Disaster Planning and Recovery Guide for Small, Medium and Micro Enterprises (SMMEs)

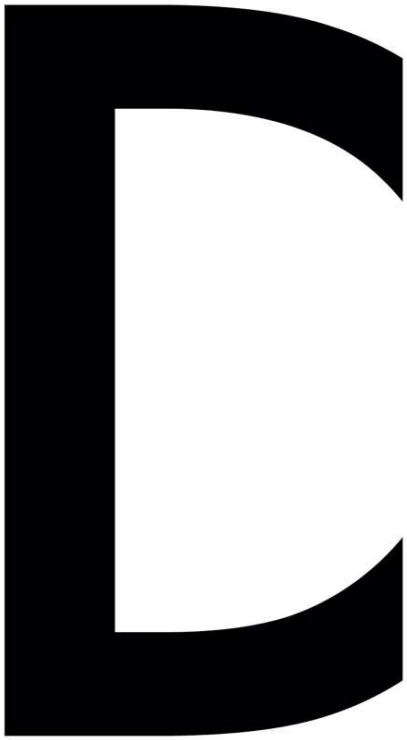
Issue 1 - September 2021

EST 1856

DURBAN CHAMBER OF COMMERCE AND INDUSTRY NPC

saiba

SOUTHERN AFRICAN INSTITUTE FOR BUSINESS ACCOUNTANTS



It is only in our **darkest hours** that we may **discover** the **true strength** of the brilliant light **within ourselves** that can never, ever, be dimmed.

Contents

A word from the CEO

Disasters can have a significant effect on the lives and livelihoods of a nation. There are many types of disasters but those that are self-inflicted may arguably be of most severe psychological impact. The unrest in 2021 in KwaZulu-Natal and Gauteng is estimated to be the most expensive blitz riot to have taken place globally in the past ten years.

According to media reports the South African Special Risk Insurance Association (SASRIA) estimated that claims linked to the civil unrest in July could amount to between R20 billion and R25 Billion.
The purpose of this Disaster Management Guide is to:

- Advocated for improved disaster management and risk educations policies of business.
- Empower the SAIBA member to guide his/her client through the Disaster Management process.
- Serve as a checklist (albeit not comprehensive) for a Durban Chamber of Commerce and Industry member or a SMME to improve preparedness for unforeseen events.

During, and immediately after a disaster it is not easy for a SMME to know what to do. In the weeks and months following the disaster, serious decisions will have to be made about the continuity of the business, tax reliefs and governmental funding programs.

The guide was drafted as a preparedness guide to assist SMME, as far as possible, to plan for a disaster. This may alleviate some of the severity of a disaster.

We hope that with this guide we can contribute to the rebuilding of the SMME sector.

Nicolaas van Wyk
CEO | SAIBA

Disaster Planning and Recovery Guide for the Small, Medium and Micro Enterprises (SMME)

Section 1. Introduction

1.1 General

SMMEs face numerous challenges in South Africa to survive and to prosper. The widespread riots across Gauteng and KZN during July 2021 illustrated how many SMMEs are exposed to business failures when the unforeseen occurs. At the same time, three provinces were declared National Disaster Areas following the worst drought in 100 years. All of this must be dealt with during a Global Covid-19 pandemic that has changed the way we do business forever.

The events of 2020 and 2021 has again illustrated to each SMME owner how unforeseen events may influence the continuity of the business. In this Guide, we do not only deal with external highly publicised disasters such as the Covid-19 pandemic and large-scale political unrest. We also deal with unforeseen events such as the death or divorce of an SMME owner. If not planned for adequately, these events may have a similar impact on the SMME business as a natural disaster.

Whereas large businesses have the financial, technical and professional resources available to deal with these unforeseen disasters, the SMME may not have the ability to deal or recover from such events.

SAIBA members advise and serve our SMME community on a daily basis. In addition, many SAIBA members are not in employment but operate through their own SMME. An unforeseen event may render the SAIBA member's own business inoperative.

The purpose of this Disaster Management Guide is:

- To advocate for improved disaster management and risk reduction policies and practices of businesses.
- To empower the SAIBA member to guide his/her client through the Disaster Management process.
- To serve as a checklist (albeit not comprehensive) for a Durban Chamber of Commerce and Industry (DCCI) member or an SMME to improve preparedness for unforeseen events.

1.2 What the Guide is not

The Guide is not a comprehensive checklist that will cover every eventuality that the SMME may face.

The Guide is furthermore written from a business perspective and not from a private personal perspective.

The Guide is not intended to replace detailed specialist advice (e.g. legal, tax and insurance). The SAIBA member and SMME member is advised to apply their professional judgement and involve specialists where required.

1.3 How should the SAIBA member use the Guide?

The Guide is designed to serve as a "mind-jogger" and foundation for applying the professional judgement of the SAIBA member and the SMME business owner.

This Guide should be used as a starting point in discussions with your client on the topic of disaster management and business continuity matters. As the conversation grows, members should consider involving specialists including but not limited to:

- Attorneys
- Tax Specialists
- Insurance advisors and brokers
- Medical advisors
- Engineers
- Computer specialists

We advise the SAIBA member to consider the contents of the Guide and augment it with his/her own experiences and own professional judgements. Our members are advised to engage with their clients on a structured basis around this very important topic.

SAIBA members should take note that there is no one-size-fits-all Disaster Management Plan. There is simply no replacement for the professional judgement applied.

Section 2. The Disaster Management Plan

The following stages should be managed by the SMME when dealing with unforeseen events.

These stages are discussed below.

2.1 Stage 1: Planning

Many SMMEs only start dealing with the unforeseen event when it occurs. As can be seen from the above illustration, the actual event should only be dealt with under stage 3 of the Disaster Management Plan.

A well-documented and carefully considered plan may be the difference between the SMME surviving the disaster or be subject to business failure. Disaster management and risk reduction policies and practices should be integral aspects of existing strategies and policies in any business.

Under this Stage 1, the SMME should:

- **Assess the risk** of a particular occurrence and then
- **Formulate an action plan** to counter the risk causing significant harm to the business and its people.

These are addressed separately below.

2.1.1 Risk assessment template

In the following table, which is split between "Controllable Risks" and "Uncontrollable Risks" the risk is described together with the impact on the various stakeholders. The table is provided for illustrative purposes. Each business is different and SAIBA members are advised to amend the table as the situation may warrant. The risk assessment table for the pharmacy, the dentist, the farmer, the contractor, the restaurant owner will differ.

UNCONTROLLABLE RISKS (Being risks that the SMME Owner has little or no control over)			IMPACT ON STAKEHOLDERS				
#	Risk description	Likelihood of risk occurring	Employees	Customers/ Public	Fixed Property	Stock/debtors/ cash	Business continuity
1	Global/National health disaster	High/Moderate/Low					
2	Widespread drought, floods or other natural disasters	High/Moderate/Low					
3	Widescale riots, looting, political unrest/war	High/Moderate/Low					
4	Collapse of government and governmental instability	High/Moderate/Low					
5	Economic risk (hyperinflation, collapse of currency)	High/Moderate/Low					
6	Collapse of infrastructure (electricity, roads, water supply)	High/Moderate/Low					

7	Adverse legislation impacting the way that business is performed (e.g. legislation governing margins on pharmaceutical products or amendment of B-BBEE requirements)	High/Moderate/Low					
8	Risk that advancements in technology will negatively impact the goods and services provided by the SMME (digitisation of the economy)	High/Moderate/Low					
9	Impact of aircraft, maritime, road and railway disasters on the SMME business	High/Moderate/Low					
10	Environmental disasters including pollution caused by hazardous material	High/Moderate/Low					
11	[Others – please describe]	High/Moderate/Low					
12	[Others – please describe]	High/Moderate/Low					
13	[Others – please describe]	High/Moderate/Low					

CONTROLLABLE RISKS (Risks that the SMME owner has control over)			IMPACT ON STAKEHOLDERS				
#	Risk description	Likelihood of risk occurring	Employees	Customers/ Public	Fixed Property	Stock/debtors/ cash	Business continuity
1	Death or disability of the business owner/partner	High/Moderate/Low					
2	Conflict between SMME business owners (e.g. family disputes, divorce, emigration)	High/Moderate/Low					
3	Reliance/dependency on key personnel (management, owners, skills) (risk of death/departure)	High/Moderate/Low					
4	Disputes with suppliers of capital (banks, investors)	High/Moderate/Low					
5	Non-compliance with laws (e.g. Consumer Protection Act, health and safety, professional standards, ethical, Competition Law)	High/Moderate/Low					
6	Poor or sub-standard goods or services delivered resulting in claims for damages and reworks	High/Moderate/Low					
7	Disputes with local and foreign tax authorities • Income Tax and CGT • VAT and PAYE • Customs	High/Moderate/Low					

8	Loss or supply base (security in supplies of goods/services/premises to the SMME)	High/Moderate/Low					
9	Loss of customer base (security in supplies of goods/services made by the SMME)	High/Moderate/Low					
10	Reputational risk impacting the goodwill of the SMME.	High/Moderate/Low					
11	Technology risk (cybercrime/loss of data, ERP system failures)	High/Moderate/Low					
12	Corruption/fraud by employees, customers and suppliers (including auditors, business advisors, bookkeepers, attorneys)	High/Moderate/Low					
13	Labour unrest strikes and business disruption	High/Moderate/Low					
14	Risk that customers/suppliers amend their B-BBEE requirements	High/Moderate/Low					
15	Non-compliance with the Occupational Health and Safety Act resulting in claims for damages	High/Moderate/Low					
16	[Others – please describe]	High/Moderate/Low					

The above list is not exhaustive and is provided for illustrative purposes only. It is advised that the list is prepared as comprehensively as possible. A risk that may be low in a particular year may become high within a few days.

In compiling the list, consider the underlying causes of disasters in the business/field/area. Consider what unforeseen events have affected the type of business or businesses in the area in which the SMME operates during the past 20 years. It would be helpful to speak to local insurance brokers, similar business owners and study regional government disaster management plans. In addition, perform research via media, search engines and publications.

The SAIBA member and his/her SMME client should meet at least once a year to reassess the items on the list, the risk ratings and the appropriate plans.

2.1.2 Preventative actions

For each of the risk that management considers to be "high" or "moderate" it is advised that the SMME business owner prepares an action plan. The following table may assist in documenting the plan.

#	Risk description	Action Plan	Estimated cost to implement	Estimated time to implement	Efficiency and effectiveness	Person responsible
1	[Describe the risk that should be addressed]	[Be as detailed as possible. This may include taking out key person insurance for key personnel, include appointing a tax advisor to do a tax health check, agree on a valuation methodology to buy out key personnel, may include increased physical security over property. This will become the official Disaster Management Plan of a business. On completion of the plan the document should: 1. Be communicated and shared with the responsible parties 2. Filed and listed in the companies document register 3. Be easily accessible when disaster strikes Refer to 2.1.3 and section 3 for further considerations.]	[The cost to implement the plan is critical. Due to cost constraints, a phased approach may need to be adopted.]	[The time to implement a plan is important. Often one will settle for a preliminary plan that can be implemented quickly even though it may be less effective.]	[The efficiency of the plan must be considered, i.e. will the plan run smoothly. The effectiveness, i.e. will it achieve the desired outcome must also be addressed.]	[It is important to peg responsibilities on a specific person. Without allocating responsibilities with a timeline, the risk will never be addressed.]

2.1.3 Key consideration when establishing a Disaster Management Plan

Section 3 of this document deals with important considerations, but at a minimum, clarity should be provided with regards to the following:

Area for which clarity must be provided in the action plan	Implementation considerations
Legal framework in the event of death, disability or incapacity of key personnel and owners.	Up to date testament, letter of wishes, key person policies and valuation methodologies (for when share of business should be transferred or bought out upon death).
Appointment of the emergency response team who is responsible for compliance with the Occupational Health and Safety Act in the case of emergencies.	Include duties in employee agreement. Communicate with employees. Consider training programmes for employee/s.
Appointment of key leadership team who is responsible for managing and co-ordinating efforts in the case of emergencies.	Include duties in employee agreement. Ensure key leadership is familiar with all aspects of plan. Consider training programmes for employee/s, including effective conflict resolution communication training.
An evaluation should be made of the amount of capital that is available when business cannot continue for a period of time.	It is strongly advised that the SMME builds sufficient resources so that it can survive business interruptions for a period of 3 weeks to 3 months without impacting business continuity.
A critical evaluation of the insurance framework of the entity is required.	This varies from property insurance, key person insurance, loss of profit insurance, insurance against negligence and insurance against riots and unrest (SASRIA). For further detail, refer to Annexure C.
Consider agreements with service providers and customers and the inclusion of force majeure clauses.	Amend current agreements to include force majeure clause if necessary. For further detail on force majeure, kindly refer to Annexure B.
Staff considerations: retrenchments, leave.	Ensure access to HR specialist when required. Ensure leave policies updated. Ensure provision made for leave and retrenchments pay-outs.

2.2 Stage 2: Early warning systems

Stage 2 of the Disaster Management Plan is to have a system of early warnings in place.

It is critically important for the SMME owner to have his/her "*ear close to the ground*".

Being aware of an impending disaster will enable the SMME owner to take advance precautions against the impact of a disaster occurring, thereby minimising the impact on business.

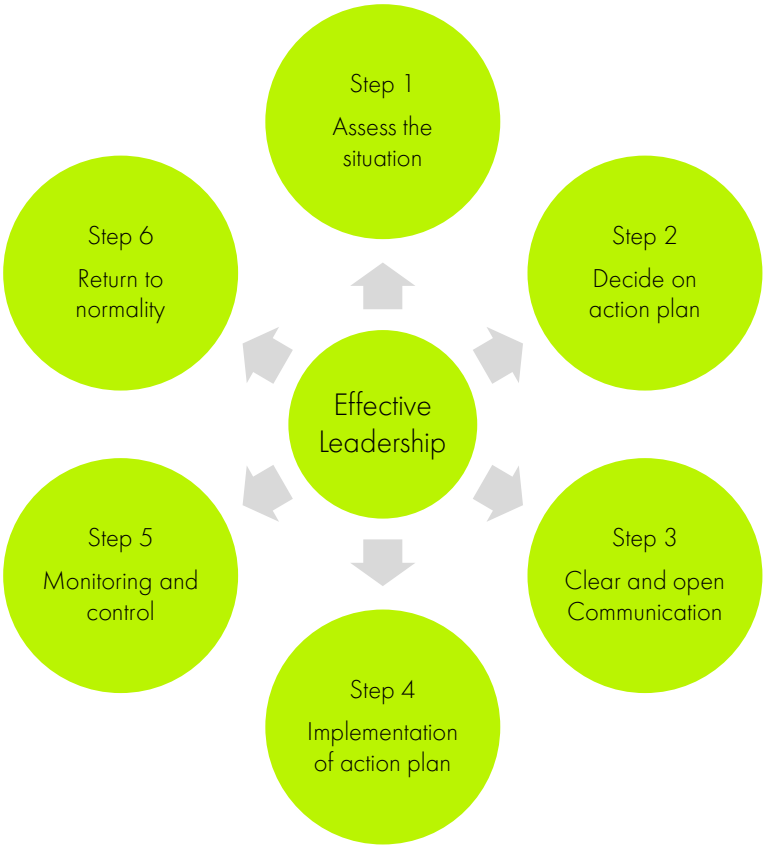
The following are activities of the SMME business owner that will enable him/her to have his/her "ear close to the ground":

- Be active in the community.
    - An SMME which is active in the community is likely to hear of matters arising through the grapevine and can also rely on the support of the community when disaster strikes.
    - Be a "good corporate citizen" and be active in community activities as far as possible. This does not always need to be financial but time and effort in community activities are often more important than financial contributions.
    - Examples of how one becomes involved and active in the community include:
        - Join industry associations or organised business initiatives.
        - Join and become actively involved in the Durban Chamber of Commerce and Industry support networks.
        - Join and become actively part of SAIBA's Practice Support Networks. Individual firms of similar size meeting on a regular basis to share ideas and discuss timely tax, management, and business topics. Members of networking groups can become a resource for technical issues. Read more here https://saiba.org.za/share/practice_support/whatsapp_groups.
        - Volunteer at a local community organisation.
        - Support local businesses by eating out regularly at a local restaurant.
        - Join local businesses and emergency units to your annual company day.
- Create positive relationships with law enforcement (private and public).
    - Join local security forums and subscribe to their newsletters.
    - We also provide further guidance published by external organisations in the Annexures to this Guide.
- Create positive relationships with emergency response units (private and public).
- Create good professional relationships with other SMME owners in the area where operations are carried on.
    - Relationships with other SMME owners in the community must be fostered.
    - Many SMME owners stand together in the time of need.
- Foster and protect an open and honest relationship with key investors, financiers and providers of long term infrastructure. (e.g. banks, private equity houses and landlord.)
- Listen to reputable news channels and read reputable newspapers.
    - The successful SMME owner is the person who is aware of the local and international environment and is aware of current affairs.
    - Subscribe to Accounting Weekly, https://accountingweekly.com/ and https://durbanchamber.co.za/.
    - Subscribe to news publications like News24 and other reputable, trustworthy sites.
- Create a network of trusted professional advisors.
    - Having a network of trusted professional advisors who are not only knowledgeable in their areas of expertise but who know your business is invaluable. These include but are not limited to:
        - Legal advisor
        - Auditors, accountants and tax advisors
        - Insurance advisors/brokers

        - B-BBEE advisors
    - Engage at least once per year with these advisors.
- Create an open-door policy with employees.
    - Trusted employees who are not afraid of speaking-up are invaluable in any organisation.
- Deal timeously and pro-actively with all tax queries with SARS and ensure that tax clearance is "green" at any given point in time.

2.3 Stage 3: Dealing with the event

The ability of the SMME to survive an unforeseen event is directly related to the quality of leadership during the time of crisis management. The responsibility of leadership may be summarised as follows:



Clear and effective leadership is at the centre of managing any crisis

Establishing effective leadership is a priority during any time of crisis.

- Leadership should preferably not rest with a specific individual but in a leadership team that will take overall responsibility for crisis management.
- The first step in crisis management for the leadership team is to assess the situation.
    - Leaders often want to take action before carefully assessing the situation.
    - This should be avoided wherever possible.
    - The leaders should dedicate time (within the constraints created by the unforeseen event) to assess the situation and decide on the appropriate action, taking into consideration and re-evaluating the current Disaster Management Plan as developed in 2.1.2.
    - Taking time when the crisis arises increases the chances that the actions decided upon are efficient and effective and reduce the risk of futile activities that will only worsen the situation.
- Once the situation has been properly assessed, the second step entails the selection of an appropriate action plan.
    - DO NOT DECIDE ON AN ACTION PLAN IF THE SITUATION HAS NOT BEEN PROPERLY ASSESSED!

  - Under a best-case scenario, the SMME owner would have previously developed an action plan and the step merely consists of the adaption/re-assessment and activation of a particular plan.
  - Under worst-case scenario, the situation has not been anticipated at all, and management must develop an action plan from scratch.
  - The action plan must adhere to the following strict priorities:
    - Safety concerns of humans must always be the first priority.
      - The action plan must firstly address the health safety of employees and the general public before any other matter is dealt with.
    - The second priority is the protection of the natural environment.
      - Harm to animals and the risk of pollution should be minimised.
    - The third priority is the protection of the SMME owners' property and infrastructure.
- The third step of the leader is to establish a system of clear and open communication channels. Not only will this reduce the negative impact of "panic" that can be created by misinformation and rumours, but it will enable the leadership team to direct resources to where needed.
  - The leadership team should establish a reliable form of communication depending on the situation. Kindly refer to Annexure E for a more comprehensive Emergency Communication plan and lists.
  - The leadership team should decide what should be communicated to whom and apply professional judgment in this process.
- The fourth step of the leadership team is to implement the chosen action plan. The action plan will depend on the nature of the unforeseen event, but it is important to highlight that there is generally no room for wrong action plans to be implemented.
- The fifth step in the process is that the leadership team should monitor and control the following:
  - The development of the unforeseen event.
  - The implementation of the action plan.
  - Depending on the observations, the leadership team should take necessary corrective actions, redirect resources and generally monitor the situation. This should be done in a calm and collected manner.
- The sixth and last step in this phase is to direct the business back to normality. This step is often overlooked but one should take cognisance of the lessons learned. This step also includes managing the consequences of the unforeseen event. This includes but is not limited to the following:
  - Managing insurance claims.
  - Managing human trauma and counselling needs.
  - Managing legal and tax consequences.
  - Managing the ability of the SMME to continue as a going concern.

2.4 Stage 4: Recovery in the aftermath

Under stage 4, the leadership team should assess how the business can recover following the unforeseen event.

Under a worst-case scenario, the existence of the business may be threatened and a business rescue plan may need to be developed. If the company is trading under insolvent conditions, the requirements of Section 22 of the Companies Act must be considered which prohibits reckless trading and may create personal liabilities for the directors. (Kindly refer to Annexure D for an extract from Section 22 of the Companies Act).

In all instances, management should act in the best interest of employees, customers, creditors and the owners. The availability of trauma counselling for the SMME owner, management, employees and families affected should be seriously considered.

The financial situation should be assessed to establish which of the following scenarios applies to the business:

- A going concern

- Cashflow constraints
- Financial distress (< 6 months)
- Financial distress (>6 months, possible business rescue)
- Liquidity

Clear distinction should be made between:

- Cashflow constraints
- Financial distress and
- Insolvency

The impact on liquidity and solvency may be addressed by any or a combination of the following:

- Consider agreements with service providers - cancel monthly subscriptions not needed, for instance, water delivery or flower deliveries to offices.
- Amend service providers agreements, for instance, the number of security guards.
- Renegotiate customer terms – if a customer cannot settle an account per usual credit terms due to disaster, arrange extension/ pay-off plan.

To establish whether the company is financially distressed, the 6-month look forward test can be applied:

- If it appears to be reasonably unlikely that the company will be able to pay all of its debts as they fall due and payable within the immediate ensuing six months (commercial insolvency test) or
- it appears to be reasonably likely that the company will become insolvent within the immediate ensuing six months (factual/balance sheet insolvency).

Business rescue should be considered when financial distress will continue for longer than 6 months. The aim of business rescue is to allow for the supervision of a distressed company by the business rescue practitioner with the objective of either rescuing the company and allowing it to trade out of its financial predicament, or offering creditors a better dividend than would otherwise be achieved through liquidation.

Companies can be insolvent commercially or factually when it:

- Cannot pay their debts as and when they fall due (commercial insolvency)
- Insolvent balance sheet – liabilities exceed assets (factual insolvency)

During the assessment process consideration should be given to involved specialist (auditors/business rescue practitioners/ legal counsel).

The Guide touches on cashflow management and improvement suggestions in Section 3.

2.5 Stage 5: Learning and adapting

Once the business returns to normality, the SMME owner with his/her leadership team should perform a "post-mortem" and critically analyse the ability of the SMME to deal with the situation.

The leadership team should take this time to adapt the Disaster Management Plan, learn from mistakes made and build and leverage the strengths identified.

This process will then form the foundation for re-assessing the risks as described under phase 1.

Section 3. Important considerations

In this section, we deal with various considerations of the SMME as he/she is applying the Disaster Management Plan as described in Section 2 above. The items discussed in this section is not exhaustive and should be augmented by the SAIBA member and SMME owner taking account of their personal experiences and expertise.

We address the following issues specifically below in more detail:

- Health and Safety precautions
- Protecting the SMMEs property
- Protecting the SMMEs records
- Protecting family wealth
- Managing business continuity during times of business interruption
- Managing employees during times of business interruption
- Managing the personal wellbeing of the SMME owner

3.1 Health and Safety precautions

"Property can be replaced but human life is irreplaceable."

In developing the Disaster Management Plan, the SMME owner should prioritise the wellbeing of employees and the general public.

The following checklist can assist the SMME owner to deal with health and safety aspects:

#	Consideration	Yes/No	How to be addressed
1	Is the SMME compliant with the Occupational Health and Safety Act and ensures that it continuously meets the requirements for the appropriate ISO accreditation, including emergency disaster supplies toolkit and evacuation plan?		
2	Does the physical premises of the SMME create a health and safety risk?		
3	Are guests required to sign the required indemnities upon entry?		
4	Does the product produced or sold by the SMME create a potential health risk to employees or the public?		
5	Is there a suitably equipped and trained health and safety officer or team appointed to deal with any medical emergencies?		
6	Is there sufficient physical protection of employees and their property against crime whilst performing their duties?		
7	Does the SMME have sufficient insurance against claims for personal injuries by employees and the general public?		

3.2 Protecting the SMME's property

The SMME's property creates the ability to operate as a going concern. Loss of property (fixed assets, stock, growing crops, cash resources and intangible assets such as goodwill and reputation) can result in the closure of the business.

The following checklist can assist the SMME owner to protect their property against unforeseen events:

#	Consideration	Yes/No	How addressed?
1	Is the SMME's insurance coverage sufficient that it can continue to operate as a going concern when disaster strikes? This should include the assessment if asset insurance and business interruption insurance is sufficient.		
2	Does the SMME have sufficient physical controls over stock and other property to minimise the risk of losses due to fire and theft.		
3	Are there sufficient internal controls in place to minimise the risk of losses due to fraud, corruption and theft committed by employees (including management), customers and suppliers (or a combination thereof).		
4	Are there sufficient controls in place to minimise the risk of losses caused due to fraud or negligence committed by professional service providers including but not limited to auditors, bookkeepers, tax compliance service providers and legal advisors.		
5	Are there sufficient controls in place to ensure that credit terms are only provided to customers with the ability to meet their obligations of the credit agreements? Consider utilising the services of a credit check service provider.		
6	Does the entity have effective controls in place to ensure that the quality of goods and services provided does not create damage to the reputation of the SMME?		
7	Is the physical property designed in such a manner and materials used so that it can withstand disasters common to the area, such as heavy winds or heavy rainfall.		
8	Are there sufficient controls in place to maintain the safety devices and is the building compliant with the Occupational Health and Safety Act. Specifically: • Are all employees familiar with building safety devices? • Does the safety officer know how to locate utilities (water, gas, electric) and how to turn them off and on.		

#	Consideration	Yes/No	How addressed?
	• Are various detection systems such as smoke alarms, carbon monoxide detectors and fire extinguishers checked at least once a month and are the batteries of safety alarms changed annually.		
9	Are the safety officer and employees familiar with the evacuation plans during emergencies. This includes access control, roll-calls etc.		

3.3 Protecting the SMME's records

The risk of business failure due to a loss of records is material. The vast majority of records are retained electronically and most of the record protection controls are directed around IT controls.

The following checklist can assist the SMME owner to protect its records against unforeseen events:

#	Consideration	Yes/No	How addressed?
1	Does the SMME have an appropriate IT strategy designed to protect its data against cyber-attack and malware?		
2	Is there an appropriate back-up strategy for: • Electronic records • Important physical records such as , insurance policies, health policies, share certificates, etc		
3	Are employees trained to use electronic equipment cautiously and be aware of actions that can lead to: • Malware infections • Loss of confidential data • Commercial espionage		
4	Are there sufficient controls over the transmission of electronic confidential data?		
5	Has the SMME instituted appropriate controls to ensure compliance with the Protection of Personal Information Act (POPI Act)?		
6	Are there sufficient controls over passwords. Is there a back-up plan to ensure access to important information if a key person becomes unavailable?		

3.4 Protecting family wealth

The Covid-19 pandemic re-emphasised the need for the SMME owner to "expect the worst" and make sure that his/her family is sufficiently cared for in the event of death or disability.

The following checklist can assist the SMME owner to protect family wealth:

#	Consideration	Yes/No	How addressed?
1	Is there sufficient life and disability cover on the lives of key personnel and owners of the SMME to ensure that their families are cared for after death?		
2	Where the SMME is a joint venture between two or more individuals, it is important that a succession plan be developed where one or more of the key owners are incapacitated. These steps may include the following: • Have the parties agreed on a valuation methodology where one of the owners wishes to exit and the other partners may buy him/her out? • Is there a methodology on how payment of the exiting owner's shares will be paid? This may include: o Key person policies o Creation of a loan account		
3	Has the exit plan been considered from a tax efficiency perspective?		
4	Are the testaments of all key personnel and owners up to date?		
5	Does the plan include care for minor children and other dependants?		
6	Is a health care proxy included on issues such as "do not resuscitate" (DNR)?		
7	Durable power of attorney: • This document names the person (or other entity) you want to pay your bills and manage your money if you become ill or incapacitated and are unable to make these types of decisions. • The person or entity working on your behalf is your representative, also known as your attorney (not to be confused with your lawyer).		

3.5 Managing business continuity during times of business interruption

Many SMMEs fail since they do not plan in advance for business disruptions.

The following checklist can assist the SMME owner to manage their loans and other liabilities:

#	Consideration	Yes/No	How addressed?
1	Has the SMME considered the level of owner's capital that should be available so that it can meet its obligations as and when they arise – even during a period of business disruption? Note: It is strongly advised that the SMME builds up sufficient owner's capital so that it can survive business disruptions of 3 weeks to 3 months.		
2	Has the business owner considered the risk if suppliers and the landlord cannot be paid within the stipulated time? Is there a contingency plan in place to extend payment terms where necessary?		
3	Do agreements include force majeure clause? (See Annexure B)		
4	Has the business owner considered availability of raw materials and stock and the impact of shortages?		
5	Has the business owner considered the impact of delay in stock supply chain due to damage of infrastructure?		
6	Has the business owner considered the impact of non-compliance to contracts already entered into, such as for the delivery of products already ordered by clients?		

3.6 Managing employees during times of business interruption

With the exception of the SMME business owner, employees are by far the most affected by unforeseen business interruptions.

Faced with uncertainties ranging from their physical and emotional wellbeing to the fear of retrenchment and financial hardship, one must expect extreme reactions from employees.

The following checklist can assist the SMME owner to manage their employees during times of unforeseen business interruption:

#	Consideration	Yes/No	How addressed?
1	Does the SMME owner have access to a human resources specialist who is familiar with labour law and who can guide the SMME owner through the legal framework? This is particularly important when retrenchments are considered.		
2	Is there an appropriate and effective method of communication available for management to inform employees of the Disaster Management Plan and the Disaster Recovery Plan? (Note: It is important for the SMME owner to control the narrative with employees and be as open and honest as possible, given potential legal constraints.)		

3.7 Managing the personal wellbeing of the SMME owner

Unlike a senior official in a large multinational entity, the SMME owner does not necessarily have access to highly skilled resources to whom many of the tasks required in this stressful time can be delegated.

As an SMME owner, a serious business interruption is likely to cause significant emotional trauma and can adversely affect the health of the owner. This in turn is likely to impact the ability of the SMME to recover from the business interruption.

The following checklist can assist the SMME owner manage his/her own personal wellbeing during emotional stress and trauma:

#	Consideration	Yes/No	How addressed?
1	Does the SMME owner have access to trusted persons who can provide emotional and spiritual support during times of crises?		
2	Does the SMME owner have access to trusted independent legal and financial advisors who can provide objective and rational support during times of crises?		

Annexure A - Document checklist for estate planning

Depending on your situation, you may need some or all of the following documents to file insurance claims, pay bills, take care of injured family members or manage the responsibilities associated with a death.

1. Birth certificate
2. Marriage certificate, prenuptial agreements and divorce agreements
3. Will
4. Bank account information to obtain account statements (current, investment and credit cards)
5. Insurance policies (life, health, disability, long-term care, auto, homeowners). Should insurance policies serve as security on assets, include a list of the company name and to which policy it relates. Ensure policies are made to a specific person, otherwise it will be distributed as per the will.
6. Share certificates
7. Transport and deeds
8. List of investments and investment brokers
9. Tax assessments
10. Medical aid information
11. Pension fund information
12. Licenses (vehicles, firearms and drivers)
13. Rental agreements
14. Partnership agreements
15. Employer details
16. Funeral policy
17. Power of attorney, living will or other medical powers
18. Trust documents
19. Medical records, including prescription information
20. Mortgage/property deeds
21. Warranties and receipts for major purchases
22. Safe deposit box information (location and key)
23. Death certificate

Annexure B - About force majeure

The following extract from a press release issued by CDH provides more clarity regarding the concept and implications of force majeure:

Force majeure is a French term meaning "superior force", which in general refers to an unforeseeable event or circumstance which is beyond the control of a party and renders the performance of that party's obligations under a contract wholly or partially impossible. This term is often used interchangeably with other terms such as "vis major" or "casus fortuitus".

Sometimes parties will regulate the consequences of a force majeure event in their contract by including a force majeure clause, and sometimes they won't. A force majeure clause would typically contain a non-exhaustive list of events, which the parties deem force majeure events, including acts of God, war, riots, earthquakes, hurricanes, imposition of sanctions, lightning, pandemics, strikes, a change in law, governmental intervention, etc.

In South Africa, if a force majeure clause has not been provided for in a contract, the common law concept of "supervening impossibility" applies by default.

The primary objective of both a force majeure clause and the common law concept of "supervening impossibility" is to excuse the failure of a party to perform its obligations as a result of the event. This would have the effect of shielding that party from the consequences of a breach of contract which would normally allow the other party to claim damages and/or cancel the contract.

The concept of "supervening impossibility" does, however, not regulate the consequences any further, and thus it is advisable to include a force majeure clause in your contract so that the consequences can be regulated in more detail and in a more bespoke manner.

Adequate attention is not always given to regulating the consequences of force majeure in a contract, possibly because one does not necessarily appreciate the likelihood of the event occurring (enter Covid-19!), or because it is not always realistic or practical in the circumstances to attempt to regulate in detail a future event which by its very nature can be extremely uncertain and unpredictable.

Source: (https://www.cliffedekkerhofmeyr.com/en/news/press-releases/2020/Regulating-the-consequences-of-force-majeure-in-your-contract.html)

Annexure C - Insurance

Before you can protect your business and what you own, you need to have an accurate record of your assets and possessions — you cannot adequately protect what you don't know that you have. Your key personnel, buildings, furniture, electronics, equipment and valuables are important to protect as you would your household assets.

You also need to understand the different types of insurance and the different types of brokers that deal with the various types.

Insurance Broker

- Personal and business asset and liability insurance, subject to specific policy conditions and wording. SASRIA is an optional extension on your asset and liability insurance and refers to riots, strikes, looting and protests insurance, but only applies:
    - if you have general liability insurance
    - damages were incurred and
    - subject to specific policy conditions and wording.

- Business interruption insurance. In general, business interruption insurance refers to fire and natural perils, subject to specific policy conditions and wording. Optional extension cover on business interruption insurance could include prevention of access, public utilities, contract site, storage sites.

- Liability insurance protects you against financial loss if a member of the public is injured, bodily harm, death or permanent disability as a result of your negligence and sues you. Optional extension cover could include work away from main premises.

    - Some policies provide limited personal liability coverage. If you think you need more coverage, increase the coverage in your existing policy and consider purchasing an umbrella or excess liability policy.

    - Umbrella liability insurance is important for those who have assets. Consider purchasing umbrella liability coverage from carriers that you currently do business with to help keep costs down.

Health Insurance

- Medical insurance

    - Ensure you understand what is included and what not, for instance, long-term care can become important during disasters.

    - Understand the tax implications.

- Disability insurance

    - Understand your plan's coverage for catastrophic or long-term injuries, including coverage for rehabilitation and the lifetime maximum the policy will pay. If the plan falls short, find out if you can switch to another plan that has better coverage, even if it costs a little more.

    - Disability insurance pay-outs could include a once-off payment or monthly payments subject to policy details.

    - Understand the tax implications.

- Life insurance
    - Often overlooked is the naming of contingent beneficiaries should one person predecease the only beneficiary or should both spouses die in a common accident.
    - Understand the tax implications.

Other insurance considerations

In addition to the above issues, the following should be considered by the business owner and built into the Disaster Management Plan:

- Compile a list of inventory and assets and update it regularly.
- Store inventory lists in a safe place away from your office.
- Photograph or video record your property's exterior, your vehicles, your large furniture, collectibles and the contents of your factory and equipment.
- Save receipts for valuable items and obtain professional appraisals of jewellery, collectibles, and artwork. Instruct a reputable estate agent to value the property and file supporting documentation.
- Review insurance policies annually. Make sure you understand the deductible and the insurance cover of the policy. You may have decided that business interruption insurance was not needed the previous year, since you started a company and sales were low, but sales may have increased substantially since the last review and business interruption insurance should be included going forward.
- Ensure the policy reflects current replacement costs and update the policy to include any improvements.
- When renting an office or factory, take note that the lessor's insurance will not cover damage to the lessees' possessions in the event of a disaster.
- Ensure you understand the value that insurance companies will pay out. You could be liable for an excess, this could vary based on the policy, but in general you should provide for 5-10%. Vehicles are generally covered for market related retail value and buildings, contents and assets generally require to be insured for new replacement value, including professional fees (ex. architecture fees).
- Ensure your broker and insurance company is licensed with the Financial Sector Conduct Authority (FSCA), previously known as the Financial Services Board (FSB).
- Communicate with your broker about other considerations related to your policy. For example, ask if the company will cancel your coverage if you ever are late with a payment or if you file several claims in a short period of time.
- After a disaster, almost all insurance companies place a 30-day moratorium on new insurance coverage. If you are considering buying a property or factory that was recently hit by a disaster, consider delaying the closing until the moratorium has expired.
- Ensure that your work equipment that you regularly use at home is covered by your office policy (it is normally not covered by your homeowner's policy).
- Consider waiting periods before policies becomes effective or before coverage goes into effect.

Annexure D - Section 22 of the Companies Act

Reckless trading prohibited

(1) A company must not—
  (a) carry on its business recklessly, with gross negligence, with intent to defraud any person or for any fraudulent purpose; or
  (b) trade under insolvent circumstances.

(2) If the Commission has reasonable grounds to believe that a company is engaging in conduct prohibited by subsection (1), the Commission may issue a notice to the company to show cause why the company should be permitted to continue carrying on its business, or to trade, as the case may be.

(3) If a company to whom a notice has been issued in terms of subsection (2) fails within 20 business days to satisfy the Commission that it is not engaging in conduct prohibited by subsection (1), the Commission may issue a compliance notice to the company requiring it to cease carrying on its business or trading, as the case may be.

Annexure E - Disaster Management and Crisis Communications

Disaster - whether natural, human or internal - will strike your business, making it a question of when, not if. As the adage goes, your reputation happens to you whether you manage it or not. Effective disaster management and crisis communication is centred around proactive reputation management, which necessitates that your business should lead the narrative when disaster strikes. Having communication channels and contact lists in place will ensure timeous and effective communication.

Communication channels

The following communication channels could be utilised during emergency situations:

- Staff WhatsApp or Discord groups
- Company webpage
- Company social media pages
- Email lists

Contact lists

Prepare and update emergency contact lists on a regular basis, including:

- Emergency numbers – ambulance, fire department, nearest police station, nearest hospital, nearest Disaster Management Centre
- Employee and employee next of kin
- Customers
- Suppliers
- Businesses in neighbourhood's contact person

Communication plan

An emergency communications plan (EC plan) is a document that provides guidelines, contact information and procedures for how information should be shared during all phases of an unexpected occurrence that requires immediate action.

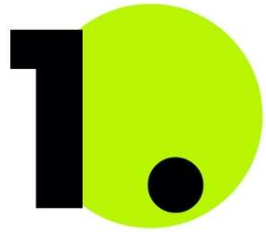
Annexure F provides a template of an Emergency Communication Plan and templates.

The golden rule of emergency communications is that ideally your organisation should be the first to respond (particularly if you are dealing with an internal crisis) and that all stakeholders should be aligned and delivering the same message across all your touchpoints. Make sure employees and other relevant internal stakeholder are aligned before taking your message public. Crisis communications war rooms with daily briefing sessions can also be useful if you are dealing with a changing crisis that demands a dynamic response.

In the modern, social media led world, events can overwhelm an unprepared business at frightening speed, making it essential to have to the right tools and plans in place.

Annexure G provides detail of an emergency email to send to your clients.

Creating your crisis communications plan



Starting off

- Define 'crisis' for your organisation
- Identify the top threats to your organisation
- Scenario plan different situations according to likelihood and impact
- Build an internal escalation process

Roles

- Identify the roles you need to respond to a crisis including:
- Strategic (leaders and decision makers)
- Tactical (monitoring and responding) Support (content creation and logging)
- Audit the skills your team has to respond
- Ensure you have cover for different roles (e.g. more than one person with social

Logistics

- Ensure team members can access key corporate comms channels or systems, and shared documents
- Set-up a channel for communicating with your team in a crisis (e.g. WhatsApp /
- conference calls).
- Build a Situation Report (SitRep) template to help track latest known information and actions taken during a crisis
- Assign a virtual/physical crisis room to be used in the event of a crisis

Building your response

- Ensure you have effective media and social monitoring in place
- Identify your priority stakeholders and how to reach them
- Have a process for responding to questions on social media
- Ensure you have an out-of-hours response team

Content and messaging

- Rehearse content creation tools
- Create a bank of ready-to-use content (e.g. signed-off messaging)
- Have a process in place for getting holding line approved quickly for use on social
- Know how to assess and respond to mis- and disinformation
- Identify and train your spokespeople

Annexure F - Emergency Communication Plan

Templates were originally posted on HubSpot and edited / tailored by LaFondazione

How to Use These Templates

This document and templates are intended for your PR and/or crisis communications team. The first page should be dedicated to guiding principles – standards for the tone and approach your company should have when responding to crises – and how these messages will be communicated in these times.

Subsequent pages are dedicated to prompts for crisis communication. It should be emphasised that these statements are intended to inspire your own, authentic, unique, and situation-appropriate response. You are encouraged to change or alter any and all wording and phrasing so that it fits with your brand

Guiding Principle

Describe the purpose of this document.

Additionally, describe what best practices should be followed when issuing statements and/or responding to media inquiries during this time, including the tone, language, and approach to wording.

Communication Channels

List the ways you will communicate crisis updated both externally (website, customer emails, social media, etc.) and internally (employee email, meeting rooms, etc.).

External

- Channel
- Channel
- Channel

Internal

- Channel
- Channel
- Channel

Disclaimer: This response template is intended for informational purposes only. It is not a substitute for professional advice. You should work with your own crisis communication, public relations, media, security, legal, and other experts on any crisis communication plan, regardless of whether you choose to use this response template or not. HubSpot is not an expert in these matters, and is not responsible for your use or reliance on any information contained in this response template. If you do not agree to these terms, you may not use this response template.

[Insert Company Name or Logo]

Crisis Management and Communication Plan

Last Updated [Date Last Updated]

Table of Contents

1. Purpose

Define the purpose of this document. Highlight when this should be referenced and what kind of information and references will be outlined.

2. Escalation Framework

Use this framework below to determine the severity of a crisis.

In the description column, describe what constitutes that definition of a crisis and what actions must be taken in response. Also include a few examples of what that crisis would look like.

In the action column, mention teams or individuals who may take action, such as legal, the PR & communications team, customer marketing, the social media team, executive assistants, the C-suite, account managers or executives, and more.

Level	Description	Action
Level 1	This is the highest level of crisis escalation and should involve an all-hands-on-deck approach. Describe this situation as immediate to your customers, partners, employees, and/or all stakeholders. Examples: list the examples of this level. Typically, they involve violence, executive misconduct, or a long-term threat of damage to your customers, the company and/or stakeholders.	• Person/Team #1: Task or action • Person/Team #2: Task or action • Person/Team #3: Task or action
Level 2	Level 2 presents a moderate potential risk or impact on business operations, customer success, and/or company reputation. Examples: list the examples of this level. These may include the risk of immediate major customer churn.	• Person/Team #1: Task or action • Person/Team #2: Task or action • Person/Team #3: Task or action

Level	Description	Action
Level 3	This is unlikely to pose a long-term risk to or impact business operations, customer success, and/or company reputation, but the team should still be on the same page for responding. Examples: Instances can include an executive leave of absence, a moderate customer impact that can easily be (or already has been) remedied, or rumours (such as a merger/acquisition).	• Person/Team #1: Task or action • Person/Team #2: Task or action • Person/Team #3: Task or action
Level 4	This is where most "crises" will fall into. They tend to be slightly bigger versions of day-to-day issues that may need a bit of extra effort to be fully resolved or addressed. Examples: Some examples include a short outage with no impact on support or an angry customer on Twitter.	• Person/Team #1: Task or action • Person/Team #2: Task or action • Person/Team #3: Task or action

2.1 Incident Response Team

Describe the purpose of this team, why it was assembled, and what it is responsible for doing.

2.1.1 First Line of Defence

Identify the key players to be informed once the company is aware of the crisis. The list should include the names of the individuals, the team/department those people are members of, and how to best communicate to each member individually. If there is an internal chat system or group email for the whole team, list that here as well.

- Person/Team #1: Email and/or Phone Number
- Person/Team #2: Email and/or Phone Number
- Person/Team #3: Email and/or Phone Number
- Person/Team #4: Email and/or Phone Number
- Group Email/Communication Method: List Here

2.1.2 Greater Response Team

Indicate which escalation level will involve the Greater Response Team. Additionally, list out the core departments that comprise the Greater Response Team, and if appropriate, note that other departments or individuals not listed below may be brought in as needed. Teams that make up a greater incident response team may include the following:

- Communications

- Customer Support
- Legal
- Partner Communications
- Social Media
- Customer Marketing
- People Ops and HR
- Product/Engineering
- Executives
- Security

3. Roles and Responsibilities

In a general crisis – regardless of escalation – what should each of these departments be responsible for once informed of the crisis? Feel free to add a row to include any other department that is right for your business.

Team	Contact Name	Roles and Responsibilities
Communications	Name	• Example Responsibility
Customer Support	Name	• Example Responsibility
Legal	Name	• Example Responsibility
Social Media/Marketing	Name	• Example Responsibility
HR	Name	• Example Responsibility
Product/Engineering	Name	• Example Responsibility
[Other Department]	Name	• Example Responsibility

3.1 Crisis Management Process

Phase 1: ALERT

Outline the actions necessary to ensure the response team is notified as soon as possible. Emphasise that if someone is unsure if he or she should alert the team to alert the team that he or she should, just in case.

Your alert system can be as simple as an internal chat system channel or email alias.

Phase 2: ASSESS

Once the Response Team has been notified, what happens next? Explain how the team will assess the (potential) crisis, gather any available information, classify the incident via the escalation framework above, and prepare to take subsequent action.

Here are some questions to answer to get you started:

- What happened?
- Where and when?
- Who was affected?
- Who is involved?
- When did we learn about the incident?
- What is the impact/likely impact?
- Is there any immediate danger?
- Do we understand the entire issue?

Phase 3: ACTIVATE

Turn your plan into action. Explain how the response team will communicate with the appropriate team members for their tasks and/or with external stakeholders for specific messaging.

In the box below, write out a few common tasks expected in a crisis situation, and delegate that task to a responsible party in the form of a department or an individual. These tasks could include incident response team communication, initial external messaging, gathering/monitoring information, finding a meeting space, team check-in cadence, etc.

Action Items	Responsible Party
Example Action	Responsible Party
Example Action	Responsible Party
Example Action	Responsible Party

Phase 4: ADMINISTER

Determine how the Incident Response Team will continue to assess, address, and resolve the incident. Once again, the type, scale, scope, and severity of the incident or crisis will determine the response. Tasks include communication to stakeholders, employees, and customers if appropriate, as well as developing a timeline, seeking external legal or technical assistance, moderating and responding to media, and updating your crisis communication plan. This section should address the steps for any crisis, whether long-term or short-term.

Action Items	Responsible Party
Example Action	Responsible Party
Example Action	Responsible Party
Example Action	Responsible Party
Example Action	Responsible Party
Example Action	Responsible Party

Part 5: ADJOURN

Once the immediacy of the crisis has dissipated, regroup as a team to go over your process for crisis management, response, and communication. Consider what changes should be made and update this plan with those changes.

Additionally, someone should make a point of documenting exactly what the process was for this crisis, alongside any successes, learnings, or shortcomings. The team should work together to grade themselves on how this situation was handled using a self-review template included in your download.

Finally, if there are any outstanding issues that need to be addressed, or if further monitoring of communication/media is necessary, delegate individuals or departments to manage those tasks.

Action Items	Responsible Party
Example Action	Responsible Party
Example Action	Responsible Party
Example Action	Responsible Party

4. Do's and Don'ts

What are the best practices for your crisis communication? During these times, it can be stressful and easy to jump to a decision that could cause more harm than good. Outline the do's and don'ts for crisis management below.

DO'S	DON'TS
☑ Example Do	⃠ Example Don't
☑ Example Do	⃠ Example Don't
☑ Example Do	⃠ Example Don't
☑ Example Do	⃠ Example Don't
☑ Example Do	⃠ Example Don't

5. Maintaining an Effective Response Plan

To help ensure your company's crisis communication plan will be effective and current, take steps to keep the plan fresh and test your team's ability to manage a crisis. This means editing this plan as needed, running mock-crisis war rooms on a set cadence, developing a training programme for all members of the crisis communication team. Outline those processes in this section.

Annexure G - Sample Crisis Communication Email

Provided by LaFondazione

Example used – Data Breach

Instructions:

Follow a simple three paragraph structure. Keep the message clear and straight-forward.

Paragraph 1: State the facts of what happened in plain language. Provide the full set of details. Avoid emotive language and simply state the events. The aim is to cut out ambiguity and to take ownership of the situation.

Paragraph 2: Outline your crisis response, in other words, the concrete actions you have taken to resolve the incident. Again, state this in simple terms and avoid fluffy platitudes. Your clients are looking to see that you are aware of the full scope of the situation, that you are taking the lead and that you have the confidence and the competence to deal with it.

Paragraph 3: An apology might be appropriate here if the situation was caused by neglect on the part of the business. If the disaster is situational or caused by outside forces, a strong commitment to resolving the situation would be more relevant. Here you want to reassure your clients and provide them with firm reassurance that you are dealing with the situation. Providing a personal contact can also help to allay any fears that the situation may have sparked and helps you to control the conversation, rather than disgruntled clients taking to social media in an effort to be heard, for example.

Example:

Subject line: Cyber Security Breach at ABC Accountants

Dear Client

At 11:55 CAT today our cyber security team detected a firewall breach. This firewall has been set-up to protect your personal data. We are monitoring the situation carefully and, as of yet, have not detected any incidents of personal data having been stolen from our accounts. We suspect that this is a minor incident and that our quick response mitigated any threat, but we appeal to you to let us know should you notice any suspicious activity on any of your personal or business accounts.

We have implemented the following steps to resolve the situation:

- A new firewall has been set-up to protect your personal information
- All data has been moved from the previous location which has now been compromised to a new secure location
- Our cyber security team is investigating the attack to identify the source

We would like to assure you that the protection of your personal information is of utmost importance to us. Our response to the situation has been immediate and we have implemented vigorous monitoring to ensure the continued protection of your data. Should you have any questions or concerns, please feel free to contact myself or our company spokesperson, Wahida Abrahams (wahida@abcaccountans.co.za).

Yours Sincerely,

Werner Snyman, CEO

Annexure H - Post-Crisis Self-Rating Template

This template should be used once you've emerged from your corporate crisis. In the table, there are section prompts for you to explain how well you believe the team did in responding to the crisis and why. Once complete, have the crisis response team speak about why certain marks were achieved and what can be done to improve them in future instances.

Post-Crisis Self-Rating Template

Have all members of your crisis communication and management team fill out this assessment. Rate your perceived performance for first response and follow up from 1-5, giving reasons as to why you ranked your performance this way. If you feel there are any learnings that can be applied for the next situation, document them in the next steps column.

	First Response	Follow Up	Next Steps
Prompt Did we respond quickly?			
Informative Did we address the basic information needs for internal and/or external stakeholders?			
Sincere Did we respond with humanity and care, showing empathy for people impacted by the crisis?			
Honest When known, did we clearly explain what happened, what is happening, and what will happen next?			
Humble If applicable, did we as a company own our mistake?			