PRINCIPLES – APPROACH – GOOD PRACTICE

# Preparing Scotland

## HAVING AND PROMOTING BUSINESS RESILIENCE

November 2013

safer scotland
SCOTTISH GOVERNMENT

# Executive Summary

Resilience, as described and promoted in Preparing Scotland[1], has many different but interconnected elements. Although the ability to prepare for, respond to and recover from emergencies and disruptions is relevant to organisations and communities of all sizes and types, how this is realised will vary according to their particular circumstances. The resilience of one organisation or group will, in turn, have consequences for others, creating a complicated network of influence: increasing or decreasing risk, promoting or discouraging resilient behaviour.

This diversity is reflected in Preparing Scotland, which recognises the different roles of a wide range of agencies, organisations and individuals, and also the important contribution of community resilience. Preparing Scotland recommends the benefits of joint working and the value of considering the management of emergencies and disruptions from different perspectives. Within that broader context, this guidance focuses on how organisations can become more resilient. In particular, it provides advice to Category 1 responders and information to other readers about the duties set out in the Civil Contingencies Act (2004) and associated Regulations. This includes recommendations concerning:

- The ability of Category 1 organisations to continue to be able to perform their functions in the event of emergencies; and
- The provision, by local authorities, of advice and assistance to businesses and other organisations about the continuance of their activities.

These duties are often expressed as 'having business continuity arrangements' and 'promoting business continuity'.

The approach recommended in this guidance to fulfilling these duties is to apply the principles of Integrated Emergency Management, described in Preparing Scotland, in the context of organisations and businesses. This approach to building 'Business Resilience' considers both:

- the logistical aspects of how organisations work, what could go wrong and how to deal with this
- the cultural aspects of organisational behaviour, learning and attitudes to risk, within which resilience will be maintained

This does not imply any enlargement of the duties of the Civil Contingencies Act, but recognises that when fulfilling these duties (and others to which they may be subject) organisations will benefit from adopting methods which fully utilise the different sources of knowledge and expertise they already possess. These principles also address the diverse nature of emergencies and disruptions, which require flexible and scalable management, how resilience can be built before and after disruptive events, and the value of an organisational culture that fosters learning.

1 Resilience is defined as 'the capacity of an individual, community or system to adapt in order to sustain an acceptable level of function, structure and identity'. *Preparing Scotland: Scottish Guidance on Resilience*

Much of this guidance will discuss issues that will be familiar to organisations that have business continuity arrangements that are aligned to British Standard BS25999 or ISO 22301. Alignment with these standards, in their most inclusive forms, will ensure substantial compliance with this guidance. Some differences in emphasis and scope will be noted regarding the cultural aspects of resilience, integration with related disciplines and the promotion of resilience.

# Questions to Ask

Disruptions can affect any part of your day to day business, and often affect several aspects at once. How would the following affect your organisation's ability to carry out its statutory duties and achieve its strategic objectives?

### Loss of Access to Premises

Days of severe weather have made some important parts of your property unsafe for use and damaged the facilities and resources it contains; they have also caused a sharp increase in demand for your services.

- How will this affect your organisation's ability to provide critical services?

### Utilities Failure

The local power supply has failed and is expected to be off for many hours. Your offices are dark, IT systems are down and your mobile phone is running out of charge. These and other consequences will be felt across your organisation:

- How will you assess the impacts elsewhere (e.g. critical equipment and activities, safety and security in public areas, loss of data)?
- How will the response be managed and staff and customers be kept informed?

### IT Disruption

A 'software upgrade' leads to a loss of personal data belonging to service users or customers and staff – and it is being sold on a criminal website. Parts of your IT systems remain faulty, output is being lost and you are being accused of failing to protect against this risk?

- How do you respond to the risk you have exposed these people to and the damage to your reputation?
- What are the practical problems to overcome and how long will this take?

### Staff

Staff may be absent for many reasons (illness, transport disruptions, caring responsibilities, school closures, etc.) some of which may be linked with increased demand for services:

- Can you demonstrate that you have enough people, with the right skill mix, including key specialists, to deliver essential services, in a safe way for the probable duration of an extended disruption?

### Equipment and Supplies

An organisation that supplies you with important equipment, consumables or services is accused of criminal negligence in supplying items likely to cause a risk to health. The supplier's credibility is in doubt and staff are occupied in remedial action:

- How would you conduct safety assessments of people who might have been affected?
- How would you source compatible alternatives and avoid falling behind on essential work?

# Contents

## Note on the legal status of guidance

The guidance is advisory only and should be read in conjunction with any relevant legislation. This guidance is not, and is not meant to be, a comprehensive description of applicable legislation or of any legal obligations. If you are in any doubt about any legal obligations which are contained in any applicable legislation or otherwise, you are advised to seek your own independent legal advice.

# 1. Introduction and Context

Resilience, as described and promoted in Preparing Scotland[1], has many different but interconnected elements. In an organisational or business context, this manifests as the practical ability to avoid disruptions to normal activity, to keep the things that matter most going and, if disruptions occur, to get back to a desired state of operation quickly – not by good fortune, but by design.

Being resilient in this way is immediately appealing. Resilient Category 1[2] responders will be more able to fulfil their duties when adverse circumstances mean we need them most. Businesses that are resilient will avoid costly losses, gain commercial advantage and be able to continue to provide the employment, goods and services we value.
And voluntary organisations will be able to continue their work to support individuals, communities and other service providers, increasing the quality of many lives.

This guidance uses the term 'Business Resilience' to mean 'the capacity of an organisation to adapt in order to sustain an acceptable level of function, structure and identity.'

For most organisations, resilience of this sort will be a means to an end and not their main objective. When working to develop resilience in an organisation, it is therefore essential to keep its objectives and the interests of the people involved clearly in focus. In this way the preparations will be seen to be relevant and the response to disruptions or emergencies will be more effective. This is consistent with the Preparing Scotland approach to developing resilience based on the doctrine of Integrated Emergency Management[3] (IEM) which includes the principles of integration, responsibility and continuity (see section 1.3). This approach to Business Resilience must therefore consider:

- the priorities, motivations and skills of individuals, teams and organisations
- relationships with external organisations and their resilience capabilities
- the formal processes and tangible resources that deliver goods or services
- the risks the organisation faces and potential emergencies that might arise

The term 'business' should be understood to include the activity of both commercial and non-commercial organisations or groups, whether small or large, and whether they are in the commercial, public or voluntary sectors.

1 Resilience is defined as 'the capacity of an individual, community or system to adapt in order to sustain an acceptable level of function, structure and identity'. *Preparing Scotland: Scottish Guidance on Resilience* http://www.readyscotland.org/ready-government/preparing-scotland/

2 The emergency services, local authorities, NHS Boards, SEPA, see *Preparing Scotland: Scottish Guidance on Resilience*

3 *Preparing Scotland: Scottish Guidance on Resilience*

## 1.1 The Civil Contingencies Act and Business Resilience

The Civil Contingencies Act and Regulations[4] place several duties on Category 1 responders, including:

- The ability of Category 1 organisations to continue to be able to perform their functions in the event of emergencies
- The provision, by local authorities, of advice and assistance to businesses and other organisations about the continuance of their activities

These are sometimes expressed as 'having and promoting business continuity'.

The legislation is also concerned with how these duties are carried out, with cooperation between partner agencies (both statutory and non-statutory) and how this relates to its other requirements – including risk assessment, maintaining plans, and emergency response and recovery.

The approach recommended in this guidance is to apply the principles of Integrated Emergency Management in the context of organisations and businesses. In this way Category 1 responders are advised to consider the requirements of the Civil Contingencies Act alongside their other responsibilities and objectives, so that the most effective, integrated ways of working can be found. Similarly, when working to develop resilience in other organisations, this approach will encourage businesses to develop resilience in a way that serves their strategic aims and utilises their existing strengths.

In this guidance the phrase 'having and promoting Business Resilience' is used to refer to these duties carried out in this way.

## 1.2 Overview of Business Resilience Guidance

This guidance provides strategic advice to Category 1 responders and information to other readers by considering:

- How Business Resilience relates to other resilience issues such as the resilience of communities and emergency response arrangements (section 1.3)
- What should be understood by Business Resilience, business continuity, and related terms (section 2)
- How these duties might best be fulfilled (sections 3 and 4)
- What the Civil Contingencies Act and Regulations require of Category 1 responders regarding their ability to continue to perform their functions and provision of advice and assistance to others about this (Annex 1)

4 The Civil Contingencies Act 2004 and the Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005 see http://www.legislation.gov.uk/ukpga/2004/36/contents and *Preparing Scotland: Scottish Guidance on Resilience*

The broader context of resilience is set out in the Preparing Scotland 'core' guidance and is outlined below. This and particular links between Business Resilience and Community Resilience[5] are discussed further in section 3.

## 1.3 Business Resilience and other Resilience Activity

Scotland's resilience depends not only on the ability of organisations such as the police or ambulance service to deal with emergencies, it also requires other public sector organisations, private businesses, households and local communities to play their role. Because the different parts of our society are closely interconnected, more or less resilience in one part will affect the whole, and good practice in one area of life may inform behaviour in another. Because our society is diverse, the varied skills of different groups and individuals will all be needed for it to work at its best. While business continuity (or similar duties) are not legal requirements for all organisations, self-interest and good management make it advisable for all organisations to develop Business Resilience in ways that are appropriate to their circumstances.

Although untrained members of the public should not attempt to perform the functions of professional emergency staff, their efforts can complement those of Category 1 responders in many valuable ways. When developing the resilience of businesses or other organisations, often the people employed there will be the only ones with the specialist skills or knowledge needed to address problems. Also, when responding to an emergency, the priorities of the emergency services, such as saving life and helping the most vulnerable, may mean that issues that are important to an individual firm may be deferred. In many cases these issues will be outwith the remit of the emergency services and will be left to the owners and employees to resolve.

Similar relationships between statutory and non-statutory roles apply when considering community resilience, where the contributions of local people are crucial. Category 1 responders may also depend on the resilience of non-statutory and voluntary organisations because of their role in the supply chain or because work has been subcontracted to them.

Preparing Scotland: Scottish Guidance on Resilience recognises these different roles and describes the overarching structures and principles that guide resilience in Scotland. Work to develop and promote Business Resilience should be consistent with this advice and should be coordinated with related areas including[6]:

5 See *Preparing Scotland: Building Community Resilience guidance* http://www.readyscotland.org/ready-government/preparing-scotland/

6 Other specialist areas of activity which may be able to contribute to developing resilience internally are listed in section 2

- Emergency Planning
- Surge Capacity Planning
- Planning for the Recovery Phase[7]
- Community Resilience[8]
- Risk Assessment (including links to community risk registers)
- Training and Exercising

In doing this, the active engagement of partner agencies will be particularly important. This includes work across regional and professional boundaries, work with voluntary and non-statutory agencies, with different parts of the commercial sector and its representative bodies, as well as the core multi-agency work within Resilience Partnerships.

## 1.4 Process and Cultural Aspects of Business Resilience

Business Resilience demands a sound understanding of the logistics, technologies and resources needed to deliver goods and services (see section 3), but as well as these 'process aspects' there are also essential 'cultural aspects' to both developing and promoting resilience. Recognising this can help organisations make fuller use of the skills and knowledge of their staff and enable them to develop a culture where Business Resilience is seen as a positive contribution to the aims of the organisation and its staff. These 'cultural aspects' include:

- identifying the groups and individuals who have an interest in developing resilience and engaging with them
- understanding their priorities, concerns and the influences upon them
- drawing on their expertise and knowledge, including informal systems and practices
- securing their commitment to, and ownership of, the process for building resilience
- supporting a learning culture in organisations and ensuring trust so that risks and 'near misses' can be discussed and lessons learned

7 See *Preparing Scotland: Recovering from Emergencies in Scotland* http://www.readyscotland.org/ready-government/preparing-scotland/

8 See *Preparing Scotland: Building Community Resilience*

In a similar way to Community Resilience, developing Business Resilience within an organisation or promoting it externally will involve making people aware of the issues, engaging their help, and providing support so they can contribute to plans and implement responses. Once engaged with this process, individuals and groups are likely to:

- be more motivated – to want to help themselves, their colleagues and their organisation
- provide specialist knowledge about their area of work, including information about risks, and suggest solutions based on this
- be more able to contribute their experience, recall previous disruptions and how they were dealt with
- be able to provide constructive criticism of proposals from different perspectives
- provide access to networks of people who can assist in other ways
- be more ready to recognise and report emerging problems, providing early warnings
- have a fuller understanding of their role and be more able to respond flexibly when faced with unexpected disruptions

This in turn may have wider resilience benefits as staff may apply the approach outside work, at home or in their local community, given the benefits it can deliver.

# 2. What is Business Resilience?

The term 'resilience' is used in Preparing Scotland core document to mean 'the capacity of an individual, community or system to adapt in order to sustain an acceptable level of function, structure and identity'. Business Resilience is this capacity or attribute of a business or other organisation. Category 1 responders that are sufficiently resilient in this sense will therefore be fulfilling their duties under the Civil Contingencies Act and Regulations to be able to 'continue to perform his or its functions'. The approach to developing and maintaining Business Resilience recommended in this guidance is to apply the principles of Integrated Emergency Management in a business or organisational context.

Although this definition and approach may appear broad ranging, it does not imply any enlargement of the duties on Category 1 responders. Rather it is a recognition of the wider context within which these organisations exist, the other requirements they face and the existing capabilities they have. This circumspect approach allows Category 1 responders to:

- Consider the duties of the Civil Contingencies Act and Regulations in the context of other requirements, legal duties, governance arrangements, strategic objectives and issues of efficiency and good practice.
- Consider existing skills and capabilities in related areas and how these are interconnected.
- Seek effective ways to meet the requirements of Civil Contingencies legislation along with other requirements, by drawing on resources already available and seeking more integrated solutions.

An important part of this work is to utilise the methods of Business Continuity Management Systems and the expertise that exists in related specialist fields. The standard ISO 22301: Societal security – Business Continuity Management System – Requirements[9] describes Business Continuity Management as a 'holistic management process…which provides a framework for building organisational resilience'. Although the scope and application of the framework and processes will vary between organisations, a number of common elements can be identified that are important to building Business Resilience generally[10]. The first four of these make up a cycle, comprising:

- **Understanding the organisation** – understanding the strategic priorities of the organisation, including key services and products; using business impact analysis to examine the effects of disruption on these, and risk assessment tools to evaluate threats; determining what is needed to recover key processes to an acceptable level.

9 See ISO 22301:2012 Societal security – Business Continuity Management systems – Requirements at http://www.bsigroup.com/

10 These are codified more formally in ISO 22301 and formerly in BS 25999

- **Deciding on a strategy** – choosing from the alternative ways available to mitigate loss; deciding on how much risk and how much loss of function is acceptable in different parts of the organisation; deciding on the level of resources to commit to building resilience in light of its potential effectiveness and the importance of delivering critical functions to protect stakeholders.
- **Developing capability** – developing the response to disruptive challenges and the plans underpinning this, including managing activations of the response, defining roles and responsibilities, clarifying resource requirements, agreeing communications arrangements and other practical issues.
- **Reviewing and maintaining Business Resilience** – ensuring plans are fit for purpose and quality assured, that they are kept up-to-date as the organisation changes and that plans are exercised and new learning is incorporated.

This cycle is supported by other components:

- **Managing the programme** – both establishing the process and ensuring that the different parts are carried out effectively.
- **Embedding resilience in the organisational culture** – this stage involves raising awareness throughout the organisation and its key stakeholders, and providing training to key staff so that these activities become part of the normal operation of the organisation and the thinking of its staff.

The cycle is viewed as continuous as each of the four stages influence the next and the outcomes of review provide a better understanding of the organisation. Although, in practice, the four stages and other components are not distinct or strictly sequential, this is often a helpful model.

This cycle will be familiar to organisations that have business continuity arrangements aligned with ISO 22301. Although accreditation to a formal published standard is not a legal requirement, the principles recommended in this guidance are consistent with ISO 22301. Organisations that are aligned with this, in its most inclusive form, will have in place many of the most important requirements necessary to fulfil their duty to be able to continue to perform their functions.

When working to develop and maintain Business Resilience by applying these processes, it is recommended that particular consideration is given to the areas where related work may be being carried out and where expertise may be available, including:

- Business Continuity Management
- Risk Management[11]
- Crisis and Communication Management
- Security Management
- Building & Facilities Management
- Information Assurance and Security
- Health, Safety and Environmental Management

11 See ISO 31000 'Risk management – Code of practice' ISO 31000 http://shop.bsigroup.com/

# 3. Having Business Resilience

The Civil Contingencies Act places a duty on Category 1 responders to plan to continue to perform their functions in the event of an emergency[12]. This guidance recommends that this is achieved by applying the principles of Integrated Emergency Management[13] to develop Business Resilience.

Organisations should develop Business Resilience in a broad and inclusive way. This is because the various parts of an organisation will generally be interdependent and because the effects of some emergencies, and the responses they require, will be difficult to predict. This will also provide opportunities to involve staff in other parts of the organisation who may be involved with related work or have particular expertise to contribute.

So that relatively small disruptions do not develop into larger problems (or secondary effects do not impede the main response), and so that organisations are able to practice their responses, maintain their skills and learn from experience, it is recommended that arrangements encompass smaller disruptions as well as large emergencies.

The resilience of an organisation requires much more than having a plan for responding to a disruption or emergency. A thorough understanding of the organisation and the risks to which it is exposed, an agreed and resourced strategy and a commitment to embed resilience in the organisation's culture through training and learning from exercises and disruptive incidents are also needed.

Developing and maintaining Business Resilience within an organisation is likely to provide opportunities to promote resilience externally. The resilience of an organisation will depend, in part, on the resilience of its supply chain, including sub-contractors and those providing maintenance contracts. These connections will provide occasions to review the resilience of both parties. This principle could be extended to include the staff working in an organisation, where, for example, employers might discuss how they would get to and from work if transport was disrupted. In this way developing resilience may also have consequences for promoting personal, community and Business Resilience.

12 Civil Contingencies Act 2(1)(c)

13 Preparing Scotland: Scottish Guidance on Resilience

## 3.1 Understanding the Organisation

### 3.1.1 Strategic Aims and Critical Activities

Increasing Business Resilience should begin with a clear understanding of the organisation concerned including its strategic aims, how it is organised and its culture. Where an organisation's aims are expressed in general qualitative terms it will be helpful to convert them to specific key outputs or activities that can be quantified, as this will be needed to prioritise recovery targets and resource requirements at a later stage. However this should not ignore important quality measures and intangibles, such as maintaining the confidence of customers, service users and other stakeholders, or maintaining the value of brands and reputations.

If the organisation has a declared set of aims and objectives, or similar statements, these can be used as a basis for this work. This will be helpful as it is important that all relevant business and service activity that the organisation is engaged in is considered, and that partial assessments are avoided. The key objectives and values of the organisation will be used to identify which processes are the most important to its wellbeing, to justify decisions about what to prioritise if some activities must be halted, and to gain the support of senior management and the resources they control, for building Business Resilience.

Once the organisation's aims are understood, arrangements should be made to identify the critical activities and processes that are needed to deliver these, and the key outputs that embody them. In smaller organisations this may be less difficult as the person developing Business Resilience may already be familiar with the operations of the whole organisation. Larger organisations will need to involve the necessary specialists from different parts of the organisation.

This work will require an understanding of the inputs, infrastructure and processes on which the critical activities depends. These may include:

- **Raw materials and consumables** – such as clinical instruments and dressings in a health centre or food ingredients in a restaurant
- **Infrastructure** – such as transport systems, IT networks and utilities
- **Machinery and equipment** – such as communication or manufacturing equipment, hand tools and computers
- **Skilled staff**, or those with special authority – such as police officers with specialist roles, social service staff who are trusted by the communities they work with, or engineers with expertise in a particular technology
- **Premises** – such as specialist manufacturing facilities, office space, secure areas and warehousing

- **Knowledge** – such as subject matter expertise, legal requirements, knowledge of operating procedures, information about service users and customers

These factors are some of the organisation's dependencies, but it may have many others, both internally and externally, that support its critical activities. These can include suppliers, contractors, competitors, government departments, regulators, trade bodies, public or media perceptions, pressure groups, and others. It is important to identify these at an early stage and to take their influence into account. Involving representatives of relevant stakeholders, where this is practical, will make this process more effective.

### 3.1.2 Business Impact Analysis

Having identified their critical activities, organisations should determine what the impact would be if these were disrupted or lost. This stage is known as Business Impact Analysis (BIA). This will provide information to inform later decisions about strategies to develop resilience and will enable the organisation to focus on areas that most threaten the continuity of its priorities.

The potential causes of disruption to an organisation's operations are almost limitless, however the *impacts* of any disruption are far fewer. For example, loss of critical system(s), denial of access to premises, damage to premises or loss of key staff and key resources can all produce similar disruption regardless of the cause. It is helpful to rate the impact of disruptions upon the critical activities and key outputs of the business in the event of an emergency. This may be done with a simple high, medium, low scale or by scoring them, from 1 to 5. The impact of potential disruptions should be measured with reference to the following (non-exhaustive) list of factors:

- implications for output or service delivery
- financial cost to the organisation
- health, welfare and safety of stakeholders
- statutory duties and legal obligations
- environmental implications
- resources required to remedy the situation
- impact of disruption on partners
- reputation

The Business Impact Analysis should also take into account the time sensitivity of each business function and process, how urgent it is to restore based on the consequences for the organisation, as this will also influence the recovery objectives.

### 3.1.3 Recovery Objectives

Ideally, after normal activity has been disrupted, it would be restored quickly and fully to the same state, or perhaps even an improved state which takes into account changes in circumstances. Speed of restoration is rarely possible when the disruption is serious or complex, so organisations must decide which parts of their operations must be restored first, to what level of activity and how quickly. The terms 'recovery time objective', 'maximum tolerable outage' and 'recovery point objective' are sometimes given to the target recovery times and the required level of function for a particular activity. These targets will be affected by a combination of high level aims and by practical operational considerations, which will include interdependencies between different activities and the particular circumstances of the disruption.

Some activities, such as saving lives or complying with legislation, will clearly take precedence over other activity but in other circumstances critical tasks may not be immediately obvious and should therefore be highlighted during planning. In addition to setting recovery objectives for activities, the resources necessary to accomplish these should be understood so they too can be identified.

### 3.1.4 Risk Assessment

Once an organisation has identified its critical activities and conducted a business impact analysis, it should carry out a risk assessment in order to identify and understand events that could disrupt these activities. This should include risks arising both externally and internally. Risk Managers within organisations and multi-agency risk assessment groups in each Regional Resilience Partnership are likely to provide complementary perspectives on risks which can be used to provide a comprehensive risk picture.

The risk assessments carried out and published as Community Risk Registers are discussed in *Preparing Scotland Risk & Preparedness Assessment* guidance. These will assist organisations to identify major external hazards and threats that could lead to emergencies. Category 1 responders will also have access to other information about external risks that is not available to the general public because of its sensitive nature. These will be important to Category 1 responders who are required to have arrangements both to maintain priority activities and to respond to emergencies.

All organisations will need to interpret information from external sources and apply it to their particular situation. They are likely to have to adjust risk assessments to take account of particular local factors relating to their activities, such as local geography, infrastructure and climate.

Organisations will also need to conduct risk assessments of potential internal events which could be disruptive. Often these will be based on the processes they carry out and the hazards associated with them, for example being dependent on a particular piece of equipment or a single team to provide an output or service. Some risks will combine external and internal features such as a dependency on a single supplier or subcontractor, being a target for crime or disorder, or the unpredictable availability of some resources.

The 'FIRM' Risk Scorecard, which considers Financial, Infrastructure, Reputational and Market Place drivers of risk, which is a feature of Enterprise Risk Management, provides a useful approach to considering a broad range of risks.[14] A feature of this is to consider internal and external risks at all levels within each category. Enterprise Risk Management also provides useful ways to identify, analyse and assess risks to provide a deeper understanding of how risks and processes are interconnected, including:

- Hazard and Operability studies (HAZOP)
- Failure Modes Effects Analysis (FMEA)
- Political Economic Social Technological Legal Environmental (PESTLE) analyses
- Inspections and audits
- Flowcharts and dependency analysis

Although the Civil Contingencies Act is concerned with the resilience of organisations faced with emergencies as defined in the Act, organisations will want to consider a wider range of circumstances. This is because the indirect effects of emergencies might still be important and might be similar to disruptions caused by more routine risks.

## 3.2 Deciding on a Business Resilience Strategy

Having used business impact analysis and risk assessment processes to identify those areas where the organisation is most at risk of disruption, senior staff must decide what approach will be taken to address the situation: what must be done to protect its operations and to allow its aims and objectives to continue to be achieved. This will be the organisation's Business Resilience Strategy.

Several factors will affect this decision, but the most important are likely to be:

- The risk treatment options and the organisation's risk appetite
- the cost of the available options to mitigate risks
- the practical constraints that arise from the operational requirements of the organisation and the nature of the risk

14 See A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000, at http://theirm.org/ISO31000guide.htm

### 3.2.1 Types of Risk and Risk Treatment

Organisations will be faced with a range of potential risks and consequences. The risk that any potential event poses can be considered as a combination of its impact, how bad the consequences would be if the event occurred, and its likelihood, the probability of the event happening. For simplicity, events can be thought of in four groups which will require different risk treatments (although there will usually be a continuous spectrum of impacts and probabilities, and these will vary over time):

| | | |
|---|---|---|
| | **High Impact**<br>**Low Likelihood**<br><br>**➜ MEDIUM RISK** | **High Impact**<br>**High Likelihood**<br><br>**➜ HIGH RISK** |
| | **Low Impact**<br>**Low Likelihood**<br><br>**➜ LOW RISK** | **Low Impact**<br>**High Likelihood**<br><br>**➜ MEDIUM RISK** |

Risks that have a low likelihood and low impact – these may require no specific action and may be dealt with through generic arrangements.

Risks that have high likelihood and low impact – these may be regarded as a normal operational overhead, similar to 'wear and tear'. To some extent they should be expected, but they may still be monitored and managed to reduce likelihood, impact and costs. They should not constitute emergencies.

Risks that have high likelihood and high impact – these will require close attention. Organisations should normally have arrangements to mitigate these risks and to respond to their consequences. Under the Civil Contingencies Act, Category 1 responders have a duty to do so.

Risks that have low likelihood and high impact – these are often the most difficult risks for senior staff to determine a strategy for. Expending effort on risk reduction and response arrangements may seem a poor investment if the event does not occur, but the costs could be very high if it does. Because of the rarity of these events, detailed analysis may not be possible and the willingness of senior staff to 'live with the risk'– their 'risk appetite'– will be a significant factor.

### 3.2.2 Risk Treatment Options

There are a number of strategies that can be adopted to manage risks. These include:

- do nothing – in some instances senior managers may consider the risk to be acceptable
- mitigate – take steps in advance, to reduce the likelihood of the disruptive event, or to lessen its impact should it occur
- change, transfer or end the process where the risk has been identified – such decisions must be taken with regard to the organisation's key objectives and statutory responsibilities
- insurance – this may provide some financial compensation or support but will not aid the organisation's response and will not meet all losses, which may include its reputation, other non-financial impacts and human consequences
- plan for Business Resilience – combine risk reduction options, a clear understanding of the organisational priorities and an ability to respond effectively to disruptions, so that the loss of critical functions is minimised

The organisation may decide to combine several of these strategies and apply different approaches to different areas. Some activities might be given a high level of protection while others are left to 'take their chance'. The approach may vary according to the characteristics of the asset or process that is being protected. Stock, continuous processes, organisational reputation and personnel, will each need a different approach.

### 3.2.3 Support of Senior Staff and Resourcing

Business Resilience arrangements are unlikely to be effective without the clear support of senior staff. One of the most important strategic actions will be to demonstrate executive level commitment to developing and maintaining Business Resilience. Part of this will be a decision to resource this work at an appropriate level, so that staff working on resilience are sufficiently senior and their budgets are appropriate to achieve the desired outcomes.

Organisations should determine and provide the resources needed to establish, implement, operate and maintain their resilience arrangements to agreed standards. This should include identifying a person with executive level authority to be accountable for Business Resilience policy and implementation within the organisation.

This should be combined with formal arrangements to sign off plans and other arrangements, and ensuring that resilience priorities feature in:

- job descriptions of senior staff
- departmental aims and objectives
- reviews of work
- standing agendas of senior staff and departmental meetings
- policy statements

Visible leadership such as support at events and through formal and informal communications with other staff can provide further evidence of a real commitment to resilience and contribute to developing a culture where it is taken seriously at all levels.

## 3.3 Developing Business Resilience

### 3.3.1 Business Continuity Plans in Context

The ability to respond to and recover from disruptive incidents and emergencies is an essential part of any resilience capability. These parts of Business Resilience may be referred to in varying ways, but here we use the term 'business continuity' plans. A Business Continuity Plan provides the framework upon which an organisation can mobilise its response to a disruptive event or emergency. But a plan, on its own, will be of limited value. For the response to a disruption or emergency to be effective, plans must be combined with the other components of the organisation's response capability, including suitably trained staff, physical resources, information resources, response management structures, authority to act, a clear understanding of the aims and priorities of the organisation, systems for activating and standing down the response, etc.

For some organisations, it will be helpful to include sections on these within the plan, as well as addressing them when building a culture of organisational resilience and when training and exercising. The process of plan development itself is an important route to engage with staff about Business Resilience and to develop the organisational culture which will be necessary when the plan is activated.

Planning is also discussed in Preparing Scotland: Scottish Guidance on Resilience.

### 3.3.2 Content of the Plan

The Business Continuity Plan should address the following issues (note – this list is not exhaustive and will depend on the context):

- **Assessing disruptive incidents**, confirm the nature and extent of an incident.
- **Safety and welfare** of those affected, staff, public, special requirements.
- **Invoking** the response arrangements, including the plan itself, criteria and authority to deploy staff and the use of other resources.
- **Coordination** – who has the authority to make which decisions? How will decisions be communicated?
- **Objectives** – what are the recovery point and recovery time objectives? What are the organisational aims and objectives to be prioritised?
- **Solutions** – how both the cause and consequence of the disruptive event will be managed; procedures and activities for delivering the response and meeting the recovery objectives.
- **Personnel** – who is involved in delivering the response, how are they called out; what are their roles and what must they do?
- **Maintaining** a response for longer periods of time and **standing down** the response.
- **Communications** – about the response/other business, with staff, service users/ customers, other stakeholders, the general public; identifying a suitable spokesperson, using informal communications, social media, media advice.
- **Record keeping** – a method for recording key information about the incident, actions taken and decisions made.

The plan should have regard to the organisation's recovery objectives and, in turn, the key resources which underpin the delivery of its critical functions. They include:

- **People** – essential personnel to deliver agreed levels of service, of appropriate skill-mix and sufficient number.
- **Data** – critical information and documents about contracts, operating procedures, clients/service users/customers, staff.
- **Facilities** – working accommodation, alternative arrangements.
- **Communications** – information and communications technology requirements.
- **Equipment and technology** – where it is stored, how it is operated, what resources are needed to operate it, who can use it.

- **Supply chain and sub-contractors** – who are the suppliers/sub-contractors, what contractual arrangements are in place, how are they contacted, are alternatives available?
- **Stakeholder interests** – staff, owners, customers/service users, local community, political/legal interests.
- **Stock** and other **physical resources** needed to produce outputs or deliver services.

The nature of an emergency may require that some functions must be enhanced, or conversely reduced or suspended. The Business Continuity Plan should consider the operational processes for implementing decisions regarding functions. For example, if a function:

- needs to be enhanced in the event of an emergency, where would the additional resources come from?
- needs to be scaled down, how would the demands on it be managed?
- is withdrawn, how would staff and customers be informed?

### 3.3.3 Developing the Plan

In developing the plan, consideration should be given to:

- keeping the plan and the arrangements it describes short, simple and user-friendly
- ensuring the assumptions upon which it is founded are realistic and consider the findings of the Business Impact Analysis
- references to other sources of information and supporting documentation – databases, lists of key contacts, resources and suppliers
- what action plans and checklists are required
- ownership of key tasks – these should be reflected in job descriptions
- document management procedures
- effective communication with stakeholders and, where appropriate, the media
- aligning with relevant contingency arrangements both internal and external to the organisation

The structure, content and detail of the Business Continuity Plan will depend on the nature of the organisation and the risk environment in which it operates. In particularly large or complex organisations, it may be necessary to have discrete local or departmental plans which integrate into one high-level plan.

### 3.3.4 Using the Plan

It is impossible to anticipate all the circumstances of a disruption and to plan for these in detail. Trying to do so will consume resources without necessarily increasing Business Resilience. Plans should be designed for use in a flexible way, allowing for the lead responder's use of judgement to select which elements of the plan to apply and, where necessary, to improvise alternative solutions based on a knowledge of the organisation's strategic objectives.

Implementing the plan will require a combination of generic management skills, to carry out planned responses, and the skills of crisis management. *PAS 200:2011*, *Crisis Management* – Guidance and Good Practice, regards a crisis as 'inherently abnormal, unstable and complex'[15] and discusses the skills needed to manage such events. This includes management in the context of:

- previously unrecognised risks or situations
- too much, too little, ambiguous or false information
- threats to the norms and values of the organisation (and sometimes to its existence)
- increased pressure magnifying differences in leadership style and culture
- trade-offs and conflicts of interest
- close external scrutiny

Depending on the particular disruption or emergency, different combinations of crisis managementand other skills will be required. When developing plans, and when training and exercising Business Resilience arrangements, organisations should engage with staff who have experience and skills in crisis management, as part of a program to consider both more and less predictable events.

## 3.4 Reviewing and Maintaining Business Resilience

### 3.4.1 Managing the Resilience Programme

In order to be effective, resilience arrangements must be regarded as an integral part of an organisation's normal management processes. The commitment of senior managers is crucial in this because:

- decisions about attitudes to risk and service prioritisation can only be taken at the top level
- they have control over resource allocation

15 PAS 200:2011, Crisis Management http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030252035

- the Chief Executive and senior management team is responsible for ensuring that effective governance arrangements are in place
- they strongly influence the culture of an organisation

Experience has shown that it is helpful to give a member of the senior management team overall responsibility for Business Resilience and/or emergency planning. By being so appointed they will act as the champion for the processes, increase the profile of the disciplines and ensure that decisions are made at the appropriate level. They will also ensure that the programme of work to develop and maintain Business Resilience has sufficient breadth to encompass all those whose skills and knowledge are needed to make it successful.

It is important to gain the support and endorsement of the Chief Executive and senior management team at the end of each stage of the planning cycle. Critically, it should be the responsibility of senior management to provide the formal assurance that arrangements are robust and meet the requirements of corporate governance and the law.

The best approach for programme management will vary by organisation but the programme is most likely to succeed if an overall coordinator is appointed and reports directly to the senior managers responsible for Business Resilience and/or emergency planning. The coordinator(s) should have:

- a good understanding of the critical aspects of the business and its key personnel and dependencies
- an understanding of business continuity, integrated emergency management and related methodologies and awareness of emergency management issues
- an awareness of relationships with other responders and specialists in related fields[16]
- good programme management, communication, interpersonal and leadership skills

In addition it should be made clear that Business Resilience and emergency planning and response are part of every manager's routine responsibilities.

For larger organisations, it may be appropriate to consider establishing a team or network of responsible managers, who will be required to dedicate appropriate time to Business Resilience and have this reflected in their job descriptions. The team should be drawn from managers within key divisions and/or locations within the organisation. It should contain the right mix of skills and experience and comprise of individuals with the authority to make decisions and commit resources.

16 See section 2

### 3.4.2 Reviewing and Updating Business Resilience Arrangements

Business Resilience arrangements, including business continuity plans, should be reviewed regularly as circumstances change:

- as part of any significant change to operational arrangements to ensure that plans remain appropriate, e.g. when there are changes to equipment, buildings, processes, suppliers, etc.
- when the organisation's strategic objectives, risk treatments, or the role of a particular department is changed
- following resilience exercises, activation of plans or 'near miss' events, to incorporate lessons that have been identified
- to ensure they remain current and can respond to changes to risk assessments
- when new risks or response options are identified

### 3.4.3 Management Sign-off and Review

The managers with overall responsibility should ensure that there is a process in place to monitor and review the effectiveness of Business Resilience arrangements. Senior managers should consider the appropriateness of the Business Resilience policy, objectives and scope, and should approve these. They should also determine whether work on Business Resilience is being carried out in a satisfactory way and whether it meets the objectives they have agreed. When they are satisfied that the required quality has been met, the appropriate senior managers should sign off these documents.

The Business Resilience arrangements should be fully documented to enable management review and internal audit. This will include:

- the Business Resilience strategy and the scope and objectives of the Business Resilience programme
- critical activities and key outputs of the organisation
- Business Impact Analyses
- Risk Assessments
- Recovery Point Objectives
- Business Continuity and Incident Management Plans
- Incident Response Structure
- Training schedule

There should be appropriate document control arrangements for these items to ensure that relevant versions of applicable documents are available at points of use and revisions have been incorporated.

### 3.4.4 Exercising Business Resilience Arrangements

Arrangements should be put in place to exercise business continuity plans to ensure they remain effective. Exercising is discussed more fully in *Preparing Scotland*: *Scottish Exercise Guidance*[17] but the following points should be considered.

When developing an exercise programme, Category 1 responders will need to consider:

- risks, impacts and capabilities to be examined and the appropriate scope for exercises
- types of exercises to be used e.g. tabletop, live-play, single or multi-agency and at what level
- the involvement of senior management in developing, executing and quality-assuring the programme
- the process for delivering exercises, including resources and expertise for planning and release of staff for participation
- the relationship between the Business Resilience exercise programme and the exercising of emergency plans
- how lessons will be identified and used to improve resilience arrangements, e.g. through debriefing and the production of exercise reports

While there is an extensive number of scenarios and possible responses, the list of impacts and capabilities is limited. Generic issues to address will include:

- denial of access or damage to facilities
- loss of key staff/skills
- loss of critical systems
- loss of key resources
- mobilisation (invoking the plan and assembling key players)
- coordination of the response and decision making
- communications (both internal and external with a range of stakeholders and the media)

17 Preparing Scotland: Scottish Exercise Guidance http://www.readyscotland.org/

## 3.5 Embedding Business Resilience in the Organisational Culture

Having robust Business Resilience arrangements requires an ongoing engagement with staff, both to promote the concept of resilience (ensuring that skills and understanding are maintained) and to draw on their expertise to improve plans and responses. *Promoting* Business Resilience is therefore an important part of *having* Business Resilience, even within an organisation.

Risk management specialists have developed Risk Architectures[18] and management systems which can contribute to the development of Business Resilience. These include working with existing governance arrangements and identifying the responsibilities of different internal stakeholders, in order to embed methodologies in the organisational culture, e.g. identifying risk management responsibilities for:

- the CEO/Board
- the business unit manager
- individual employees
- the risk manager (and specialist risk management functions)
- internal audit manager

Organisations with arrangements of this type will be able to draw on them to help in the development of a culture of Business Resilience.

Promoting Business Resilience is discussed more fully in section 4.

18 A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000, at http://theirm.org/ISO31000guide.htm

# 4. Promoting Business Resilience

Local authorities are required to take appropriate steps to provide advice and assistance to businesses and other organisations about the continuance of their activities[19], including organisations within the commercial and voluntary sectors in their areas. Although this duty is placed uniquely on local authorities, other Category 1 responders are required to cooperate with them in their delivery of this duty. They will also contribute to the resilience of other organisations through various aspects of their normal work, including crime and fire prevention, warning and informing, and managing their supply chains to ensure their own resilience. It is recommended that local authorities fulfil this duty by promoting Business Resilience externally in the ways described in this guidance (see section 2), including giving due consideration to:

- the priorities, motivations and skills of individuals, teams and organisations
- the relationships with external organisations and their resilience capabilities
- the formal processes and tangible resources that deliver goods or services
- the risks the organisation faces and potential emergencies that might arise

It is recommended that local authorities approach the promotion of Business Resilience in a structured way that makes use of the full range of their established networks with external organisations. This should be a coordinated long-term effort, endorsed by senior staff, with the regular small-scale involvement of a wide range of their departments. Resilience specialists should support and facilitate an authority-wide programme as well as producing specialist initiatives that complement it. The aim should be to promote a culture of Business Resilience where key concepts become familiar and are seen as important in achieving normal business goals, so that individual organisations are then motivated to develop arrangements for themselves. Work in this area should focus on the following objectives:

- raising awareness of Business Resilience
- helping businesses, voluntary sector organisations and others engage with these issues and see their value
- providing reliable and appropriate information for organisations wishing to develop their Business Resilience

This approach is analogous to that of promoting community resilience amongst the general public or raising awareness of topical issues in specific communities. The particular format for this programme should be tailored to suit each area and the ways in which the local authority conducts its activity more generally. The approaches described below are recommended as building blocks from which to develop.

19 Civil Contingencies Act 4(1)

Because advice relating to Business Resilience is already available[20] and specific arrangements will vary between firms (and because implementation is best addressed by firms themselves once an interest in Business Resilience has developed), local authorities are advised to focus their efforts on engaging with businesses and other organisations, and on reinforcing the key principles of Business Resilience. It is not the role of local authorities to develop detailed plans or deliver in-depth training or intervention on the behalf of other organisations unless they specifically choose to do so.

## 4.1 Recommended Elements in a Strategy to Promote Business Resilience

### 4.1.1 Use Existing Networks

Local authorities are involved in many different networks through which they communicate with outside agencies and conduct their business. They should make full use of these to raise issues of Business Resilience and to communicate key messages in ways that are appropriate to the context. For some departments and services this might consist simply of making reference to resilience issues in some of the information they provide or as links on websites. For others, where advice is being given about ongoing projects or activities, or where services are being subcontracted, more specific advice or discussions are recommended. To assist with this, simple arrangements should be put in place to help staff throughout the local authority consider how resilience messages could be incorporated in communications, or resilience items added to agendas. This approach should include:

- briefing staff in different areas and departments about Business Resilience (stressing its relevance to their concerns and considering their comments)
- identifying key, generic Business Resilience messages
- encouraging resilience to be considered when reviewing communications and project plans and adding relevant items
- ensuring links to more detailed follow-up information are readily available
- providing advice and support to non-resilience specialists
- reporting on usage and follow-up

### 4.1.2 Get Support from Senior Staff

As with internal Business Resilience, promoting external Business Resilience requires the awareness and support of staff across the local authority. This is unlikely to be achieved without the visible support of executive level staff. One of the first priorities therefore should be:

20 See Annex 3

- to demonstrate to senior staff the direct benefit of promoting Business Resilience to issues that concern them.

This should include, demonstrating the likely cost-effectiveness of the proposed programme and securing their support. This should be followed up with regular reports of progress and selected opportunities to become directly involved.

### 4.1.3 Involve Staff from All Areas

Efforts should be made to actively engage staff across the local authority with the programme of Business Resilience promotion. This should follow the pattern of engagement with external organisations, i.e.:

- starting with the priorities of those being approached
- demonstrating the relevance of Business Resilience to their work
- explaining that a small effort in this area may have significant benefit for them and for the organisations with which they work
- demystifying the subject – keeping messages simple and dispelling myths
- following up with support and advice

### 4.1.4 Subcontracting and Joint Working

Local authorities can have a significant influence on the resilience of other organisations when awarding contracts or carrying out joint work with external partners. This includes agreements from the relatively small, such as letting of individual properties and local maintenance or supplies contracts, to large-scale infrastructure work. Granting contracts or engaging in joint work with organisations without having confidence in their resilience is a risk that local authorities should work to avoid. For critical services this would be likely to constitute a failure to observe statutory duties and, in other areas, this could potentially endanger service users, or result in financial and reputational losses. It is recommended that local authorities have processes in place which ensure that they consider the resilience of organisations with which they do business. The degree of scrutiny should be proportionate to the potential impacts of disruption to service provision of contractual failure.

Developing and implementing these procedures will require the combined efforts of resilience and procurement staff, with the support of service managers. They should take into account how potentially difficult choices between more reliable and less expensive service providers would be made and authorised. For work with smaller firms or voluntary organisations, these processes should be linked to the provision of advice about Business Resilience to enable the firm to fulfil the requirements of the local authority.

### 4.1.5 Resilience Specific Events and Groups

Interest groups can be a valuable addition to planning and promoting Business Resilience. As well as having groups within the local authority to take forward the programme of Business Resilience promotion, local authorities should consider establishing a group for external stakeholders including representatives of:

- Local business organisations from different sectors
- Chambers of commerce
- Voluntary sector representatives
- Local authority business liaison staff
- Local authority Business Resilience leads – including representatives from neighbouring local authorities
- Local authority communications team

The remit of this group could include:

- Raising awareness of Business Resilience
- Identifying, accessing and publicising specialist advice
- Providing critical feedback on local authority Business Resilience initiatives
- Identifying opportunities to promote Business Resilience (e.g. through local events and seasonal initiatives)
- Events planning, including training events

The specific format, scope and work programme should be developed according to local circumstances and should be of benefit to external members as well as to the local authority's Business Resilience aims. Although groups of this sort will be of value by providing a visible focus and access to networks for Business Resilience work, only a very small proportion of local businesses will be directly involved in or influenced by the group, so this approach should be used in conjunction with others of broader impact.

### 4.1.6 Combine Different Approaches According to Target Audiences

Local authorities should combine different approaches according to their circumstances and the audiences they are trying to reach. When choosing which combination of approaches to use, their likely success in reaching and influencing different types of business (and other organisations) should be considered. This will allow approaches to be prioritised and targeted appropriately. To do this, planners should match interventions to the size and type of business sectors[21] and voluntary organisations in their area as well as to the size and type of businesses themselves. Relying solely or largely on one approach, e.g. website, annual conference, is not recommended, as the impact on some target groups is likely to be low.

### 4.1.7 Business Focus

When introducing Business Resilience to external organisations, begin with messages that are relevant to their main concerns – showing an awareness of the circumstances in which they operate. As the initial aim, in most cases, will be to raise awareness of Business Resilience and to show that it is worthwhile, it will be helpful to start by gaining a clear understanding of the priorities of the organisations being approached and then considering how resilience relates to them, e.g. how their priorities might be disrupted and how the potential disruption could be avoided. Setting up meetings with a predetermined 'resilience agenda' may discourage individuals and organisations who do not yet see this as a priority. It is therefore recommended that Business Resilience is presented as contributing to the aims and objectives of organisations rather than as a separate, independent item.

### 4.1.8 Focus on the Probable Rather than the Extreme

Avoid presenting Business Resilience as being largely concerned with 'major incidents' and external emergencies. Rather, stress that it is about ensuring that the most important things continue to get done even in adverse circumstances. Although the requirements of the Civil Contingencies Act are based on 'emergency' capabilities, for some people, emphasising the response to external emergencies may make Business Resilience seem more remote or something that is the province of emergency responders only.

Developing skills in dealing with smaller or 'everyday' problems, which are more familiar and seem more plausible, may help to demonstrate the value of resilience to business people. These skills can then be extended to deal with more serious situations once interest has been engaged. Examples of this business-centred, rather than emergency-centred, approach include:

21 See Businesses in Scotland Key Facts: http://www.scotland.gov.uk/Topics/Statistics/Browse/Business/Corporate/KeyFacts

- encouraging leadership by normal service managers rather than by emergency professionals
- basing training on plausible, less sensational scenarios
- encouraging staff to solve problems and develop plans themselves

### 4.1.9 Dispelling Myths

Some businesses will have misunderstandings or may have had negative experiences regarding business continuity. These might include views that it is not cost-effective, is only for big businesses, or is concerned with issues that are peripheral to many businesses. These, and similar views, may form an obstacle to engaging with business and should be considered when approaching external organisations. An approach to Business Resilience that gives priority to the goals of the organisation, the concerns of the staff and a proportionate investment in resilience, is recommended to address these views.

### 4.1.10 Measuring Outputs and Assessing Effectiveness

It is recognised that measuring resilience is difficult and assessments must sometimes be subjective. Measuring the effectiveness of promoting Business Resilience will be challenging as it involves self-assessment by external agencies of their own resilience (which may involve bias or which they may not wish to share) and comparisons with a baseline assessment that may not exist. Feedback from small groups, e.g. people attending resilience events, may not reflect general opinion and should also be interpreted cautiously. As direct output measures may be unavailable, local authorities should consider other measures to assess the effectiveness of their interventions, including:

- whether they have an active programme of engagement with business and other organisations.
- whether the targets of the programme match the pattern of local business and voluntary sector activity.
- whether the programme is integrated with other related areas of work e.g. promoting community resilience, internal Business Resilience, promoting local enterprise, and with the core activities of departments across the local authority.
- whether the programme is well-structured and has support from senior management.
- whether procurement and subcontracting processes place significant weight on Business Resilience when awarding contracts.

### 4.1.11 Coordinate the Different Components of the Approach

The different components of the chosen approach to Business Resilience promotion should be coordinated and managed, including:

- ensure top level support for the proposed approach.
- identify a suitable manager for the programme – important skills will include: project management skills, an ability to work across departments and with external business and voluntary organisations, and to present Business Resilience as relevant to normal business objectives.
- agree responsibilities for implementing the programme of work in each part of the local authority – develop an internal network of people at middle-management level who can act as a programme board, advise on implementation in their areas and ensure recommendations are applied by colleagues.
- identify external links and networks used by each department and consider how these can be used effectively.
- agree how procurement will consider and take account of Business Resilience.
- agree key Business Resilience messages and advice, where and how these will be publicised and identify reliable sources of more detailed advice.
- identify and utilise connections with other local authority work, resilience specific events and opportunities provided by heightened media coverage of resilience.
- involve others – work with partner organisations and representatives of stakeholders when developing and reviewing this work.
- develop arrangements to confirm that this work is being taken forward, to provide support and leadership for staff carrying out this work and to identify and learn lessons.

# 5. Annexes

## Annex 1: The Legislative Context

The statutory duties concerning:

- the ability of Category 1 organisations to continue to be able to perform their functions[22],
- the provision, by local authorities, of advice and assistance to businesses and other organisations about the continuance of their activities.

relate primarily to their ability to meet the challenges of emergencies. 'Emergencies' are defined in the Act[23] as events or situations, including war and terrorism, which threaten 'serious damage' to human welfare, the environment or security. The National Risk Register[24] sets out the most serious risks which could lead to such events.

However, these requirements are not limited to their ability to respond to the emergency itself but include the effects of the emergency on the organisation. In order to develop and fulfil the requirements of the Act, planners will therefore need to consider related non-emergency Business Resilience. This may be significant in its own right but also because of its relevance to capabilities that support emergency functions. These include the management of the indirect effects of emergencies, the ability of organisations to sustain emergency capabilities and to recovery (in preparation for subsequent emergencies) and also to some aspects of work with partner organisations.

### 5.1 Having Business Resilience

The Civil Contingencies Act 2004 and the Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005 set out the following duties in relation to being able to continue to be able to perform organisational functions.[25]

All Category 1 responders must maintain plans to ensure:

- that if an emergency occurs, as far as this is reasonably practicable, they can continue to perform their functions, and
- that if an emergency occurs or is likely to occur, so far as necessary or desirable, they can perform their roles of preventing the emergency; reducing, controlling or mitigating its effects; or taking other action in connection with it.

These two duties can be summarised as: having appropriate level of Business Resilience to continue priority activities and to respond to the emergency.

22 Civil Contingencies Act (2004) 2 (1) (c)-(d)

23 Civil Contingencies Act 1(1)-(5)

24 See National Risk Register https://www.gov.uk/government/publications/national-risk-register-for-civil-emergencies-2013-edition

25 See section 2(1)(c)-(d) and 4(1) of the Act and Part 7 of the Regulations

The regulations also set out some aspects of how these duties must be performed, stating that Category 1 responders:

- must have regard to any relevant risk assessments that have been carried out as part of the duties under the Act
- may maintain plans which relate to a particular emergency or a particular kind of emergency
- must maintain plans which relate to more than one emergency or more than one kind of emergency
- must, when maintaining plans, include arrangements to exercise the plan and to provide training for an appropriate number of suitable staff
- must have regard to any relevant arrangements to warn and to provide information the public about emergencies

### 5.1.1 Voluntary Sector Organisations

In performing the above duties, Category 1 responders must have regard to the activities of voluntary organisations which are relevant to emergencies and which operate their area. In this context, this means those whose purpose is to prevent an emergency, or to reduce, control or mitigate its effects, or those with a similar role. Whether or not the voluntary organisation carries out other functions in addition to these, does not affect this duty.

## 5.2 Promoting Business Resilience

Local authorities have additional duties connected with the provision of advice and assistance to other organisations about the continuance of their activities when faced with emergencies[26]. Local authorities:

- must provide advice and assistance to businesses at large about continuing their activities when affected by emergencies
- may provide advice and assistance to individual businesses about continuing their activities when affected by emergencies
- may provide advice and assistance to businesses in identifying and obtaining help from a competent and experienced business continuity consultant

26 These are set out in of Part 7 of the Regulations and arise from section 4(1) of the Act, Where they are referred to as to as 'relevant responders'.

The regulations also set out some aspects of how these duties must be performed. Local authorities:

- must consider relevant community risk registers when doing these things
- must consider any advice and assistance being provided by other responders in their area and need not duplicate that work
- must co-operate with other local authorities in the same partnership area in fulfilling these duties
- may perform these duties jointly with another responder or may make arrangements with another responder to perform the duty on its behalf
- may charge for the cost of providing advice and assistance on a cost recovery basis

These duties refer to 'commercial' activities and 'emergencies'. 'Commercial' is not a straightforward term to define. It should not be taken narrowly to mean only private sector businesses operating for a profit. Others, including charities, building societies and credit unions, carry out commercial activities; they operate as businesses, generate financial benefits and should be considered in performing this duty.

However, this does not mean that local authorities should concentrate solely on emergencies, as defined this way, when working to promote Business Resilience. Thankfully, most organisations will have direct experience of serious emergencies only rarely, and perhaps never in the case of those due to hostilities. Discussing a broader range of more commonplace disruptions is likely to be a more productive way to engage businesses, as very severe emergencies may seem less credible, too difficult to manage, or a problem for the emergency services. Pursuing this indirect route may lead from resilience against smaller disruptions to a greater ability to deal with higher impact events, although the approach taken should be tailored to the circumstances.

### 5.2.1 Voluntary Sector Organisations

Local authorities have equivalent duties to provide advice and assistance to voluntary organisations, with the exception that they need only provide this to those voluntary organisations which they consider 'appropriate'. In determining whether a voluntary organisation is 'appropriate' in this context, the regulations set out the following factors which must be considered:

- the nature and extent of activities the organisation carries out, particularly, the extent to which the organisation contributes to (i) the prevention of emergencies; (ii) the reduction, control or mitigation of the effects of an emergency; (iii) other actions in connection with an emergency; (iv) social welfare.
- the size of the organisation (e.g. staff employed and turnover).

- whether the advice and assistance is likely to improve the organisation's resilience in the event of an emergency.

As the voluntary sector is large and diverse, it is unrealistic to expect local authorities to provide advice and assistance for all organisations. Rather, they should prioritise their efforts to those where its uptake would be likely to strengthen emergency resilience or social welfare in their region.

### 5.2.2 Geographic Scope

These local authority duties apply only in relation to businesses and voluntary organisations which operate in the local authority's area. This includes those which operate in the area for a period of time without being resident, for example, music festivals or major construction projects.

The additional duties placed on local authorities can be summarised as:
**taking appropriate steps to promote Business Resilience within the commercial and voluntary sectors in their area.**

### 5.2.3 Other Category 1 Responders and Promoting Business Resilience

The regulations require other Category 1 responders in the area to cooperate with local authorities who are delivering these duties. In addition to initiatives led by local authorities, other Category 1 responders can promote Business Resilience in several ways:

- by influencing their suppliers and sub-contractors, thereby also improving the resilience of the Category 1 responder itself
- through the normal work of the organisation which will have Business Resilience consequences, e.g. crime prevention and fire prevention initiatives
- by 'warning and informing' work which makes organisations and the public more aware of risks

## Annex 2: Selected Glossary

**Business Continuity** – Strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level.

**Business Impact Analysis** – The process of determining the impacts on the organisation from interruptions to business operations or processes.

**Business Resilience** – A holistic approach, demonstrating how resilience can contribute to the overall strategic aims and objectives of an organisation. It extends the scope of business continuity management and emphasises the human and cultural aspects.

**Community Resilience** – Communities and individuals harnessing local resources and expertise to help themselves in an emergency, in a way that complements the response of emergency responders.

**Crisis** – An abnormal situation which threatens the operations, staff, customers or reputation of an enterprise.

**Enterprise Risk Management** – (ERM) – a strategic business discipline that supports the achievement of an organisation's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks.

**Incident Response Structure** – Organised arrangements to provide effective direction, coordination and deployment of resources required to respond to an incident.

**Maximum Tolerable Period of Disruption (or outage)** – Maximum Tolerable Period of Disruption is the maximum allowable time that the organisation's key products or services is made unavailable or cannot be delivered before its impact is deemed as unacceptable.

**Recovery Phase** – Process of rebuilding, restoring and rehabilitating following an emergency or disaster, and continuing until the disruption has been rectified, demands on services have been returned to normal levels, and the needs of those affected have been met.

**Recovery Point Objective (RPO)** – The point in which information used by an activity must be restored to enable that activity to operate on resumption.

**Recovery Time Objective** – Recovery Time Objective (RTO) refers to the maximum acceptable length of time that can elapse before the lack of a business function severely impacts the organisation.

**Risk Appetite** – Total amount of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time.

**Risk Treatment** – Process of determining those risks that should be controlled (by reducing their likelihood and/or putting impact mitigation measures in place) and those that will be tolerated at their currently assessed level.

**Single Point of Failure (SPOF)** – The part of a service/activity/process whose failure would lead to the total failure of a key business activity.

**Surge Capacity Planning** – Development of arrangements to deliver an increased volume of those goods or services that are normally provided.

## Annex 3: Further Reading and References

How Prepared Are You? Business Continuity Management Toolkit

Business Continuity Guide for Small Businesses

ISO 22301 Business Continuity Management

Ready Scotland

Preparing Scotland Guidance




First published by the Scottish Government, November 2013
ISBN: 978-1-78412-024-5 (web only)

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

Produced for the Scottish Government by APS Group Scotland
DPPAS15058 (11/13)

Published by the Scottish Government, November 2013

**w w w . s c o t l a n d . g o v . u k**