PASAI

"Pacific Auditors Working Together"

CAROSAI

Towards Greater Accountability

Business continuity planning

A guide for Supreme Audit Institutions

Design and Production by NAO Communications
DG Ref: 009978-001 | Printed by SLS Print

Business continuity planning

A guide for Supreme Audit Institutions

Contents

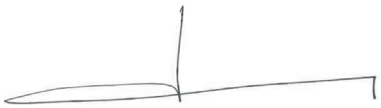
Foreword

INTOSAI's motto is `Mutual Experience Benefits All'. This Guide puts this motto into practice by drawing on experiences from Pacific and Caribbean Audit Offices to identify best practices in preparing for and managing disasters. All Supreme Audit Institutions need Business Continuity Plans so that when disasters strike the organisation is ready and prepared. However, the risks facing the small nations of the Pacific and Caribbean are more immediate and present than for many larger nations. In putting together this Guide, the authors spoke to many staff in our regions who had lived through hurricanes, civil unrest, floods and earthquakes. For them business continuity planning is not an abstract exercise but an attempt to deal with things better in the future and to minimise some of the trauma and destruction they suffered at first hand.

Their experiences have helped shape this Guide and we are grateful for their time and openness. The way this gratitude can be repaid is by others taking what they are saying seriously and applying their hard won knowledge. This Guide is their challenge to other SAIs to profit from their difficulties.

We are also grateful for the work done by the UK National Audit Office, in particular David Goldsworthy and Sarah Shakespeare, in producing this Guide.

Ms Dorothy Bradley
Auditor General, Belize
Chair, Caribbean Organisation of
Supreme Audit Institutions



Mr Francois Monti
Président de la Chambre territoriale
des Comptes, New Caledonia
Chair Pacific Association of
Supreme Audit Institutions

February 2013

Chapter 1
Introduction

Purpose of the guide

This guide provides advice to Supreme Audit Institutions (SAIs) on how to put in place a business continuity plan. It is aimed particularly at those SAIs located in disaster prone areas which may have limited experience in putting such plans in place.

In recent years a number of SAIs have experienced severe disruption following natural and man-made disasters, examples include earthquakes in Haiti, hurricanes in Grenada and the Cayman Islands, and the tsunami in South-East Asia.

In the aftermath of an emergency, an SAI may not only need to recover its ability to function quickly and easily, but also provide appropriate assistance to its government in responding to the emergency.

Due to the potential impacts of disasters it is important for an SAI to plan in advance and put business continuity arrangements in place that will help it recover and start functioning as soon as practically possible.

This guide is based on the UK Government advice for small businesses on developing a business continuity plan *HM Government business continuity toolkit*.

We hope this guide will provide a clear framework which SAIs can use to develop their own business continuity plan.

Disasters

Many developing countries or small island states are in disaster prone areas. When a disaster occurs it can have a significant impact on the country and its ability to operate normally. The UN ISDR defines disaster as:

"A serious disruption of the functioning of a community or society causing widespread human, material, economic, or environmental losses which exceed the ability of the affected community or society to cope using its own resources. A disaster is a function of the risk process. It results from the combination of hazards, conditions of vulnerability, and insufficient capacity or measures to reduce the potential negative consequences of risk."

Disasters will most likely have the following elements: disruption to normal pattern of life; impact on human health including death, injury and hardship; destruction or damage to government systems, buildings and essential services; and the need for providing assistance for the population including shelter, food and medical assistance.

Disaster management cycle

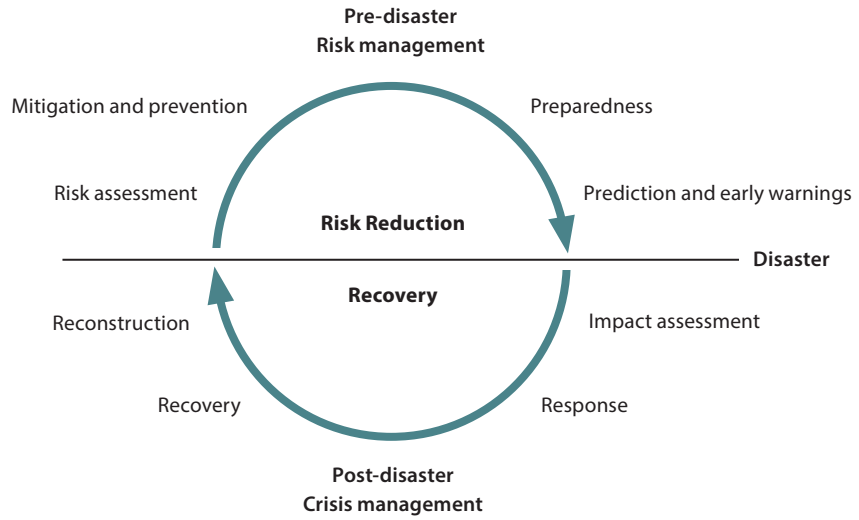
The main focus of disaster management is to reduce or avoid loss caused by disasters to assure prompt assistance to victims and to achieve rapid and effective recovery. Disaster management is often a shared responsibility between government, the private sector and civil society. Countries normally define their own disaster management policies to establish and maintain adequate arrangements to deal with their vulnerability to disaster.

The disaster management cycle (**Figure 1**) can be divided into three phases: the pre-disaster phase, the emergency phase, and the post-disaster phase. This guide is on the pre-disaster phase of the disaster management cycle and aims to help SAI prepare in case a disaster occurs. One of the best ways for an SAI to prepare is to develop a business continuity plan.

The INTOSAI Working Group on Accountability for and the Audit of Disaster-Related Aid (WG AADA) is developing a series of guides to help SAI's audit different phases of the disaster management cycle. These include:

- audit of disaster preparedness: Guidance for Supreme Audit Institutions (in draft);
- adapting audit procedures to take account of the increased risk of fraud and corruption in the emergency phase following a disaster (in draft);
- auditing post-disaster aid (in draft); and
- the use of geospatial information systems (in draft).

Figure 1 Disaster management cycle



Source: INTOSAI Working Group on Accountability for and the Audit of Disaster – Related Aid

Chapter 2
Business continuity planning

Starting early

Planning before an incident occurs helps the SAI get up and running in the quickest possible time. Business continuity planning identifies which parts of the business, the SAI cannot afford to lose and helps it plan how to maintain these if an incident occurs.

When undertaking business continuity planning it is important to ask four key questions:

- What are the SAI's key products and services?
- What are the critical activities and resources to deliver these?
- What are the risks to these critical activities?
- How will you maintain these critical activities in the event of an incident?

To develop a business continuity plan the SAI needs to take the following steps:

a understand its business activities;

b develop a business continuity strategy;

c develop and implement a business continuity response; and

d test, maintain and review the plan.

Figure 2 The Supreme Audit Office of Palm Island

Palm Island has a population of 200,000 and is relatively low-lying island. It is often subject to hurricanes, with the last major one three years ago.

The Supreme Audit Office of Palm Island has around 40 staff and undertakes a range of audits across government departments. It undertakes compliance, financial and performance audit. It also audits donor funds spent on the island if requested. The Auditor General has decided to develop a Business Continuity plan for her office.

Source: National Audit Office

Understanding the organisation

To develop a business continuity plan it is essential to have good understanding of the organisation to help plan any response to an emergency. Two key tools to help with this process are business impact analysis and risk assessment.

Business Impact Analysis

Undertaking a business impact analysis and a risk assessment will enable a better understanding of the organisation. A business impact analysis identifies and documents key products and services, the critical activities required to deliver these; the impact that a disruption of these activities would have on the SAI; and the resources required to resume the activities.

A business impact analysis is performed in four steps:

a List key products and services the SAI provides.

b Consider the impact of a disruption on the SAI's ability to deliver its statutory responsibilities and on its stakeholders.

- Identify the resources and facilities needed to deliver these products and services.
- Identify the maximum length of time the SAI is able to manage a disruption to each of its key products without threatening either viability or loss of reputation to the organisation.

c Identify when key products and services will need to be resumed. This is often called the Recovery Time Objective. When setting the objective take into account the assessment of how long the organisation is able not to deliver on key products and services and then a build in a margin to take account of unforeseen difficulties.

d Write up final list.

An SAI's key products and services are likely to be:

- Compliance audit
- Financial audit
- Performance audit
- Briefings to parliamentary committees
- Auditing programmes which have donor funding
- Provision of client advice or specialist products
- Comptroller function
- Corporate functions-Human Resources/Finance/Information Technology/media.

The maximum length of time that disruption in service is acceptable will likely vary by product/service. For instance, it may be important to re-establish the Comptroller function in hours while a country may be able to manage without Performance Audit for several months. To set maximum times it is useful to refer to statutory requirements and the SAI objectives.

One of the most important elements is writing-up the business impact analysis. This should clearly identify by service what time is needed to restore it back to operation.

Once there is a clear understanding of what needs to be recovered and when, the next step is quantifying the resources required to maintain the critical activities, these could include:

- People
- Premises
- Technology
- Information/key documents
- Suppliers, contractors/partners
- Key stakeholders/Parliament/Accountant General.

After a disaster occurs, the SAI's function might change temporarily. For instance, Grenada undertook spot checks of government stores and undertook cash counting. Therefore when considering when functions and resources are needed it is useful to carefully consider what functions a SAI may be required to perform after an incident occurs.

Figure 3 Palm Island Supreme Audit Office's Business Impact Analysis

The Auditor General decided to undertake a Business Impact Analysis for her Audit Office and invited her senior team to two facilitated sessions lasting two hours to consider the questions. She then appointed one of her colleagues to write-up the session and fill in any blanks. This included checking the statutory requirements and ensuring all the office's objectives were considered. Overall this work took around a week. The Auditor General felt confident, now that she had completed the Business Impact Assessment, that she was well placed to proceed to the next stage.

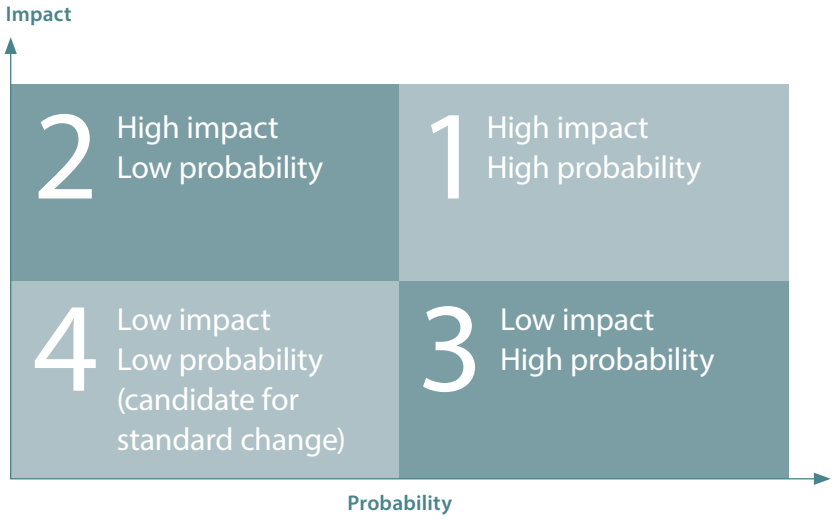
Source: National Audit Office

Risk Assessment

Assessing the risks the organisation faces enables effective planning of the risk reduction activities. The risk assessment looks at the likelihood and impact of a variety of risks that could cause business interruption. The risk assessment should be based on the critical activities and resources identified in the business impact analysis.

The first step is to identify and document the risks to your organisation. There will be two main types of risks, generic risks to any organisation and specific risks that impact on a SAI (**Figure 4**).

Figure 4 Risks to a Supreme Audit Institution



Source: UK government risk register, NAO risk register, NAO analysis

Once the main risks have been identified it is useful to consider how likely they are to occur and the impact. It can be useful to consider them in four categories:

- Low Impact, low likelihood
- Low Impact, high likelihood
- High Impact, low likelihood
- High Impact, high likelihood.

Once the risks have been categorised and ranked this allows the SAI to make an informed decision about what action to take. There are four main options about what decision to make:

a Treat: develop a plan to manage/minimise impact if the risk occurs.

b Tolerate: accept the risk as the costs of implementing any risk reduction strategies outweigh the benefits.

c Transfer: transfer the risk. This could either be done through insurance or contractual arrangements.

d Terminate: it might be appropriate to change, suspend or terminate the service, product, activity or process. This approach is most likely to be considered where the activity has a limited life span.

In practical terms it is probably worth focusing on the risks that have a high impact. Risks identified as having low impact, low likelihood may not need to be managed, while risks that are low impact, high likelihood could be managed through good internal procedures if required.

Figure 5 Palm Island Supreme Audit Office's risk assessment

The Auditor General of Palm Island decided to undertake a combination of both a facilitated workshop and interviews with senior staff for the risk assessment to ensure all risks and possible actions were considered. In the workshop with senior staff they considered what risks faced the Audit Office and then graphed the risks based on impact and likelihood of occurring. As a result the Audit Office is aware that it needs to consider the impact of a hurricane or tropical storm would have on its ability to operate. For example, one of the risks identified was that under law only the Auditor General can sign-off the audited accounts, as a result the Office needs to think about how to manage the impact if the Auditor General became incapacitated.

Source: National Audit Office

Chapter 3
Develop a business continuity strategy

Once the SAI has identified the essential services and when they need to be functioning after an incident, the next stage is developing a business continuity strategy.

A business continuity strategy. is about developing an action plan for dealing with the anticipated risks and bringing back the activities within the identified time scales. The strategy will include identifying and undertaking appropriate actions to mitigate the individual risks as well as how to handle the risks should they occur.

The plans developed should provide all the information required to ensure the Audit Office can prevent or minimise the risk as well as manage the immediate incident and recover the required functions within the timescales previously identified.

This section will identify potential mitigations that can be put in place based on identified risks through using case examples.

We have outlined some potential mitigations by resource type, and when they would be appropriate to implement within a business continuity plan in **Figure 6** on pages 14 and 15.

Based on Grenada's experience (Figure 6) the following mitigating actions might be useful:

- People: have contact details for staff and ensure during the hurricane season everyone knows the emergency contact number for the office. Have a plan in place to manage staff demands on their time if an incident occurs.
- Premises: maintain external environment including pruning trees, and checking the structure of roofs. Put in place appropriate buildings and contents insurance.
- Technology: during the hurricane season put computers in protective casing every evening. When the warning is sounded, put computers in a watertight place. Put in place a contract to recover IT functionality in an emergency with a private sector supplier. Remove all technology to a secure location if the building after an incident is unable to be secured.
- Information: identify essential documents and other key pieces of information e.g. opening and closing balances. Keep in fire proof safe. Ensure data is backed up and kept off site in a secure location – even off island or away from the region. Remove all confidential files to a secure location if it is impossible to secure the building from potential looting.
- Suppliers: identify suppliers/contractors to assist after an incident including IT, building specialists, office furniture suppliers. Identify other audit offices that may be able to provide you with assistance if required.

- Stakeholders: perform spot checks on government stores to stop looting. Audit aid assistance provided. Have a communication strategy in place to deal with parliament and other key stakeholders. Identify what, if any, media presence is required and whether a press officer is required after an incident.

The Haiti Audit Office suffered heavily when the island was struck by an earthquake in 2010. It took two to three months to get set up and they had to occupy temporary accommodation with limited storage facilities and staff. The Audit Office was not a high priority for international aid assistance. They needed support from an SAI which understood their government/accountability structure. From Haiti's experience the following mitigating actions may have been useful:

- People: identify contractors/private sector that can provide assistance with staff knowledge and resource.
- Premises: identify alternative premises with suitable storage facilitates.
- Stakeholders: raise profile of audit office to ensure they understand the need to provide assistance. Seek assistance from other sources including INTOSAI. Build partner relationships with other audit offices with a similar government/accountability system that would be able to provide assistance in an emergency.

After the 2004 Tsunami in South-East Asia newly constructed housing was demolished because the wood was illegally procured. Therefore after an incident it may become important to provide assurance that aid money is spent in accordance with local rules; e.g. around procurement. Possible mitigations include:

- Being in a position to undertake compliance and financial audit of aid money after a major incident.

In Guyana after severe flooding in 2012 food, drugs, water and other essentials had to be bought and disbursed. The Government asked the SAI to undertake an audit of these expenses during this period. The SAI found this task difficult as several key documents were destroyed during the flood period and there were many breaches of procurement rules. Therefore in any disaster planning the SAI may need to consider what type of audit assistance it may be required to carry out during a disaster. Possible mitigations include:

- Information: Identifying likely audits to be undertaken in a disaster related incident e.g. procurement, asset checks.
- Stakeholders: working with government to identify appropriate procedures and check required in an emergency which ensures speed, but also provides an audit trail.
- Information: develop audit plans that can be quickly implemented using the Guides the INTOSAI Working Group on Accountability for and the Audit of Disaster-Related Aid (WG AADA) developed on auditing disaster related aid.
- People: Train audit personnel on how to undertake audit of disaster related audit according to audit plans developed and government emergency procedures.

Figure 6 Suggested mitigations for loss of resources

People	Premises	Technology	Information	Suppliers and Partners	Stakeholders
Business as usual					
Collect and maintain contact details of all staff and next of kin.	Ensure premises are structurally sound e.g. check recent condition surveys.	Maintain an inventory of what technology and software is owned and what products/ services need the technology.	Ensure data is backed-up and kept off site e.g. external hard drives.	Identify who the SAI's suppliers are for essential products to undertake work e.g. paper.	Identify key stakeholders and put mechanisms in place to provide information to stakeholders.
Understand what knowledge and skills staff currently have.	Check that you have building and contents insurance in place.	Hold CDs of key pieces of software in a safe place to enable loading on to alternative machines.	Identify essential documents and ensure they are stored securely.	Have more than one supplier for essential products.	Build stakeholder engagement around importance of SAI.
Develop process map and documentation of key tasks/roles to enable staff to undertake roles.	Check that nearby vegetation and trees are regularly pruned and maintained and that nearby debris is removed promptly.	Ensure that there is appropriate IT security in place to reduce risk of IT breaches. Ensure that sensitive electronic documents are appropriately protected.	Identify which client documents are essential for audit and pass list to client.		Understand how key stakeholders and citizens receive information e.g. social media, radio talk shows, and newspapers.
Develop a succession plan.	Have an up-to-date asset management register. Have an asset management register of all assets owned by SAI eg desks, computers.	Develop and implement an IT security plan.			
Mitigations in case an incident occurs					
Ensure staff are able to undertake more than one role. Cross-train/multi-skill.	Set up procedures for staff to work at home or other locations.	Hold older equipment as emergency replacement or spares.	Keep copies of essential documents in a secure location off-site, e.g. bank safety deposit box.	Identify alternative suppliers for key products/services.	Identify how the audit office can provide assistance after an island-wide incident.
Identify and arrange for contractors/ consultants who can be called on in an emergency.	Establish an agreement to relocate staff to alternative accommodation if the main accommodation is out of action.	Consider purchase or access to backup generators or water purifiers.		Obtain canvas or plastic sheets to be able to protect key resources and make sure staff know how to secure such sheets.	Identify potential sources of donor funding for audit office in an emergency.

Figure 6 Suggested mitigations for loss of resources continued

People	Premises	Technology	Information	Suppliers and Partners	Stakeholders
Mitigations in case an incident occurs continued					
Establish methods to communicate with staff in case of emergency.		Use private sector to repair/rebuild equipment in case of emergency. Identify appropriate IT security specialists in case of an incident. Identify appropriate responses if IT security breach occurs.			Ensure that the SAI is part of the government national disaster plan. Identify how other audit offices could be of assistance including regional networks. Ensure the Audit Office has appropriate links/ contacts with the main communication channels.
Mitigations when an incident is likely to occur					
Refresh staff knowledge around how the office will communicate in an emergency.	Ensure fire doors and windows are closed and are as watertight as possible. Desks are clear of documents, and essential IT equipment.	Protect technology if warning of incident e.g. protective covers, in lockers. Store essential technology in a watertight, structurally sound location. Allow staff to take home laptops.	Ensure all documents are stored safely and not left loose. Identify and keep essential documents in alternative location. Remind clients which documents are essential for audit and require safe storage.	Keep backup spare emergency supplies. Store additional supplies at another location.	Provide INTOSAI regional groups with key contact numbers in an emergency. Make preliminary contact with the appropriate communication channels.
Mitigations for after an incident has occurred					
Enable staff to work half-days/shift pattern. Provide counselling to staff if required.	Only use office for essential/high priority work. Secure premises from looting and vandalism e.g. guards. Use asset management register to assess what assets have been damaged or lost.	Have facilities to undertake manual audit if required.	Assess what documents have been lost. Assess what essential client documents have survived.	Ensure you have access to cash to pay staff.	Contact INTOSAI regional network to provide update on incident, and request required assistance. Contact stakeholders and provide required updates. Make contact with the appropriate communication channels.

Source: National Audit Office analysis of case studies, HM Government business continuity toolkit

Figure 7 Case Example Grenada

The Grenada Audit Department suffered extensively from a hurricane. There was damage to the roof, computers, office furniture, financial records, and the utilities supply. The premises suffered extensive destruction from a fallen tree and a damaged roof. As a result the buildings' contents were exposed to the elements for a number of days. Everything in the library was soaking wet and damaged, most of the office furniture was damaged, and 15 computers were lost with three remaining in working order. The roof was temporarily covered in canvas, but water started entering the building again.

The utilities supplies were disrupted but the Audit Department had a standby electricity generator. The computers did not regain function quickly as the IT staff deployed from the government took a while to arrive as there was a lot of work to be done in other government departments. As a result a lot of electronic documents were lost because the IT staff arrived too late and the computers became unsalvageable.

The personnel of the Audit Department recovered quite quickly apart from those who were injured. The personnel worked half days for a few weeks after the hurricane to allow them to deal with personal issues arising e.g. damage to their own homes.

Upon entering the Audit Department after the hurricane it was found that hard copies of files were destroyed. The Auditor General states that reconstructing records can be very difficult if not impossible. Although it had some skill in reconstruction of records after helping the Ministry of Finance recover from a fire in the early 1990s.

Due to a lack of staff and a damaged building there was a higher threat of theft and vandalism to the equipment and files.

Staff were unable to work from the office or conduct regular audit work because the premises were damaged. Due to the damage across the whole island it was difficult to obtain other premises. It also took a while for the Audit Department to become fully functional due to the difficulty in obtaining the necessary computers and office furniture. The audit personnel carried out surprised inspections on government stores. The Auditor General said these checks resulted in no evidence of looting.

The Supreme Audit Institutions of neighbouring islands like Trinidad, Barbados, and St Lucia provided assistance and the Caribbean Regional Organisation of Supreme Audit Institutions (CAROSAI) provided two replacement computers. However, assistance was limited by their budget.

Source: Interview with Director of Audit, Grenada Audit Department, October 2010

Chapter 4
Practical aspects of a business continuity plan

Preparing a plan

The SAI's government may have a disaster plan in place. To help the SAI be effective and obtain all the assistance required before, during and after an incident, it will be important to link into the country plan, and know who in government to contact if there is a disaster. We recommend that while the SAI is developing its business continuity plan it investigates whether the government has a disaster plan in place, and how the SAI plan feeds into it.

To develop, plan, implement and review a business continuity plan the following aspects are needed:

- Leadership.
- Plan for implementing the business continuity plan.
- Clear understanding of roles and responsibilities.
- Regular updating to maintain the plan.
- An emergency pack for when an incident happens.

To ensure that the business continuity plan is established and maintained it is important that it has full support from the Auditor General and senior management. To ensure a successful delivery and maintenance of a business continuity plan it is necessary to:

- Appoint someone in senior management to be accountable for the plan.
- Appoint a team of people to take the programme of work forward.

One of the key tasks of senior management will be to identify what is the scope, aims and objectives of business continuity management in the organisation and what are the key activities required to deliver these.

Once the policy has been developed and agreed the next stage for the team is to ensure that the business continuity plan is implemented, this will likely involve:

- Communicating the plan to SAI staff including what it means for them.
- Communicating the plan to relevant external stakeholders which could include government, clients, parliament and donors.

- Arranging training for staff based on the suggested mitigation strategies outlined in the plan.
- Ensuring that any mitigation strategies put in place are enacted e.g. building and contents insurance.
- Testing the business continuity arrangements.

Once a business continuity plan has been developed it is important to maintain the plan and periodically review it to ensure it still meets the needs of the business. The accountability for this should sit with senior management. This is likely to include:

- keeping the business continuity plan up to date;
- promoting business continuity across the organisation e.g. through induction for new staff, refreshing current staff when the hurricane season starts; and
- updating the business continuity plan as a result of lessons learned and emerging good practices.

Emergency pack

One of the most useful actions is to prepare an emergency pack in advance. This pack will help you in an incident. Items to include are:

- Key documents: business continuity plan, contact details of the staff, insurance documents, building site plan, contact details for key stakeholders, passwords and user names for the SAI social media accounts.
- Equipment: spare sets of office keys, torch and batteries, walkie-talkies, CB radios, pads of paper, office stationery (pens, post-it notes), envelopes, stamps, memory stick, disposable camera, gaffer tape, window tape, top-up money for mobile phone.

Audit after an incident

After a major incident the ability for government to undertake its normal business may be impaired. As a result the Audit office may have a part to play in providing assurance that financial expenditure is 'true and fair' and regular, and the money spent is good value.

This is likely to form two stages: be in a position to audit donor funding if needed (see guidance prepared by the INTOSAI Working Group on Accountability for and the Audit of Disaster-Related Aid) and provide assurance on government expenditure.

In the case example on Grenada it undertook surprise inspection checks on government stores. It would be useful to have a discussion with key stakeholders in government to agree what type of support an audit office can provide to help both achieve their remits and make best use of limited resources.

Assistance from the wider audit community

As part of the business continuity planning process it is useful to consider what if any support may be required from the wider audit community. Areas of support could come from:

- INTOSAI IDI.
- Regional networks e.g. CAROSAI, PASAI, AFROSAI-E, EUROSAI; OLACEF, ARABOSAI, ASOSAI, CREFIAF.
- Donors the SAI works with.
- Existing relationships with other SAIs.
- Neighbouring SAIs.

The assistance that could be sought include: extra staff to help the audit office get back up and running in the short term and to undertake the increased work involved in auditing donor funding; replacement equipment; and emergency funding.