Business Resilience

An Introduction to protecting your business

CFPA-E Guideline No 2:2013 N

CFPAEUROPE

FOREWORD

The European fire protection associations have decides produce common guidelines in order to achieve similar interpretation in European countries and to give examples how damage from natural hazards can be effectively limited by preventive and defensive measures, normally learnt from experience. CFPA Europe also develops and ratifies guidelines for all aspects of fire prevention, and safety and security related problems.

The objectives of CFPA are to improve safety and security and to prevent the consequent loss of life and destruction of property and business. The market imposes new demands for quality and safety.

The measures of Natural Hazards Guidelines concern not only operators, businesses, specialists and plant officers, but also the population and local administration. This is due to the fact that in contrast to fire, the impact of natural hazards as a result of drought, are often very widespread.

The proposals within this guideline have been produced by The UK Fire Protection Association and the author is Adair Lewis from the UK.

The Guideline has been compiled by Natural Hazards Group in the Guidelines Commission and adopted by all fire protection associations in the Confederation of Fire Protection Associations Europe.

These guidelines reflect best practice developed by the countries of CFPA Europe. Where the guidelines and national requirement conflict, national requirements must apply.

Copenhagen, 7 Mars 2013
CFPA Europe

Jesper Ditlev
Chairman

Helsinki, 7 Mars 2013
Guidelines Commission

Matti Orrainen
Chairman

CFPAEUROPE®

Contents

1 Introduction

This document provides an introduction to ways in which management can adopt measures which will help a business survive the effects of a significant and potentially damaging event, such as a flood or a terrorist incident. This approach to business resilience delivers a framework on which a company can build, whatever its size and whatever the nature of its business.

Being prepared for the worst situation that could occur is a sensible policy for dealing with lesser disruptions, and the process of business continuity management planning will inevitably increase the resilience of your business to disruptions of any size. The process of identification of potential threats, the ways in which their incidence and consequences may be reduced and consideration of the most effective response will prove to be vital tools to any organisation in the wake of a major incident or disaster. Experience proves that it is a lot easier to plan for the likely effects of potential disaster coolly and objectively in advance, than react in the aftermath.

2 What is business resilience?

Business resilience is about safeguarding your business, its people and assets. It should be part of your everyday management planning. If and when you are faced by disaster, that preparation can help minimise the impact and help speed recovery. Thus, business resilience and planning should be regarded as a priority for any business and
is equally as critical for small companies as it is for large organisations.

Every year, a significant number of businesses face an event that is unplanned, unwanted and sometimes challenges their survival. That threat may come as a result of fire or flood, theft, fraud or a threat of terrorist action. Statistics show that some 80% of affected businesses do eventually recover, but no matter what the cause, businesses that successfully recover to thrive again are those that have:

- Assessed the likely impact on the business of significant and potentially damaging events
- Planned their response in advance
- Tested the effectiveness of the plan and revised it where needed
- Invested time, thought and, where necessary, money in managing the risk.

3 Threats to the business

A well-managed company will already have assessed the everyday hazards that might threaten the business and will have put in place control measures in relation to:

- People
- Fire
- Security
- Computers networks and communications.

Reminders of the common hazards that should be considered are given in the checklist in Annex 1 at the end of this document. Business managers may wish to look at these reminders when assessing their own businesses.

In addition to the common hazards that may have a direct affect on the business, events that may affect key suppliers should also be considered. For example, although the likelihood of an occurrence such as volcanic action or a major flood may be low in the area in which the business is located, it may be more likely in the area in which a supplier is located and the impact on the key supplier may be severe.

While hazards that may threaten a business cannot be totally eliminated, the likelihood of such an event can be identified and anticipated and the potential impact reduced by incorporating into the organisation an awareness of risk issues and the measures taken to control them. This is often referred to as Business Continuity Management. It aims to provide a framework within which a business can respond to significant events. Embedding a risk-aware culture instils confidence in all those who have an involvement, be they suppliers, stakeholders, customers or staff, that their interests are being protected.

4 Continuity management structure

There is a simple structure that can help you put your plan in place.

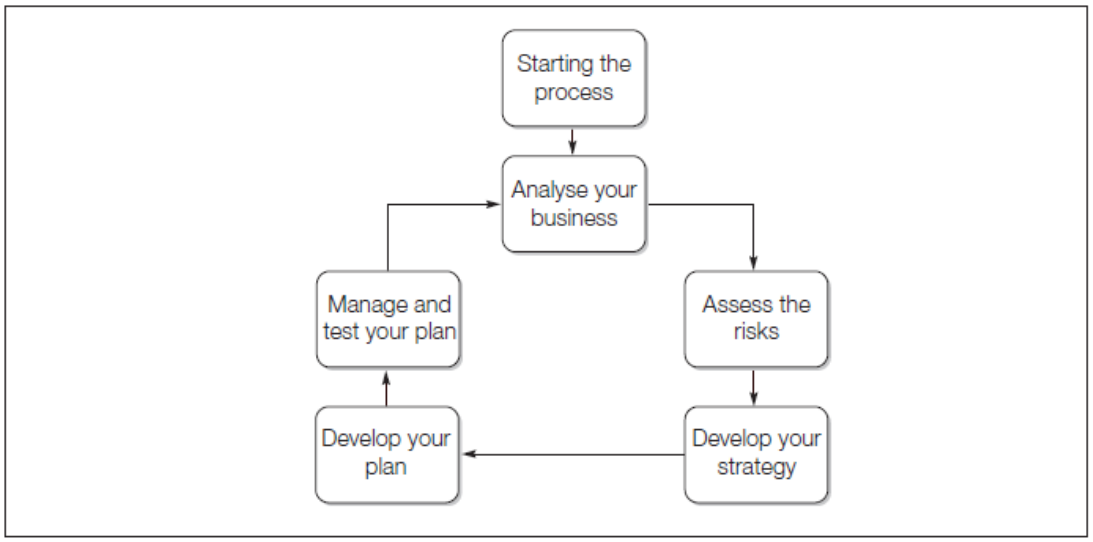

Figure 1: Continuity management cycle

Not all plans need to be complicated but they do need to be easily understood, they need to be comprehensive but suitably tailored to the needs of your organisation. The business continuity management planning process will make a substantial difference to the possibility of surviving an

incident. While it may seem an extra burden to prepare a plan, emergency situations place severe pressure on individuals to make decisions and take action under stressful conditions. Experience proves that such planning makes a substantial difference to the chances of surviving an incident when all the potential issues have been considered objectively beforehand. It is important, however, that the plan is kept up to date so that it reflects your business as it is, not as it was.

Some large organisations have a company fire brigade that is able to provide a rapid response by fire fighters that are familiar with the premises and processes being undertaken. On sites where there is a company fire brigade, this vital resource should be consulted when the business continuity plan is being prepared as they will have a key role to play in the event of an emergency.

5 Starting the Process

Planning for business resilience is the responsibility of everyone who owns or manages a business. No matter what the size of the operation, similar principles will apply:

- A senior member of staff should take charge of business resilience matters, which should be given the same importance in business planning as, for example, quality management, cash flow or health and safety.

- The business resilience 'manager' should assemble a small team of people to survey the nature and mode of operation of the business. The task is to survey the business and make a list of its key features and areas of operation.

- The responsibility for managing business resilience must be clearly established - everyone in the business should understand the importance of resilience, understand their role (if any) in the plan and know who is in charge.

- The scope of the work should be established since, for example, an organisation may already have an adequate and up-to-date plan for recovery from a failure of its computer system. Such plans would, however, need to be part of the main plan when complete.

6 Analyse Your Business

This part of the process is aimed at establishing which processes and functions are critical to the operation of the business and how quickly the impact of their loss will be felt.

Simply put, the task here is to ask:

- Which are the most critical areas of the business? (See Annex 1.)
- How quickly would losing a function or process have an adverse effect?
- What equipment, staff and systems are necessary to maintain or recommence these critical functions?

You should consider:

- Physical assets, including buildings, plant and machinery and stock
- Processes, systems and communications
- Computer systems and the data held on them
- Staff
- Customers and suppliers

Remember to consider service level agreements or legal and contractual obligations that will need urgent attention. It is often useful to list the functions in each department of your business and then grade them in terms of criticality from, say, 1 (low) to 5 (high). Then to each function allocate a time frame within which the impact would begin to be felt; this may for example be within four hours, within 24 hours, within 1 week. Once this is done, you will have a matrix identifying the priority areas of your business in terms of potential impact and you are ready to move on to the next stage once you are happy the analysis is correct and has been reviewed with appropriate colleagues.

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

7 Assess the Risks

When thinking about the risks in your business, it is necessary to consider:

- How likely is it to happen?
- What will be the effect if it does?

Your answers to these questions will help you to gauge the threat from the risks identified so far. For instance, how much would you lose in cash terms if a particular function were off-line? How long could you afford it to stay off-line? Your assessment of these factors will guide you to the measures you need to take to protect your business.

During this assessment process the insurer(s) of the business should be consulted as their claims experience may provide a valuable insight as to events that may otherwise be forgotten.

There are a number of ways in which you can analyse the information already gathered. Firstly, ask 'What if' questions. For example:

- What if sales data were unavailable for an extended period?
- What if we couldn't get into the building for two weeks?
- What if we had no power supply?
- What if we had no means to pay invoices?
- What if our major supplier went out of business?

Secondly, consider the worst-case scenario. This is less about the nature of the event and more about the effects of such an event. For instance, a major fire might destroy large parts of your premises and plant. This could lead to no production, loss of finished stock and an inability to supply customers: how would they respond? How could you communicate with them to ensure that they are not lost to you permanently? The same fire may have destroyed all your records, computer hardware and tooling specifications; how can you maintain cash flow or replace destroyed tools?

Finally, consider your staff. Identify those with special skills, knowledge or responsibilities that will be vital in different time frames after the event – within the first four hours, the first day and so on. Assess the risk that such staff may not be available.

8 Develop Your Strategy

The work done so far should have identified the way your business is organised, the risks facing it and the potential damage to the business from a range of scenarios. Developing your strategy is really about deciding what level of risk you are prepared to accept; this in turn will help you decide on the actions to be taken. It may be prudent to consult your insurer, who will be able to offer advice, guidance and solutions to some of your risk management problems. There are various options open to you:

- Accept the status quo
- Reduce the likelihood and/or the effect of the risks to a manageable level
- Eliminate the risks entirely or reduce them to a negligible level.

The first option could be seen as something of a gamble, as it relies on the ability to recover from an event quickly and completely; however, your analysis and assessment work will have identified for you the dangers inherent in this approach – by the time you have recovered, customers may have found an alternative supplier or perhaps competitors will have stepped into the breach.

The third option can involve considerable expenditure, so the middle way is often the preferred route. Here, you should reduce as far as is practicable the risk of something happening – together with lessening its effects. Your Continuity Plan then details the way in which you will deal with any remaining risk in the event of an incident.

You should also consider the use of outside assistance as part of your recovery strategy. It may be possible to agree a reciprocal deal with another company to use facilities at each other's premises in the event of loss at either – such facilities could range from canteen to computer networks. Alternatively, contracts can be agreed with
a specialist supplier for the provision of suitable temporary buildings and equipment when needed: this is known as a 'cold site'. A 'hot site' by contrast is one where you have access to fully equipped premises, usually within hours of the original event.

Alternatively, you can rely on the market and simply take premises of the right size in a suitable location when you need them – but, when developing your strategy, don't forget the time delay in obtaining all necessary consents, completing legal processes and fitting the property out for occupation.

9 Counter Terrorism

At a time of heightened awareness and when central and local government are radically revising arrangements for emergency planning and response, it is vital that business plays its part in improving the resilience of the community. Does your business or its products make you particularly at risk from terrorism? Does your location - in a city centre, for example - make you vulnerable to denial of access to your premises following an event, even though they may not be directly damaged? The implementation of appropriate measures will help reduce the risk from terrorist action and improve the resilience of your business. You should consider the following:

- Manage staff securely: take up references; request proof of qualifications; verify the identity of new employees before confirming a job offer.

- Manage contractors securely: use only established reputable contractors; investigate contractors' processes for validation of staff; institute procedures involving passes and

photographs to identify the persons working at your premises; agree procedures for temporary replacements when the usual staff are unavailable.

- Develop procedures and ensure all staff are aware of the actions they should take in the event of a bomb warning or similar threat at the premises, in the surrounding area, or in the event of an instruction to evacuate the premises by the emergency services. The procedures will be different from those used to evacuate the premises in the event of a fire as in the case of a bomb threat the fire alarm should normally not be used. This is because in this case it is often necessary to direct staff out of a particular exit to avoid the device rather than leaving via the nearest available route. Hence alternative measures to alert staff should be put in place and rehearsed.

- Muster points should be established remote from the premises (much further away than the assembly points used at the time of fire evacuations). Visitors and contractors must be accounted for in any evacuation. Bear in mind that it might sometimes be necessary to contain people within the building - if there is an external bomb threat, for instance. In such cases:

  - Designate a safe area where people can gather, away from windows and glazing (an area in a basement or stairway is often suitable). Protection against flying glass is vital and can significantly reduce the number and severity of injuries following an explosion.
  - Ensure that the area has access to toilets and drinking water
  - Survey the area prior to use to ensure that it is blast resistant.
  - Ensure that staff can be regularly updated as events develop and do not feel isolated.

Figure 3: The company occupying the tower block, which was severely damaged by a vehicle bomb, was back in business in alternative premises within 48 hours thanks to an effective contingency plan

10 Develop Your Plan

In writing your plan it is important to use simple, clear, non-technical language so that everyone who will need to use it can readily understand. Remember, that what is a common expression in one part of your business may be unintelligible jargon in another. Your plan should include:

- **A clear statement of purpose and scope**. Include here a statement of support from senior management to ensure that the plan carries sufficient weight within the business.

- **Recovery management team**. Involve those people needed to get things moving and take the necessary decisions. Include deputies to cater for holidays and absences and bear in mind that incidents may occur at night or weekends. You may want to have additional members who join the team at later stages to work on elements of the recovery. Ensure that responsibilities are clear and that members of the crisis team know exactly how their communications will work. State where and when the team will meet, on-site or off-site, depending on circumstances.

- **Recovery procedures**. Be specific about the initial actions to be taken in the first few hours following an incident and specify reporting procedures so that progress can be monitored. Maintain up to date inventories of equipment and software so that replacements can be ordered. Ensure that mobile telephones will be available to team members.

- **Public relations**. Your public response to an incident may be the difference between success and failure in recovery terms. Remember that damage to your company's reputation or brand can do just as much damage as a fire. Plan how you will deal with the public, customers, suppliers and the media. There should be a single point of contact within the crisis team.

- **Staff.** Plan to communicate with staff to ensure that they know the up to date position. Use telephone cascades, local press advertising or other means as necessary.

- **External information**. Include here contact information for emergency services, utilities, insurance, neighbouring businesses. Outline the information each will need immediately after an incident.

Further information is set out in the CFPA-E Guideline on protection against floods.

11 Manage and Test Your Plan

Your plan is now complete and its contents have been publicised throughout the company to ensure that everyone is aware not only of their roles in the event of an incident, but also, especially, their responsibility to prevent problems in the first place. You could use this as an opportunity to identify and meet any relevant training needs. However, this cannot be a one-off exercise. Businesses change and your plan must also change if it is to remain effective. So, make sure that the plan is reviewed and revised frequently and reflects the current position. You should aim to exercise your plan after it is completed and following significant changes. You can test in a number of ways:

- Paper-based exercises can be useful. Get a group together and question the plan's provisions. Ask the 'what if' questions again. Listen to the feedback and amend the plan if necessary.

- Test your telephone cascade by sending a test message, without warning, to the people at the top of the cascades. The last person on each cascade can then be contacted to see when they received the message. This helps you to check that your communications structure is working and, again, make changes if needed.

- Full rehearsal means putting your plan into operation in a simulated environment. Though you will probably not be able to use alternative premises unless you have contracted for a 'hot site', the opportunity to have recovery management team members working together can highlight any shortcomings in planning or implementation.

Alternatively, it is possible to recruit a consultant company to help you test your plan - ask your insurance company for guidance on this option. Finally, ensure that the recovery management team have the information and resources they will need to operate successfully in the aftermath of an incident, whether serious or minor. You should have an 'emergency box' or boxes, which should be located in a secure place with at least one box being stored off-site. These boxes should be accessed quickly following an incident and contain items such as:

- Full copy of the Continuity Plan
- Staff lists with contact/cascade details
- Inventories
- External contact details
- Site plans
- Keys
- First aid kit
- Torches
- Batteries
- Writing materials and stationery
- High visibility jackets and hard hats

12 Summary

Business Continuity Management is a matter of proper business planning. There are numerous packages available in bookstores and via the internet which include templates to help construct a plan. Reference should also be made to national guidelines or standards.

Whatever method is used, the key to the process is knowing your own business, analysing it and addressing any problems identified. The approach must be to:

- define the process, principles and terminology of business continuity management;
- provide a framework for preplanning, anticipation and response;
- describe evaluation techniques and criteria

Last, but not least, make sure that your insurance cover is adequate and up to date and that its scope is broad enough to provide the financial help your business will need following damage. But whilst insurance has an important role to play, this does not guarantee continued existence of the business following a disaster. Don't forget, if you need to move to alternative premises, check your insurance cover to ensure continued cover at your new address.

13 European guidelines

Fire

Guideline No 1:2002 F - Internal fire protection control
Guideline No 2:2013 F - Panic & emergency exit devices
Guideline No 3:2011 F - Certification of thermographers
Guideline No 4:2010 F - Introduction to qualitative fire risk assessment
Guideline No 5:2003 F - Guidance signs, emergency lighting and general lighting
Guideline No 6:2011 F - Fire safety in care homes for the elderly
Guideline No 7:2011 F - Safety distance between waste containers and buildings
Guideline No 8:2004 F - Preventing arson – information to young people
Guideline No 9:2012 F - Fire safety in restaurants
Guideline No 10:2008 F - Smoke alarms in the home
Guideline No 11:2005 F - Recommended numbers of fire protection trained staff
Guideline No 12:2012 F - Fire safety basics for hot work operatives
Guideline No 13:2006 F - Fire protection documentation
Guideline No 14:2007 F - Fire protection in information technology facilities
Guideline No 15:2012 F - Fire safety in guest harbours and marinas
Guideline No 16:2008 F - Fire protection in offices
Guideline No 17:2008 F - Fire safety in farm buildings
Guideline No 18:2013 F - Fire protection on chemical manufacturing sites
Guideline No 19:2009 F - Fire safety engineering concerning evacuation from buildings
Guideline No 20:2012 F - Fire safety in camping sites
Guideline No 21:2012 F - Fire prevention on construction sites
Guideline No 22:2012 F - Wind turbines – Fire protection guideline

Guideline No 23:2010 F - Securing the operational readiness of fire control system
Guideline No 24:2010 F - Fire safe homes
Guideline No 25:2010 F - Emergency plan
Guideline No 26:2010 F - Fire protection of temporary buildings on construction sites
Guideline No 27:2011 F - Fire safety in apartment buildings
Guideline No 28:2012 F - Fire safety in laboratories

Natural hazards
Guideline No 1:2012 N - Protection against flood
Guideline No 2:2013 N - Business Resilience – An introduction to protecting your business

Security
Guideline No 1:2010 S - Arson document
Guideline No 2:2010 S - Protection of empty buildings
Guideline No 3:2010 S - Security system for empty buildings
Guideline No 4:2010 S - Guidance on key holder selections and duties

14 Annex 1: Company activities linking business resilience planning to perceived threats.

This list of areas for attention will not be complete but within them a typical business will find topics around which to assemble a plan of action.

- Basic operation
- Economic effects
- Market factors
- Company departments
- Personnel
  - Administration
- Finance
- Legal
  - Production
  - Information technology
  - Storage and despatch . . . and the rest
- Logistics
  - Goods inwards
  - Production
  - Goods outwards
- Key people, key operations
- Utilities (electricity, gas, water, internet access)
- Business interruption planning (people, premises, equipment, materials, capacity)
- Equipment (expensive, vulnerable, irreplaceable)
- Health and safety compliance

15 Annex 2: Plans

Training plan

A plan for training, exercise and control should be created to get an overview of the information and training needs and that mandatory training and drills are performed with the correct regularity.
The plan should contain requirements and objectives, how the tasks will be monitored and by whom.

Emergency plan

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

- *Evacuation plan*
  - Schematic plans with symbols and comments about evacuation routines such as evacuation routes, assembly points, alarm management and fire extinguishing equipment.
  - Symbols should be easy to understand and comply with the applicable requirements and standards.
  - Evacuation plans should be clearly visible and the content be read and well known by all who are in the business.

- *Accident guide*
  - Checklist that briefly describes the correct behavior in different types of incidents. The list should be adapted to your business specific risks.
  - The incident guide should be placed at appropriate locations and the content be read and well known by all who are in the premises.

- *Alarm List*
  - A list with names and telephone numbers of managers, supervisors, maintenance contacts and other competences to be contacted in an accident.
  - The list should be readily available and well known to people who are expected to carry out the protection.

- *List of emergency actions*
  - Checklist of emergency actions, brief descriptions of what needs to be done in the event of an accident such as emergency-stop, alarm buttons, start of emergency systems, barriers, risk information, etc.

- The list should be readily available and known to the site staff.

- *Priority salvage*
  - List of important assets in priority order, such as unique machines, tools, drawings, stored information, spare parts, etc.
  - The list should be easily accessible and be presented to the fire and rescue service or other responsible person.
  - The list should be considered as confidential information and not be disseminated to unauthorized people.

- **Startup plan**

A plan with check lists to easily verify that all necessary measures are taken in the acute phase of the emergency plan to get started with the recovery of the business. These checklists can vary depending on the type of event. The list shall be available in crisis management room and be used at crisis management meeting.

- **Caretaking plan**

  - A plan to quickly be able to take care of the damaged activities. The aim is to rapidly put in resources to deal with the personnel involved as well as rehabilitate and save the environment, equipment and buildings. This is to minimize the downtime, prevent rumors and reduce secondary damage.
  - List of neighbors, authorities, mass media and internal operations that are affected and need
    information about what happened.
  - List of specialist expertise to take care of expected damage (including mental and physical health of personnel).
  - List of expected materials for decontamination.
  - Template/responsibilities of security procedures for staff at the site of the accident.
  - Emergency routine for priority salvage.

- **Back-up plan**

A back-up plan is created based on how the activities shall be carried out during time of recovery. What is damaged and what can be used of existing resources? What are the alternatives and what is most important? The aim is to operate all or part of the activities during recovery to normal operations.

- A good basis is an existing risk analysis which may provide information about the measures proposed at an expected accident. Even weak links (critical elements) in the activity can be seen and possibly where and how businesses can be operated at a loss of function.
- Can a change be made of the utilization of other activities within the company, for example, changing shifts and the use of machinery in a different way?

- Can logistics be changed, for example by alternate torrents?
- Check for external options outside the company? Who has the capacity and the method? Is it approved?

- **Recovery plan**

A recovery plan describes the activity to recover to normal operation. It is essential in long-term aspects and requires good decisions to get a quick and cost effective solution and a short downtime.

- Create a list (instructions) on vital resources, premises, control devices, etc.
- Create a list (instructions) of possible suppliers of equipment and spare parts.
- Create a plan to manage time-critical resources such as carrying contract, back-up agreements, etc.
- Create a template for procurement routines and approvals (permits) to reduce downtime.
- Review the need of developing and improvement of the business and product.

European Guideline

16 Annex 3: Checklists

Have the emergency plan's various parts taken into consideration?

- Evacuation
- Assembly points
- Alarm Management
- Emergency actions
- Support to the rescue service
- Internal information
- Occupational health care and needs of staff
- *Priority salvage*
- Orders and information

Are the following tasks allocated?

Management:

- Decide on crisis management room
- Call management team and other selected
- Organise the emotional support center
- Contact the insurer
- Decisions about the priority of different actions
- Assign someone to survey, the 'helicopter view'
- Use of all the elements in the plan for contingency planning

Operational:

- Keep record of all actions
- Listen to radio and watch TV
- Establish communications networks.
- Contact skills/resources outside the team
- Make up the schedule for common status briefings
- Prepare information to staff
- Develop drawings and other documentation
- Plan for meals (including for the crisis management group).
- Plan for staff replacement (including crisis management group).

Information:

- Information to concerned people
- Information to telephone exchange and reception.
- Establish media contacts (local radio, papers and television)
- Submit press release
- Prepare possible press conference

- Inform customers and vendors
- Use only confirmed facts in information

Press conference

- Coordinate with emergency service, police, health and other involved organizations
- Determine the local (availability, size, light, sound, technology, ventilation, etc.)
- Determine the time
- Inform the telephone exchange and the customer reception areas
- Who directs the Conference?
- How to check that the right people are present? (Only the media.)
- How to deal with language?
- How to deal with cultural and religious issues?
- Who represents your company?
- Plan for interviews afterward
- Have a prepared and copied press release to hand out