DigiPlex Business Continuity and Crisis Management Manual

Document Number:	Revision:	Issue Date:	Owner
BCP-MAN-01-00-DGS	A	June 2018	CEO

1.0 Introduction

Business continuity management (BCM) should be a fit-for-purpose, business-owned and -driven

activity that unifies a broad spectrum of business and management disciplines, including crisis management, risk management and technology recovery, and should not be limited to information technology disaster recovery (ITDR) (see Figure 1). BCM is directly linked to corporate governance and establishes good management practice.

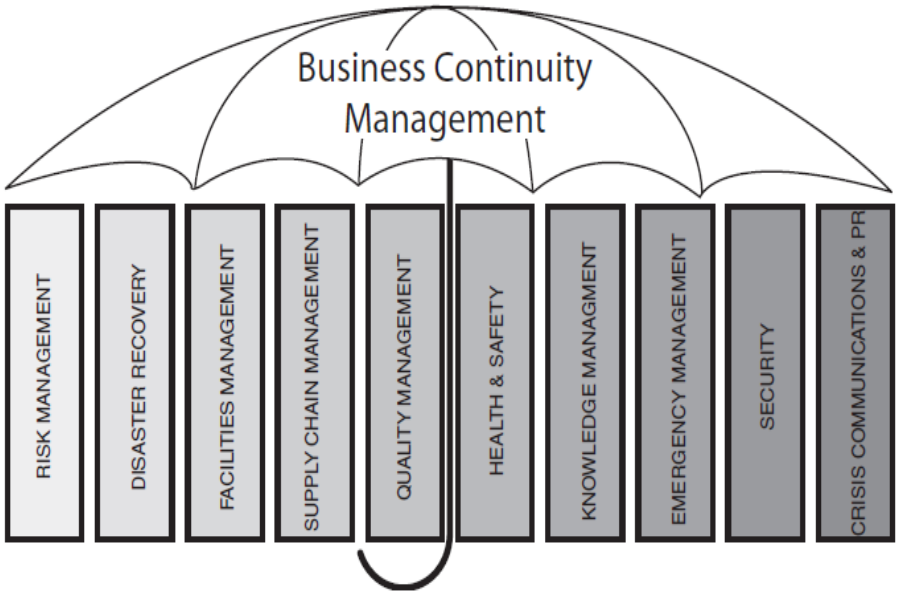


Figure 1 — BCM — the unifying process

BCM establishes a strategic and operational framework to implement, proactively, an organisation's resilience to disruption, interruption or loss in supplying its products and services. It should not purely be a reactive measure taken after an incident has occurred. BCM requires planning across many facets of an organization (see Figure 2); therefore, its resilience depends equally on its management and operational staff, as well as technology, and requires a holistic approach to be taken when establishing a BCM programme.

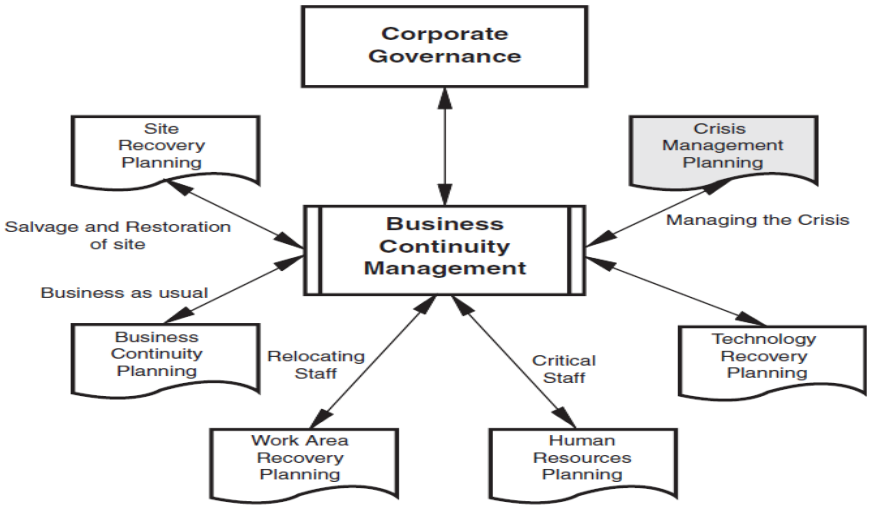


Figure 2 — BCM relationships

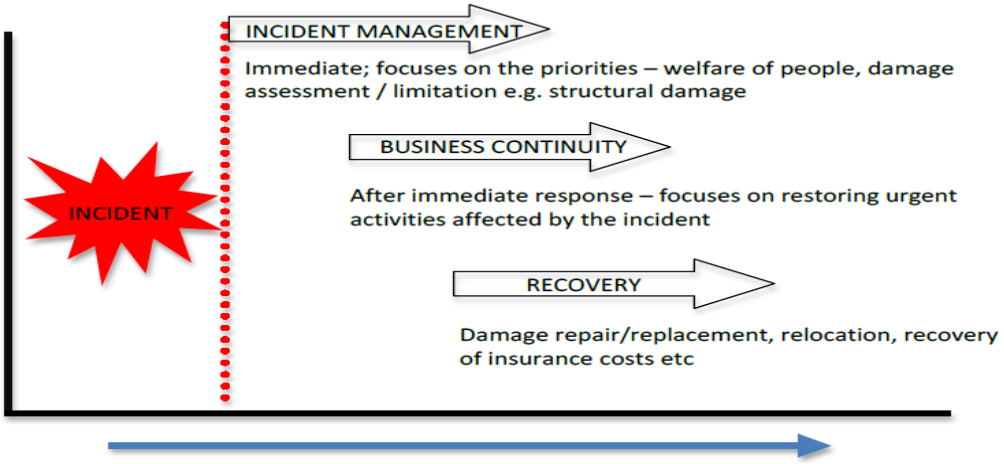
This Manual provides the framework for the effective management of crisis events in order to protect the interests of DigiPlex' stakeholders. It sets out the detailed requirements and minimum levels of achievement necessary to implement the crisis management elements of our Business Continuity Policy Statement – BCP-POL-01-00-DGS.

Managing a crisis effectively (or preventing an incident becoming a crisis) will depend on speed of response and this means having in place:

- clear procedures and lines of responsibility
- staff and other resources that can be deployed at short notice to deal with a sudden crisis
- agreed principles for dealing with the media
- immediate access to relevant information which will be required by media and others.

Business Continuity Management (BCM) is a process that enables DigiPlex to proactively identify and plan to minimise the impact of risks that could affect its objectives, operations and infrastructure. BCM provides the capability for DigiPlex to ensure continuity of after a disruption and to protect its reputation as a leading datacentre owner operator wherever we operate.

The Business Continuity process starts with “Incident Management” as illustrated below1



When a disaster strikes any business organization, three important aspects of managing the incident, recovering from the disaster and ensuring Business Continuity come into play. Though these terms are interrelated, they are different, as they attempt to do various functions as a part of the whole.

Major Incident Plan (MIP), Disaster Recovery (DR) and Business Continuity (BC) Plans are interrelated but distinct. DR details of procedures and steps to recover from a disaster. Major Incident Plan details are steps to be taken to handle the crisis. The BC Plan lists the steps to be taken to ensure continuity of mission-critical business operations. A Major Incident Management Plan and DR Plan are components of the overall BC Plan.

2.0 Definitions

Business continuity (BC)- This aspect of disaster planning involves the processes and procedures a business should put in place to ensure that mission-critical business functions can keep operating during and after a disaster. The emphasis is on maintaining business operations rather than setting right the damage to infrastructure.

Crisis - *Crisis* is defined as: "An intense, unexpected and unstable state that disrupts normal operations, has undesirable outcomes and requires out-of-the-ordinary measures to restore

order and normality" such as disruptive event which affects a business’s facilities, IT systems, data, personnel etc. which leads to a stoppage in production. The halt in production will have a cascading effect on revenues, profitability, production schedules, business reputation, customer goodwill etc.

A crisis could be internal or external in nature. It could be a major crisis or a minor one. Depending on the severity of the crisis, the business may be exposed to adverse publicity. If it is a publicly traded business, the adverse publicity may drive down share value, leading to shareholder unrest.

Crisis Management - *Crisis Management* is the management at a strategic level of the medium and long-term consequences of a Major incident. It will have as its priorities the maintenance of business continuity and the restoration of customer, shareholder and public confidence.

Major Incident Plan- is a part of the overall BC plan. The Major Incident Plan contains the communication and decision-making components of the BC plan. A well thought of and documented Major Incident Plan will facilitate communication between all stakeholders with safety considerations being paramount. It will also detail steps to be taken for impact assessment as also interaction with media regarding the crisis and action being taken to contain it.

Disaster Recovery- A Disaster Recovery (DR) Plan deals with the recovery procedures to be put in place when a disaster strikes. A multitude of significant events can halt production. Natural calamities, cyber-attacks, fire, equipment sabotage, labor strife etc. can affect production. The DR Plan documents the procedures, policies and actions that limit the disruption and the steps that need to be taken for recovery. By making a careful impact assessment of various disasters on critical functions, steps can be taken to mitigate, reduce or eliminate the risks.

Emergency Management - Emergency Management is the direct management of the response to an incident and will have as its short-term priorities the preservation of life, protection of property and the prevention of escalation.

3.0 Commitment and Objective

DigiPlex is committed to implementing appropriate management strategies and processes that will identify and manage possible emergency and crisis events associated with all our business activities.

We will:

- identify potential crisis scenarios associated with all our business activities and take appropriate action to prepare for these and other unforeseen events as part of our risk management process.
- prepare appropriate site plans to manage crisis events that could affect our business where appropriate, support our customers in preparing for, and responding to, emergency and crisis events that affect their operations and activities.
- ensure regulatory, legislative and customer requirements will be met.
- train key management staff in the principles of crisis management and undertake appropriate exercises to test and evaluate our plans.
- regularly review our business Continuity management plans to ensure that they remain relevant, robust and effective
- work closely with our customers, our supply chain, the emergency services and other government organisations in the development and execution of our response to emergency and crisis events.
- evaluate our response to exercises and incidents and identify lessons to be learned, so that improvements can be made.
- Regularly review the suitability and effectiveness of our systems to identify improvements that we need to make to be more able to meet our needs and those of our customers and people who have an interest in our work.

3.1 Objectives

DigiPlex's response to an emergency or crisis event will have the following objectives:

- preservation of life and relief of suffering
- protection of property and the environment
- maintenance of business continuity
- minimisation of financial and reputational losses
- restoration of public and customer confidence
- restore normality (or the best that can be achieved) as soon as possible

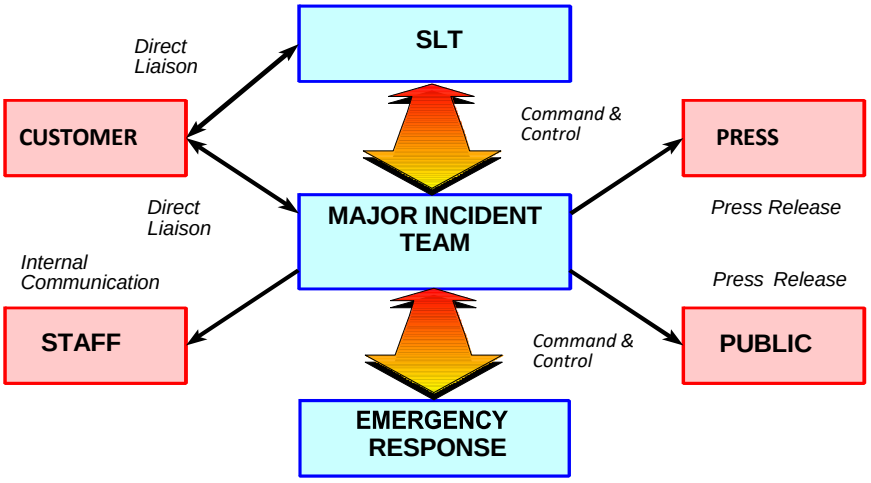
4.0 Scope

DigiPlex's Sites are expected to have plans in place which address the potential crisis or emergency scenarios appropriate to the type of business being undertaken. Specific tasks include:

- identification of possible/likely crisis scenarios based on a formal risk assessment
- development of Emergency Response Procedures, or Major Incident Team Plans or Business Continuity Plans for each Site and the support functions, which should include:
  - organisation and resources
  - information requirements
  - specific procedures for managing identified crisis scenarios
  - specific plans for business continuity and disaster recovery

5.0 Responsibility and Authority

The diagram below shows the Roles and functional elements



5.1 Major Incident Team

- Act to ensure/monitor the overall strategic direction of Business Continuity Management across DigiPlex
- Ensure that the Business Continuity Management Policy and Manual is enforced and resourced appropriately for the benefit of all parts of DigiPlex .
- Responsible for the overall direction of the crisis management response and for making timely executive decisions as required. The Senior Leadership Team will retain responsibility for the on-going management of the business not affected by the crisis.
- Major Incident Team Leader (CEO/COO) - Responsible for the management of the Major Incident Team and supporting staff and will have delegated executive authority to take the necessary measures to bring the crisis under control.

5.2 Compliance & Assurance Director

- Work in partnership with site and group representatives on Business Continuity Management issues
- Support those services in exercising Business Continuity Plans at both group and site level
- Manage, monitor and report on the progress of the Business Continuity Management Strategy and Delivery Plan as required
- In collaboration with other stakeholders make arrangements to promote Business Continuity awareness, advice and assistance.
- Make arrangements to support DigiPlex in undertaking risk and business impact analysis.
- Report on the performance of the Business Continuity Management System to the SLT

5.3 Site Managers /Directors

Site Managers/Directors are responsible for undertaking or delegating:

- Undertaking of a Business Impact Analysis for their area of responsibility
- Preparing a Business Continuity Plan for their area
- Ensuring that arrangements are made to test, maintain and review recovery plans that are their responsibility
- Ensure that site business continuity arrangements are regularly reviewed
- Report on service continuity performance as required
- Ensure that the completed plans are periodically tested.
- To convene any sub groups and support teams that will be required to develop and deliver the objectives and priorities
- Ensure Emergency Response Procedures (ERP) remain current

5.4 Emergency Response Team

Responsible for the execution, monitoring progress and reporting achievement, of agreed actions. The Emergency Response Team leader is the Site Manager /Director and is responsible for briefing the Head of Operations and implementing the Major Incident Teams decisions.

5.5 Human Resources Team.

Responsible for the HR aspects of the major Incident including notification of family/relatives of staff affected by the incident, handling the immediate and long-term needs of the families and supporting other staff affected by the incident.

5.6 Technical Advisors

Responsible for providing specialist technical advice as required covering areas such as technical, legal, political and financial issues.

6.0 Process Overview

Part of good management practice is the preparation of plans covering predictable events. Although a crisis is unlikely to be predictable, many crisis situations can be identified, and appropriate major incident planning measures can and should be taken against these scenarios.

Managing a crisis effectively (or preventing an incident becoming a crisis) will depend on speed of response and this means having in place:

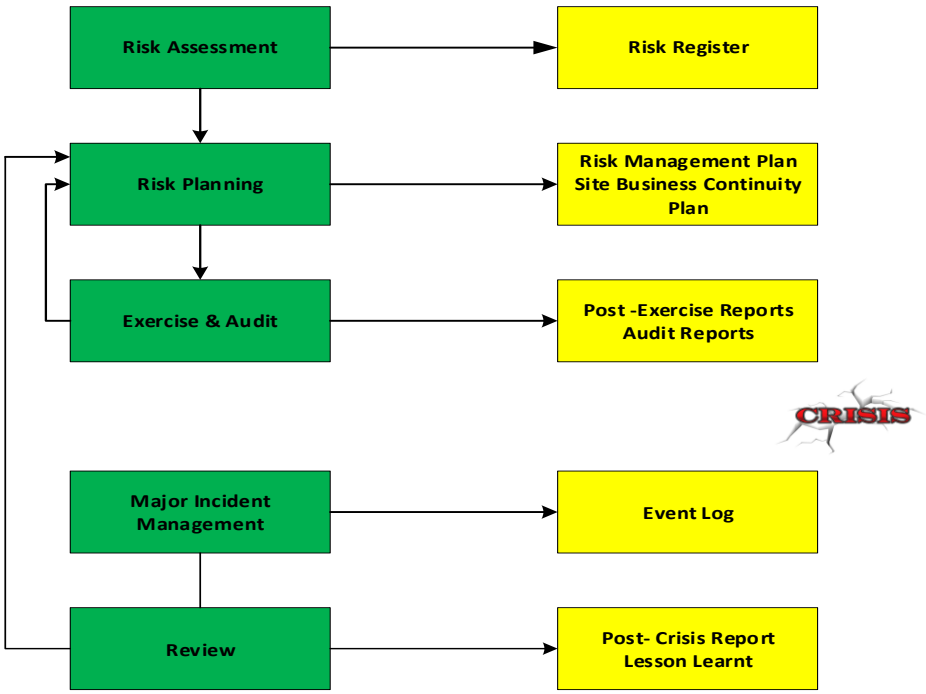
- Clear procedures and lines of responsibility
- Staff and other resources that can be activated at short notice to deal with a crisis
- Agreed principles for dealing with the media
- Instant access to relevant background information which will be required by media and others

The key stages in preparing for a Major Incident are:

- Risk Identification and Assessment
- Risk Planning
- Training
- Review/audit

The aim of these activities will be to reduce the likelihood of a crisis as far as practicable and to prepare contingency plans for critical risks.

The figure illustrates these key activities and identifies the main outputs. The existence of an appropriate Major Incident Management Plan that can provide a framework for the major Incident management actions is a vital part of the whole management process.



7.0 Risk Assessment

The first stage in any crisis management process is to carry out a detailed risk assessment. This will normally be undertaken as part of the normal project or business risk assessment process and will identify a number of risks whose potential impact on the business is sufficiently severe for more detailed risk assessment activities to be undertaken.

DigiPlex has two Risk Management Processes for this at a Strategic level the Risk Management Process, MAN-03-00-DGS describes the process of risk assessment. This Identifies the possible threats to the business that could have a catastrophic impact on DigiPlex's business.

At a Site level the Asset Identification Risk Management Process (IT-PROC-01-00-DGS) describes the process of Risk Assessment linked to our Assets and identifies situations (and combinations of situations) which could develop, and which could constitute a Major incident

8.0 Business Impact Assessment

A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment. Operations may also be interrupted by the failure of a supplier of goods or services or delayed deliveries. There are many possible scenarios which should be considered.

The BIA will identify how quickly essential processes have to return to full operation following a disaster situation.

Each Site shall perform the following BIA process using form BCM-MAN-01-01-DGS :-

Identifying critical activity

- Identifying the relevant strategic process(S) they support
- Allocation of the priority scale and Recovery Time Objective (RTO)
- Recording the impact of disruption on critical activities
- Detailing interdependencies/suppliers/Single Points of Failure (SPOF)
- Documenting workarounds
- Determining minimum resource requirements (staff quantity and skill sets, accommodation requirements, equipment (Inc. vehicles) and vital documentation and ICT (software and networks)).

9.0 Crisis Prevention

To avoid the circumstances which can lead to a crisis situation, it is essential that policies and practices are put in place which identify and control risks. These systems and the training given to the individuals operating them are likely to be very closely scrutinised during a crisis and in any subsequent inquiry. Key systems include:

- **Internal control processes (ISO 9001)** designed to ensure compliance with corporate governance requirements and protect the value and assets of DigiPlex.

- **Safety management systems (OSHAS 18001)** designed to ensure compliance with all statutory Health and Safety legislation, prevent accidents and provide a safe and healthy working environment.

- **Environmental protection systems (ISO 14001)** designed to meet all statutory environmental protection requirements and to reduce any adverse impact on the environment.

- **Special management systems (ISO 27001)** relating to activities such as Information Security.

10.0 Incident Management

Incident Management is managed daily using the Incident Management Procedure OP-PROC-02-00-DGS. Should a disruptive event occur then the Major Incident Management Plan would come into operation.

The Major Incident Management Plan provides the management structure to respond to a major incident using personnel with the necessary responsibility, authority and competence to manage an incident.

11.0 Incident Escalation Levels

Incidents differ in their severity and in the seriousness of their implications for DigiPlex and our customers. Escalation codes reflect five levels of severity shown in the table below. In addition, High Risk Change Management activities require notification to the Senior Leadership team so that they are aware of the changes being undertaken and be prepared should an incident occur.

Priority Level 1—Critical: Life Safety or Catastrophic Failure Actual or Imminent IT Load Loss

Priority 1 Incident Examples	Action to be taken
• An injury that causes death or injury for which hospital admittance is necessary (for one person or more). • A building fire for which evacuation or fire department response is necessary. • Hazardous material released into the environment. • A natural disaster with obvious building damage. • Equipment failure that causes or could cause an SLA Breach to more than 1 customer • PDU or other electrical distribution failure with IT load loss. • One or more server racks down with IT load loss. • UPS on battery because of a distribution failure–recovery not likely. • UPS system on bypass–servers are on raw utility power. • Total loss of water to the building–recovery not likely. • Large-scale cooling system failure. IT load loss is imminent. • An event that causes actual or imminent loss of IT load.	When EOPs are available and recovery is possible: Do the applicable EOPs. Escalate immediately to SLT When applicable EOPs are *not* available: Escalate immediately to SLT SLT activate Major Incident Plan .

High Risk -Change Management Examples	Announcing a Procedure in Progress
• Work that can cause catastrophic facility failure. • Work on a live, critical system at N capacity (no redundancy). • Work on a power or cooling component that represents a single point of failure in a critical system. • Removal of a critical control system from service.	• Send a notification to SLT that describes the work to be carried out

Priority Level 2—High : Loss of Redundancy or System-Wide Vulnerability

Priority Level 2 Incident Examples	Action to be taken
• An injury that results in emergency medical care, or when medical care beyond first aid is necessary for two or more persons. • Equipment failure that causes or could cause an SLA breach to a customer • Chiller failure–if the system is at N capacity. • Chilled water pump failure–if the system is at N capacity. • Loss of BMS control or monitoring to the building • Fire system malfunction. • Power transferred to generators automatically or manually.	• Do the applicable EOPs. • Escalate as soon as possible to SLT • Decision taken by CEO, Head of Operations to activate Major Incident Plan
High Risk - Change Management Examples	**Announcing a Procedure in Progress**
• A procedure that decreases redundancy on one or more critical systems. • Work related to critical environment systems that has a possible effect on the critical load.	• Send a notification alert to SLT that describes the change.

Priority Level 3—Medium N+1 Redundancy Remains (Business as Normal)

Priority Level 3 Incident Examples	Action to be taken
• An injury for which medical care beyond first aid is necessary for only one person. • Chiller failure–if the system has N +1 or more redundancy remaining. • Chilled water pump failure–if the system has N +1 or more redundancy remaining. • Fire alarm started because of a malfunction or non-emergency issue.	• Do the applicable SOPs.

• Other events that decrease the capacity of control systems, but do not cause system failures.	
Moderate Risk- Change Management Examples	**Announcing a Procedure in Progress**
• Scheduled maintenance on the conditioned power distribution system. • Scheduled maintenance on an isolated UPS (no live load). • Large-scale work that does not jeopardize existing redundancies (N+1 or more). • Fire system isolation. • Other procedures that cause a reduction in control or monitoring system capacity.	• No announcement needed

Priority Level 4 Low: Minor Issues

Priority Level 4 Incident Examples	Action to be taken
• An injury for which only first aid treatment is necessary. • Individual IEC, CRAH or CRAC issues.(Not SLA Affecting) • Small leaks (oil, coolant, water). • Filter issues.	• Do the applicable SOPs for regular maintenance or repair.
Low Risk - Change Management Examples	**Announcing a Procedure in Progress**
• Regular activities with minimal risk of effect on the critical load.	(Not applicable)

Level 5 —Planned: Request

Priority Level 5 Event Examples	Action to be taken
• Customer Request • Sales Opportunity	• Request Fulfillment

12.0 Records

A formal record of events is an essential document both for the immediate management of the crisis and for the subsequent analysis of the crisis to learn any lessons. It is possible that such a log may have to become evidence in any legal proceedings arising from the crisis. The log is used to record information received, the decisions made and by whom and any communication with external bodies. The information recorded will provide a verifiable chronology of events from the start. For each incoming and outgoing message and any significant event or decision, the following information must be recorded:

a. Date and time of message/event/decision

b. Message originator – name, organisation, contact number

c. Message recipient

d. Summary of information

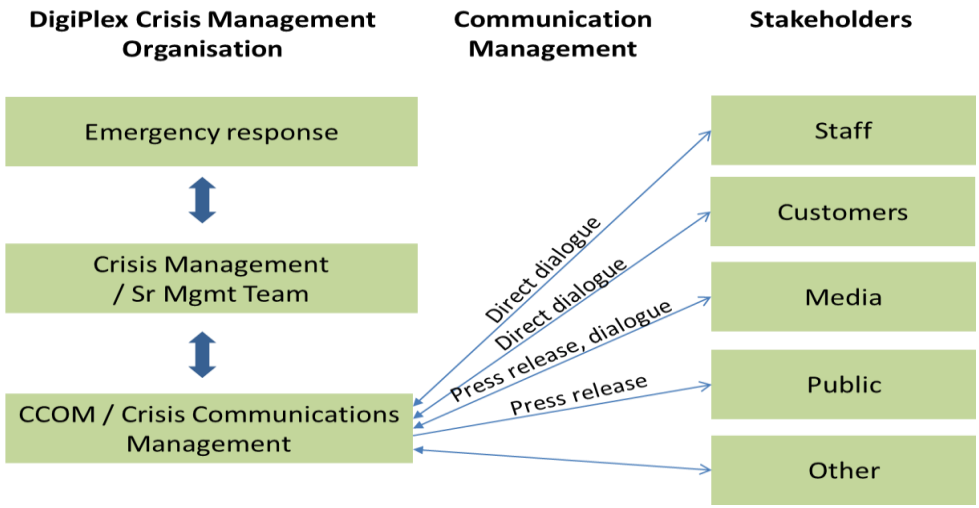
e. Action taken

f. Initials to confirm that the necessary action has been taken

13.0 Communication

The requirement for rapid, accurate information is greater than ever during a serious crisis situation. Handling a crisis properly demands thorough preparation work and a well-thought out communication strategy. Experience from past events and research in this field shows that communication issues comprise up to 70 or 80 percent of an emergency management team's activities during an emergency.

All communication externally shall be via the crisis communication management team what to say and what to do and offer recommendations as to how we handle and coordinate PR work in a crisis situation.



Further information is contained within DigiPlex Group Procedure – CRISIS Communication Plan -CCOM-MAN-01-00-DGS

14.0 Ending the Major Incident

The management of the major incident should not stop until the crisis is truly resolved. Removing the major incident management measures is an important decision that should be made by the Major Incident Leader after an in-depth examination. The following issues should be addressed:

- Declare an end to the Major Incident - It is most important for the company to signal an end to the crisis situation

- Follow up - Stay in touch with the community after a crisis, especially with those directly affected. Keep the media informed of any updates in the situation, and let them know the Major Incident has ended
- Make amends to those affected and then do whatever is necessary to restore your company's reputation in the community
- Assist staff in coming to terms with their experience. Staff who exhibit signs of trauma following a crisis or request assistance in coming to terms with their experience should be referred for professional debriefing and counselling as necessary
- Have a formal debriefing - Debrief members of your Major Incident management team. Analyse the outcome and the media coverage - both positive and negative
- Persons and organisations that have helped in the crisis should be thanked in writing
- Change internal policies or institute new ones to minimise a repeat of the crisis
- Revise this Business Continuity Management plan to reflect what has been learned

15.0 Learning the Lessons

An investigation should be carried out as soon as the crisis is declared over, to determine what went wrong and how the problem was handled. A well-planned debriefing will address the psychological aspects of the crisis and provide information to help improve the Major Incident Plan or Site Business Continuity Plan. Each participant in the major incident team and the main contributors at the location of the emergency should complete a report of his actions, thoughts and suggestions for improvement.

The Major Incident Leader should conduct a debrief of all those involved in the crisis. The results of the debriefing sessions should be used to improve the crisis plan and to identify changes in procedures or processes that are required.

16.0 Site Business Continuity Plans

Each site plan shall define

1. purpose
2. Scope and objectives
3. Activation criteria and procedures,
4. Implementation procedures, roles, responsibilities, and authorities
5. Communication requirements and procedures,
6. Internal and external interdependencies and interactions
7. Resource requirements, and information flow and documentation processes

17.0 Crisis Training

Training of key personnel is essential. Training will be required in several specialist areas such as handling the media and specific technical skills that might be required at certain sites as well as training and familiarisation of the whole Emergency Response Team in operating in a typical crisis environment. This training should precede any formal exercises to test specific aspects of a Major Incident and Site Business Continuity Plans.

Prior to any training taking place, the following steps need to have been taken:

- Potential crisis scenarios have been identified

- Key staff likely to be involved in the management of a crisis have been identified
- A training needs analysis has been performed

17.1 Training

Unlike the emergency services, responding to a crisis situation is not likely to be considered to be part of the normal day-to-day activities for the nominated major incident management team. The importance of training in a properly structured manner is important if the full potential of all the parties involved is to be realised. Key training topics that are likely to be relevant to those involved in a crisis response are:

- **Awareness**. All members of the Emergency Response Team should be aware of possible crisis scenarios and the crisis management organisation and procedures. Training should provide an overview of the key management issues, the importance of team-working and the effects of stress.
- **Media Relations**. Training should cover press and broadcast media communication, the preparation of media press statements and briefs and familiarisation with media handling techniques. For senior staff, likely to be involved in facing journalists, individual practical training in interview and news conference techniques should be undertaken.

17.2 Exercises

Exercises are an important management tool for informing and motivating personnel and giving confidence to those who may be required to respond in a crisis. They bring together those who may be involved with responding to an incident and they allow scrutiny of their responses under controlled conditions. They also provide the only comprehensive way of realistically evaluating contingency plans.

Exercises should reflect reality as far as is practicable. They can establish and reinforce relationships between those taking part, often under stressful conditions. They bring people from different areas together to work as a team, to realise clear goals and to get to know and respect each other's strengths and weaknesses.

17.2.1 Exercise Types

Exercises take four basic forms and their use is dependent on the state of development of the crisis management strategy and the target audience:

- **Seminar**. Seminar exercises are designed to inform participants about DigiPlex the procedures that would be used to respond to an incident. Those involved can be either new to the job, established personnel or those recently identified as key staff. This type of event will bring staff together to inform them of current developments and thinking. These events may take the form of lectures or panel discussions and are primarily designed to focus on one aspect of the response. The emphasis of this type of exercise is on problem identification and solution finding rather than decision making.

- **Table-Top**. Table top exercises are small scale, pre-planned, paper based exercises which aim to test plans, procedures and people in a controlled environment. They provide the few players involved with an opportunity to interact with and understand the roles and responsibilities of the other stakeholders taking part. They can engage players imaginatively and generate high levels of realism. Participants will get to know the people with whom they may be working in responding to a crisis. Those who have worked together and know each other will provide a much more effective response than those who come together for the first time when a real crisis occurs.

- **Drills**. Drills consist of limited activation and mobilisation of personnel and response teams in response to a hypothetical crisis scenario. Drills offer opportunities for personnel to receive "hand-on" crisis management training, demonstrate their capabilities, and validate, to a limited extent, capabilities documented in crisis management plans. Drills can be distinguished from exercises by their limited depth and breadth of participation (generally 2-3 groups), focus on a subset of specific crisis/emergency objectives, involvement of only one or two sites or locations, and limited or no deployment of personnel or equipment. Realism plays an essential part in ensuring that key staff react to a crisis situation in the appropriate manner.

- **Live**. Live exercises range from a small-scale test of one component of the response through to a full-scale test of the whole organisation. Live exercises provide the best means of confirming the satisfactory operation of emergency communications and procedures. Live exercises provide the only means for fully testing the crucial arrangements for handling the media.

- Depending on the customer involved, there may be a few mandatory exercises run throughout the year by various agencies and full or partial participation in one or more of these may be helpful in rehearsing some or all the local response.

17.2.2 Exercise Planning

A graduated programme of exercises should be planned so that all participants have gained appropriate experience before being confronted with a live exercise. It should be noted that significant resources are required to plan and implement realistic and effective live exercises and therefore all participants should have received appropriate training to make best use of time and resources.

The more realistic an exercise, the more beneficial it is to the company and the individuals concerned. The temptation to manipulate the timing of an exercise to avoid any disruption of normal business should be avoided – a degree of disruption is inevitable, and crises tend to strike at the least convenient times.

To provide the maximum value from an exercise, details of the scope and timing of the exercise should be restricted to the planning staff. The elements of surprise,

uncertainty and pressure are major elements of a crisis that need to be replicated as far as possible.

17.2.3 Post- Exercise debrief Review

Provision should be made for objective observation of the exercise by persons from outside the Crisis Management Team. Consideration could also be given to the use of outside consultants who could give feedback at appropriate points, highlighting the repercussions of an action just taken.

The value of an exercise is in testing the crisis management planning and the performance al individuals within the crisis management organisation. Information gathering at all stages is required to give an accurate picture of the response to events as they unfolded. Each exercise will produce lessons to be learned that may need to be incorporated in the Business Continuity Management Plan in readiness for the next exercise or a real-life crisis. The Emergency Response Team should be debriefed as soon as possible after the end of the exercise to ensure it is fresh in people's minds.

Whatever type of exercise is chosen it is important to record and evaluate the event. Provision of a succinct report of successes, failures and corrective actions to which management can refer is a vital part of the overall learning process. In the event of a crisis, previous exercise reports demonstrate to stakeholders, and any subsequent formal inquiry, the commitment of the organisation to the safety of people, property and the environment.

18.0 Audits

DigiPlex's approach to managing Business Continuity, including policy implementation, effectiveness and compliance levels, shall be independently reviewed and documented at regular intervals, or when significant changes to the security implementation occur, via an internal audit programme.

18.1 Internal Audit

The QA & Compliance Manager will undertake Compliance Audits within Departments and on Operating Sites within the DigiPlex Group to ensure that statutory requirements, contractual requirements and good practice is being adhered to. The system audit on DigiPlex Group to ensure compliance with procedure will be undertaken at announced dates.

The Senior Manager or nominated representative of the area being audited will be made aware of the remedial measures required and will implement the necessary works. The Senior Manager will sign off the form to ensure the identified issues have been addressed.

18.2 External Audit

In addition to the audits carried out internally, we may be subject to inspections by Statutory Agencies, and / or the Client.

Further information is contained within DigiPlex Group Procedure QA-PROC-03-00-DGS – Management System Audits; QA-PROC-04-00-DGS– Internal Audits, QA-PROC-05-00-DGS- External Audits

19.0 Management Review

Continuous improvement in the Business Continuity Management is the goal. It is recognised that communication, such as by informing staff members of successes as well as failures, plays a vital part in motivating them to improve performance. To this end the BCMS provides for continuous Management Review to assess the degree of compliance with the performance standards and the effectiveness of the system. The results of these independent audits shall be reviewed by DigiPlex's Senior Leadership Team.

Further information is contained within DigiPlex Group Procedure MAN-PROC-07-00 – DGS Management Review

20.0 Evidence of Compliance

To demonstrate compliance with this Manual, the following documentation is to be available for audit:

Digiplex Group

- Business Continuity and Crisis Management Manual
- Related policy statements and procedures
- Risk assessment of DigiPlex's activities
- Crisis Communication Manual
- Crisis Communication plan(s)
- Major Incident Plan
- Internal Audit reports
- Management Review Records

DigiPlex Sites

- Procedures
- Risk assessment of Sites activities
- Business Impact Assessments
- Business continuity and disaster recovery plan(s)
- Audit/review records
- Testing / Exercise Records