Auditing Business Continuity Management Plans
Assess and Improve Your Performance Against ISO 22301
Second Edition
Auditing Business Continuity Management Plans

Assess and Improve Your Performance Against ISO 22301

Second Edition

John Silltow
# Contents

*Introduction* vii

1. Overview of business continuity and the role of audit 1
2. Setting the business continuity management policy 17
3. Developing the business continuity programme 37
4. Understanding the organization and its continuity requirements 61
5. Developing the business continuity strategy 99
6. Incident recovery 129
7. The continuity plans 153
8. Exercising and maintaining the continuity plans 183
9. Bringing business continuity into the culture 205

**Appendix 1** Certification to BS ISO 22301 217

**Appendix 2** Risk 221

**Appendix 3** Auditing the business continuity life cycle 233

**Appendix 4** Auditing the project 241

**Appendix 5** Document management 247

**Appendix 6** Gold-silver-bronze command structure 251

**Appendix 7** Business continuity policy statement 255

**Further reading** 267
The purpose of this book is simple: it is to help make organizations better prepared for incidents and their recovery. How it goes about this is a little more complex.

Most managers will be familiar with the concept of internal audit. Its role is to assess and evaluate the activities and functions of an organization against standards, guidelines, best practice and regulatory issues, to form a view on whether those activities or functions are performing effectively. Audit can then provide recommendations or views on how functions and processes may be changed to improve efficiency or reduce risks. Using the results of these audit reviews from across the organization the head of audit can then provide an assurance statement to top management.

This role uniquely places internal auditors in the situation of having to understand systems and processes at a sufficient depth to make recommendations on their improvement as well as being conscious of the risks that both drive an organization or function forward as well as threatening its very existence. Their views have to be balanced with operational needs in formulating their assurance statements.

This book is therefore written with the internal auditor as the core focus. It achieves its aims by providing the depth of information and knowledge that is needed to understand each part of the business continuity process. It also looks at the risks and threats that exist.

There are other players within and external to an organization that will have a direct or review role within the business continuity project and programmes. Few of them will work to the same depth as internal audit and all of them will find some value in this book, perhaps from a better understanding of an issue or a greater appreciation of how one thing impacts another.

Internal audit is not an operational function responsible for making decisions but rather it is charged with evaluating operational decisions in relation to the achievement of organizational objectives. When it comes to a project as large and complex as business continuity there is a good case for audit being a part
of the project team, albeit in an advisory role. It still remains for the business and the appropriate managers to make the decisions, but by using their audit team as advisers they will have on board experts in risk and control who will input information and ideas that may not have been considered before.

Whilst the book has been built around experience and research, it also draws on the International Standard ISO 22300 family. This set of Standards generically entitled Societal security form a comprehensive basis on which to build a business continuity management system. These Standards have been developed from the British Standard BS 25999, Business continuity management and other related Standards as well as contributions from many people and organizations around the world. Certification to ISO 22301:2012 Societal security — Business continuity management systems — Requirements can be achieved by any organization.

Every section of the book provides an audit view with suggestions for some of the subject areas that can be reviewed. Some of these are supplemented by ‘audit scope’ ideas to help frame a potential audit and get the best out of any reviews. Many suggestions cover issues that the business continuity project team will also look at. This is not to imply that work should be unnecessarily re-performed, merely that where aspects are important auditors should be sure that the work has been, or will be, completed. In some cases who actually achieves the piece of work will not be particularly important.

Examples from real life are used to highlight some of the issues. Mostly these are not the headline-grabbing incidents but those where staff were out of their depth or unhappy or where nobody thought ahead to the consequences of a particular decision. They all illustrate how easy it is to ‘just miss’ and end up either poorly prepared or with an incident.

Inevitably there is overlap in the book between chapters. Business continuity is a relatively simple concept but the ramifications are complex. This means that the same items come up from different perspectives as the story evolves. The overlap should, however, reinforce the message and allow for different perceptions to be explored. It also allows for the reader to dip into chapters without reading the book right through. This can be very useful if you have a simple audit to do and just need some quick ideas.
1
Overview of business continuity and the role of audit

Setting the scene

This chapter provides an overview of business continuity planning and looks at the role of audit within the business continuity management framework. It considers the different types of audit and their place in the process. From this it highlights that the internal auditor conducts the most detailed review work and therefore has most input to a business continuity programme.

Introduction

Business continuity management is not about creating a great plan that, once written, sits in a desk drawer and gathers dust. It is not about creating a great plan and not telling anyone about it. It’s not about letting consultants build a great plan for you and then expecting all staff to welcome it with open arms and immediately adopt it.

It is about working with staff, unions, emergency services, partners, suppliers and many others to build a plan that all can work with and all can see the sense in. It’s about involving the emergency services who just may have to rescue your staff. It’s about communicating with your staff who may, one morning, find their place of work is no longer accessible due to flooding. It’s about reassuring your customers who have paid you to provide a service and you cannot because your factory has no power. It’s about satisfying your neighbours and the public at large that while your business is burning down you are minimizing the impact upon them. It’s about telling people what is going on in a full and positive manner.
Essentially business continuity management involves:

- identifying the organization’s key products and services;
- identifying the prioritized activities and resources required to deliver them;
- evaluating the threats to these activities and their dependencies;
- putting arrangements in place to resume these activities following an incident;
- making sure that these arrangements will be effective in all circumstances.

This is not a small exercise and should not be considered a quick task.

**Overview of business continuity**

Business continuity management can be defined as the management process that provides a framework for building capability that safeguards the objectives of the organization including its obligations.

Essentially therefore business continuity planning continually confronts the likelihood or otherwise of an incident. Such a business interruption may be something minor or major, but the important thing is that there are processes in place to enable management control to be gained when it does occur.

Depending on the length or severity of the interruption, significant consequences or the very sustainability of the organization may hinge on management’s ability to re-establish critical business functions. Usually these business functions have been established and developed over a period of years, but management must rebuild and get them up and running within hours or days of the business interruption. This is a difficult situation and rebuilding the complex business environment in a timely manner requires a well thought-out plan in place ready to be executed.

Business continuity planning is therefore the main answer to an unexpected business interruption. It is a proactive management-led incident management programme driven by business requirements.

There is, however, one other aspect that should not be overlooked. The very act of reviewing the business and its processes will identify areas that need to be strengthened or altered to enable them to cope. By its very nature, therefore, an exercise to build business continuity in an organization will strengthen that organization against incidents.

*Consider the not-for-profit organization with three separate buildings. When it decided to implement a business continuity system, its review of
Overview of business continuity and the role of audit

IT systems identified that all IT traffic was routed through building 1. This meant it had both a traffic bottleneck and a single point of failure. These issues automatically increased its chances of an incident. Consequently it introduced a new connection between buildings 2 and 3 that meant that voice and data traffic could then be routed directly between buildings or re-routed if there was a problem. As a result it increased its resilience before it even developed any business continuity plans.

No organization can have complete control over the business environment in which it operates. There are a number of issues that will be outside its control, from the weather, through the utility services to the attitudes of staff and customers.

There are external influences, such as regulations and industry guidelines, that support the promotion of greater resilience among organizations, public agencies and the wider local community.

There are also the standard external threats for all organizations, such as fire, flood, power outages, epidemics and terrorism. These do not discriminate between the not-for-profit, private or public sector, or between large, medium and small organizations. However, all those sectors and businesses have their own threats and risks in addition, which need to be faced as part of the price of doing business.

Consequently, every organization needs to have in place a plan to recover key business processes following an incident. The recovery plan, however, has to consider not just likely events, but also those that may be considered unlikely or perhaps even impossible.

A process like scenario planning that formulates strategies for organizations that are way beyond that organization’s everyday business assumptions may be useful to outline some of these ‘unthinkable’ options. With this process the business works through the key ‘what if’ scenarios that face it to develop solutions. Most of these will be the normal extensions to business risk, such as a key supplier collapsing or a new rival product, but some will be pitched well beyond this. Considerations such as currency devaluation, finite supplies of a key commodity running out and sequestration of assets may be part of these ‘what if’ scenarios.

Just as the organization can develop strategies to deal with all these ‘what if’ options, it can also build some or all of these into its business continuity management processes to ensure it can survive if the worst happens.
Some of these ‘what if’ options are global in nature and there are recommen-
dations that all businesses include such threats in their business continuity
plans. An example of this is the risk of a bird-flu pandemic. Much has been
published on this subject to help all businesses understand this risk and take
steps to ensure that there is a continuity plan in place to prevent it from
destroying the business.

The other point about a business continuity process is that it needs to match
the organization. It may sound obvious, but a large organization needs a large
plan while a small organization needs a small one. This aspect clearly has an
impact on the cost and time involved in building a plan and in the recovery
processes put in place.

While dealing with the incidents that are likely to affect an organization, the
plan must be realistic and achievable. Failure to do this will lead to the plan
falling into disuse and being unusable if the time comes to rely on it.

The plan creates an incident management team empowered by top managment
or equivalent to control any interruptions of the business. Properly constructed,
this incident management team has the capability of responding appropriately
to any interruption of any scale. If the incident is then found to be one that
was envisaged and planned for, the appropriate business continuity plan can
be invoked.

As a management controlled programme, a business continuity plan reduces,
by a variety of means, the consequences of a business interruption to a level
acceptable to management. Because of the processes involved in building the
plan, it also provides a tested approach that, when invoked, will enable a
known and agreed level of recovery to take place.

This can be achieved because each business function has been analysed to
define the consequences of an outage of service. These consequences are then
assessed by management, which defines the point at which the consequences
are unacceptable. That point becomes the recovery time frame, although it is
also known as the recovery time objective. Each business function may have
a separate recovery time objective.

The business continuity plan identifies the recovery alternatives that cost-
effectively restore critical business functions within an acceptable time frame.
In doing this it needs to take into account the time that the business process can
remain functioning in a limited way. This duration is known as the maximum
tolerable period of disruption. At the end of that period the business function
will no longer be recoverable.
Overview of business continuity and the role of audit

Management authorizes and approves the recovery solutions. As a result, the recovery plan is developed around the recovery solution authorized by management.

The business continuity plan objectives are to:

- ensure continuity and survival of the business;
- provide protection of corporate assets;
- provide management control of risks and exposures;
- provide preventative measures where appropriate;
- take proactive management control of any business interruption.

Business continuity planning provides a balance between acceptable potential losses and acceptable one-time and annual costs. The business continuity plan can also assist management in providing customer confidence and service satisfaction, as incident management control can assist the business in maintaining market share, and can provide the basis to promote a positive image.

Subsequent chapters will deal with all these issues in greater detail but as a pictorial overview to the processes involved, Figure 1 may prove helpful.
NOTE: The numbers indicate the relevant chapters

Figure 1 Business continuity process flow diagram
The role of audit

Organizations are structured to have several lines of defence, although they may not generally consider it that way. These are shown in Figure 2 below.

Essentially, the first line is the operational managers and staff who have the day-to-day responsibility for managing the organization’s risks. The risk management functions look after the second line with internal audit providing an independent assessment of work of the first two lines.

The first line of defence is operational managers and staff. They have day-to-day responsibility for managing risk. The first line implement policies, procedures, processes and controls.

The second line of defence is the risk committee, risk managers, compliance and regulatory inspectors. Risk committees and risk managers coordinate, facilitate and oversee the management of risk and compliance within the organization’s risk appetite.

The third line of defence is internal audit activity supported by the audit committee. Internal audit provide independent assurance in respect of the effectiveness of governance, risk management and control.

Figure 2 The three lines of defence

The definition of ‘audit’ contained in ISO 22301, is:

‘Systematic, independent and documental process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.’
There are two main categories of audit that most organizations will be familiar with:

**Internal audit**

Internal audit is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It provides assurance that the risks the organization is exposed to are being effectively managed. These risks include those relating to business continuity management. The role, responsibilities and accountability of internal audit is defined in its charter, which is approved by the audit committee and senior management.

Larger organizations may also have other functions such as compliance, operational risk, quality and health and safety, which also contribute to the assurance process.

**External audit**

External audit is a statutory function charged with ensuring the accuracy and veracity of the annual report and accounts. To achieve this, the external auditors will undertake their own assurance work, which can include an assessment of business continuity plans. They will also place reliance to a greater or lesser degree on the work conducted by the internal audit function, if there is one.

**Other review bodies**

Whilst there are a number of potential review bodies, for business continuity purposes there are some others that need specifically to be considered.

**Compliance**

Compliance auditing is the second line of defence. It has the role of examining and evaluating defined activities of an organization to measure adherence
Overview of business continuity and the role of audit

to legal, regulatory, contractual and procedural obligations. Essentially compliance auditing determines whether a process or transaction has or has not followed applicable rules. If rules are not complied with, the auditor determines the cause and recommends ways to prevent future non-compliances.

The rules being tested can be:

- those created by the organization for itself through its policies, plans and procedures;
- those imposed on the organization through external laws and regulations; or
- those external standards that the organization has chosen to follow (e.g. ISO 22301).

Many organizations have a specific compliance function. That function may have its own independent reporting line or it may become a part of internal audit but separate to the day-to-day work. Sitting within audit can make compliance functions more powerful as they can then also report through the audit committee.

Certification audit

Organizations wishing to obtain certification to ISO 22301 will need to undergo audits by an external assessor (or certification body) approved by their country’s accreditation body. These accreditation bodies are members of the International Accreditation Forum (IAF), which has established Multilateral Recognition Arrangements (MLA) between its accreditation body members. These reduce risk to business and its customers by ensuring that an accredited certificate may be relied upon anywhere in the world.

The compliance audits by the certification body take place at specific stages of the project and then regularly after the certification is awarded (Appendix 1). In performing these compliance audits the certification body can rely on the work undertaken by other auditors, including internal, external and compliance auditors.

Essentially a certification audit is similar to a compliance audit. The difference is that the auditors are acting on behalf of the standards body and have been accredited to undertake this specific task.
Organization

ISO 22301 puts a strong focus on the organization having control systems in place to monitor, measure and analyse performance and thus to be able to address adverse trends or results. Such nonconformities need to be identified and then suitable action taken to control, contain or correct them, along with any consequences arising.

Suitable documentation needs to be developed to enable issues and findings to be recorded as well as logging any actions taken. Such documentation needs to be retained and protected against any future need.

The Standard also expects top management to review the business continuity management system (BCMS) at planned intervals to ensure its continuing suitability, adequacy and effectiveness. These reviews should take into account follow-up actions from previous reviews as well as the need for any change or opportunity for improvement.

In addition, the organization may choose to have a dedicated team to undertake self-assessment audits and/or to employ external consultants for all or part of the project. Depending upon the contract, the external consultants may then be responsible for all detailed review and audit work or they in turn may work with others, such as internal audit and other business functions.

Focus on internal audit

Internal audit, unlike any other review body noted, has a remit to provide assurance to management. For this reason, internal audit will have to undertake a greater depth of review to be able to fully understand how the various processes and activities operate and interact. It cannot provide any valid assurance until it has done so. The primary focus of this book, therefore, is on the role of the internal audit function. However, certification auditors, compliance auditors, external auditors, consultants and others in the business continuity sphere will also find this material very useful.

That internal audit is expected to undertake detailed audit reviews does not prevent others from undertaking the same or similar work. However, directing this book at this more detailed level provides a wider scope for ensuring that the business continuity process is appropriate, robust and fit for purpose.
Providing assurance

There are three primary roles for internal audit within business continuity:

- to provide independent and objective assurance to management on the business continuity management framework;
- to contribute as consultants to the business continuity process if required;
- to take part in the organizational approach to contingency planning and consider the risks to its own activities.

The primary purpose of providing assurance to management is a simple concept that is identified in the audit charter and underpinned by a wide variety of activities designed to ensure that when audit provides assurance to management it knows:

- what aspects are encompassed in the business it is reporting on;
- that the process conforms (as far as possible) to best practice in the sector or marketplace;
- that risks taken are commensurate with the risk appetite of the business; and
- that mitigating strategies, offsetting activities and/or residual risks are known and recorded.

Assurance mapping

While top management is responsible for ensuring that business-critical risks are being assured and adequately managed, the task of assurance is often provided by a broad range of functions.

For example, assurance can be provided from a number of sources both internal and external and can provide confidence to stakeholders, comfort to managers and trust and credibility to the organization. However, ineffective or over assurance can become burdensome, impacting on the effectiveness of front line service delivery.

Increasingly, therefore, ‘assurance maps’ are being requested by audit committees who want to take comfort in the knowledge that all of the pieces of the assurance jigsaw are joined up, with no gaps in coverage and the minimum of assurance overlaps.

An assurance map is therefore a tool to ensure key risks are assured across the organization.
The assurance mapping process is concerned with identifying all of the sources of assurance received across the organization. Once identified, the information can then be collated and analysed in order to provide a better understanding of the roles and scope of the work undertaken by the various assurance providers both within and external to the organization.

The primary drivers for the assurance mapping process are:

- To inform internal audit planning – through the identification of assurance provided from other review and inspection bodies, to avoid duplication and identify potential assurance gaps to key risk areas.
- To inform the annual governance statement – this requires an indication of the level of assurance that the systems and processes that comprise the organization’s governance arrangements can provide.
- To ensure sources of assurance are properly reported and that appropriate action is being taken on risk and internal control related issues identified by the internal and external auditors and other review and inspection bodies.

**Auditors as consultants**

Because internal audit is part of the business and is aware of the day-to-day constraints and issues, as well as the risks and risk appetite of the business, it is well placed to be part of any business continuity programme.

The role of internal audit, however, is advisory and as such it cannot make operational decisions, as this would conflict with its independence. For example if an auditor made the decision that a business would use a specific supplier for stationery purchases, then the audit department would have lost its independence on the matter and could not subsequently review that decision.

It is recognized within the audit profession that while there is an absolute requirement for independence, there may also be a wealth of skills within the audit department that management could use to its advantage in undertaking fairly specific operational tasks. In view of this it is possible for an auditor to be engaged by management as a ‘consultant’ to undertake one or more tasks. The difference here is that the consultancy is covered by a contract drawn up by management, and that the auditor is acting in his or her own capacity. Any operational decisions they make are under that contract and this does not prevent another auditor from subsequently reviewing those decisions and having the independence to make a judgement on them.
Overview of business continuity and the role of audit

Business continuity for the audit function

The business continuity plan for internal audit, as for most other support functions, should be based upon developing a controlled resumption of the service as space and equipment becomes available and as the business returns to full operation.

In the short term, during a recovery, it may be appropriate to release internal audit staff to the business to assist in operational activities or to carry out special reviews to ensure that any revised procedures introduced during the emergency still provide an adequate degree of operational control.

Risk

Within business continuity there is frequent mention of ‘risk’. It is therefore worth considering this aspect a little further here. A fuller overview of risk and some of the tools for assessing it are discussed in Appendix 2.

Although risk appears in business continuity terms as a threat to an organization or system, it can also be a positive. Identifying a risk (or weakness) may provide the organization with the opportunity to change the system, or process, involved and turn the risk to an advantage (an opportunity). So undertaking the investigations and analyses required to determine a business continuity system may lead to changes in organizational behaviour to the advantage of the organization, its staff and systems.

A risk assessment is required to identify key sources of risk within an organization, reduce them where possible and ultimately provide the basis for the development of containment and/or recovery measures. In order to achieve this, it is important to understand the likelihood of a particular threat occurring, identify its causes and evaluate the potential effects on the business.

Of course, these factors can change markedly between risks, organizations and sectors. For example a communications failure could cause serious losses in a matter of minutes within a financial institution but may not impact a manufacturing process for some hours. Conversely a delivery delay could wreak havoc in a ‘just in time’ manufacturing environment while only mildly affecting a financial institution.
All organizations therefore need to be aware of the risks that they face in everyday trading. These will include:

- **business risks** – e.g. a competing business;
- **data risks** – e.g. loss or compromise of data;
- **environmental risks** – e.g. weather-related activities like floods;
- **regulatory risks** – e.g. new legislation that affects business trading;
- **personnel risks** – e.g. low morale among staff leading to poor customer service;
- **reputational risk** – e.g. product recalls that lead to loss of confidence in a brand.

There are many types of risks and it must be emphasized that the above list is just a small selection of high-level ones.

Risk is therefore the awareness that something threatens the organization. The next stage is to consider how this risk could materialize. The above list provides an example in each selected category but there are many others. One that should never be overlooked is the risk that your surrounding businesses and neighbours bring.

Consider the following real examples.

- *The head office of a financial institution was located very close to an army reserve base. Any bomb threat or other incident at the army facility closed the road leading to the financial institution.*
- *In another location a bomb had actually exploded. The area cordoned-off by the emergency services encompassed several blocks. Due to the dangerous structures that needed to be demolished, local businesses, even though unaffected by the original incident, were unable to recover materials from their sites or to serve customers. Several went out of business as the cordon was maintained for six months.*
- *The data centre for one company was located on the first floor above the kitchen of a pizza parlour. The main computer was in fact directly above the cooking ranges. The only exit stairs from the data centre also went through the kitchen.*
- *Company X purchased a site to develop as a dark site, a location where their mainframe computer systems would be. The systems were largely unattended and operated from a control bridge at head office many kilometres distant. There were therefore several risks to this site and the company made the decision not to advertise who owned the site.*
Overview of business continuity and the role of audit

Unfortunately no one mentioned this to the seller’s agents who put up a ‘sold to company X’ board.

- A subsequent incident at this same site showed that the electronic systems had been designed by the systems’ contractors to fail ‘safe’. To fail safe meant no one got trapped inside. Unfortunately for company X this also meant that all the security systems switched off and the doors and gates were unlocked.

Apart from commiserating with company X, these examples highlight the range of risks that can occur and particularly that what may be a good recovery model in one way, can lead to problems in another direction. It is for this reason (and others) that real testing of continuity plans has to be undertaken. Desk checking is just not thorough enough.

Another point to emphasize is that the smaller the business, the more likely an incident is to prove fatal to the business. This is due to the lack of alternative options open to a smaller business. For example they cannot quickly change their business model. They are also less likely to have the cash flow to support extended operation without money coming in. Unfortunately, they are also less likely to have invested in a robust recovery plan due to the cost of that process.

Each organization needs to consider what exactly it is that makes a risk materialize and when the impact of that risk becomes an issue. These aspects will vary between organizations and it is said that one man’s risk is another man’s opportunity.

Performance evaluation and monitoring

ISO 22301 identifies the need for business continuity to be managed, monitored and reviewed. The onus for this starts with top management and works down, ensuring that everyone in the organization is aware of their responsibilities for and within the business continuity framework. As part of this process, there is a need to document events and issues so that there is a clear record of what has happened and how it has been handled.

Conversely, there is also a need to document events that haven’t happened and issues that have been considered but not pursued. All of these aspects are considered further in the following chapters.
PDCA model

ISO 22301 applies the ‘Plan–Do–Check–Act’ (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization’s BCMS.

This ensures a degree of consistency with other management systems standards and thereby supports consistent and integrated implementation and operation with related management systems such as:

- ISO 9001;
- ISO 14001;
- ISO/IEC 20000-1;
- ISO/IEC 27001;
- ISO 28000.

The relationship to the PDCA model and the issues discussed in each section are highlighted at the beginning of each chapter.

The PDCA model itself is discussed further in Chapter 3 and Appendix 3.