TechTarget | SearchDisaster Recovery

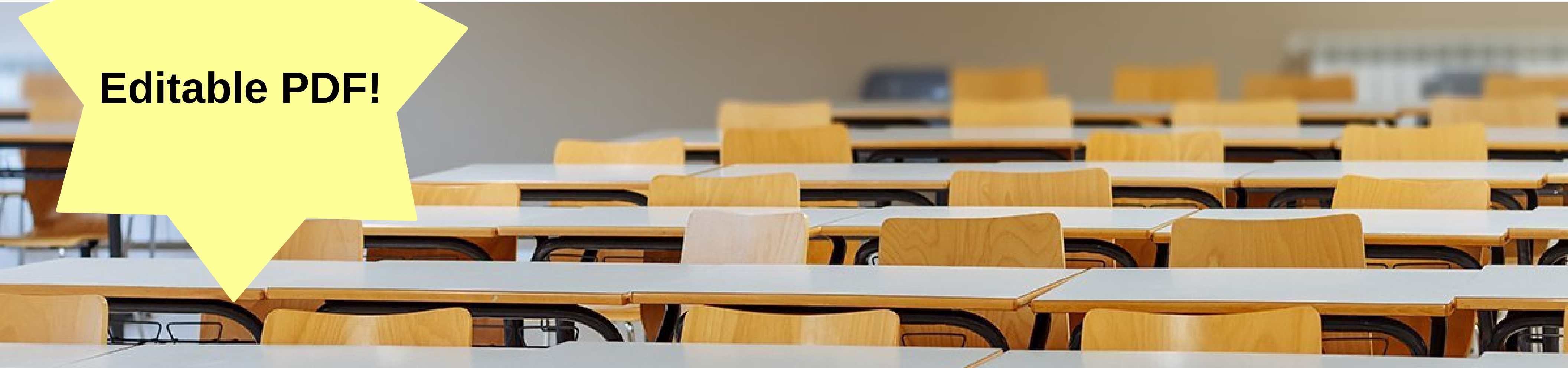
E-guide

PRO+ Content

Incident Response Plan

By Paul Kirvan, CISA, CSSP, FBCI, CBCP

Editable PDF!



Revision History

Revision date	Items revised	Author

Table of contents

SECTION ONE – PLAN BODY **5**

1.1 Introduction 5
1.2 Incident Management Plan Overview 6
1.3 Scope 6
1.4 Exclusions 7
1.5 Planning Scenarios 7
1.5.1 Limited or No Access to the Building *7*
1.5.2 Loss of Data Communications, e.g., WAN, Routers *7*
1.5.3 Loss of Technology, e.g., Computer Room, Network Services *8*
1.5.4 Loss of People, e.g., Illness, Death *8*
1.6 Recovery Objectives 9
1.7 Assumptions 9

SECTION TWO – INCIDENT RESPONSE AND MANAGEMENT **10**

2.1 Logical Sequence of Events 10
2.2 Local Incident Management Teams 11
2.2.1 General Information *11*
2.2.2 Team Overview *13*
2.2.3 Local Incident Management Team *13*
2.2.4 Damage Assessment Team *13*
2.2.5 Regional Incident Management Team *14*
2.2.6 Threat Assessment Center *14*
2.3 Incident Management Team Activities 15
2.3.1 Local IM Team Activities *15*
2.3.2 Regional Incident Manager Activities *15*
2.3.3 Regional IM Executive Activities *15*

SECTION THREE – NOTIFICATION, ESCALATION, AND DECLARATION **166**

3.1 Introduction 16
3.2 Notification Process Overview 16
3.2.1 Initial Notification 16
3.3 Notification Process (Emergencies only) 17
3.3.1 Local IMT Notification and Notification of External Client, Vendor and *17*
Business Partner *17*
3.4 Incident Response Assembly Locations 18
3.5 Escalation Process (Emergencies only) 19

3.6 PLAN AUTHORIZATION AND DECLARATION 20
3.7 DECLARATION PROCESS (EMERGENCY ONLY) 20

SECTION FOUR – INCIDENT RESPONSE CHECKLISTS 21

4.1 KEY PERSONNEL CONTACT LIST 21
4.2 KEY VENDOR CONTACT LIST 25
4.3 INITIAL INCIDENT RESPONSE CHECKLIST 26
4.4 LOCAL INCIDENT MANAGEMENT TEAM TASK CHECKLIST 27
4.4.1 Local Incident Management Team Meeting *28*
4.5 LOCAL INCIDENT MANAGER TASK CHECKLIST 28
4.5.1 Incident Response Recommended Actions *29*
4.5.2 Actions Following a Disaster Declaration *30*
4.6 LOCAL EOC COMMAND STAFF TASK CHECKLIST 31
4.7 LOCAL EOC OPERATIONS STAFF TASK CHECKLIST 32
4.8 Pre-Incident Preparations *33*
4.8.1 Actions Following an Incident and Prior to a Disaster Declaration Being Made *34*
4.8.2 Support for Local Incident Management Team Meeting *34*
4.8.3 Actions During and After the Disaster *35*
4.8.4 Post-Event Maintenance Activities *35*

SECTION FIVE - APPENDIXES 36

5.1 INCIDENT MANAGEMENT FORMS 36

Section One – Plan Body

1.1 Introduction

General information

This manual was developed for BUSINESS NAME , herein referred to as BUSINESS NAME , and it is classified as the confidential property of that entity. Due to the sensitive nature of the information contained herein, this manual is available only to those persons who have been designated as members of one or more incident management teams, or who otherwise play a direct role in the incident response and recovery processes.

Unless otherwise instructed, each plan recipient will receive and maintain two copies of the plan, stored as follows:

- One copy at the plan recipient's office
- One copy at the plan recipient's home

For additional copies, contact XXX-XXX-XXX

The following teams will appear throughout this plan:

- Threat Assessment Center
- Regional Incident Management Team
- Damage Assessment Team
- Local Incident Management Team

The incident management planning effort for BUSINESS NAME recognizes and affirms the importance of people, processes, and technology to the corporation.

It is the responsibility of each BUSINESS NAME manager and employee to safeguard and keep confidential all corporate assets.

1.2 Incident response plan overview

Overview and objectives

This incident management plan establishes the recommended organization, actions, and procedures needed to

- Recognize and respond to an incident;
- Assess the situation quickly and effectively;
- Notify the appropriate individuals and organizations about the incident;
- Organize the company’s response activities, including activating a command center;
- Escalate the company’s response efforts based on the severity of the incident; and
- Support the business recovery efforts being made in the aftermath of the incident.

Existing incident management plans should conform to the Incident Management Policy statement found in Section 6.2 of the Appendix.

This plan is designed to minimize operational and financial impacts of such a disaster, and will be activated when a local Incident Manager (or, in his/her absence, one of his/her alternates) determines that a disaster has occurred.

Specific details on incident response and subsequent business recovery actions and activities are included within the respective local recovery team plans.

1.3 Scope

This incident management plan includes initial actions and procedures to respond to events that could impact critical business activities at BUSINESS NAME AND LOCATION . This plan is designed to minimize the operational and financial impacts of disasters.

The BUSINESS NAME Incident Response Plan is designed to provide an initial response to any unplanned business interruption, such as a loss of utility service or an avian influenza outbreak, or a catastrophic event such as a major fire or flood. This document defines the requirements, strategies and proposed actions needed to respond to such an event.

1.4 Exclusions

This plan specifically excludes the following from its scope: BUSINESS NAME AND LOCATION

- Facilities not located at the

1.5 Planning scenarios

This plan was developed to respond to an incident that could render the BUSINESS NAME out of service or inaccessible. In addition, it is designed to respond to situations other than the above scenarios, e.g., an avian flu outbreak. The plan is designed to respond to scenarios such as the following:

1. No access to buildings or floors at the specific location
2. Loss of data communications and the network infrastructure
3. Loss of technology
4. Loss of professional staff (e.g., via a flu outbreak)

1.5.1 Limited or no access to the building

Any incident that renders the BUSINESS NAME AND LOCATION either totally inaccessible/unusable or partially accessible to the tenants

This scenario could produce one or more of the following impacts:

- Loss of the business facility or the facility is rendered inaccessible
- Loss of access to selected work space areas, such as building floors affected by a localized event, e.g., a fire
- New equipment/facilities must be acquired
- Incident management and recovery actions must be implemented
- Event causes business interruption or closing

1.5.2 Loss of data communications, e.g., WAN, routers

Any incident that disables or destroys the WAN router infrastructure and its communication capabilities located at BUSINESS NAME , with a potentially disruptive effect on business operations.

This scenario could produce one or more of the following impacts:

- Loss of access to the WAN
- Loss of access to the Internet and intranet
- Incident is declared and incident recovery actions are implemented
- Use of recovery strategies, commercial hot site, reciprocal agreements, and manual operations as a temporary measure
- Business shutdown
- Need for new facilities/equipment

1.5.3 Loss of technology, e.g., computer room, network services

Any incident that disables or destroys the entire computer room facility or its processing capacity located at BUSINESS NAME , with a potentially disruptive effect on business operations.

This scenario could produce one or more of the following impacts:

- Loss of use of the computer room facility
- Loss of voice/data communications services
- Incident is declared and incident recovery actions are implemented
- Use of recovery strategies, commercial hot site, reciprocal agreements, and manual operations as a temporary measure
- Business shutdown
- Need for new facilities/equipment

1.5.4 Loss of people, e.g., illness, death

Any incident that disables or renders the professional staff at BUSINESS NAME unable to perform normal business functions, with a commensurate negative effect on business operations.

This scenario could produce one or more of the following impacts:

- No impact to building access or technology infrastructure
- Insufficient professional staff to perform minimal business operations
- Lack of suitably cross-trained staff
- Business shutdown
- Need for temporary staff

1.6 Recovery objectives

This incident management plan has been developed to meet the following objectives:

1. Provide an organized and consolidated approach to managing initial response and recovery activities following an unplanned incident or business interruption, avoiding confusion and reducing exposure to error.
2. Provide prompt and appropriate response to unplanned incidents, thereby reducing the impacts resulting from short-term business interruptions.
3. Notify appropriate management, operational staff and their families, customers, and public sector organizations of the incident.
4. Recover essential business operations in a timely manner, increasing the ability of the company to recover from a damaging loss at LOCATION .

1.7 Assumptions

This plan has been developed and is to be maintained on the basis of the following assumptions:

- A complete interruption of the BUSINESS NAME office and associated facilities has occurred, and there is no access to the office, critical equipment or business data.
- A partial or total loss of professional staff at BUSINESS NAME AND LOCATION has occurred due to employee illness resulting from a disaster, whether natural or man-made, including avian flu or a similar outbreak, and only a limited number of healthy employees are available to continue normal business operations.
- Recovery from anything less than complete interruption will be achieved by using appropriate portions of this plan.
- Sufficient staff with adequate knowledge will be available to facilitate recovery.

Section Two – Incident response and management

2.1 Logical sequence of events

The following high-level checklist describes the recommended emergency response:

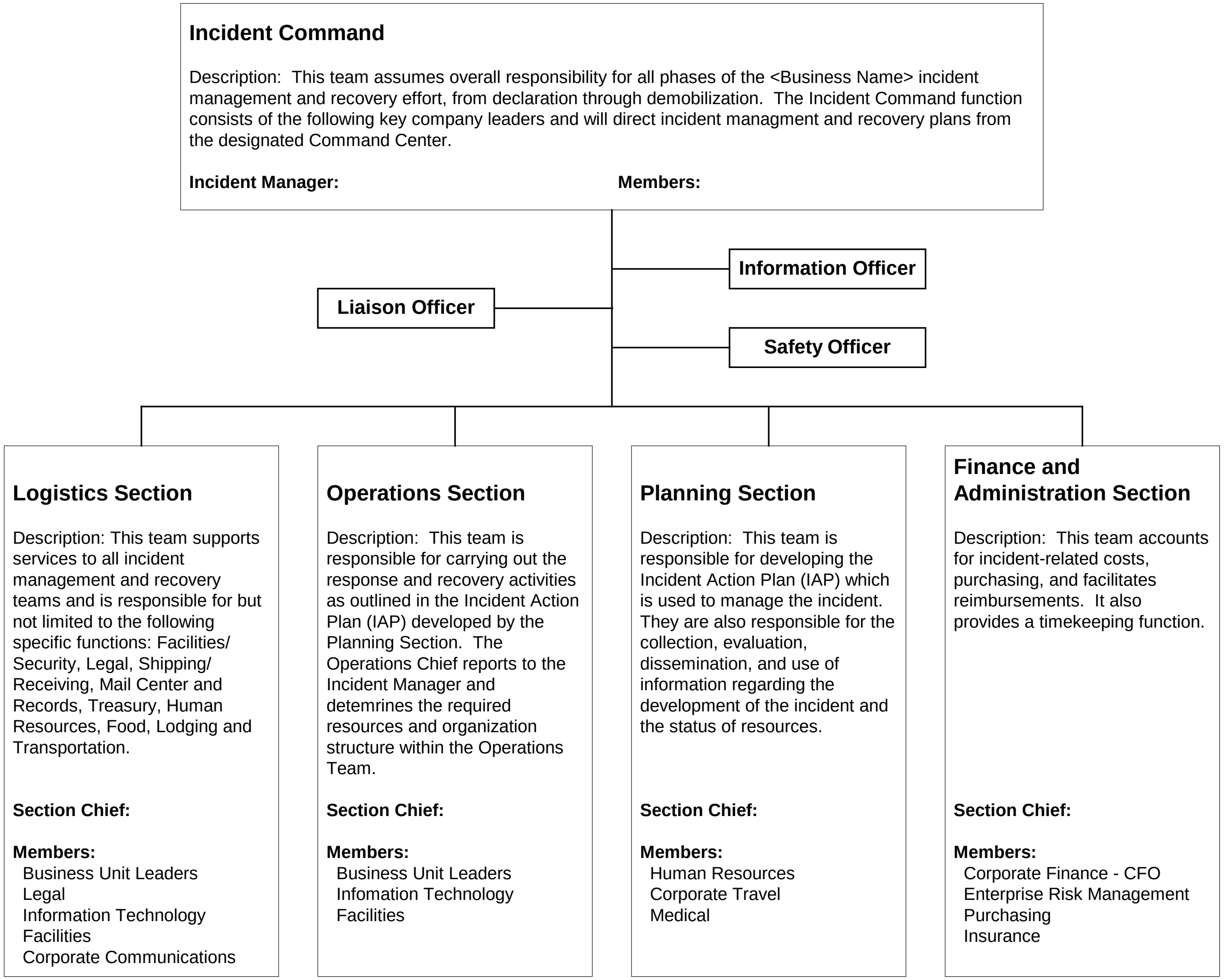
INITIAL INCIDENT RESPONSE CHECKLIST

Incident occurs.	
First person to observe incident at LOCATION follows local emergency procedures and notifies the local Damage Assessment Team (DAT) and/or building security of incident.	
The local DAT assembles, investigates the incident using a checklist, and determines if the local Incident Management Team (IMT) needs to be activated. If it is necessary, the DAT also notifies public authorities and/or dials 911.	
If needed, the DAT will notify and activate the local Incident Management Team (IMT). The IMT designates a point of contact (POC) for the incident. The POC launches a notification process.	
If life and safety are at immediate risk - the IMT Leader and his/her staff shall act first to ensure their own survival as well as the survival of all staff, and then communicate when feasible.	
As soon as possible, the IMT POC notifies the Regional Incident Manager PHONE NUMBER and the Threat Assessment Center (TAC) PHONE NUMBER of the incident.	
The TAC establishes local incident coordination with the IMT point of contact, assesses the incident; and notifies senior management of the incident.	
The Regional Incident Manager notifies the Regional IM Team of the incident.	
TAC determines if the situation requires escalation, based on inputs from the Damage Assessment Team and IMT.	
Assuming the situation warrants escalation, the IMT reviews the situation, briefs the TAC and Regional Incident Manager, and initiates the disaster declaration process.	
If a disaster is not declared, IMT POC advises TAC and Regional Incident Manager.	
If a disaster is declared, the local IMT 1. Notifies the TAC and Regional Incident Manager 2. Activates the Emergency Operations Center (EOC) 3. Activates the BC-IM plan 4. Launches emergency response procedures	
The Regional Incident Manager consults with the TAC on the incident. Feedback from the TAC is relayed to local IM Team point of contact.	
All BUSINESS NAME staff is notified of the incident and of operational status.	
The incident management and business continuity plans continue until the incident has been resolved.	

2.2 Local incident management teams

2.2.1 General information

A successful recovery from a disaster can only occur with total coordination of all incident management and recovery activities. In a crisis, each team has specific functions that contribute to the success of the recovery. The following diagram depicts the structure of a local incident management team, particularly in the aftermath of an incident. It is based on the Incident Command System (ICS).



Incident Command

Description: This team assumes overall responsibility for all phases of the <Business Name> incident management and recovery effort, from declaration through demobilization. The Incident Command function consists of the following key company leaders and will direct incident managment and recovery plans from the designated Command Center.

Incident Manager:

Members:

Information Officer

Liaison Officer

Safety Officer

Logistics Section

Description: This team supports services to all incident management and recovery teams and is responsible for but not limited to the following specific functions: Facilities/ Security, Legal, Shipping/ Receiving, Mail Center and Records, Treasury, Human Resources, Food, Lodging and Transportation.

Section Chief:

Members:
Business Unit Leaders
Legal
Information Technology
Facilities
Corporate Communications

Operations Section

Description: This team is responsible for carrying out the response and recovery activities as outlined in the Incident Action Plan (IAP) developed by the Planning Section. The Operations Chief reports to the Incident Manager and detemrines the required resources and organization structure within the Operations Team.

Section Chief:

Members:
Business Unit Leaders
Infomation Technology
Facilities

Planning Section

Description: This team is responsible for developing the Incident Action Plan (IAP) which is used to manage the incident. They are also responsible for the collection, evaluation, dissemination, and use of information regarding the development of the incident and the status of resources.

Section Chief:

Members:
Human Resources
Corporate Travel
Medical

Finance and Administration Section

Description: This team accounts for incident-related costs, purchasing, and facilitates reimbursements. It also provides a timekeeping function.

Section Chief:

Members:
Corporate Finance - CFO
Enterprise Risk Management
Purchasing
Insurance

2.2.2 Team Overview

To implement the recovery strategies, the following teams are defined:

- Local Incident Management Team (IMT)
- Damage Assessment Team (DAT)
- Regional Incident Management Team (RIMT)
- Threat Assessment Center (TAC)

2.2.3 Local Incident Management Team

The local IMT assesses the physical and operational status of the LOCATION immediately following an incident; determines the need for personnel evacuations; reviews the situation with building security and building management as needed; reviews the situation with local public sector agencies (e.g., police, fire, EMT) as needed; provides input to the process for declaring a crisis or emergency as needed; and organizes and deploys an Emergency Operations Center (EOC) to manage all planning and operational aspects of the incident. The local IMT also makes an effort to reduce and control the impact of the incident to the LOCATION.

Members:

Name	Office

2.2.4 Damage Assessment Team

The DAT assesses the physical condition of the LOCATION immediately following an incident; evaluates the damage and/or destruction to physical and technology assets to determine if an evacuation is indicated and what the prospects for recovery may be; reviews the situation with building security and building management, as well as local public sector agencies (e.g., police, fire, EMT) as needed; and provides input to and/or recommends a disaster declaration if necessary.

Members:

Name	Office

2.2.5 Regional Incident Management Team

Comprised of regional company executives and the Regional Incident Manager, the RIMT provides coordination and oversight during a regional incident that may affect an individual office or multiple offices in a geographic area.

Members:

Name	Office

2.2.6 Threat Assessment Center

The Threat Assessment Center provides a centralized and standardized means of validating and assessing threats and other incidents. Using information obtained from multiple sources, including local IMTs and Regional Incident Managers, the TAC provides single-source reporting to senior management and other stakeholders so that preemptive measures can be determined and implemented on a timely basis.

Members:

Name	Office

2.3 Incident Management Team activities

This plan provides detailed action steps for each member in the Incident Management Team structure.

2.3.1 Local IMT activities

Detailed checklists that summarize recommended local Incident Management Team and team leader activities can be found in Sections 5.4 and 5.5.

2.3.2 Regional incident manager activities

Detailed checklists that summarize recommended Regional Incident Manager activities can be found in Section 5.8.

2.3.3 Regional IM executive activities

Detailed checklists that summarize recommended Regional Incident Management Team executive activities can be found in Section 5.9.

Section Three – Notification, escalation and declaration

3.1 Introduction

During any business interruption, personnel safety is the primary concern. Managers should periodically review emergency response and evacuation procedures with their staff to ensure familiarity with safety procedures.

Employees should notify their manager of any operational disruption or emergency situation. In the event of an emergency, BUSINESS NAME managers NAME(s) are authorized to declare a disaster on behalf of the LOCATION office.

The notification plan is designed for use in mobilizing the Incident Management Team. If partial mobilization is needed, the appropriate portion of the plan can be executed accordingly. When primary IMT members cannot be reached for their part in the notification plan, their alternates will be contacted.

3.2 Notification process overview

3.2.1 Initial notification

Telephone notification process:

During normal business hours, contact personnel at the following numbers in the order listed:

- Office telephone (If unavailable, leave a voicemail message)
- Cellular
- Pager
- Text page (if available)
- Home telephone
- Any other number the person has listed in the employee's list.

During non-business hours, contact personnel at the following numbers in the order listed until someone is reached:

- Home phone
- Office (leave voicemail if no answer)
- Cellular
- Pager

- Text page (if available)
- Any other number the person has listed in the disaster recovery documentation.

Automated notification process:

When using an automated notification system during normal business hours, contact personnel at the following numbers in the order listed:

- Office telephone (If unavailable, leave a voicemail message)
- Cellular
- Pager
- Text page (if available)
- Home telephone
- Any other number the person has listed in the employee's list.

When using an automated notification system during non-business hours, contact personnel at the following numbers in the order listed until someone is reached:

- Home phone
- Office (leave voicemail if no answer)
- Cellular
- Pager
- Text page (if available)
- Any other number the person has listed in the DR documentation.

3.3 Notification process (emergencies only)

Communication during a crisis is critical. As such, follow local notification protocols in an emergency.

3.3.1 Local IMT notification and notification of external client, vendor and business partner

Should an incident occur, the following call tree will be utilized at LOCATION.

Temporary staff				
Name	**Office phone**	**Home phone**	**mobile/Pager**	**Location**

3.4 Incident response assembly locations

Primary assembly area

Name
Address
Address
City/State/Zip
Phone/Fax
Email

Secondary assembly area

Name
Address
Address
City/State/Zip
Phone/Fax
Email

Tertiary assembly area

Name
Address
Address
City/State/Zip
Phone/Fax
Email

3.5 Escalation process (emergencies only)

The process for escalating an incident at BUSINESS NAME is as follows:

Step 1: Follow local established emergency escalation and life/safety protocols. If these are not available, the first BUSINESS NAME employee to become aware of an incident should immediately report it to local management, who will escalate the information to the local Incident Management Team Leader (NAME) or his/her designated (NAME) alternate .

Step 2: Follow local established emergency escalation and life/safety protocols. If these are not available, the Damage Assessment Team should conduct an assessment of the situation. If the severity of the incident warrants, the IMT Leader or point of contact will inform the Regional Incident Manager, Threat Assessment Center, Business Continuity Management and BUSINESS NAME management of the situation.

Step 3: Follow local established emergency escalation and life/safety protocols. If these are not available, based on the results of the local IMT assessment, and if the severity of the incident warrants, the Regional Incident Manager will coordinate with Regional Incident Management Team executives on the situation as soon as feasible by phone, email, teleconference or MessageOne.

Step 4: Follow local established emergency escalation and life/safety protocols. If these are not available, based on the results of the TAC assessment, and if the severity of the incident warrants, the TAC will notify designated senior management as deemed necessary to manage the situation; this can be done by phone, email, teleconference or MessageOne.

Step 5: Continue to follow local established emergency escalation and life/safety protocols. If these are not available, based on the results of local, regional and TAC discussions (via conference bridge and/or MessageOne technology), a decision will be made on declaring a disaster:

a. IF a disaster IS NOT declared, the IMT Leader or Incident Manager will coordinate with other local management and Corporate Services staff to restore normal business operations accordingly.
b. IF a disaster IS declared, the IMT Leader or Incident Manager, in coordination with the BC Team, will invoke the BC-IM plan.

Step 6: IF a declaration is made, the IM point of contact will update the TAC, the Regional Incident Management BUSINESS NAME Team and management in LOCATION as soon as possible.

3.6 Plan authorization and declaration

When the Incident Management Team is notified of the event, they will immediately contact the local business leadership on the incident, asking them to remain on standby. The IMT will report to the scene of the event, or where directed, and coordinate additional activities with local building management and the Damage Assessment Team. The call tree notification process begins after the authorization has been given to declare a disaster. Alternatively, if an automated notification system or service is available, launch that process as soon as possible.

3.7 Declaration process (emergencies only)

The disaster declaration process at BUSINESS NAME in LOCATION is as follows:

1. ONLY the management team in charge BUSINESS NAME or his/her appointed alternate has the authority to declare of a disaster at BUSINESS NAME.

2. A disaster declaration at BUSINESS NAME MUST generally meet one or more of the following criteria:

   A. The incident is a major, prolonged or indefinite disruption to business as usual.

   B. The incident is of sufficient magnitude (casualties/fatalities/property and/or facility damages/business disruptions, etc) and warrants the enacting of emergency response and incident management measures to ensure continuity of operations at BUSINESS NAME .

   C. The incident has met and/or exceeded the threshold of disaster declaration criteria for appropriate major public sector entities on a local, regional, national or international level.

   D. Not declaring the incident a "disaster" poses a direct threat to the viability of BUSINESS NAME as a business.

Section Four – Incident response checklists

4.1 Key personnel contact list

Incident Management Team							
Last name	First name	Title	Department/Location	Work phone	Home phone	Alternate phone	Pager/Cell phone

Executive Management Team							
Last name	**First name**	**Title**	**Department/Location**	**Work phone**	**Home phone**	**Alternate phone**	**Pager/Cell phone**

Planning Section							
Last name	First name	Title	Department/Location	Work phone	Home phone	Alternate phone	Pager/Cell phone

Operations Section							
Last name	First name	Title	Department/Location	Work phone	Home phone	Alternate phone	Pager/Cell phone

Logistics Section							
Last name	First name	Title	Department/Location	Work phone	Home phone	Alternate phone	Pager/Cell phone

Finance / Administration Section							
Last name	First name	Title	Department/Location	Work phone	Home phone	Alternate phone	Pager/Cell phone

4.2 Key vendor contact list

Vendor name	Last name	First name	Title	Office phone	Cell phone	Fax number

4.3 Initial incident response checklist

The task checklists in the following pages should be followed in the event of an incident at the office or surrounding area. Follow the recommended sequence of actions below during the initial minutes after the occurrence of an incident.

INITIAL INCIDENT RESPONSE CHECKLIST

Incident occurs	
First person to observe incident at LOCATION follows local emergency procedures and notifies the local Damage Assessment Team and/or building security of incident.	
The local Damage Assessment Team assembles, investigates the incident using a checklist, and determines if the local Incident Management Team needs to be activated. If it is necessary, the DAT also notifies public authorities and/or dials 911.	
If needed, the DAT will notify and activate the local Incident Management Team. The IMT designates a point of contact (POC) for the incident. The POC launches a notification process.	
If life and safety are at immediate risk - the IMT Leader and his/her staff should act first to ensure their own survival as well as the survival of all staff, and then communicate when feasible.	
As soon as possible, the IMT POC notifies the Regional Incident Manager PHONE # and the Threat Assessment Center PHONE # of the incident.	
The TAC establishes local incident coordination with the IMT point of contact, assesses the incident; and notifies senior management of the incident.	
The Regional Incident Manager notifies the Regional IM Team of the incident.	
TAC determines if the situation requires escalation, based on inputs from the Damage Assessment Team and IMT.	
Assuming the situation warrants escalation, the IMT reviews the situation, briefs the TAC and Regional Incident Manager, and initiates the disaster declaration process.	
If a disaster is not declared, IM POC advises TAC and Regional Incident Manager.	
If a disaster is declared, the local IMT 1. Notifies the TAC and Regional Incident Manager 2. Activates the Emergency Operations Center (EOC) 3. Activates the BC-IM plan 4. Launches emergency response procedures	
The Regional Incident Manager consults with the TAC on the incident. Feedback from the TAC is relayed to local IM Team point of contact.	
All BUINESS NAM staff is notified of the incident and of operational status.	
The incident management and business continuity plans continue until the incident has been resolved.	

4.4 Local IMT task checklist

The following recommended sequence of actions should be facilitated after completion of the Initial Response checklist in Section 4.3.

LOCAL INCIDENT MANAGEMENT TEAM TASK CHECKLIST

Gather information about the incident from first-hand contact, available first responders, employees, and others; relays to Incident Manager.	
Account for all staff/guests on (and if applicable off) premises.	
Administer first aid and/or ensures life/safety measures as appropriate.	
Inform building security and the property management firm if they are not already aware of the incident: • Building security: PHONE # • Property management firm: PHONE #	
Inform security of the situation as soon as possible: • Security: PHONE #	
Inform the Incident Manager as soon as possible: • IM Team Leader: PHONE #	
Conduct an initial assessment of the incident's likely impact on local operations; coordinate with DAT.	
Disseminate information to local employees on the incident.	
Provide information about the incident to first responder organizations.	
Establish and maintain communications with Regional Incident Manager, Threat Assessment Center, and the appropriate business unit.	
Provide input as directed to the disaster declaration process.	
If disaster is declared, support the IM plan response.	
If a disaster is not declared, support recovery from the incident and restore operations accordingly.	
Support launch of Emergency Operations Center (EOC) according to IM plan.	
Provide ongoing review and analysis of incident(s) with dissemination of information to staff, Regional Incident Manager, and TAC as needed.	
Coordinate with counterparts in other regions as part of ongoing incident analysis.	
Coordinate with Operations Section leadership as well as third-party organizations to ensure that required resources are in place and ready for delivery to affected venue.	
Support Public Information Officer, Safety Officer and Liaison Officer roles.	
Support management of the incident and restores operations accordingly.	
Support post-event demobilization plan as needed.	
Assist IMT and Incident Manager as directed.	
Provide post-event report of activities.	

4.4.1 Local IMT meeting

Contact local IMT leader to ensure that the IMT has set an initial meeting and venue. Ensure that the presence of IMT members is recorded using the EXHIBIT 4 - RECOVERY TEAMS PERSONNEL ASSIGNMENT FORM found in the Recovery Forms section of this document.	
Ensure that any missing IMT members, their alternates and any additional personnel are notified of the meeting. See the KEY CONTACTS section of this guide for a complete list of IMT members and alternates, and their contact information.	
Obtain a current situation report from the IMT and Damage Assessment Team. Address the following key issues: 1. Type of event (fire, tornado, terrorism, power outage, telecomm outage, etc.) 2. Specific location of event, if known (building, floor, side of floor, etc.) 3. Magnitude of the event 4. Time of event 5. Suspected cause 6. Emergency/evacuation procedures status 7. Police and fire departments notified 8. Injuries and fatalities 9. Building access status (current access, near-term potential access) 10. Immediate impact to business operations 11. Potential for news media attention	
Establish schedule of updates for Threat Assessment Center to monitor ongoing emergency response procedures. Commence providing TAC updates.	
Ensure that a member of the local IMT documents, in chronological order, incident milestones and actions taken using the EXHIBIT 1 – BUSINESS INTERRUPTION REPORT template in the Recovery Forms section of this guide. This form will be used as a tool to update the IMT, TAC and/or other senior management.	
If required, provide advice to local senior management whether employees should be sent home. Local senior management will develop a statement, determine method of communicating updates and communicate to employees.	
Follow up to ensure that local management has decided whether or not to intercept 800# phone lines with a customized emergency voice recording.	
Follow up to ensure that local management has decided to launch/not launch the MessageOne emergency notification service, in addition to/in lieu of 800# service arrangements.	

4.5 Local IMT checklist

The following recommended sequence of actions should be provided by the local incident team leader and/or incident manager after completing the Initial Response checklist in Section 5.3.

LOCAL INCIDENT MANAGER TASK CHECKLIST

Assumes overall leadership of all incident management activities.	
Receives information about the incident from IMT, first responders, employees, and others; contacts the Damage Assessment Team.	
Delegates the accounting for of all staff/guests on (and if applicable off) premises.	
Ensures that first aid is being provided; ensure that life/safety measures are being delivered.	
Informs local Business Continuity Management Team of situation as soon as possible: • Business Continuity Management Team: BUSINESS NAME	
In coordination with Damage Assessment Team, assesses the incident's likely impact on local operations.	
If assessment of the incident suggests a serious event that could adversely impact operations, advises Threat Assessment Center (TAC) as soon as possible.	
Provides input as directed to the disaster declaration process.	
Based on input from Regional Incident Manager and Threat Assessment Center, determines if/when to declare a disaster.	
If a disaster is declared, facilitates activation of IM plan; informs others (TAC, Regional Incident Manager); launches call notification via MessageOne or calling tree.	
If a disaster is not declared, manages recovery from the incident and restore operations accordingly.	
Leads the launch of Emergency Operations Center according to IM plan; assumes role of Incident Manager.	
Leads the launch of Public Information Officer, Safety Officer and Liaison Officer.	
Ensures that Public Information Officer establishes regularly updated communications with Incident Manager and other units, e.g., Regional Incident Manager, as needed.	
Manages the incident and restores operations accordingly.	

4.5.1 Incident response recommended actions

Incident Management Team leader will develop recommendations for senior management on what overall response strategies should be implemented to facilitate the recovery of business operations in the most timely, efficient and cost-effective manner.	
Consider information gathered in earlier incident and damage assessments including, but not limited to, the following: ▪ The area(s) affected by the disaster; ▪ Anticipated duration of incident; ▪ Availability of required employees; ▪ Any special timing issues such as relationship to month-end, quarter-end, etc.; ▪ Any special business issues (e.g., unusual business volume or backlog, unusual contractual obligations); ▪ Regulatory obligations; ▪ Salvageable equipment and supplies (as documented in the ASSESSMENT & EVALUATION FORMS); ▪ Availability of equipment and supplies at potential alternate or off-site locations; ▪ Salvageable records required for recovery activities; and ▪ Records which require intensive reconstruction activities.	

Develop critical business function recovery priority lists for the following periods: ▪ 8 hours ▪ 12 hours ▪ 24 hours ▪ 72 hours or longer	
Recommend to the Executive Management Team and Threat Assessment Center the location(s) where critical business functions and IT operations can be recovered based upon the following priority: ▪ Return to building ▪ Local sites ▪ Other sites ▪ Vendor location	

4.5.2 Actions following a disaster declaration

Based on responses from the Threat Assessment Center, and input from local management and public sector organizations, the IMT leader will launch an incident management plan that facilitates a safe and rapid evacuation of staff and locates the safest venue to activate an Emergency Operations Center based on the following priority list: 1. 2.	
If not already identified locally, IMT leader should identify and communicate the recommended assembly site(s) to local IMT members, local management, local public sector organizations, and the Business Recovery Team.	
Ensure that the local IMT convenes a meeting to review response and recovery options, Emergency Operations Center setup procedures, and other related activities, as specified in the incident management plan.	
Relay the current situation report from the Threat Assessment Center and/or the Regional Incident Management Team. General points to be covered include the following: 1. Type of event (fire, tornado, terrorism, power outage, telecomm outage, etc.) 2. Specific location of event, if known (building, floor, side of floor, etc.) 3. Magnitude of the event 4. Time of event 5. Suspected cause 6. Emergency/evacuation procedures status 7. Police and fire departments notified 8. Injuries and fatalities 9. Building access (current access, near-term potential access) 10. Immediate impact to business operations 11. Potential for media (e.g., television, radio) attention	
Establish a schedule for updates to regional IM team(s).	
Assign an IMT member responsibility to document, in chronological order, incident milestones and actions taken using the EXHIBIT 1 –	

BUSINESS INTERRUPTION REPORT template in the Recovery Forms section of this guide. This form will be used as a tool to update the Threat Assessment Center and other senior management.	
Provide input to the Threat Assessment Center and/or Executive Management Team whether employees should be sent home. The EMT will develop a statement, determine method of communication for further updates and communicate to employees, e.g., using MessageOne or other approved service.	
The IMT leader will decide whether or not to intercept 800# phone lines with a customized emergency voice recording. <u>Main Message in the first 24 hours:</u> *“Welcome to* BUSINESS NAME *. We’re sorry, but our normal business operations have been interrupted due to* XXXX *. Please be patient as we are making every effort to recover operations as soon as possible. We expect to resume normal operations on or about .”* The following persons are authorized to implement this message: Name: Name: Work: Work: Home: Home: Cell: Cell:	
Support local Incident Managers as required.	
Assist with acquisition of resources as needed.	
Provide regular incident updates to TAC.	
Provide regular regional incident updates to IMTs and points of contact (POC).	
Establish communications process/ timeline for RIMT.	
Coordinate phone calls, conference calls for RIMT.	

4.6 Local EOC command staff task checklist

Assuming an Emergency Operations Center is established by the local IMT Leader or Incident Manager, the following recommended sequences of actions should be facilitated by individuals assigned to the specific positions defined below.

IM TEAM PUBLIC INFORMATION OFFICER TASK CHECKLIST

When activated, establishes communications with organizations as indicated in incident management plan, e.g., Incident Manager, local management, Regional Incident Manager, and Threat Assessment Center .	
Establish regular time frames for reporting incident and recovery status to designated organizations.	
Process incoming messages from and external organizations, including police/fire/EMS and the media.	
Coordinate activities with Liaison Officer.	
Distribute approved messages to designated parties when directed.	

Assists IMT and Incident Manager as directed.	
Provide post-event report of activities.	

IM TEAM SAFETY OFFICER TASK CHECKLIST

When activated, monitor and manages physical safety conditions.	
Develop measures to ensure safety of personnel.	
Assist in the administering of first aid and/or ensure life/safety measures as needed.	
Monitor Emergency Operations Center (EOC) personnel for stress, etc.	
Assist Incident Manager as directed.	
Provide post-event report of activities.	

IM TEAM LIAISON OFFICER TASK CHECKLIST

When activated, interface with any/all public sector entities as appropriate, e.g., police, fire, EMS, OEM, government agencies.	
Disseminate information and messages to appropriate departments and individuals.	
Coordinate activities with Public Information Officer.	
Assist Incident Manager as directed.	
Provide post-event report of activities.	

4.7 Local EOC operations staff task checklist

Assuming an Emergency Operations Center is established by the local IMT Leader or Incident Manager, the following recommended sequences of actions should be facilitated by individuals assigned to the specific positions defined below.

PLANNING TEAM LEADER TASK CHECKLIST

When activated, prepare Incident Action Plan (IAP).	
Maintain situation and resource status.	
Coordinate BCM activities.	
Coordinate the preparation and dissemination of incident documentation.	
Provide location for subject matter and technical expertise.	
Prepare demobilization plan as needed.	
Assist Incident Manager as directed.	
Disseminate information and messages to appropriate departments and individuals.	
Provide post-event report of activities.	

LOGISTICS TEAM LEADER TASK CHECKLIST

When activated, organize and coordinates the provision of services (HR, communications, medical, food, transportation and housing) and support (supplies, facilities and ground support) to the incident.	
Disseminate information and messages to appropriate departments and individuals.	
Assist Incident Manager as directed.	
Provide post-event report of activities.	

OPERATIONS TEAM LEADER TASK CHECKLIST

When activated, direct and coordinates all tactical operations associated with the incident.	
Disseminate information and messages to appropriate departments and individuals.	
Assist Incident Manager as directed.	
Provide post-event report of activities.	

FINANCE TEAM LEADER TASK CHECKLIST

When activated, facilitate various administration and financial activities.	
Monitor incident costs and maintains financial records.	
Address insurance and workmen’s compensation issues.	
Facilitate procurement activities, e.g., contracts.	
Monitor timekeeping and related activities.	
Disseminate information and messages to appropriate departments and individuals.	
Assist Incident Manager as directed.	
Provide post-event report of activities.	

4.8 Pre-incident preparations

Establish regional response plans and procedures for dealing with incidents.	
Establish communications process for disseminating information about an incident to the RIMT.	
Point of contact for compiling information on incidents and reporting to TAC and senior management.	
Train alternate(s) assigned as backup to Regional Incident Manager.	

4.8.1 Actions following an incident and prior to a disaster declaration being made

Gather input from the local Incident Management Team, Damage Assessment Team, and local senior management.	
Analyze the input and complete an initial assessment of the situation. Attempt to determine the potential for an evacuation or other activity that would negatively impact operations at the site.	
Forward the assessment results and any other intelligence to the Threat Assessment Center for analysis and action.	
Coordinate incident analysis with regional peers.	

4.8.2 Support for Local Incident Management Team meeting

Contact local IMT leader via Public Information Officer to ensure that the IMT has set an initial meeting and venue.	
Obtain a current situation report from the IMT and Damage Assessment Team. Key talking points include the following: 1. Type of event (fire, tornado, terrorism, power outage, telecomm outage, etc.) 2. Specific location of event, if known (building, floor, side of floor, etc.) 3. Magnitude of the event 4. Time of event 5. Suspected cause 6. Emergency/evacuation procedures status 7. Police and fire departments notified 8. Injuries and fatalities 9. Building access status (current access, near-term potential access) 10. Immediate impact to business operations 11. Potential for news media attention	
Ensure creation of a schedule of updates for Threat Assessment Center to monitor ongoing emergency response procedures. Commence providing TAC updates.	
Ensure that a member of the local IMT documents, in chronological order, incident milestones and actions taken using the EXHIBIT 1 – BUSINESS INTERRUPTION REPORT template in the Recovery Forms section of this guide. This form will be used as a tool to update the IMT, TAC and/or other senior management.	
Ensure that local management has decided whether or not to intercept 800# phone lines with a customized emergency voice recording.	
Ensure that local management has decided to launch/not launch the MessageOne emergency notification service, in addition to/in lieu of 800# service arrangements.	

4.8.3 Actions during and after the disaster

Ensure that InfoExchange xxx-xxx-xxx is updated as follows: Regional Incident Manager: Office: Cell: Home: VP: Office: Cell: Home:	
Provide a brief situation report including: ▪ Nature of the incident (e.g., physical damage, life safety issues) ▪ Potential impact to business units ▪ Actions taken by local IMT and DAT ▪ Actions taken by local management ▪ Actions taken by employees ▪ Actions taken by others ▪ Estimated time to return to normal operations	
Identify local EOC location and contact information.	
Continue updates on agreed-upon schedule.	
Follow up to ensure that BUSINESS NAME team leaders have notified their respective recovery team members. Document notifications in the EXHIBIT 1 - PERSONNEL NOTIFICATION CONTROL LOG found in the Recovery Forms section of this guide.	
Notify any other BUSNESS NAME contacts and third parties as deemed necessary. See the KEY CONTACTS section of this guide for contact information.	
Follow up to ensure that information regarding the status of the incident and the company's response to it is regularly communicated to the appropriate individuals and organizations.	
Be available to answer questions and provide input to other organizations as they enter the incident response/recovery process	
Be available to answer questions and provide input to other organizations as they enter the post-incident recovery and evaluation process.	

4.8.4 Post-event maintenance activities

Assess regional incident management readiness.	
Assess avian influenza readiness in region.	
Maintain IM program through quarterly team training and updating of IM plan documentation and checklists.	

Section Five - Appendixes 5.1

Incident Management forms

Exhibit 1: Incident report

Date	Nature of incident	Time/Details	Action taken	Directive

Exhibit 2: Incident objectives and strategy form

Date/Time:				
Incident name:				
Expected duration:				
Completed by:				
Objectives/strategies to be completed in the first 3 hours:				
Objectives/Strategies	**IMT Leader**	**Assigned Date/Time**	**Status**	**Completed Date/Time**
Objectives/strategies to be completed in the first 8 hours:				
Objectives/Strategies	**IMT Leader**	**Assigned Date/Time**	**Status**	**Completed Date/Time**
Objectives/strategies to be completed in the first 15 hours:				
Objectives/Strategies	**IMT Leader**	**Assigned Date/Time**	**Status**	**Completed Date/Time**

Objectives/strategies to be completed in the first 24 hours & after:				
Objectives/Strategies	IMT Leader	Assigned Date/Time	Status	Completed Date/Time

Exhibit 3: Personnel notification control log

Date/Time:					
Name	**Status**	**Location assignment**	**Phone number**	**Work from**	**Work to**

Exhibit 4: IMT personnel assignment form

Date/Time:					
Incident name:					
Recovery team:					
#	**Name**	**Recovery title/Role**	**Date/Time**	**Work from**	**Work to**
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

11					
12					
13					

Exhibit 5: Critical equipment assessment and evaluation form

Incident name:				**Date/Time:**
Recovery team:				**Completed by:**
Condition key:				
OK - Undamaged				
DBU - Damaged but usable				
DS – Damaged; needs salvage before use				
D - Destroyed				
#	**Equipment (Itemize)**	**Condition**	**Time to salvage**	**Comments**
1				
2				
3				
4				
5				
6				