[4] Refer to Central Crisis Management Team, Chapter 3.1.5

3.8 Training

Crisis Management should be trained regularly. Besides the participation of the operator's internal entities, the participation of external stakeholders such as infrastructure/network providers, police forces, fire department, other operators, representatives of communities, etc. is recommended. Additionally, the participation of observers is advisable.

There are different forms of exercises that could be used for the training of Crisis Management.

Training should be conducted regularly on all levels (central/regional) of the organization.

3.8.1 Communication/Alert Exercises

- Participants include members of the Central Crisis Management Team, the additional Crisis Team members and Support Staff
- The aim is to test communication lines, the function of alert procedures, the exchange of alert messages, and to test backup communications
- Participants are required to report the estimated arrival time at the crisis room or to join an ad-hoc telephone conference
- Train at least two times a year, and additionally after organizational changes or changes of personnel

3.8.2 Tabletop Exercises

- Participants include members of the Central Crisis Management Team, the decision level of other stakeholders (head of ops center, other crisis management groups)
- Invite observers of other rail operators or authorities, police, fire departments, etc.
- All players/participants are together in one room (2-3 P/entity, decision maker + advisor/ specialist, telephone backup if required)
- A moderator introduces the scenario/story, gives inserts, and guides the discussion
- The participants discuss decisions and find solutions
- The progress of exercise is 'static', no variations in outcome
- Questions, problems are logged for followup
- Train at least once a year on central level (and regional level), and additionally after organizational changes or changes of personnel

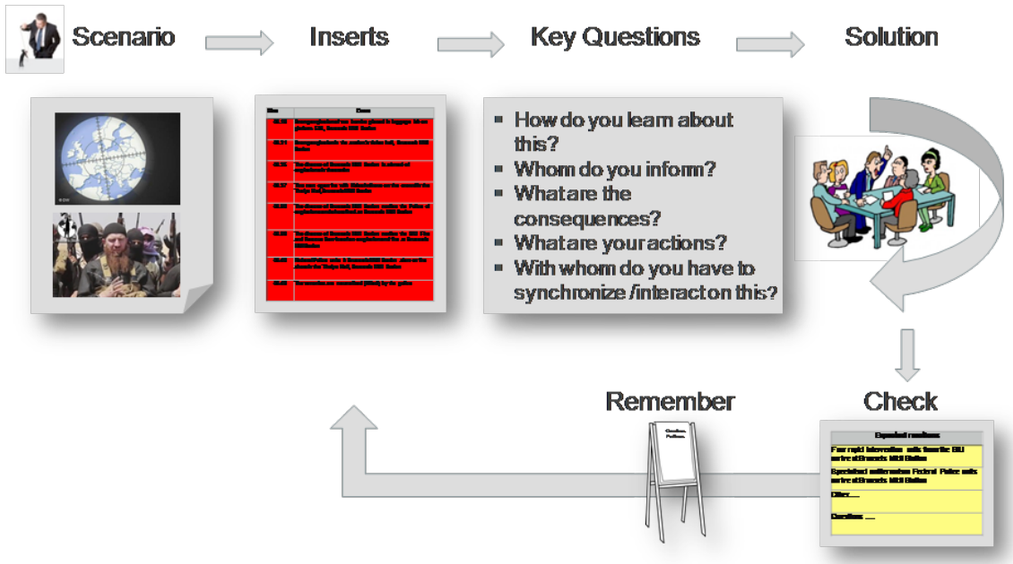


Figure 3: *Structure of the table-top exercise*

3.8.3 Command Post Exercises

- Similar to a tabletop exercise but the players/participants are within their 'normal' environment (operations center, crisis center, office)
- The communication between players is by normal means (mail, phone, fax, telco, vico)
- A coordinator releases inserts, messages, he acts as 'third parties', and covers any artificialities of the exercise, a detailed script is required
- The coordinator might use ad-hoc inserts to provoke a certain action or to guide the exercise into a desired direction
- Exercise has to be carefully separated from the real world, it requires a high amount of preparation
- Observers could be present at the ops centers
- May be part of countrywide exercises or required as proof of concept on a local level (e.g commissioning of tunnels, train stations, etc.)
- Problems and weak points become evident
- Train at least once a year on central level

3.8.4 Full (Live) Exercise

- Players/participants from operational level (drivers, safety personnel, security forces, police, military, fire departments, actors)
- May be required as proof of concept on a local level (e.g commissioning of tunnels, train stations, etc.)
- Suitable to introduce the operator's staff, police forces, fire departments to the requirements and specialties of the rail environment
- Often at a single location with a special training focus (e.g. evacuation, terror attack on station, evacuation, fire, etc.)
- Scalable in terms of participants, resources, duration, etc.
- May be integrated in a command post exercise
- Press/media may be invited
- If possible, train several times a year with different themes and in different locations or as required

There are other forms of exercises, but they are generally variations and/or combinations of those above.

Despite performing regular training, additional Crisis Management exercises should be conducted after large organizational changes, the implementation of new procedures or the integration of new personnel.

It is important to let police or military forces train regularly on your rolling stock or on your infrastructure. They have to know the specialties of your operations by heart, to allow for a successful intervention.

Employees such as specialists, support staff or security personnel are likely to find themselves involved in the early stages of a crisis. It is important to identify these people for training to ensure they respond appropriately (e.g. evaluation of a situation, reporting requirements, acting in the crisis center, attending to the systems, knowing the procedures, and acting as liaisons).

3.9 Cooperation

In the light of Security and Crisis Management, it is recommended to establish security and safety partnerships with other operators. This should especially been done if they are operating within the same system (e.g. different operators in one city), using the same infrastructure (stations, tracks) or addressing the same authorities.

The cooperations should include:

- a high-level cooperation/agreement to cooperate,
- exchange of information on threats, etc.,
- development of joint emergency plans (where joint infrastructures, resources, stakeholders are affected),
- joint exercises.

The cooperations could include:

- mutual support in crisis or emergency situations (e.g. by providing transport for security personnel, equipment),
- etc.

Local authorities, police, and fire departments should also be part of these cooperations.

3.10 Evaluating and Updating your Crisis Management Plan

After

- organizational changes, introduction of new processes or technologies, change of responsibilities, etc.,
- experiences gained during emergencies, actual crisis situations (also by others!),
- new evolving threats and/or
- exercises,

Your CM plan (as well as the underlying emergency or contingency plans) should be evaluated and adjusted.

For this process, specialist literature generally recommends the Plan-Do-Check-Act (PDCA) cycle.

This cycle is an iterative four-step problem-solving process typically used in business process improvement. In this context, this means the following:

	Measures
Plan	Develop/write your CM Plan and required emergency plans, etc. (e.g. by using these recommendations) [When a CM Plan is in place, this involves making the necessary adjustments].
Do	Put them in force, train your personnel, practice
Check	After • organizational changes, introduction of new processes or technologies, change of responsibilities, etc. • experiences gained during emergencies, actual crisis situations (also by others!) • new evolving threats and/or • exercises, • check if your plan is effective/has worked. [After first implementation of a CM plan, you should use exercises for a first evaluation. After a crisis, it is a task of the CMT to collect and distribute the lessons learned].
Act	Identify deficiencies and weaknesses of your plans. What has worked and what not? What was the cause of any deficiencies? Adjust your plans as required > Plan

Table 9: *Plan-Do-Check-Act (PDCA) cycle*

4 Conclusion

The recommendations given in this document are tailored for the needs of rail, public transport, and related infrastructural operators. They are aimed at a low level of preparation in order to be suitable for all sizes of entities. These recommendations should be discussed at the operator and adjusted to its specific needs. Operators who already have a Crisis Management organization in place can use these recommendations as a reference for further ideas or practices.

5 Outlook

Crisis Management cannot be regarded in isolation in an operator's efforts to continue its business. If business processes are severely interrupted, one should have a "Plan B" or fallback levels available.

According to IBM: "The ability of an organization's business operations to rapidly adapt and respond to internal or external dynamic changes – opportunities, demands, disruptions or threats – and continue operations with limited impact to the business" is called Business Continuity.

In a next step, UIC and its partners should conduct a deeper analysis of Business Continuity, providing its members again with best practices and recommendations.

UIC will start to provide additional checklists, practical advice or good practices in a toolbox. They can be used to further improve or extend these recommendations in selected areas, according to the operator's needs.

Additionally, a guideline for a generic security plan/concept is under preparation by UITP, with the collaboration of UIC.

6 Annex

6.1 Checklists

6.1.1 Crisis Management Team – Meeting Agenda

Preparations:

WHAT	WHO
• Decide on CMT meeting • Decide circle of participants (Central CMT and extended CMT members [if required]) • Determine protocol keeper	Chair
• Send invitations to CMT members and ensure receipt • Prepare "War Room" (meeting facility) • Have support personnel available • Establish communication with other crisis teams/staff • Prepare briefing, situation reports, documentation • Prepare list with participants	Crisis Coordinator Crisis Support Team

Meeting:

WHAT	WHO
• Open meeting • Check attendance/greeting and introduction of participants • Introduce agenda and scope of meeting • Address members for contributions/speeches • (especially with telephone or video conference)	Chair
General briefing of situation/impacts/facts	Crisis Coordinator Crisis Support Team
• Media coverage • Additional information • (Preliminary) evaluation/assessment	Attendees

• Measures and decisions
• Tasks:
  • Requirement of further expertise/adjust participants, resources/ personnel or support
  • Information requirements (internal/external)
  • Release of media announcements/statement
	Determined by CMT (documentation!)

Next meeting	Chair
Minutes	Support Staff

6.1.2 Crisis Management Team – Meeting Minutes

DATE	TIME	PLACE
dd.mm.yyyy	*hh:mm - hh:mm*	*<place>*

Participants:

NAME	ENTITY	PARTICIPATING
Last, first	*e.g. Head of Operations, Freight Division*	*hh:mm - hh:mm*
...		

Situation report:

SUMMARY

REPORT	TIME	ATTACHMENTS
e.g. Briefing Situation Center	*dd.mm.yyyy - hh:mm*	*yymmdd_Sit-Rep_SC_1.ppt*
Media Summary	*dd.mm.yyyy - hh:mm*	*yymmdd_Med-Rep_Com_1.doc*

Additional Reports (Schematics):

Area / Entity	*e.g. Freight Operations*
Time	*dd.mm.yyyy - hh:mm*
Incident	...
Effects / Consequences	...
Measures taken / required	...
Resources	...
Information Requirements	...
Attachments	*yymmdd_Rail-Dam_1.doc*

(Other contributions or information could be attached, using this formal)

Measures and Decisions Taken:

Nr	Decision	Assigned to	Status	By / until
1.	*e.g. Deploy all security guards to stations <a>, <b>, <c>*	*Head of Rail Sec Operations*	*Initiated*	*Compl. by hh:mm*
2.	*e.g. Evacuate office buildings in stations*	*Head of Station*	*Initiated*	*Compl. by hh:mm*
3.	*...*			

Next meeting:

DATE	TIME	PLACE
dd.mm.yyyy	*hh:mm - hh:mm*	*<place>*

Participants for next meeting:

NAME	ENTITY	PARTICIPATING
Last, first	*e.g. Head of Medical Service*	*Presence*
Last, first	*e.g. Liaison Officer Rail Police*	*Video conference*
...		

Special Agenda Points for Next Meeting:

WHAT	WHO
Preparation of Media Release	*Head of Communication*
Liability for….	*Legal Counsel*

Attachments:

yymmdd_Sit-Rep_SC_1.ppt
yymmdd_Med-Rep_Com_1.doc
yymmdd_Rail-Dam_1.doc
…

Released by:

Chair *Co-Chair*

INTERNATIONAL UNION
OF RAILWAYS

COLPOFER

UITP

International Union of Railway
www.uic.org/security