INFORMATION AND COMMUNICATION TECHNOLOGY SERVICE CONTINUITY MANAGEMENT SUB-GUIDELINE

Version 0.1

19 January 2018

Table of Contents

1. INTRODUCTION

The South African Public Service transformation is, at a strategic level, informed by public service-wide strategic priority areas and is guided by principles of equal access to services, increased productivity and lowering of costs. In this regard the continuance of the business of government in support of service delivery, thus business continuity, is of utmost importance.

As government is the custodian of extensive information holdings it relies upon its information assets for fiscal, policy and service delivery initiatives. The management of public information requires government to protect the integrity and availability of the information assets in its care. As information is the backbone of the achievement of business objectives and government service delivery, security breaches to integrated government services can cause crippling effects on the service delivery by the public service, with major inconveniences to the users of services.

There is an increasing realisation that public service delivery and its sustainability can be radically improved by unlocking the capability of Information and Communication Technology (ICT) as business enabler. To derive value from ICT as a strategic resource is not achievable in absence of or within a weak secure ICT environment that fails to ensure the confidentiality, integrity and availability of information within the underlying ICT systems and business processes. Achieving ICT security requires the effective management of risk, which encompasses risks from physical, human and technology related threats associated with all forms of use and or processing of information within the institution.

In recent years ICT has become integral to many of the essential activities carried out by institutions. The advent of the Internet and other electronic networking services together with the current and developing capabilities of systems and applications, has also meant that those institutions have become more and more dependent on reliable, safe and secure ICT infrastructures.

At the same time the need for business continuity management (BCM), including incident preparedness, disaster recovery planning, and emergency response and management, has become steadily more prevalent in developed and developing economies. Failures of supporting ICT services (including information security issues such as systems intrusion and malware infections) are recognized as having the potential to impact the continuity of business operations. As a result managing ICT and related continuity and other security aspects forms an essential component of business continuity requirements. In addition it is often the case that critical business functions that require business continuity are usually dependent upon ICT. This dependence means that disruptions to ICT can constitute strategic risks to the reputation of an institution and its ability to operate effectively.

Failures of ICT services, including the occurrence of security issues such as systems intrusion and malware infections will impact the continuity of business operations. ICT readiness is an essential component for many institutions in the implementation of business continuity management and information security management. In order for an institution to achieve ICT readiness for continuity, it needs to put in place systematic processes to prevent, predict and manage ICT disruption and incidents which have potential to disrupt ICT services.

2. PURPOSE

The 2014/2015 Auditor General Consolidated General Report on National and Provincial audit outcomes, mentions that only 31 % of the auditees have IT controls that are embedded and functioning effectively, 47 % of them continue to experience challenges with design of DRP (Disaster Recovery Plan) while 22 % have challenges with the implementation of adequate IT Service Continuity controls. The most common findings were as follows:

- The disaster recovery plan and backup procedures are not adequately designed;
- Backups are inadequately controlled;
- Persistent Unavailability of Services;
- Disaster recovery plan are there but outdated;
- Disaster recovery plan are not approved and maintained;
- Disaster recovery plan are approved but not tested;
- Lack of implementation of DRP;
- SITA Transversal DRP testing not complied with;
- Mostly the recommended DR mitigation strategies are expensive and institutions do not have funds to implement the recommendations;
- No specific skills to manage DRP; and
- Business Continuity not existing and ICT is expected to manage BCP.

The purpose of this guideline is to guide and assist government institutions with ICT service continuity planning challenges they face on a daily basis.

3. SCOPE

This guideline encompasses most ICT processes and technology that supports critical business functions. The successful implementation of this depends on commitment of senior management and the support of all institutional officials within all spheres of the institution and the respective suppliers.

4. LEGAL FRAMEWORK

4.1. **Section 195(1) of the Constitution of the Republic of South Africa of 1996** (Constitution)**,** as amended, provides that public administration must be governed by the democratic values and principles in a professional, accountable and development oriented way whilst promoting efficient, economic and effective use of resources, including IT.

4.2. **Section 3(1) of the Public Service Act (PSA) of 1994,** as amended, mandates the Minister for Public Service and Administration (MPSA) to establish norms and standards that inform proper management and functioning of national and provincial departments.

4.3. These norms and standards referred to in **Section 3(1)** include *inter alia* matters relating to the optimal utilization of IT as a valuable and scarce resource.

4.4. **Chapter 5, Part 1 of the Public Service Regulations (PSR) of 2016,** as amended, enjoins departments (institutions) to manage Information Technology effectively and efficiently. The Batho-Pele principle of offering equal access to services, increase in productivity and lowering of cost, shall inform the acquisition, management and use of information technology and IT not be acquired for its own sake.

4.5. **Section 14 of the Public Administration Management Act (PAMA)** of 2014 provides that the Head of an Institution must—

a) Acquire and use information and communication technologies in a manner which—

(i) leverages economies of scale to provide for cost effective service;

(ii) ensures the interoperability of its information systems with information systems of other institutions to enhance internal efficiency or service delivery;

(iii) eliminates unnecessary duplication of information and communication technologies in the public administration; and

(iv) ensures security of its information systems (confidentiality, integrity and availability);

b) Use information and communication technologies to develop and enhance the delivery of its services in the public administration;

c) Align the use by staff of information and communication technologies to achieve optimal service delivery; and

d) Promote access to public services through the use of information and communication technologies.

4.6. **Chapter 8 of the Minimum Information Security Standards (MISS)** provides that institutions must make provisions for contingency planning (see Chapter 2 "Definitions") aimed at preventing and/or combating any disaster or emergency. The contingency plan must be geared for saving lives, safeguarding property and information and ensuring that activities can continue with as little disruption as possible.

These aims can be achieved only through well-organized action in which all the available means and manpower are used in a coordinated and effective way to put preventative and/or control measures into operation, and through regular practice of the contingency plan.

5. BUSINESS CONTINUITY MANAGEMENT

Government institutions are required to be prepared and to re-establish business or services as swiftly and smoothly as possible.

Information service continuity should be embedded in the institution’s business continuity management systems. Business continuity plans should include the evaluation of security risks in line with the directions set by institution’s Business Continuity Plan.

Business continuity represent the capability of the institution to continue delivery of products and / or services at acceptable predefined levels should an unexpected event occur following a disruptive incident.

Business continuity encompasses a set of planning, preparatory and related activities which are intended to ensure that an institution's critical business functions will :

- Be protected against unavailability of critical services;
- Reduce the likelihood of occurrence;
- Prepare for, respond to, and recover from disruptive incidents when they arise; and
- To ensure that critical services are recovered to an operational state within a reasonably short period.

Business Continuity Management (BCM) is a holistic management process that identifies potential events threatening an institution's continuity of business activities and provides a framework for building resilience and capability for an effective response that safeguards the interests of the institution from disruptions.

BCM activities include but are not limited to incident preparedness, ICT service continuity management (ISCM), disaster recovery planning (DRP) and risk mitigation in order to increase the resilience of the institution.

Note: **Business Continuity Management (BCM) is not an ICT responsibility**. Therefore ICT should ensure that the ICT Service Management Continuity supports the institution’s Business Continuity Planning as a subset.

6. BUSINESS CONTINUITY MANAGEMENT AND ITS RELATED ICT OUTPUT AND DESIRED OUTCOME

Activities involved in BCM include incident preparedness, operational continuity management, disaster recovery planning (DRP) and risk mitigation which focus on increasing the resilience of the institution and by preparing it to react effectively to incidents and recover within predetermined timescales.

An institution therefore sets out its BCM priorities and it is these which drive the IT Service Continuity activities. In turn BCM depends upon ICT Service Continuity to ensure that the institution can meet its overall continuity objectives at all times, and particularly during times of disruption. ICT disaster readiness activities aim to:

- Improve the incident detection capabilities;
- Prevent a sudden or drastic failure;
- Enable an acceptable degradation of operational status should the failure be unstoppable;
- Shorten recovery time;
- Minimize impact upon eventual occurrence of the incident;
- Minimizing risk of delays;
- Guaranteeing the reliability of standby systems;
- Providing a standard for testing the plan;
- Minimizing decision-making during a disaster;
- Reducing potential legal liabilities; and
- Lowering unnecessarily stressful work environment.

5.1. MANAGEMENT LEADERSHIP AND COMMITMENT

To be effective an ICT Service Continuity program should be a process fully integrated with the institution's management activities, driven from the top of the institution, endorsed and promoted by top management.

A number of professional IT Service Continuity practitioners and staff from other management disciplines and institutions may be required to support and manage the ICT Service Continuity program. The quantity and competence of resources required to support such a program will be dependent upon the size and complexity of the institution.

Top management should demonstrate leadership and commitment with respect to ICT Service Continuity by:

- Establish roles, responsibilities and competencies for ICT Service Continuity Management;
- Ensuring that the policies, structures, processes and objective are established for the ICT continuity management and are compatible with the strategic direction of the institution;
- Supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility;
- Ensuring the integration of ICT Service Continuity Management system requirements into the institution's business process;
- Ensuring that the resources needed for the ICT Service Continuity Management system are available;
- Communicating the importance of effective ICT Service Continuity Management and adherence to the DRP requirements;
- Ensuring that the DRP achieves its intended outcome(s);
- Directing and supporting persons to contribute to the effectiveness of ICT Service Continuity;
- Promoting continual improvement;
- Define a criteria for accepting risks and the acceptable levels of risk;
- Actively engaging in exercising and testing;
- Ensuring that internal audits of ICT Service Continuity are conducted; and
- Monitoring and Evaluation (M & E) to determine measurable criteria to evaluate the effectiveness of the ISCM system.

5.2. RISK ASSESMENT

The purpose of the risk assessment is to identify, analyse and evaluate risks that impacts on Business Continuity. After defining recovery requirements, each potential threat may require unique recovery steps. Common threats include:

- Earthquake;
- Fire;
- Flood;
- Cyber-attack;
- Sabotage (insider or external threat);
- Hurricane or other major storm;
- Utility outage;
- Terrorism/Piracy;
- War/civil disorder;
- Theft (insider or external threat, vital information or material);
- Random failure of mission-critical systems; and
- Power cut.

5.3. BUSINESS IMPACT ANALYSIS

A Business Impact Analysis (BIA) is the process to analyse activities and the effect that a business disruption might have on them. It differentiates critical (urgent) and non-critical (non-urgent) institution functions/activities. Critical functions are those whose disruption is regarded as unacceptable. Perceptions of acceptability are affected by the cost of recovery solutions. A function may also be considered critical if dictated by law.

It is important that whilst an analysis of the disaster aftermath is calculated, reputational loss and financial loss should always be taken into consideration. Systems register, system owners and all interdependencies should always be considered when a business impact analysis is conducted. All interim and alternative plans including manual processes should also be taken into consideration.

For each critical (in scope) function, the following values should be assigned:

- **Minimum Business Continuity Objective** (MBCO) – minimum level of services and / or products that is acceptable to the institution to achieve its business objectives during a disruptions;
- **Recovery Point Objective** (RPO) – measures the ability to recover information by specifying a point to which information used by an activity must be restored to enable the activity to operate on resumption. It determines the maximum

acceptable for the data loss. For example is it acceptable for the company to lose 2 days of data?

- **Recovery Time Objective** (RTO) – period of time following an incident within which the product / service / activity must be rescued or resources must be recovered; and
- **Maximum Tolerable Period of Disruption** (MTPD). The recovery point objective must ensure that the maximum tolerable data loss for each activity is not exceeded. The recovery time objective must ensure that the MTPD for each activity is not exceeded.

Next, the impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the following information:

- The business requirements for recovery of the critical function, and/or
- The technical requirements for recovery of the critical function.

Note: BCM is not an ICT responsibility

7. ICT SERVICE CONTINUITY

As a subset of the BCM process, ICT Service Continuity refers to a management system which complements and supports an institution's BCM and/or Information Security Management System (ISMS) program, to improve the readiness of the institution to:

- Respond to the constantly changing risk environment;
- Ensure continuation of critical business operations supported by the related ICT services;
- Be ready to respond before an ICT service disruption occurs, upon detection of one or a series of related events that become incidents; and
- To respond and recover from incidents/disasters and failures.

Failures of ICT services, including occurrence of security issues such as system intrusions and malware infections will impact on the continuity of business operations. Thus managing ICT and related continuity and other security aspects form a key part of business continuity requirements. In a majority of cases critical business functions that require Business Continuity are dependent on ICT. Thus disruptions to ICT can constitute a strategic risk to the ability of the institution to operate in times of disruptions.

ICT services must be ready to support business operations in the event of emerging events and incidents, and related disruptions that could affect continuity (including security) of critical business functions. It also enables the institution to measure performance within which ISCM should perform.

It is advisable that whilst embarking on a plan for ICT Service Continuity, SITA redundancy plans (for the departments using SITA) on data lines be taken into consideration and be properly understood.

8. ICT SERVICE CONTINUITY GOVERNANCE STRUCTURES

The institution should form a Disaster Recovery team that will assist in the entire disaster recovery operations. The team should be composed of core members from all institutions with representative from the top management. The team will also be responsible for overseeing the development and implementation of the disaster recovery plan.

8.1 DISASTER RECOVERY LEADER

The disaster recovery leader should oversee the entire disaster recovery process and is responsible for making all decisions related to the disaster recovery efforts. He/she should be the first person to take action in the event of a disaster. This person should evaluate the disaster and should determine what steps need to be taken to get the institution back to business as usual.

This person's primary role should be to guide the disaster recovery process. All other individuals involved in the disaster recovery process should report to this person in the event that a disaster occurs, regardless of their business unit and existing managers. All efforts shall be made to ensure that this person be separate from the rest of the disaster management teams to keep his / her decisions unbiased. The disaster recovery leader should report to the executive management team (ie.Exco).

Roles and Responsibilities

- Establishment and convening of emergency teams;
- Crisis management;
- Make the determination that a disaster has occurred and trigger a DRP and related processes;
- Be the single point of contact for and oversee all the DR teams;
- Organize and chair regular meetings of the DR team and leads throughout the disaster;
- Report to the management team on the state of the disaster and the decisions that need to be made;

- Organize, supervise and manage all DRP test and author all DR updates;
- Set the DR into motion after the disaster has been declared;
- Determine the magnitude and class of the disaster;
- Determine what systems and processes have been affected by the disaster;
- Communicate the disaster to the other disaster recovery teams;

8.2 ICT Disaster Recovery Team

This team should oversee the entire disaster recovery process. They should be the first team that should take action in the event of a disaster. This team should evaluate the disaster and determine what steps need to be taken to get the institution back to business as usual.

Roles & Responsibilities

- Set the DRP into motion after the disaster recovery leader has declared a disaster;
- Determine the magnitude and class of the disaster;
- Determine what systems and processes have been affected by the disaster;
- Communicate the disaster to the disaster recovery teams;
- Determine what first steps need to be taken by the disaster recovery teams;
- Keep the disaster recovery teams on track with pre-determined expectations and goals;
- Keep a record of money spent during the disaster recovery process;
- Ensure that all decisions made abide by the DRP and policies set by the institution;
- Ensure that the secondary site is fully functional and secure;
- Create a detailed report of all steps undertaken in the disaster recovery process;
- Notify all relevant parties once the disaster is over and normal business functionality has been restored ; and
- After the institution is back to business as usual, this team should be required to summarize any and all costs, the team should also provide a report to the Disaster Recovery Leader summarizing their activities during the disaster.

9. OUTCOMES AND BENEFITS OF ICT SERVICE CONTINUITY

The benefits of effective ICT Service Continuity for the institution are that it:

- Understands the risks to continuity of ICT services and their vulnerabilities;

- Identifies the potential impacts of disruption to ICT services;
- Encourages improved collaboration between its business managers and its ICT service providers (internal and external);
- Develops and enhances competence in its ICT staff by demonstrating credible responses through exercising ICT continuity plans and testing IT Service Continuity arrangements; and
- Provides assurance to top management that it can depend upon predetermined levels of ICT services and receive adequate support and communications in the event of a disruption.

Thus ICT Service Continuity provides a meaningful way to determine the status of an institution's ICT services in supporting its business continuity objectives by addressing the question “is our ICT capable of responding” rather than “is our ICT secure”.

10. THE PRINCIPLES OF ICT SERVICE CONTINUITY

ICT Service Continuity is based around the following key principles:

- **Incident Prevention** - Protecting ICT services from threats, such as environmental and hardware failures, operational errors, malicious attack, and natural disasters, is critical to maintaining the desired levels of systems availability for an institution;
- **Incident Detection** - Detecting incidents at the earliest opportunity will minimize the impact to services, reduce the recovery effort, and preserve the quality of service;
- **Response** - Responding to an incident in the most appropriate manner will lead to a more efficient recovery and minimize downtime. Poor response can result in a minor incident escalating into something more serious;
- **Recovery** - Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data. Understanding the recovery priorities allows the most critical services to be reinstated first. Services of a less critical nature may be reinstated at a later time or, in some circumstances, not at all; and
- **Improvement** – Lessons learned from small and large incidents should be documented, analysed and reviewed. Understanding these lessons will allow the institution to better prepare, control and avoid incidents and disruption.

11. THE ELEMENTS OF ICT SERVICE CONTINUITY

The key elements of ICT Service Continuity can be summarized as follows:

- **People**: the specialists with appropriate skills and knowledge, and competent backup personnel;

A disaster recovery plan includes clearly written policies and specific communication with employees to ensure that both regular and replacement personnel with their details are selected, and that they are informed should a disaster occur. There must also be assurance that the replacement personnel can actually perform the duties assigned to them in an event of an emergency. Periodic training and cross-training is often used to accomplish this. This training includes updates to existing job positions and testing to confirm proficiency. Some of the issues related to this activity verify that (1) policies are being enforced, (2) testing is effective, and (3) training takes place.

- **ICT Facilities**: According to identified risks, the institution should devise strategies for reducing the impact of unavailability of the normal ICT facilities. This may include one or more of the following:
    1. Data centre, disaster sites, computer rooms;
    2. Server-, storage-, switching fibre-, networking-, and cabling infrastructure;
    3. Unified computer stacks (blades, access/concentration/core switches, storage);
    4. Architectures for server, storage, network virtualization, application and desktop delivery;
    5. Management software and software automation data centres (asset and configuration management, capacity planning, billing/chargeback, SLA management, service catalogue management etc.) ;and
    6. End to end private or public cloud architectures.

In considering the use of the alternative premises the following should be taken into consideration

- Site security;
- Staff access;
- Proximity to existing facilities;
- Availability; and
- Cost.

- **Technology**
    - Hardware (including racks, servers, storage arrays, storage devices and fixtures);
    - Network (including data connectivity and voice services), switches and routers; and
    - Software, including operating system and application software, links or interfaces between applications and batch processing routines;

- **Data**: application data, voice data and other types of data;
- **Processes**: including supporting documentation to describe the configuration of ICT resources and to enable the effective operation, recovery and maintenance of ICT services; and
- **Suppliers**: other components of the end-to-end services where ICT service provision is dependent upon an external service provider or another institution within the supply chain, e.g. a financial market data provider, telecoms carrier or internet service provider.

12. DISASTER RECOVERY PLANNING

There are three basic strategies that feature in all disaster recovery plans: (1) preventive measures, (2) detective measures, and (3) corrective measures.

Preventive measures will try to prevent a disaster from occurring. These measures seek to identify and reduce risks. They are designed to mitigate or prevent an event from happening. These measures may include keeping data backed up and off site, using surge protectors, installing generators and conducting routine inspections.

Detective measures are taken to discover the presence of any unwanted events within the ICT infrastructure. Their aim is to uncover new potential threats. They may detect or uncover unwanted events. These measures include but not limited to installing fire alarms, using up-to-date antivirus software, holding employee training sessions, and installing server and network monitoring software.

Corrective measures are aimed to restore a system after a disaster or otherwise unwanted event takes place. These measures focus on fixing or restoring the systems after a disaster. Corrective measures may include keeping critical documents in an offsite location (can be a department in a different province), after a "lessons learned" brainstorming session.

A disaster recovery plan should answer at least three basic questions: (1) what is its objective and purpose, (2) who will be the people or teams who will be responsible in case any disruptions happen, and (3) what will these people do (the procedures to be followed) when the disaster strikes.

13. ICT SERVICE CONTINUITY POLICY

The institution should have a documented ICT Service Continuity policy. Initially, this may be at a high level with further refinement and enhancement as the entire ICT Service Continuity process matures. The policy should be regularly reviewed and updated in line with institution needs and should be consistent with the wider institutional BCM objectives.The ICT Service Continuity policy should provide the institution with documented principles to which it will aspire and against which its ICT Service Continuity effectiveness can be measured. It should:

- Establish and demonstrate commitment of top management to an ICT Service Continuity program;
- Include or make reference to the institution's ICT Service Continuity objectives;
- Define the scope of IT Service Continuity including limitations and exclusions;
- Be approved and signed off by top management;
- Be communicated to appropriate internal and external stakeholders;
- Identify and provide relevant authorities for the availability of resources such as budget; personnel necessary to perform activities in line with the IT Service Continuity policy; and
- Be reviewed at planned intervals and when significant changes, such as environmental changes, change of an institution's business and structure, occur.

It is recommended that the ICT service continuity policy contains the elements mentioned below

13.1 AWARENESS, TRAINING, SKILLS AND KNOWLEDGE

The institution should identify appropriate strategies for maintaining core ICT skills, awareness, and training and knowledge retention. This may extend beyond employees to contractors and other stakeholders who possess extensive ICT specialist skills and knowledge. Strategies to protect and provide those skills and awareness may include:

- Documentation of the way in which critical ICT services are performed;
- Multi-skill training of ICT staff and contractors to enhance skill redundancy;
- Separation of core skills to reduce the concentration of risk (this might entail physical separation of staff with core skills or ensuring that more than one person has the requisite core skills);
- Knowledge retention and management;
- Raise, enhance and maintain awareness through ongoing education / training and information program for executives and relevant employees;
- Establish a process for evaluating the effectiveness of awareness creation; and
- Ensure that staff is aware of how they contribute to achievement of the ICT Service Continuity objectives.

13.2 SOLUTION DESIGN

The solution design phase identifies the most cost-effective disaster recovery solution that meets two main requirements from the impact analysis stage. For ICT purposes. This is commonly expressed as the minimum application and data requirements and the time in which the minimum application and application data must be available.

An effective intellectual property protection strategy is vital for every institution and should be always be implemented.

Outside the ICT domain, preservation of hard copy information, such as contracts, skilled staff or restoration of embedded technology in a process plant must be considered. This phase overlaps with disaster recovery planning methodology. The solution phase determines:

- Secondary work sites (if required, depending on severity of disaster and risk to the institution);
- Telecommunication architecture between primary and secondary work sites;
- Data replication methodology between primary and secondary work sites;
- Applications and data required at the secondary work site;
- Physical data requirements at the secondary work site; and
- Crisis management command structure.

13.3 IMPLEMENTATION

- Activate governance structures;
- Embed Information Security Management / DR plans and procedures;
- Test; and
- M & E reporting.

The implementation phase also involves policy changes, material acquisitions, staffing and testing.

3rd party contracts should include an engagement model that accommodates DR testing.

13.4 TESTING AND INSTITUTIONAL ACCEPTANCE

The purpose of testing is to achieve institutional acceptance that the solution satisfies the recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws or solution implementation errors. Testing may include:

- Technical swing test from primary to secondary work locations (if so required);
- Technical swing test from secondary to primary work locations (if so required);
- Application test;
- Business process test; and
- Crisis command team call-out testing.

The DR plan should be tested regularly, because environments continually change. Tests and disaster recovery drills and exercises should be conducted on a regular basis. An institution should conduct exercises and tests that:

- Are consistent with the scope and objectives of the DRP;
- Are based on appropriate scenarios that well planned with clearly defined aims and objectives;
- Minimize the risk of disruption of operations; and
- Produce formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements.

All institutions should comply with the SITA DR testing to ensure continuity of its Transversal Systems (BAS, Persal, Logis etc.)

13.5 TESTING AND VERIFICATION OF RECOVERY PROCEDURES

The following is proposed as a recovery checklist template

- Define mission-critical institutional functions and establish a hierarchy of operational importance;
- List mission-critical personnel and their job functions;
- List equipment needs of personnel;
- Determine a site relocation for contingency;
- Establish a recovery event task list;
- Document current computer data backup methods and frequencies;
- Identify hard copy documents vital to the department that cannot currently be re-created electronically;
- Identify mission-critical items vital to departmental operations that would be required in the event of a disaster emergency;
- Form an internal ICT emergency response or crisis committee with employees assigned to specific crisis functions. The size of the committee is up to the

department and its needs;

- Create a crisis management media kit. Be prepared for any media or press coverage, providing samples of communications to be sent in an emergency;
- Create a systematic schedule for updating the DR plan, the plan should be reviewed and updated semi-annually; and
- Measure and evaluate – test the plan. If a disaster were to occur, you should create an evaluation check list, asking “How did we do?”.

As work processes change, previous recovery procedures may no longer be suitable. These checks include:

- Are all work processes for critical functions documented?;
- Have the systems used for critical functions changed?;
- Are the documented work checklists meaningful and accurate?; and
- Do the documented work process recovery tasks and supporting disaster recovery infrastructure allow staff to recover within the predetermined recovery time objective?.

Given ever-changing business objectives, one common need in disaster recovery is to perform an audit of the disaster recovery capacity of an institution. The purpose of such audit is to discover how closely an institution's disaster recovery readiness aligns to actual institutional objectives. When conducting an audit of a disaster recovery plan, factors such as alternate site designation, training of personnel, and insurance issues are considered. In conducting a disaster recovery audit, the individual or team performing the audit uses a number of procedures and processes to achieve the objectives of the audit. Successful disaster recovery audits clear state their objectives in an audit plan.

13.6 MAINTENANCE

Maintenance cycles of a DRP manual are broken down into three periodic activities.

Confirmation of information in the manual;

Roll out to staff for awareness; and

Specific training for critical individuals.

- Testing and verification of technical solutions established for recovery operations;
- Testing and verification of institution recovery procedures; and
- Put in place steps to make sure that the DRP is a living document that is approved and updated regularly.
- An institution should acquire key personnel to maintain and update the DR plan.

The DRP maintenance should be incorporated into change management procedures so that any changes in the environment are reflected in the plan itself.

Issues found during the testing phase often must be reintroduced to the analysis phase.

13.7 RESOURCES

ICT Infrastructure Management is vital in ensuring that the required IT **resources** can be recovered within business. It is important that specialized technical resources are maintained and checked. Checks include:

- Application security and service patch distribution;
- Hardware operability;
- Application operability;
- Data verification;
- Data application; and
- Virus definition distribution.

13.8 DOCUMENTATION

To maximize effectiveness, disaster recovery plans are documented and written in a manner that is easily understood by those who will need to use them. In addition, the plan must also be readily available as well, since digging for a hard-to-find or misplaced disaster recovery plan at a time of a disaster can complicate the effect of the disaster. Disaster plans are most effective when updated frequently. DR Plans should also cover new and existing threats. Adequate records need to be retained by the institution.

13.9 CONTROLLING THE BACKUPS

Regardless of classification, the availability of all data should be maintained by means of periodic back-ups and recovery mechanisms. All data should be incorporated as part of a backup procedure.

- **Off-site storage of back-up media**: Back-ups of sensitive, critical, and valuable information should be stored in an environmentally-protected and access-controlled site, situated in an area where the possibility of the risk occurring at this site is minimal. To prevent it from being revealed to or used by unauthorized parties, all sensitive, valuable, or critical information recorded on back-up media (tapes, CDs, etc.) and stored outside institution offices should be covered adequately in the existing contract/arrangement of the service provider;

- **Safeguarding of sensitive information backups**: Back-ups containing sensitive information should be encrypted;
- **Data Retention**: An institution’s minimum and maximum retention periods are often based on contractual, legislative, regulatory, or industry requirements. Information should be retained for as long as necessary but for no longer than the data owner requirements;
- **Archival Storage Data Retention Schedule**: All archival back-up data stored off-site should be reflected in an up-to-date directory which shows the date when the information was most recently modified as well as the nature of the information;
- **Archival Storage Data Media**: All media on which sensitive, valuable, or critical information is stored for periods longer than six (6) months, should not be subject to rapid degradation. Such media should be tested at least annually to ensure that the information is still recoverable;
- All public service related files are to be stored on the institution’s network file server. No public service related files are to be stored on local hard drives. This is critical as no local drives are backed up. The ICT institution will not be able to recover any lost files that were stored on local drives; and
- Personal files should not be stored on network servers – under no circumstances are personal, non-business related files to be stored on an institution’s file servers. In the event of PC theft where confidential data was stored on the local drive, the employee will be held responsible for the loss of such data.

13.10 DRILLS

Practice drills should be conducted periodically to determine how effective the plan is and to determine what changes may be necessary. The auditor’s primary concern here is verifying that these drills are being conducted properly and that problems uncovered during these drills are addressed and procedures designed to deal with these potential deficiencies are implemented and tested to determine their effectiveness.

A document should be drawn up depicting contact details of all staff plus alternate contact numbers, e-mail id's, etc. This is a live document and can become out of date very quickly. Therefore, it should be updated frequently.

13.11 COMMUNICATION ISSUES

Good disaster recovery planning ensures that both management and the recovery team have disaster recovery procedures which allow for effective communication. This can be accomplished by ensuring contact information is easily accessible and that drills conducted test for communication abilities. A good disaster recovery plan includes not only internal communication considerations but external issues as well. Such external communications considers issues related to communication between the institution and outside individuals and institutions, such as business partners. Procedures to test this communication capability generally mirror those of the institution itself. The disaster recovery evaluates these procedures and assumptions to determine if they are reasonable and likely to be effective. Some techniques used by a DR auditor in evaluating readiness include testing of procedures, interviewing employees, making comparison against the DR plans of other company and against industry standards, and examining company manuals and other written procedures. The auditor can verify through direct observation that emergency telephone numbers are listed and easily accessible in the event of a disaster.

13.12 ICT EMERGENCY PROCEDURES

A single person in charge, who knows the steps to take, as per the IT Disaster Recovery Plan will bring order out of the potential chaos which follows a disaster. This person should know what steps are to be taken in the face of a disaster, as detailed in the ICT Disaster Recovery Plan, such as:

- Declare the disaster and set the IT Disaster Recovery Plan in motion;
- Send in First Responders;
- Ensure all staff are contacted and informed of the disaster declared;
- Evacuation of staff where needed;
- Sending the injured etc. to hospital;
- Alerting Emergency Services;
- Ensure only the designated person interacts with the media and public;
- Frequently update staff, stakeholders, media and public in an open and honest manner without being alarmist;
- Start-up alternate production centres if needed; and
- When normalcy is restored, withdraw the Disaster declaration.

In short, the designated person will be in overall charge of all components of the ICT Disaster Recovery Plan.

13.13 ENVIRONMENTAL ISSUES

Environmental issues mentioned below are examples of disasters to take cognisance of:

- **Flooding**

  If there's a list of items to ban in your server room, water should be on there. To keep your datacenter a dry zone, choose a room without water pipes behind the walls and ceiling. Water leaking through ceilings can be such a danger that some datacenters deploy "umbrellas" over server racks just to safeguard against it. A preventative measure to ensure that water—if it does somehow get in your server room—doesn't damage your equipment is to have it on a raised floor. If it isn't on a raised floor, then avoid using carpet in your server room. Not only does it soak up water, it increases the risk of static electricity. Your server room location also matters, as some places in your building might not be suitable. Generally, your server room should not be in your basement because of increased flooding risk. Finally, consider getting a water sensor that constantly monitors the server room and can alert you when there's danger.

- **Fire**

  Fire protection can be tricky for a server room because water can damage electrical equipment just like fire. You need to ditch the sprinkler system as your first line of defense against fire your server room. Instead, your primary suppression system should be a gas or dry-chemical based. In the past, Halon used to be the common choice for many organizations, but its toxicity and environmental unfriendliness makes it a less-than-ideal choice. Instead, consider agents such as FM-200 or HFC 125 for your fire suppression needs, with water as a backup. Just be sure to have an emergency power shut off button in the room so when the water dumps, no electricity is flowing through the equipment.

- **Theft**

  Theft is another type of disaster that can result in massive damage—more than an earthquake in fact. Best practices to reduce risk of theft include keeping access to the server room under lock and key, eliminating external entry points, installing a surveillance system, and requiring biometric scanning for entry. If you have any windows in your server room, you should cover them or otherwise prevent entry through them. You don't want to spend a lot on limiting entry through the doors and have someone just break a window to get in.

- **Power Outages**

  Limit the chances of a complete power outage in your server room by deploying a backup power generator that can run your equipment indefinitely. A gas generator should suffice, as that can be constantly refilled. Until that generator comes online however, you'll need an uninterruptible power supply (UPS) to ensure power stays flowing. If you don't have a backup generator, use the time that the UPS buys you to safely power down your server room equipment.

13.14 SUPPLIERS

The institution should identify and document external dependencies which support ICT service provision and take adequate steps to ensure that critical equipment and services can be provided by their suppliers within predetermined and agreed time frames. Such dependencies may exist for hardware, software, telecoms, applications, third party hosting services, and environmental issues, such as air conditioning, environmental monitoring and fire suppression. Strategies for these services may include:

- Storage of additional equipment and software copies at another location;
- Arrangements with suppliers for the delivery of replacement equipment at short notice;
- Rapid repair and /or replacement of faulty parts in the event of an equipment malfunction;
- Dual supply of utilities such as power and telecoms;
- Emergency generating equipment; and
- Identification of alternative / substitute suppliers.

The institution should include ICT and business continuity management requirements in contracts with its partners and service providers. Contract schedules should include reference to each party's obligations, agreed service levels, response to major incidents, cost assignment, exercising frequency and corrective actions.

13.15 MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION

ICT Service Continuity will eventually be monitored through MPAT.

14. ESTABLISHING ICT SERVICE CONTINUITY

IT service continuity is likely to be more efficient and cost effective when designed and built into ICT services from their inception as part of an ICT Service Continuity strategy which supports the institution's BC objectives. This ensures that ICT services are better built, better understood and more resilient.

The institution should develop, implement, maintain and continually improve a set of documented processes which will support ICT Service Continuity.

These processes should ensure that: the ICT Service Continuity objectives are clearly stated, understood and communicated, and top management's commitment to ICT Service Continuity is demonstrated.

15. REFERENCES

[1] South Africa. Promotion of Access to Information Act 2 of 2000

[2] South Africa. Electronic Transactions and Communication Act No 25 of 2002

[3] South Africa. Regulation of Interception of Communications and Provision of Communication Related Information Act No.70 of 2002

[4] South Africa. Minimum Information Security Standards (MISS) of 1996

[5] South Africa. National Strategic Intelligence Act 39 of 1994

[6] South Africa. Public Service Regulations, Chapter 5 Part II, 2001 - Government Notice No. R.1 of 5 January 2001

[7] ISO/IEC 22301: 2012 Societal Security – Business Continuity Management Systems – Requirements

[8] ISO/IEC 27031: 2011 Security Techniques – Guidelines for Information and Communication Technology readiness for business continuity

[9] ISO/IEC 24762: 2008 Information Technology – Security Techniques- Guidelines for information and communications technology disaster recovery services

[10] South Africa. State Information Technology Act No.88 of 1998

[11] International Institution for Standardisation: ISO / IEC 27031, 2011

[12] South Africa: Western Cape Government Disaster Recovery Plan

[13] South Africa: KZN Treasury Disaster Recovery Plan