BUSINESS CONTINUITY PLAN

Status:	Approved
Custodian:	IT Directorate
Date approved:	2013-12-04
Decision number:	SAQA 07102/13
Implementation date:	2013-12-05
Due for review:	2016-12-03
File number:	

CONTENTS

1 INTRODUCTION

The concept of Business Continuity Planning (BCP) has over the past few years, become a major business management requirement. For example the King II report highlights the responsibility of the board to support business sustainability under normal as well as under adverse operating conditions. The internationally recognized Standard ISO 17799 and the BS7799 requires that a managed process be implemented for developing and maintaining business continuity throughout an organization. The subject has been well researched and a great deal of documentation and advice is available. Specialist BCP companies have emerged, offering the business community a range of business continuity products and services, including:

- Off-site recovery facilities;
- Planning methodologies; and
- Software based Disaster Recovery Planning (DRP) systems ;

This has given rise to the evolution of DRP specific terminology and acronyms. Disaster Recovery Planning is also known as BCP (Business Continuity Planning) or BRP (Business Resumption Planning). It has become generally acknowledged that the planning process should go beyond catering for major disasters such as earthquakes, fire and flood, to include the less threatening emergencies like power outages, server downtime and limited access to the workplace, which start out as minor emergencies, but can quickly escalate to full blown disasters.

There can be no standard methodology regarding BCP as much depends on:

- The type of business addressed;
- The main office environment (campus or single building);
- Enterprise locations infrastructure;
- Existing vulnerabilities;
- Reliance on networking and location of servers;
- Executive management attitudes; and
- Cost of putting BCP in place.

In line with the SAQA policy on Business Continuity, this document presents the SAQA plan for all aspects of BCP and serves as an important background to the detailed action plan, which due to its changeable nature is presented as separate documents per directorate.

2 GOALS AND OBJECTIVES

The goal of the plan is to prevent loss of life, reduce property damage and minimise impact on the overall business i.e.:

- Minimise and support the number of decisions that must be made during a crisis;
- Minimise the dependence on any specific person during the crisis;
- Minimise the need to perform crisis actions by trial-and-error when a crisis occurs; and
- Minimise the need to develop new procedures, programs or systems during a crisis so that all components necessary to assist the site during a crisis are documented and stored off-site, ready for use.

The overall objective of the plan is to provide the information and procedures necessary to: -

- Rapidly respond to a disaster or emergency situation;
- Notify necessary trained personnel;
- Assemble business recovery teams;
- Rapidly recover services to clients; and
- Rapidly resume normal business functions.

3 CORPORATE RESPONSIBILITIES

3.1 CRISIS CONTROL UNIT

3.1.1 CONCEPT

The concept of a Crisis Control Unit requires careful explanation. The unit should not exist as a day-to-day ongoing business entity, but the members come together as a team, to orchestrate all matters relating to an actual or potential disaster and the ongoing task of Disaster Recovery Planning, including the implementation of disaster prevention activities. The unit members include some of the most senior members in the organisation and are ultimately responsible for all aspects of disaster prevention and disaster recovery, relating to SAQA.

Any team, even at this level, requires an internal orchestrator to ensure that the team operates effectively despite ongoing day-to-day responsibilities that are not disaster related. With this in mind a senior management role has been created in the group viz. Crisis Control Officer (CCO). The CCO will be a senior person with a good understanding of the business and business practices together with a detailed knowledge of the Information Technology on which the business has become so dependant. The CCO together with his/her deputy, will be responsible for the development, ongoing maintenance and testing of an effective Disaster Recovery Plan and disaster prevention measures. The CCO must ensure that all members of the Crisis Control Unit understand all aspects of the Business Continuity Plan and are fully aware of their respective responsibilities in this area.

Whilst the Crisis Control Unit carries ultimate responsibility for all facets of disaster recovery, specific responsibility lies in the “across all business units” disaster related activities. The Crisis Control Unit, through the Crisis Control Officer will also be responsible for ensuring that each Strategic Business Unit (SBU) has developed a business specific Business Continuity Plan which clearly states and covers the key business processes of the unit and is in line with the corporate Business Continuity Plan, as determined by the Crisis Control Unit.

3.1.2 RISKS AND BALANCES

From a crisis control perspective the perennial question is “How much is enough?” What would happen in a major disaster if the entire Crisis Control Unit were lost? On the other hand it does not make sense to have a Crisis Control Unit that is so large that it becomes unwieldy.

The plan assumes that the required quorum of the Crisis Control Unit will remain functional, in a post disaster situation.

3.1.3 CRISIS CONTROL UNIT MEMBERS

Title	Name	Major DR Function
Chief Executive Officer	Joe Samuels	Leadership and group PR
IT Director	Herman Ohlhoff	Crisis Control Officer
CFO	Mark Albertyn	Financial Support
NLRD Director	Yvonne Shapiro	Database Administration
HR Director	Victor Booysen	Staff matters
ACS Director	John Arnesen	Communication

3.1.4 DISASTER DECLARATION AUTHORITY

A major disaster (evacuation of site) will take place as per SAQA’s Procedures on Emergency Evacuation.

3.1.5 EXTERNAL CRISIS CONTROL CENTRE

Given a major disaster where the site is destroyed or inaccessible, the Crisis Control Centre will be:

- The outsourced offsite backup environment. (DRSA);
- The home of the Chief Executive Officer; or
- The home of the IT Director.

3.2 BUSINESS SUPPORT UNITS (BSUS)

Along with the Crisis Control Unit, the Business Support Units also have “across all business units” functionality. In all major disaster situations the specific business units will be reliant on the performance of the BSUs. Each BSU has defined areas of responsibilities in the event of a disaster. However in the event of any unplanned circumstances, the BSU's will fall directly under the control of the Crisis Control Unit in terms of rearranged priorities or other changes to the plan.

The Business Support Units are shown below, together with senior management.

BSU (Directorate)	**Manager**
Executive Office	Joe Samuels
Information Technology	Herman Ohlhoff
Finance	Mark Albertyn
NLRD	Yvonne Shapiro
Human Resources	Victor Booysen
DRR	Jody Cedras
Advocacy and Communication Support	John Arnesen
DFQEAS	Nadina Coetzee
CAS	Paul West
International Liaison	James Keevy
Research	Heidi Bolton

3.3 STRATEGIC BUSINESS UNITS

Whilst the IT Director is responsible for the maintenance of the SAQA Plan, each Strategic Business Unit needs to be thoroughly familiar with the BCP strategy and have their specific unit recovery teams and Business Continuity Plans in place.

4 COUNTER DISASTER STRATEGY

SAQA will implement standard security options.

From the IT perspective the organisation has implemented logical access control, fire detection and fire prevention for the server room in line with accepted best practices.

4.1 KEY PERSONNEL

This is an area that is very difficult to define in a BCP strategy, in spite of the fact that the simultaneous loss of several key personnel, would certainly constitute a major disaster.

Personnel development is an ongoing organisational activity based on:

- Effective recruiting;
- Training;
- Succession planning; and
- Fast tracking of highly promising staff.

The above processes become effective over time and cannot be replicated in a disaster environment. At best, key personnel can be replaced with trusted outsourced resources, internal or external to the group.

The SAQA approach to BCP is premised on the assumption that sufficient key skills will be available to implement the recovery process, even if some of these skills are outsourced.

4.2 RISK ANALYSIS

The ongoing risk analysis process under the control of the Crisis Control officer isto:

- Consider all potential disaster scenarios and potential impact on the business;
- Rank each scenario in terms of potential eventuality;
- Discard scenarios that are never likely to occur, or that we can do nothing about;
- Categorise and rank remaining disaster scenarios in terms of impact on the business; and.
- Define each potential disaster within each scenario category.

4.2.1 DETERMINE VULNERABILITY TO UNCONTROLLABLE FACTORS

Table 1 presents a 'threat / vulnerability worksheet' by which the likelihood of most types of disasters can be measured. The priority risks calculated for each type of disaster is based on physical location and the immediate environment of the SAQA office and computer centre, as well as social and natural conditions in this area.

Table 1 – Threat / Vulnerability Worksheet
Note: Priority risks are rated on a scale of 1 to 3, where 1 represents the highest level of risk

Possible Threat	Likelihood				Vulnerability				Priority Risks
	H	M	L	NA	H	M	L	NA	
ELEMENTS									
Earthquake			√				√		**3**
Tornado / Heavy Winds		√				√			**3**
Flooding		√					√		**3**
Fire	√				√				**1**
Severe Thunderstorm	√				√				**1**
Hail Damage		√					√		**3**
Lightning	√				√				**1**
Drought		√					√		**3**
PEOPLE									
Medical Outbreak		√			√				**1**
Civil Unrest		√				√			**1**
Industrial Action / Strikes		√			√				**1**
Denial of Access	√				√				**1**
Computer Crime	√				√				**1**
Industrial Sabotage		√					√		**3**
Bomb Threat / Blast		√			√				**1**
Transportation Accident		√				√			**2**
Unauthorised Access		√				√			**2**
Individuals Undocumented Knowledge	√				√				**1**
TECHNOLOGY									
Telecommunications Failure									
Telephone Line Failure	√				√				**1**
Network Failure	√				√				**1**
Power Shortage / Failure	√				√				**1**
UPS Failure		√				√			**2**
Computer Hardware Failure									

Possible Threat	Likelihood				Vulnerability				Priority Risks
Workstation Failure	√						√		**2**
Server Failure	√					√			**1**
Printer Failure	√					√			**2**
Computer Software Failure									
Upgrade compatibility	√					√			**1**
Over Customisation	√					√			**2**
Unlicensed Software		√				√			**2**
E-mail Retention & Deletion		√			√				**1**
E-mail Content	√				√				**1**
Document Loss or Destruction									
Legal Documents		√			√				**1**
Employee Records		√			√				**1**
Service Level Agreements		√			√				**1**
Data Backups & Restores	√				√				**1**
Hacking	√				√				**1**
Air-conditioning Failure	√					√			**2**
Computer Virus Attack	√				√				**1**

4.2.2 DETERMINE VULNERABILITY TO CONTROLLABLE FACTORS

The following areas should be examined on a regular ongoing basis:

- Potential fire hazards;
- Health and Safety;
- Insurance cover;
- Susceptibility to computer virus;
- Susceptibility to hackers and computer fraud;
- Back up and restoration of data and software;
- Access security; and
- Availability and configuration complexity of hardware and network components.

The fire department will be required to sign off on the SAQA House building in terms of its fire safety. Thereafter, a fire hazard inspection will be regularly conducted by the Facilities Supervisor and the Crisis Control Unit.

4.2.3 COUNTER DISASTER MEASURES

4.2.3.1 Physical Access

A secure physical access system is in place where all staff and any visitors are signed in upon entrance to and exit from the SAQA House building.

4.2.3.2 Health and Safety

It is the responsibility of the Facilities Supervisor and the Health and Safety Committee to ensure compliance with the OHS Act and to have at least one fire drill per annum.

Emergency telephone numbers for Police, Fire Department and Ambulance will be displayed throughout the building.

4.2.3.3 Off-Site Recovery Centre

SAQA has a signed contract with an off-site recovery company (Disaster Recovery South Africa (denoted by DRSA in the remainder of this document) who have recovery premises situated in Midrand. The recovery site is on standby and accessible at all times.

The recovery centre is equipped with several computer rooms that are wired and cabled to meet all server requirements. The centre also provides office space and desks, together with wired and cabled workstation positions. Telephone, Internet and Fax facilities are included in the contract; standard canteen facilities are also available. The contract presently provides sufficient office facilities to cater for a fair sized recovery team (20 seats). The recovery centre will provide SAQA access to a battle box, in which to pre-store important recovery tools such as chequebooks, forms, a copy of the entire BCP, copies of important contracts and copies of application software.

DRSA provides network and telecommunications capabilities that would enable SAQA to quickly switch current networks and telecommunications links to the recovery site.

The contract with DRSA provides SAQA with at least 6 testing days per annum; this enables the organisation to regularly test and confirm the viability of the disaster recovery process and backup media.

This recovery option caters for a range of potential disaster situations, including the destruction of the entire SAQA home site, in which case selected recovery teams would move into the recovery site, working in shifts around the clock if required.

The recovery site provides immediately available facilities for a limited number of staff for a limited timeframe. The Site provides SAQA with the ability to resume business as fast as possible albeit with a skeleton staff complement.

Remote access is provided for other staff to access e-mail and other data files.

4.2.3.4 Fire Prevention

The SAQA House building is required to comply with Fire Safety Regulations. At present there are only fire hoses and fire extinguishers at each end of the floors. A fire detection and prevention system has been installed in the server room, and the walls (dry walling) have fire retardant properties.

4.2.3.5 Uninterruptible Power Supply (UPS)

SAQA has taken a decision not to install a generator in the SAQA House building. SAQA has a number of UPS's and these are serviced quarterly.

4.2.3.6 Server and Database Redundancy

No redundancy is implemented for individual server motherboards, CPU's or server cards. However, server virtualisation has been implemented allowing for the quick rebuild of a server in the event of failure.

Furthermore, for the non-virtualized servers, servers of similar configuration are used on-site and can be configured to host additional applications for a short period of time. The data can be restored using the Tivoli backup system with the relevant back-up tapes and database backups.

4.2.3.7 IT Hardware Availability and Ease of Configuration

The selection of hardware for the SAQA computer centre is an important issue and is significantly influenced by the suppliers' ability to rapidly replace hardware, in times of emergency. This avoids configuration problems with replacement hardware.

4.2.3.8 Data and Software Back Ups

A full backup of SAQA servers is made every weekend and daily incremental backups are made during the week. A copy of the weekend backups is sent off-site to Metrofile every week. Furthermore, a month-end full backup is also made and stored at Metrofile for 1 year. An LTO5 device is used with the Tivoli Storage Management software package to manage all backups and produce a log file. Reports of the backups are printed, reviewed and filed daily.

4.2.3.9 Communication Lines

SAQA relies on telephones lines to perform its business. In the event that existing lines are interrupted, cell phones will be utilised.

4.3 DISASTER CATEGORIES AND LEVELS

Potential disasters are categorised as shown in Table 2. Emergency situations that are covered by the day-to-day operational procedures have not been categorised.

The category reflects the severity and nature of the disaster. For example a Category 1 Disaster is the most severe and means the total or partial evacuation of the SAQA offices. Total and partial evacuation can be caused by different circumstances, not always the destruction of the entire site.

The level reflects a description of the disaster within the category. Similar types of recovery procedures are required for the levels within the same disaster category.

4.3.1 LOGIC BEHIND THE CATEGORY DEFINITIONS

This section describes the logic behind the categorisation of the potential disaster situations. Every effort has been made to group and standardise disaster situations, in order to prevent unwieldy and confusing disaster definitions. Emphasis is placed on the major disaster scenarios that cause the most serious disruption to the business.

4.3.1.1 Category 1 Disasters

Category 1 disasters require the total or partial evacuation of the SAQA offices. In this instance, the evacuation will take place as per SAQA's Procedure on Emergency Evacuation. This could happen for several reasons:

- Destruction of SAQA House, through fire, flood etc;
- Prolonged denial of access to SAQA House by the authorities due to toxic fumes, civil unrest, etc;
- Destruction of the entire Computer Room environment;
- Prolonged power outage; and
- Hygiene factors such as the prolonged loss of water supply.

Category 1 disasters need to be further described to cater for the following situation:

Category 1 - Level 1 Disaster
The requirement to evacuate SAQA House coupled with the destruction of all documentation and hard copy records on site, at the time of the disaster.

Category 1 - Level 2 Disaster
The requirement to evacuate SAQA House and documentation and hard copy records remain intact and available at the site.

4.3.1.2 Category 2 Disasters

Essentially Category 2 disasters define emergency situations that do not require the total evacuation of staff from SAQA House. Potential causes for the declaration of a category 2 disaster are:

- Server malfunction;
- Database corruption;
- Loss of equipment through theft;
- Short-term denial of access to SAQA House by the authorities due to toxic fumes, civil unrest, etc;
- Short-term power outage;
- Short-term downtime of network and/or telecommunications infrastructure; and
- Hygiene factors such as the short-term loss of water supply.

By and large, category 2 disasters tend to be short-term in nature, with the anticipated "time to repair" being the major measurement criteria. Any major extension to the anticipated time to repair could well cause a category 2 disaster to be escalated to category 1.

4.3.1.3 Category 3 Disasters

Category 3 disasters are typically those of a temporary duration (Max 8 hours) examples of which are as follows:

- Temporary loss of network connectivity;
- Temporary loss of telephone connectivity;
- Server malfunction; and
- Staff illness.

4.3.2 TABLE 2 – DISASTER CATEGORIES AND LEVELS

Cat	Disaster Description	Circumstance	Potential Injury	Evacuation
1	Destruction of the entire SAQA House. Including documentation.	Fire flood	Yes	Yes
2	Loss of services that require total evacuation to recovery site.	Toxic fumes due to nearby explosion etc.	Unlikely	Yes
3	Loss of services that do not initially require total evacuation to recovery site.	Equipment loss/malfunction or network failure.	No	No

The BCP includes as many category 2 situations as is deemed necessary.

Some typical category 2 emergency situations are:

- Power loss due to cable faults (generator will not help);
- Telephone and FAX analogue lines down; and
- Staff walkout.

4.4 MONITORING AND ESCALATION

A major disaster such as the destruction of the entire SAQA House does not require a great deal of decision making in terms of do we evacuate? Or don't we evacuate? It has to happen as fast as possible. Most other disaster situations need to be carefully monitored on an ongoing basis and where necessary escalated to a level where evacuation of SAQA House is required. The escalation process is largely based on informed estimates regarding time to repair, in conjunction with documented business unit requirements.

The evacuation process is complex, intense and expensive. The establishment of an effective environment at the off-site recovery centre takes anything from two to five days, depending on the nature of the evacuation. The Crisis Control Unit is expected to have its finger on the pulse of the situation at all times and make decisions which are balanced and cost effective. An example would be the destruction of the computer room environment. Essentially there are two approaches that can be taken, namely:

- Evacuate, set up at the recovery site and run the business with a skeleton staff complement, until such time as the computer room is fully restored; and
- Set up an emergency computer room in one of the boardrooms or meeting rooms at SAQA House. Equipment not syndicated at the recovery centre could be purchased

and quickly installed. This approach would allow the business to resume, with a full staff complement.

The decision-making required in the above example is significant as it involves risk analysis, assessment of supplier guarantees in line with Service Level Agreements (SLA) and a degree of intelligent gambling.

4.5 RESTORATION AND RETURN

Once a category 1 disaster situation (with evacuation) has been successfully handled and insurance claims intimated in line with the recovery plan, the rebuilding and restoration phase begins. The existing premises may be restorable or new premises sought. The Crisis Control Unit is expected to lead and manage this phase of the recovery process, in accordance with executive and shareholder expectations. The restoration process must ensure that all the required disaster prevention measures are effectively implemented at the restored or new home site.

As the restoration process nears completion so another intensive planning process is initiated i.e. the return of staff and service facilities to the restored or new home site. The return process needs to be carefully considered as it involves human resources and the set up of an IT environment that might well have changed significantly since the disaster took place. Temporary emergency procedures need to be replaced by the standard operating procedures etc.

5 MAINTENANCE OF THE OVERALL BCP PLAN

The development of a detailed Overall BCP is an ongoing exercise. The business changes over time as does the staff complement. It is therefore vital that any given recovery plan reflects the current status of the business. The counter disaster strategy is also reviewed regularly.

5.1 BUSINESS IMPACT ANALYSIS

Members of the BCP project team led by the Crisis Control Officer regularly conduct in depth interviews and discussions with the senior management in each strategic business unit. This is done in order to ascertain the vulnerability of each unit to each applicable disaster scenario together with the potential business impact. These interviews are key to the maintenance of an effective recovery plan for the strategic business unit covering each disaster category.

The questionnaire-based interviews are designed to establish and ascertain (for each disaster category) the following:

5.1.1 CURRENT/NORMAL REQUIREMENTS

It is important to establish the requirements for the current working environment including:

- High level process flowchart of unit business;
- Exposure to SLA related financial penalties;
- Number of staff;
- Number of PCs and their configurations;
- Number and type of printers required;
- Telephone and Fax requirements;
- Reliance on server and network up time;
- Vital stationery and documentation;
- Telecommunications requirements;
- Current supplier list with contact information; and
- Current client list with contact information.

The above information would be crucial in setting up the unit in new premises after a major disaster.

5.1.2 MINIMUM (POST DISASTER) REQUIREMENTS

It is equally important to establish the minimum requirements for each disaster category, in the post disaster situation. Relocation of staff to the off-site recovery centre may be necessary after a major disaster, in which case the facilities will be significantly more limited than the current environment.

The key question is, "What are the minimum requirements to keep the unit functional with acceptable client service, in the post disaster situation for each disaster category?"

5.1.3 MAXIMUM RECOVERY TIME

Ascertain the maximum recovery time for each disaster situation at a detailed level. It is important to establish:

DAY	ACTIONS AND REQUIREMENTS
Disaster Day	What is the vital requirement in terms of business continuity
Disaster Day + 1	Vital minimum actions and requirements to ensure business continuity
Disaster Day + 2	What can wait for a day
Disaster Day + 3	What can wait for 2 days
Disaster Day + N	Survival functionality maintainable

5.1.4 RECOVERY TEAMS AND ROLES

The cross-unit recovery functions will be orchestrated by the Crisis Control Unit, e.g. IT connections etc. Each strategic business unit must however supply its own recovery teams for each disaster category, from the purely business perspective. The following considerations will apply:

- Definition of the roles in each recovery environment;
- Select staff and reserves to fill roles; and
- Designate team leadership responsibilities.

5.1.5 PUBLIC RELATIONS

Most disasters will impact clients, suppliers and staff in other units within the organisation. In the event of a major disaster the Crisis Control Unit will issue certain notification and assurances, such as press releases etc. in accordance with the agreed plan.

Outside of the corporate issues, each business unit must have plans and contact lists in place in order to communicate effectively with clients and suppliers in each disaster scenario.

5.2 DEVELOPMENT OF THE PLAN

The documented outcome of the business impact analysis supported by the implemented counter disaster strategy, places the DRP project team and each business unit in a position where meaningful recovery plans can be developed for each disaster category.

Essentially the plan for each unit is based on:

- Rapid access to emergency contact lists;
- Clear and concise "to do" lists that have been prioritised, with responsibility allocations, for each disaster category and level;
- Well-trained and responsible recovery teams; and
- Communication, communication and more communication.

Training of the members of the recovery teams is an essential function of each business unit manager in association with the Crisis Control Officer.

5.3 CAPTURING AND MAINTAINING THE PLAN

In today's world business is constantly changing, which means that the BCP must be fluid and changeable, due to the ongoing changes in business circumstances and staff turnover. The details of the plan must therefore reside in a database that can be easily altered, to cater for new developments. The current updated "to do" activities and contact lists must be available on demand.

A master copy of the database resides on a SAQA server and can easily be downloaded onto unit managers' laptops. Changing the data in the BCP database requires access control and verification.

6 TESTING THE PLAN

Testing the plan is an ongoing responsibility of the Crisis Control Manager. Regular tests need to be conducted with regard to each disaster scenario where this is viable, clearly it would be impossible to simulate the loss of the entire home office for testing purposes, however components of the BCP plan can be tested individually, these include:

- Testing the ability to recreate the computer centre configurations at the off-site recovery centre. (IT DR Test);
- Testing the ability to restore data and software from back up media;
- Testing the recovery procedures with regard to the loss of a critical telecommunications link;
- Testing the ability to switch networks and telecommunications links to the off-site recovery centre;
- Testing the recovery process related to the prolonged loss of power;
- Testing the recovery process related to the loss of the Internet, E-Mail etc; and
- Testing the ability of the business unit to continue functionality by using concise and detailed procedural documentation. (Possibly reverting to a manual operation).

The above testing procedures will enable SAQA to more accurately gauge restoration times and will assist in "fine-tuning" the plan based on test results.

6.1 INSPECTIONS

The testing process includes the regular inspection of counter disaster procedures and components i.e.

- Maintenance contracts;
- UPS battery health;
- Fire protection systems;
- Log Files (daily);
- Capacity utilisation (daily);
- Fire drills;
- Wiring; and
- Lightning protection.

7 TRAINING

Training is an important aspect of the plan. It is crucial that the crisis control unit, business support units and business unit recovery teams have an intimate and up to date knowledge of the recovery procedures related to each disaster category. It is fair to say that the more complete the training, the less panic there will be in a disaster situation.

8 A RECOVERY PROCESS SCENARIO

This section broadly describes the activities that will take place, given a major disaster i.e. Category 1. The scenario painted assumes a worst-case situation with loss of the entire site and injuries.

8.1 IMMEDIATE ACTION

Depending on the nature of the disaster immediate action could well be largely instinctive and thus heavily dependent on training received. The nature of immediate action will depend on the time of the disaster, during office hours, at night after office hours or over a weekend. If staff is on the premises the top priority is their safety and treatment if required.

The Crisis Control Officer will communicate with SAQA's Emergency Controller as per SAQA's Procedures on Emergency Evacuation who will:

- Contact emergency services if required. Fire Brigade, Ambulance, Medical Services;
- Orchestrate the provision of any required first aid, by trained staff;
- Ensure execution of fire drills and roll calls, if required; and
- Provide required assistance to emergency teams.

The uninjured staff recovered from shock, will be sent or taken to their homes after permission is given to be moved from the assembly point.

Once all that can be done for the well being of staff is completed, the Crisis Control Officer will arrange an immediate meeting of the Crisis Control Unit, at one of the external crisis control centres, if required.

8.2 DISASTER DECLARATION

The members of the Crisis Control Unit will be informed of any deaths or injuries to staff and visitors, through the disaster. The Crisis Control Officer or stand-in will ensure that each member has the latest version of the recovery plans.

If possible and required, the Crisis Control Unit will visit the site to evaluate the full extent of the disaster.

A disaster will be declared at the appropriate level and the recovery plans will be triggered. It is assumed that evacuation and relocation will be necessary.

8.3 ANNOUNCEMENT AND NOTIFICATION

Depending on the number of members of the Crisis Control Unit present, many of the following actions will take place concurrently:

- The member representing Human Resources may be mandated to arrange staff counselling or other actions to comfort and re-assure staff;

- Press releases will be prepared in line with the recovery plan and the appropriate media notified;

- Major corporate clients will be contacted and advised of the disaster and the recovery process, either immediately or at the earliest suitable time;

- The off-site disaster recovery centre will be notified in line with laid down procedures;

- Metrofile will be instructed and authorised to deliver the latest back-up canisters to the off-site recovery centre, in accordance with agreed and documented procedures;

- The recovery team leaders and/or deputy leaders of each business support unit and strategic business unit will be contacted and notified of the disaster declaration. The recovery team leaders will be instructed and authorised to notify the members of their respective recovery teams and proceed with the implementation of their sections of the documented disaster recovery plan;

- Suitable voice-mail responses on telephone numbers will be arranged at the earliest opportunity; and

- The members of the Crisis Control Unit will determine the time and frequency of future meetings of the unit, to monitor the plan implementation.

8.4 UNIT RESPONSIBILITIES

This section does not attempt to describe the recovery activities as defined and updated in the detailed BCP plans, but rather, to describe unit responsibilities, particularly at the "across all units" level. The responsibilities of the Crisis Control Unit have already been covered in detail.

8.4.1 DIRECTORATES BUSINESS SUPPORT UNITS

8.4.1.1 Human Resources

This unit is represented in the Crisis Control Unit and has the responsibility for staff matters, in conjunction with the individual Directorates.

- Staff re-assurance;
- Staff temporary relocation; and
- Communication with staff family in the event of death or injury.

8.4.1.2 Finance and Insurance

This unit is represented in the Crisis Control Unit and plays an important role in ensuring effective business resumption in the post disaster environment by:

- Where necessary arranging the required cash flow to enable the recovery process;
- Where necessary arranging for the authorisation of additional official signatories in the post disaster situation;
- Assisting the Directorates in the analysis of Service Level Agreements and the potential financial penalties related thereto;
- Managing post disaster structure and equipment insurance claims arising from the disaster;
- Managing claims related to consequential losses arising from the disaster;
- Managing key personnel insurance claims arising from the disaster;
- Managing personal injury claims arising from the disaster; and
- Managing claims from SLA penalties occurred in the post disaster environment.

8.4.1.3 Communication (ACS)

This unit is represented in the Crisis Control Unit and plays an important role in the post disaster communication and re-assurance process by:

- Assisting Directorates in ongoing contact with and re-assurance of clients;
- Assisting with ongoing marketing related communications with SAQA and its clients; and
- Assisting Information Technology in maintaining communication with the strategic business units in the post disaster environment.

8.4.1.4 Information Technology

This unit is represented in the Crisis Control Unit and plays a vital role in the post disaster recovery and return after restoration environments. Information Technology provides the operational platform for all business related units. Information Technology has an excellent knowledge and understanding of the business unit post disaster requirements, as the IT recovery plan is largely based on:

- Impact on overall business of prolonged downtime for each business unit;

- Business Unit recovery priorities related to the business as a whole;
- Minimum recovery requirements for each business unit, with associated recovery timeframes; and
- Business Unit exposure to SLA related financial penalties.

Regular post disaster communication between Information Technology and the Crisis Control Unit, largely through the Crisis Control Officer is therefore critical.

8.4.2 DIRECTORATES

The individual Directorates are responsible for the development of their own business specific BCP plans, including notification of unit specific clients and service providers. From an overall recovery perspective it is important that each business unit provides the Crisis Control Unit with accurate and detailed post disaster requirements, as the entire plan is largely developed around these requirements and priorities.