

Generally Accepted Practices
For
Business Continuity Practitioners
Drafted by:

Disaster Recovery Journal
And
DRI International



DRI International

I. Preface

The Business Continuity focus will become a standard discipline and established profession when Business Continuity professionals put their minds together to create Generally Accepted Business Continuity Practices.

The DRJ Editorial Advisory Board Generally Accepted BC Practices Committee in concert with DRI International is continuing its effort to create universally accepted Business Continuity Practice guidelines.

The Generally Accepted Business Continuity Practices subject areas align with the ten DRII Professional Practices:

1. Project Initiation and Management
2. Risk Evaluation and Control
3. Business Impact Analysis
4. Developing Business Continuity Strategies
5. Emergency Response and Operations
6. Developing and Implementing Business Continuity Plans
7. Awareness and Training Programs
8. Maintaining and Exercising Business Continuity Plans
9. Public Relations and Crisis Coordination
10. Coordination with Public Authorities

The Professional Practices tell you what you need to do and the Generally Accepted BC Practices will tell you how to do it.

The DRJ has also partnered with the following organizations to assist in the creation of the Generally Accepted BC Practices:

- Association of Records Management Administration (ARMA)
- DRI International (DRII)
- Financial Services Technology Consortium (FSTC)
- Standards Australia/Standards New Zealand
- National Fire Protection Association (NFPA)

Please review the document and consider assisting in this effort as it is an opportunity to make an impact in the Business Continuity industry.

I. Introduction

A. Mission Statement

To be recognized as a leading source of “sound” Generally Accepted Practices by providing a depository of knowledge and recommendations offered by skilled Business Continuity Professionals.

B. Scope

Best Practices will be compiled from submittals by experienced Business Continuity Professionals from the public and private sectors, as well as user groups and/or related organizations, in regards to the industry standard Professional Practices. The Best Practice Committee will review the submittals quarterly for approval. The approved submittals will reside on the Disaster Recovery Journal website for all practitioners to access and implement within their respective organizations.

The process of developing the matrix consisted of contacting all associations and better understanding what processes they had in place either via direct input or via web sites

The DRJ EAB Best Practice effort is not attempting to replace the vertical space, they are trying to build an abstract of the work that the organizations are doing and then pull the detail together for a view of the overall. This process is not to re-create the wheel it is to provide the input for all professionals to use

- This is a two step approach:
 - Phase I: Initially address the high level
 - Phase II: Initiate a Drill down process to flesh out the details based on industry

II. Professional Practices

A. Background

In order to set the precedent, the definition of DRII/BCI Professional Practices will be noted prior to each Generally Accepted Practice.

The Professional Practices in whole will not be identified within this document however, the link below can be reviewed for full detail on these joint Practices:

<http://www.drii.org/displaycommon.cfm?an=2>

This information will allow for the practitioner to identify the background or the “what” (Professional Practice) to be associated with the “how” (Generally Accepted Practice).

DRII/BCI Professional Practice Narrative:

- Establish applicable procedures and policies for coordinating response, continuity, and restoration activities with external agencies (local, state, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes or regulations.

Generally Accepted Practices (GAP) Notice:

- This document is to serve as a repository of knowledge which is to be applied across various verticals
- This document contains a conceptual basis for Program development vs. an auditable checklist

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	1	Determine who your local and regional public authorities are and their potential impact on your plans including, but not limited to DHS (terrorism), emergency management, fire, police, public utilities and your local & nationally elected public officials.	<ul style="list-style-type: none"> - Determine who is responsible for liaison with each area of expertise - Meet regularly with each authority internally and/or externally - Participate in joint activities - Support authority initiatives, especially those affecting your business and area. - Communicate regularly with internal staff who are members of or volunteers for public authorities. - Maintain information about your countries national Security Department (such as the United States' Department of Homeland Security (DHS)) asset & vulnerability identification, cross-sector analyses & prioritization programs, protection programs, threat assessments, etc. 	<p>Examples of groups and individuals to know:</p> <ul style="list-style-type: none"> - Local emergency management offices (city, county, region, etc.) - Elected & appointed officials including but not limited to, mayor, county judge, council members, etc. - Fire chief, police chief, (EMS) Emergency Medical Services head, public (or service provider) utility head and designated interface, etc - United States DHS interface - Your National Security Terrorism organization.

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	2	Understand potential impact of laws, regulations, codes, zoning, standards or practices <u>concerning emergency procedures</u> specific to your location and industry	<ul style="list-style-type: none"> - Determine responsibility for maintaining current knowledge of laws, regulations, etc. to include assignments for public meeting attendance, press release and other release reading, and meeting with public officials. - Hold regular meetings to discuss changes for or impact to current response, emergency and recovery procedures. - Participate in local emergency planning committee meetings. - Partner with other organizations with interest in similar or the same laws, regulations, zoning, etc. for information sharing and “encouragement” support. - Leverage your internal legal department. - Assign lobbying responsibility to “encourage” laws, regulations, zoning, etc 	<p>Examples of when this knowledge may be important:</p> <ul style="list-style-type: none"> - Hazardous material response, movement and receipt may require specific notification and coordination. - Understanding governmental regulations (ie: OSHA) - Heavy or “large” equipment or objects moves may require permits and coordination. - Radio frequency may be regulated - Response supply access may be limited (local & vendor site) - Expected resources may not be available if preempted by higher authorities <p>Examples of organizations:</p> <ul style="list-style-type: none"> - EHMA-East Harris County Manufacturers Association - LEPC-Local Emergency Planning Committee - Industry associations - Area support groups <ul style="list-style-type: none"> o Building & “block” associations - Neighborhood Associations <p>Lobbying points of reference:</p> <ul style="list-style-type: none"> - Direct and association lobbying efforts - Zoning commissions - Appraisal District Boards - Water supply boards

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	3	Determine organizational interface protocol, identification and training requirements and assign appropriate internal staff or support representative(s).	<ul style="list-style-type: none"> - Assign an internal liaison responsibility for each area of expertise - Include information in the regular validation process - Reinforce interface protocol at all levels during training exercise, etc. - Develop Policy and operational procedures to support and define the activity. - Hold joint meetings to discuss and establish expectations for internal and external response, emergency and recovery procedures - Resolve any conflicting issues and coordinate and document resolutions for implementation. - Verify reporting requirements and frequency for applicable events. 	<p>Match expertise with requirement</p> <ul style="list-style-type: none"> - PIO (Public Information Officer) - PR (Public Relations Officer) - Technical staff interface - Fire team - Hazmat team - Facilities support <p>Example groups include:</p> <ul style="list-style-type: none"> - Area councils - Local Emergency Planning Committee (LEPC) - Volunteers Active During Disaster (VOAD) - Citizen Emergency Response Team (CERT) <p>Note: These lists are not all inclusive</p>
Preparedness	4	Document the forms and processes to be used before or during an event or exercise to ensure activities and participants, etc. are captured for review and Plan response and recovery improvements.	<ul style="list-style-type: none"> - Include this responsibility to the persons assigned liaison responsibility for each area of expertise - Include information gathered in internal procedures - Validate information on a regular basis - Include information gathered in internal procedure validation exercises and training. - Hold joint information sharing meetings and exercises to review results of information gathered during an event. - Include this process in future updates of your plan and training and awareness program. - Determine if permits are required specific (public authority provided) request and/or reporting forms - Ensure Legal Department review liability issues 	<ul style="list-style-type: none"> - ICS (Incident Command System) forms - Process flow charts - Communication interface forms - Staffing forms - Contact lists - Chemical descriptions & affects

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	5	Document the public authority groups and individual contacts, their communication protocol required and status reporting process.	<ul style="list-style-type: none"> - Determine who is responsible for liaison each area of expertise - Validate information gathered on a regular basis to ensure information is current on a quarterly basis. - Develop or obtain forms/reports to be used at time of incident. - Develop Post Incident Review (PIR) process and timelines. - Work with local Public Information Officers (PIO) to understand and follow protocol. - Ensure that any permit required activities, which may require several stages of interface throughout the process such as pre-approval, coordination or monitoring, and post event reporting and review, are completed as required. - Participate with public authorities during an event or exercise to and validate any coordination specifically required expertise, equipment, training and protocols. 	<ul style="list-style-type: none"> - Contact lists with details - Interface methods documentation & forms - Insurance confirmation forms, etc. - Permit reporting forms - Post Incident Review documents - U.S.A. National Center for Crisis & Continuity Coordination: www.nc4.us/nc4/index.php <p>Public authority groups examples:</p> <ul style="list-style-type: none"> o Fire o Police or Deputy Police o National Guard <p>Volunteer and non-Profit group examples:</p> <ul style="list-style-type: none"> o Volunteer fire o CERT-Citizen Emergency Response Team o LEPC-Local Emergency Planning Committee o Salvation Army o Baptist men <p>Public-private incident management partnership examples:</p> <p>http://www.mnisac.org/ https://www.chicagofirst.org/ http://www.pittsburghcoalitionforsecurity.org/ http://www.bensbusinessforce.org http://mnisac.org/Partnerships-Homeland-Security.htm</p>

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	6	Document each public authority group's information sources that apply to your full Business Continuity Management processes.	<ul style="list-style-type: none"> - Determine who is responsible for liaison each area of expertise - Maintain source locations and include in internal documentation. - Validate information on a regular basis (quarterly recommended). - Incorporate information in internal disaster scenarios and procedure validation exercises. 	<p>Examples of sources to monitor include:</p> <ul style="list-style-type: none"> - NWS (National Weather Service) email service - Website "Alert" pages - Court (legal system) notifications through business journals, website, etc. <p>http://www.tropicalstormrisk.com/ http://www.noaa.gov/ http://neic.usgs.gov/neis/bulletin/ http://www.nws.noaa.gov/ http://www.nhc.noaa.gov/ http://www.prh.noaa.gov/ptwc/ http://www.emsc-csem.org/Html/ALERT_email.html</p> <p>Local Metro traffic cameras (Houston) http://www.houstontranstar.org/</p>
Preparedness	7	Ensure information that may be required immediately by public authorities during an incident is readily available.	<ul style="list-style-type: none"> - Assign an internal liaison responsibility for each area of expertise - Include in the planning a liaison to work with the local officials on site at the time of an incident. Ensure they understand the role and the information that would be required of them. - Provide regular information and resource tours for public authorities and internal liaisons to ensure appropriate information sharing. - Document and provide, appropriate, type and location information (maps, graphs, spreadsheets, etc.) being certain to maintain appropriate confidentiality. 	<p>Examples of information required:</p> <ul style="list-style-type: none"> - Electrical and telecomm sources, - Floor plans - Hazardous Waster Storage facilities (ie: PCB's) - Chemical storage & supplies - Laboratories, - Organizations site layout information - Secure areas, - Water - Foam for fire suppression <p>Note: This list is not all</p>

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
				inclusive
Preparedness	8	Document the levels of support available to your organization's response and recovery Plan.	<ul style="list-style-type: none"> - Assign an internal liaison responsibility for each area of expertise - Hold joint meetings or exercises to discuss internal and external response, emergency and recovery procedures and the overall support that will be provided based upon different scenarios. - Resolve any conflicting issues and coordinate and document resolutions for implementation. - Include information gathered in future updates of your plan. - Include the information gathered as part of the Plan and response validation process. - Evaluate support during critical time periods such as days 1 through 5 of your requirements and procedures as they relate to public authority interface. 	<ul style="list-style-type: none"> - Public authority policy - Hazardous material clean-up (may need EPA approval, reporting etc.) - Non-profit charter policy (Red Cross, United Way, Baptist Men, Salvation Army, etc.) - Citizen group policies (CERT, etc.) - Ham Radio operators
Preparedness	9	Obtain and review your facility(s) and regional access issues.	<ul style="list-style-type: none"> - Assign an internal liaison responsibility for each area of expertise - Include information gathered in internal procedures - Validate information on a regular basis - Include information gathered in internal procedure validation exercises. - Obtain maps and identify alternate routes - Validate facility / business access requirements such as ID's, etc. - Define local access and digress issues such as timing with other business, etc. 	<p>Examples of access issues:</p> <ul style="list-style-type: none"> - "All clear" parameters - Evacuation and return routes - Official escape and return routes of personal and commercial roadways, waterways and airway <p>- Special transport routes (chemical, size, etc.)</p> <p>Note: This list is not all inclusive</p>
Preparedness	10	Identify and document organizational and other resources potentially available in support of public authorities and other organizations.	<ul style="list-style-type: none"> - Assign an internal liaison responsibility for coordinating with external liaisons and evaluating possible mutual aid assistance. - Include information gathered in internal procedures and documentation. - Validate information on a regular basis - Include information gathered in disaster validation scenarios. - Include information gathered in internal risk assessment and mitigation processes 	<p>Examples of supporting resources:</p> <ul style="list-style-type: none"> - CERT-Citizen Emergency Response Team - Sea ports - EOC Centers -Emergency (or Joint) Operation Centers - Evacuation support centers - Fire facilities - Hospitals,

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
			<ul style="list-style-type: none"> - Provide regular information and resource tours for public authorities and internal liaisons to ensure appropriate information sharing. - Document and provide, appropriate, type and location information (maps, graphs, spreadsheets, etc.) being certain to maintain appropriate confidentiality. 	<ul style="list-style-type: none"> - Key vendors, - LEPC-Local Emergency Planning Committee resources - Television & Radio stations - National Guard - Police - Red Cross - Supply warehouses - United Way - Salvation Army - Baptist Men <p>Share item examples:</p> <ul style="list-style-type: none"> - Hazardous materials - Chemicals - Fuel supplies - Water & foam (fire suppression) sources - Communication devices & support equipment - Ham radio - Equipment (trucks, back hoes, ships, etc.) - Organizational contacts - Locations - Skills and Training parameters - Shelter capability - Ability to provide food to emergency workers/community - Satellite web capability: www.google.earth.com
Preparedness	11	Acquire public authority reports of area vulnerabilities and risks and include complimentary and appropriate mitigation and response procedures in your organizations Business Continuity Plan and	<ul style="list-style-type: none"> - Assign an internal liaison responsibility for each area of expertise - Maintain current public and internal studies and assessments and include in future updates of your plan. 	<p>Examples studies, assessments etc.:</p> <ul style="list-style-type: none"> - Flood plain maps - Risk assessments - Monitoring systems

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
		risk assessment process.	<ul style="list-style-type: none"> - Include applicable information in the risk assessment, BCP development, internal change control process and validation processes - Partner with local authorities on assessments. - Contact local authorities to obtain information. 	<ul style="list-style-type: none"> - Road extensions - Bridge capacities - Land use studies - Debris Management <p>Examples of where to obtain information:</p> <ul style="list-style-type: none"> - Department of Transportation (DOT) - Environmental Protection Agency (EPA) - Regional Councils (HGAC Houston Galveston Area Council) <p>Note: This list is not all inclusive</p>
Preparedness	12	Document organizations staff members that may be a member of a public authority or support group.	<ul style="list-style-type: none"> - Require each internal team to maintain and communicate this information to the appropriate internal team (BCP, Emergency management, etc.) for consolidation and distribution. - Work with legal to ensure all liability issues have been addressed. - Compare the list to internal response lists to ensure that internal readiness and response are not affected - During training and team selection to ensure all participants are aware of their organizational responsibilities and identify any conflict with responsibilities within the community. - Have Legal Dept. review liability & legality issues 	<p>Public authority groups examples:</p> <ul style="list-style-type: none"> - Fire - Police or Deputy Police - National Guard or any military affiliation <p>Volunteer and non-Profit group examples:</p> <ul style="list-style-type: none"> - Volunteer fire - CERT-Citizen Emergency Response Team - LEPC-Local Emergency Planning Committee - Salvation Army - Baptist men - Defense Force - <p>Note This is not an all inclusive list</p>

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	13	Document local and regional supporting infrastructure resources.	<ul style="list-style-type: none"> - Assign an internal liaison responsibility for each area of expertise - Include information gathered in internal procedures and documentation. - Validate information on a regular basis - Include information gathered in disaster validation scenarios. - Include information gathered in internal risk assessment and mitigation processes - Visit each location on a regular basis and include in internal operational and response, emergency and recovery procedures. 	Infrastructure examples: <ul style="list-style-type: none"> - Roadmaps - Contour maps - Pipelines - Waterlines - Power plants and grids - Communication lines & hubs - Railroads - Bridges - Water and fuel supplies
Preparedness	14	Obtain a copy of and review the Emergency Operations Procedures of the Local Authorities,	<ul style="list-style-type: none"> - Assign an internal liaison responsibility - Require appropriate review and analysis against internal procedures, documentation and validation exercises. Note: Information sources are staff who are members of these groups and direct from the public authority & volunteer groups	Public authority policy & procedure manuals: <ul style="list-style-type: none"> - Fire - Police - Transportation department - HAZMAT
Preparedness	15	Participate in local Emergency Management, Business Continuity and other organizations that support your industry.	<ul style="list-style-type: none"> - Assign the responsibility of coordination of an appropriate interface to executive management. - Include responsibility to internal Public Relations (PR) and/or Public Information Officer (PIO). - Work with Legal Dept. to ensure liability issues are addressed. 	Types of organizations: <ul style="list-style-type: none"> - CERT-Citizen Emergency Response Team - Sea ports support - EOC Centers -Emergency (or Joint) Operation Centers - Fire departments - Hospitals, - LEPC-Local Emergency Planning Committee resources - National Guard - Police - Red Cross Disaster services - United Way - Salvation Army - Baptist Men

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	16	Utilize an accepted standard of incident command format that interfaces with local/regional/etc. authorities and their implementation.	<ul style="list-style-type: none"> - Train and validate training for ICS - Use the ICS format in all response, emergency and recovery procedures as well as operational procedures where applicable. - Hold regular meeting with and participate in or observe public authority ICS implementations and activities. - Review information gathered for possible changes to internal procedures. 	<ul style="list-style-type: none"> - National Incident Management System (NIMS) - Incident Command System (ICS) forms
Preparedness	17	Review public authority and 3 rd party support activities with industry peers & other company offices.	<ul style="list-style-type: none"> - At networking meetings, conferences, professional organizations, mutual aid partners, white papers, magazine input, etc. - Work with Legal Dept. to ensure liability and legal issues associated with discussion and distribution. - Document lessons learned in controls, preparedness, detection, mitigation response, recovery and training Plans 	<ul style="list-style-type: none"> - Association of Contingency Planners
Preparedness	18	Determine requirements to participate in National Programs.	<ul style="list-style-type: none"> - Assign an appropriate interface to the programs - Maintain currency with the programs and provide input to the programs when open for review. - Coordinate programs, etc. as applicable with authorities at all levels - Partner with international appropriate interfaces - Ensure Legal Dept. reviews each interface. - Determine potential impact or support of National Programs 	<ul style="list-style-type: none"> - U.S. Presidential Directives 5, 7 & 8 - National Strategy for Homeland Security - Homeland Security Act - National Strategy for Physical Protection of Critical Infrastructure - National Strategy for Cyber Security - National Infrastructure Protection Plan (NIPP) - National Preparedness Goal - National Incident management System (NIMS) April 2005 report <p>Note: List is not all inclusive.</p>

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Response & Recovery	1	Monitor documented status information sources included on local, regional and national Warning Systems, Press Releases, radio and television reports, etc.	<ul style="list-style-type: none"> - Assign maintenance of monitoring status information. - Include gathered documentation in the internal response, emergency and recovery procedures and operational procedures. - Ensure resources are available for person monitoring status to have internet access, weather radios and cable TV and radio availability minimum for monitoring. If necessary include satellite phones. 	<p>Examples of sources to monitor:</p> <p>http://www.tropicalstormrisk.com/ http://www.noaa.gov/ http://neic.usgs.gov/neis/bulletin/ http://www.nws.noaa.gov/ http://www.nhc.noaa.gov/ http://www.prh.noaa.gov/ptwc/ http://www.emsc-csem.org/Html/ALERT_email.html</p> <p>- Pacific Disaster Center http://www.pdc.org/core_rva.php - Houston area Metro http://www.houstontranstar.org/</p>
Response & Recovery	2	Document the actual events including all incoming information and recommendations and comments by participants, clients and observers to facilitate post event analysis.	<ul style="list-style-type: none"> - Assign event documentation responsibility - Maintain effective documentation forms and process - Include gathered documentation in the internal response, emergency and recovery procedures and operational procedures. 	<ul style="list-style-type: none"> - ICS (Incident Command System) forms - Process flow charts (RTO, RPO, etc.) - Communication interface forms - Staffing forms - Contact and contacted lists - Procedure changes & issues occurring

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Response & Recovery	3	Communicate availability of and document use of resources for public authorities.	<ul style="list-style-type: none"> - Obtain executive approval - Assign an internal liaison responsibility for coordinating with external liaisons the availability of possible mutual aid resource assistance. - Assign the mutual aid documentation and reporting responsibility - Maintain currency of mutual aid resources - Work with legal to ensure liability issues are addressed 	Share item examples: <ul style="list-style-type: none"> - Hazardous materials - Chemicals - Fuel supplies - Water & foam (fire suppression) sources - Communication devices & support equipment - Ham radio - Equipment (trucks, back hoes, graders, ships, etc.) - Organizational contacts Other items may also be considered depending on need, availability and industry
Response & Recovery	4	Report required incidents to public authorities in the format, frequency and through the required contact agency.	<ul style="list-style-type: none"> - Include acquisition of this information during the Planning & preparedness phase - 'Funnel' reporting through your internal assigned interface(s) - Work with legal to ensure liability issues are addressed since reports probably will become public information 	Examples include: <ul style="list-style-type: none"> - Hazardous material spills - Fires - Bomb threats - Construction activities - Unusual (visible) activities

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Training, Exercise & Awareness	1	Participate in local and regional training and exercises as appropriate to support organizations requirements	<ul style="list-style-type: none"> - Document available public authority offered training possibilities - Use public training as appropriate to support internal requirements - Obtain internal executive approval - Assign executive management responsibility for the exercise participation decision - Document appropriate participation roles and responsibility - Assign internal staff specific participation responsibility - Document and review activities and results - Work with legal to ensure liability issues are addressed 	<p>Training examples to consider:</p> <ul style="list-style-type: none"> - Emergency Management training - HR-Human Resource training - Joint support training (VOAD, CERT. etc.) - Security (police) and fire training - Handling of hazardous materials - Evacuation training - Incident Command System training <p>Exercise examples to consider:</p> <ul style="list-style-type: none"> - Fire drills - Terrorist drills - Hazardous material drills - Evacuation drills - Emergency Operations Center (EOC). <p>Note: These lists are not all inclusive</p>
Training, Exercise & Awareness	2	Share internal training for the response and recovery Plans developed including documentation validations and certification process, table-tops, walk-through's, component validations, etc.	<ul style="list-style-type: none"> - Document available shared training possibilities - Obtain internal executive approval - Assign an internal liaison to coordinate including public authorities in internal approved training - Work with legal to ensure liability issues are addressed 	<p>Training to consider sharing includes:</p> <ul style="list-style-type: none"> o Documentation validations o Certification process o Table-tops o Walk-throughs o Component validations o Equipment maintenance procedures <p>Note: This list is not all inclusive</p>

Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Training/Exercise & Awareness	3	Monitor public authority exercises and event response and review their event management, on-going recovery status and Plan implementations.	<ul style="list-style-type: none"> - Assign a liaison to monitor public authority activities - Review the information gathered and integrate into internal appropriate procedure documentation - Participate in events and review public releases related to the event. - Inquire about up-coming events through regular conversations with local authorities 	Example sources to monitor include: <ul style="list-style-type: none"> - Newspapers - Trade and association newsletters - Television and radio announcements - Websites of the public authority and participating organizations Note: This list is not all inclusive
Training/Exercise & Awareness	4	Notify and include authorities in organizational exercises where applicable.	<ul style="list-style-type: none"> - Assign executive management responsibility for the decision of including public authorities in internal activities. - Assign a liaison to communicate and coordinate the internal event schedule and any on-going event status - Provide an event overview to the authority to aid their review and "follow along" - Maintain currency of event public authority inclusion - Document roles and authorities - Review all resulting activities and participation. - Work with legal to ensure liability issues are addressed. 	<ul style="list-style-type: none"> - Up coming exercises - Fire Drills

Coordination with External Agencies

	#	What	How	Points of Reference
Post Event or Exercise	1	Review public authority event or exercise documentation; plan objectives, participants and final reports for lessons learned and Plan and training modifications and procedures improvements.	<ul style="list-style-type: none"> - Assign a reporting process and a person responsibility for the information gathering - Document an appropriate reporting format for the information - Assign information review responsibility - Include reviewed information into the internal change control process - Use any available public information your staff members who are members of the public authority have concerning the event. 	Examples of information sources include: <ul style="list-style-type: none"> - Local Emergency Managers - Board of Supervisors Minutes/Meetings - LEPC Coordinator - Websites of the public authority and participating organization - Obtain information from the exercise or event source.
Post Event or Exercise	2	Communicate internal event or exercise results to public authorities when their support was utilized, could have been utilized or had an effect on your recovery.	<ul style="list-style-type: none"> - Obtain executive authorization for information to be shared with public authority and the associated confidentiality. - Assign a high level communication liaison - Review to be reported information for inclusion into the internal change control process and - Communicate public authority response to information received. - Assign a liaison to “encourage” public authority participation if their assistance “could have been utilized” and adjust internal procedures to cover requirements until their participation or resources are available. - Work with legal to ensure liability issues are addressed 	<ul style="list-style-type: none"> - Exercises - Fire Drills - Actual events
Post Event or Exercise	3	Participate in post event public discussions and round-tables.	<ul style="list-style-type: none"> - Assign an executive management and/or PR person to determine the participation role - Assign a public authority post event liaison - Document a reporting, and evaluation process and a procedure for post event information integration. - Work with legal to ensure liability issues are addressed 	<ul style="list-style-type: none"> - Forums - Workshops - Conferences - Networking events

Coordination with External Agencies

	#	What	How	Points of Reference
			<ul style="list-style-type: none"> - Prepare by reviewing released event information - Monitor local papers, etc. to determine when & where information will be released. 	
Post Event or Exercise	4	Coordinate future internal exercises and objectives with local authorities.	<ul style="list-style-type: none"> - Define and document possible future events to coordinate - Receive approval by executive management of events and roles and responsibilities - Meet with public authority to review event possibilities and the roles and responsibilities and obtain their recommendations and approval - Report final coordination plans with executive management for approval. - Document coordination reporting format and assign documentation responsibility - Work with legal to ensure liability issues are addressed 	

DRII/BCI Professional Practice Narrative:

- Develop, coordinate, evaluate, and exercise plans to communicate with internal stakeholders (employees, corporate management, etc.) external stakeholders (customers, shareholders, vendors, suppliers, etc.) and the media (print, radio, television, Internet, etc.)

Generally Accepted Practices (GAP) Notice:

- This document is to serve as a repository of knowledge which is to be applied across various verticals
- This document contains a conceptual basis for Program development vs. an auditable checklist

Crisis Communications				
Sub-Topic	#	What	How	Point of Reference
Planning	1	Ensure the company's Communications Department has identified key resources designated to initiate crisis communications with employees, business partners, vendors, government and external media.	<ul style="list-style-type: none"> - Have Senior Management identify any additions or deletions of key resources. - Consider including: government, employees, customers, media/Communications Department, business partners, vendors, etc. - Obtain Senior Management approval on sponsorship for designated and trained internal resources. 	<ul style="list-style-type: none"> - Stakeholder listing (company, rep. name, primary and alternate contact information, etc.) - Implement standard sign-off forms or agreements as evidence of approval.
	2			
	3			

Crisis Communications

Sub-Topic	#	What	How	Point of Reference
Develop	1	Develop Crisis Communication Plans with internal personnel (management, staff, response teams, etc.)	<ul style="list-style-type: none"> - Obtain contact (during and after business hours) information for personnel. - Establish notification lists for Senior Management. - Establish notification lists for Crisis Management teams. - Establish notification lists for internal departments. - Establish notification lists for other response teams 	
	2	Document procedures and identify tools to manage relationships and communications process with external partners: business partners, governmental agencies, vendors, etc.	<ul style="list-style-type: none"> - Identify and obtain contact (during and after business hours) information for external partners - Establish credentials for key contacts for future events; also identify access levels for credentials. - Establish relationships in advance of emergency events. - Develop ongoing procedures / tools to manage relationships with the external partners. - If appropriate to the environment, partner with HR to automatically update / maintain the contact lists. 	

Crisis Communications

Sub-Topic	#	What	How	Point of Reference
	3	Develop Crisis Communication Plans with the media	<ul style="list-style-type: none"> - Identify and obtain contact (during and after business hours) information for media representatives (internet, radio, tv, print, etc.) - Establish credentials for key media representatives for future events; also identify access levels for credentials. - Establish relationships in advance of emergency events. - Develop ongoing procedures / tools to manage relationships with the stakeholders. - Establish designated internal / external locations for media briefings. 	
	4	Develop an Awareness and Education Program for Staff and Management	<ul style="list-style-type: none"> - Partner with Security and Facilities to identify methods for integration with existing programs. - Identify the media type, frequency, methods of distribution, etc. regarding the program. 	
	5			

Crisis Communications

Sub-Topic	#	What	How	Point of Reference
Implement	1	Establish communication methods (i.e., 800 number, website, pager distribution lists, conference lines, etc.)	<ul style="list-style-type: none"> - Partner with the Human Resources and Telecommunications Dept., etc. to establish an 800 # that can be activated at time of an event to communicate status information to employees as well 800 numbers for crisis communication teams, etc. - Develop distribution lists for various management teams, response teams, etc. 	

Crisis Communications

Sub-Topic	#	What	How	Point of Reference
	2	Contain media personnel during an event.	- Work with physical security and management to direct media personnel to designated location(s).	
	3	Educate employees to direct media inquiries to the Communications Department.	- Print and distribute memo instructing employees to direct any media inquiries to the PR Department	
	4			

Crisis Communications				
Sub-Topic	#	What	How	Point of Reference
Exercise	1	Develop Exercise	<ul style="list-style-type: none"> - Determine participants. - Schedule times and locations. 	
	2	Facilitate Exercise	<ul style="list-style-type: none"> - Monitor the progress and keep everyone on a time schedule. 	
	3	Involve appropriate external parties during exercise events.	<ul style="list-style-type: none"> - Extend invitations to department representatives to participate in the exercise. - Carefully select the time during the event to involve the media, if at all. 	
	4			

Crisis Communications				
Sub-Topic	#	What	How	Point of Reference
Maintain	1			
	2			
	3			
	4			

DRII/BCI Professional Practice Narrative:

- Pre-plan and coordinate plan exercises, and evaluate and document plan exercise results. Develop processes to maintain the currency of continuity capabilities and the Plan documents in accordance with the organization’s strategic direction. Verify that the Plans will prove effective by comparison with a suitable standard, and report results in a clear and concise manner.

Generally Accepted Practices (GAP) Notice:

- This document is to serve as a repository of knowledge which is to be applied across various verticals
- This document contains a conceptual basis for Program development vs. an auditable checklist

Maintaining and Exercising BC Plans				
Sub-Topic	#	What	How	Points of Reference
Maintaining – Quality Review Program	1	Reference subject area #6		
	2	Minimum requirement of corporate standard	<ul style="list-style-type: none"> • Understand what your corporate standard is. 	
	3	Site self assessment review contact info at least quarterly	<ul style="list-style-type: none"> • Require each location review contact info at least quarterly 	
	4	Site self assessment review requirements at least semiannually	<ul style="list-style-type: none"> • Require each location to review plan requirements at least semi annually 	
	5	Site self assessment review procedures at least annually	<ul style="list-style-type: none"> • Require each site to review the procedures at least quarterly 	
	6	Make other reviews when organizational change requires	<ul style="list-style-type: none"> • Incorporate major organizational changes into plan 	

Maintaining and Exercising BC Plans				
Sub-Topic	#	What	How	Points of Reference
	7	Develop plan content guidelines.	<ul style="list-style-type: none"> Determine key data to review and develop guideline around those requirements 	
	8	Management reporting	<ul style="list-style-type: none"> Report findings to senior management 	
	9	Base any quality requirements on existing regulations (e.g., audit, legal, ISO, SOX, HIPAA)	<ul style="list-style-type: none"> Consider all existing regulations governing your organization and build quality requirements around them 	
	10	Corporate Program Office full reviews to be done year (percentage of total existing plans)	<ul style="list-style-type: none"> Develop a plan for the corporate office to do a detailed assessment of a percentage of plans 	

Maintaining and Exercising BC Plans				
Sub-Topic	#	What	How	Points of Reference
Exercising	1	Develop exercise objectives and scope	<ul style="list-style-type: none"> Consider all risks when developing exercise 	

Maintaining and Exercising BC Plans				
Sub-Topic	#	What	How	Points of Reference
	2	Use scorecard to grade objectives	<ul style="list-style-type: none"> Develop a scorecard to grade objectives 	
	3	Publish after-action list	<ul style="list-style-type: none"> Publish list of after-actions to management 	
	4	Test at least annually. Certain areas benefit from more frequent exercising based of level of criticality.	<ul style="list-style-type: none"> Consider criticality of the function to the organization to determine level of testing required 	
	5	Manage/track exercise actions	<ul style="list-style-type: none"> Develop a process to track actions to confirm closure 	

Maintaining and Exercising BC Plans				
Sub-Topic	#	What	How	Points of Reference
Exercising – Discussion-based	1	Hold workshop to produce new or updated BC plan data and procedures	<ul style="list-style-type: none"> Bring all critical functions together 	
	2	Execute an interactive walkthrough of a documented plan	<ul style="list-style-type: none"> Discuss scenario against documented plan 	
	3	Execute an interactive session for data collection to develop plan content	<ul style="list-style-type: none"> Discuss scenario against critical data 	

Maintaining and Exercising BC Plans				
Sub-Topic	#	What	How	Points of Reference
	4	Hold tabletop exercises to facilitate the understanding of policy, roles & responsibilities, response and recovery approach and priorities	<ul style="list-style-type: none"> Bring critical functions into a conference room to discuss response to a scenario 	
	5	Execute with individual business units (aka departments)	<ul style="list-style-type: none"> Develop a scenario for a single business unit 	
	6	Execute with several units together as a joint exercise	<ul style="list-style-type: none"> Develop a scenario for multiple business units 	

Maintaining and Exercising BC Plans				
Sub-Topic	#	What	How	Points of Reference
Exercising – Operation-based	1	Hold notification exercises to exercise the notification system to be used at time of emergency (ATOE) to ensure accuracy, length of time for notification & that appropriate personnel have access to plan ATOE	<ul style="list-style-type: none"> Exercise the documented notification process 	
	2	Hold relocation exercises	<ul style="list-style-type: none"> Move critical functions to planned recovery location to validate location is acceptable 	

Maintaining and Exercising BC Plans

Sub-Topic	#	What	How	Points of Reference
	2a	Functional	<ul style="list-style-type: none"> Technology: O/S restore: restore systems or applications without interfaces. Business: Single business units or particular processes (functions). 	
	2b	Integrated	<ul style="list-style-type: none"> Technology: O/S, Applications & Network: Multiple systems and interfaces between them. Business: Multiple units from same location testing all or most processes in highest risk tier. 	
	2c	Comprehensive	<ul style="list-style-type: none"> Technology: All systems & components of the production site. Business: All units from same site validating capabilities for all functions for a given risk tier. 	

DRII/BCI Professional Practice Narrative:

- Prepare a program to create and maintain corporate awareness and enhance the skills required to develop and implement the Business Continuity Management program or process and its supporting activities.

Generally Accepted Practices (GAP) Notice:

- This document is to serve as a repository of knowledge which is to be applied across various verticals
- This document contains a conceptual basis for Program development vs. an auditable checklist

Awareness and Training Programs				
Sub-Topic	#	What	How	Points of Reference
Training and Awareness	1	Establish objectives and components of Corporate BCM Awareness and Training Program	<ul style="list-style-type: none"> • Inform management of current state of recovery preparedness and associated risks • Obtain upper management support to develop awareness and training programs • Develop a partnership with Internal Audit • Write a Training and Awareness Policy • Promote employee and management awareness regarding recovery preparedness • Ensure employees are familiar with their Business Continuity Roles and Responsibilities • Define desired outcomes from Awareness and Training program • Ensure relevant employees, customers, suppliers and other stakeholders are aware of the business continuity initiatives • Establish and use metrics to identify key areas of focus, and measure progress in improving quality, reliability, and security 	HB 221:2004, Standards Australia/Standards New Zealand, Business Continuity Management. ASIS Guidelines Network Reliability Interoperability Council (NRIC) Standard

Awareness and Training Programs

Sub-Topic	#	What	How	Points of Reference
	2	Identify Functional Awareness and Training requirements	<ul style="list-style-type: none"> • Determine the level of awareness through planned drills or simulated exercises • Determine the drivers causing the need for Training and Awareness (e.g. Customer, Business or Regulatory) • Complete needs analysis to determine requirements of Awareness and Training program • Benchmark against other corporations within Peer Group or Industry • Periodically survey employees to determine their level of awareness • Apply lessons learned from actual disasters 	Network Reliability Interoperability Council (NRIC) Standard
	3	Develop Awareness and Training Methodology	<ul style="list-style-type: none"> • Determine who target audience is • Determine if Training Materials will be the same for all audiences • Determine if Training is Mandatory or Volunteer • Tie Awareness and Training involvement to Annual Performance Review and Compensation 	HB 221:2004, Standards Australia/Standards New Zealand, Business Continuity Management.
	4	Acquire or develop Awareness and Training Tools	<ul style="list-style-type: none"> • Develop Training Tools internally, using the "Needs Assessment" as a foundation • Information share with peers within your industry sector, to identify commonly used training practices 	

Awareness and Training Programs

Sub-Topic	#	What	How	Points of Reference
	5	Identify external Awareness and Training Opportunities	<ul style="list-style-type: none"> • Attend regular meetings of organizations that include business continuity in the scope of their activities (i.e. ASIS, BOMA, RIMS, ISSA, ISACA) • Complete FEMA Independent Study courses • Attend training opportunities offered by State, County or local emergency management office • Attend CERT Training and promote employees to attend 	
	6	Identify alternative options for Corporate Awareness and Training	<ul style="list-style-type: none"> • Lessons learned from previous tests and actual incidents should be built into the testing cycle • Keep apprised of industry trends for BC Training Programs 	
	7	Develop and Deliver various types of Training Programs (i.e. Computer based, classroom, test-based and instructional guides and templates	<ul style="list-style-type: none"> • Use a combination of walk through, live and simulation training methods • Consider consolidating Disaster Recovery Training and Awareness with Corporate Information Security Training • Consider creating a video to demonstrate evacuation drills • Consider using contests to generate interest 	

Awareness and Training Programs

Sub-Topic	#	What	How	Points of Reference
	8	Develop Awareness Programs (i.e. Management, Team Members, New Employee Orientation and current employee refresher program)	<ul style="list-style-type: none"> • Identify key stakeholders to include in Training and Awareness program • Distribute key contact information to new employees on wallet cards (ie. Hotline number for status during outage) • Require annual training for all employees • Schedule Awareness training to coincide with National Business Continuity week • Provide management with monthly status updates on all training and awareness activities 	
	9	Identify Other Opportunities for Education	<ul style="list-style-type: none"> • Attend conferences/meetings of the following: <ul style="list-style-type: none"> ➤ Business Continuity Organizations ➤ Local Business Continuity groups ➤ Certification entities ➤ Industry specific forums • Enroll in Business Continuity/Disaster Recovery college courses • Attend Business Continuity/Crisis Management drills at the state or local level • Read Business Continuity periodicals • Refer to Business Continuity web-sites 	Refer to Appendix listing all Business Continuity groups in the US

DRII/BCI Professional Practice:

- Design, develop, and implement Business Continuity and Crisis Management plans that provide continuity within the recovery time objective and recovery point objective.

Generally Accepted Practices (GAP) Notice:

- This document is to serve as a repository of knowledge which is to be applied across various verticals
- This document contains a conceptual basis for Program development vs. an auditable checklist

Developing and Implementing BC Plans				
Sub Topic	#	What	How	Points of Reference

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
Pre-Planning Activities for Developing a Plan	1	Ensure that an executive sponsor is assigned as oversight and authority for the plan development and implementation process. If this was accomplished as part of the Initiate Project phase, this will be a validation step.	<ul style="list-style-type: none"> • Identify the highest level management for the process, business function, or technology that is being targeted for the planning effort and request that level of management's support either directly or by appointed designee. (Preferred sponsor is executive level management, e.g. CFO, CIO, market Presidents/Executives) • Meet with designated executive sponsor. Review the planning process, the expected deliverables, resource requirements, and communication flow for status reporting and review of issues as the plan development effort proceeds. • If the organization does not have a reporting format established, develop one that management agrees will meet its need for information on status, planned activities, risks, constraints and potential problems. • If sponsor has not reviewed the project plan details for plan creation, review the approach to be taken for the plan development phase and when specific scope, schedule and cost information will be provided. 	<ul style="list-style-type: none"> • <u>NFPA 1600:2004. Standard on Disaster/Emergency Management and Business Continuity Programs.</u> Chapter 4, Program Management. • <u>PAS 56:2003. Guide to Business Continuity Management.</u> Introduction and Figure 2: BCM Relationships. • <u>HB 221:2004. Standards Australia/Standards New Zealand, Business Continuity Management.</u> Introduction and Chapter 2.1-Developing the BCM Program, Step 1: Commencement. • <u>Practitioners Guide to Business Continuity Management.</u> Chapter 2, Commencement of BCM; and Section 2.05, Gaining the Commitment of Others.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	2	Ensure that a business continuity policy is defined.	<ul style="list-style-type: none"> Ideally, there should be a policy for the organization as a whole but if one does not exist, then request the executive sponsor to issue a general policy statement for the process and functional areas being covered by this planning effort. (THE Policy should be an enterprise Policy with attached executive directive and the next level organizations clarifying implementation and directive as required.) 	<ul style="list-style-type: none"> <u>NFPA 1600:2004. Standard on Disaster/Emergency Management and Business Continuity Programs.</u> Chapter 4 (Program Management). <u>PAS 56:2003. Guide to Business Continuity Management.</u> Section 5.2 (Policy) <u>HB 221:2004. Standards Australia/Standards New Zealand. Business Continuity Management.</u> Introduction and Chapter 2.1 (Developing the BCM Program, Step 1: Commencement) <u>Practitioners Guide to Business Continuity Management.</u> Chapter 2 (Commencement of BCM) <u>Federal Executive Branch Continuity of Operations (COOP).</u> FPC-65, June 15, 2005

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	3	Define, clarify, and develop sponsor communication.	<ul style="list-style-type: none"> • Request approval of strategy from executive sponsor and senior leadership team(s). • Seek advice on content from process or functional leaders for each organizational tier that is in scope and establish appropriate QA reviews/approvals for planning effort and content. • Communication should include BCP implementation stages and status for clarification and support potential assurance. • Communication/report requirements should identify and track function by who's responsible, who's accountable, who's consulted and who's informed. • Communication/report requirements can be mapped out using a RACI table identifying function (responsible / accountable / consulted / informed) per #5 below. 	<ul style="list-style-type: none"> • <u>Practitioners Guide to Business Continuity Management</u>. Section 2.05, Gaining the Commitment of Others; and Section 2.12, The Establishment Checklist.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	4	Develop, present, and obtain approval for preliminary planning assumptions and exclusions.	<ul style="list-style-type: none"> • Prepare a formal scope statement that outlines the assumptions and constraints for the BCP. • Obtain assumptions and exclusions from executive management and verify with Plan development interviewees • Review any additional assumptions and exclusions obtained from interviewees with executive management prior to inclusion, • The planning effort should address all plans required to ensure overall integrated continuity/disaster recovery. • Present scope statement for formal signoff. 	<ul style="list-style-type: none"> • <u>HB 221:2004, Standards Australia/Standards New Zealand, Business Continuity Management.</u> Introduction, and Chapter 2.1- Developing the BCM Program, Step 1: Commencement. • <u>Practitioners Guide to Business Continuity Management.</u> Chapter 2, Commencement of BCM; and Section 2.06, Establishing the Infrastructure of BCM.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	5	Review the organizational structure and document the management hierarchy that will be in scope of the planning effort.	<ul style="list-style-type: none"> • Identify functional leaders • Identify process owners • Verify organizational/structural analysis with executive sponsor and/or senior leadership team(s) 	<ul style="list-style-type: none"> • <u>PAS 56:2003. Guide to Business Continuity Management.</u> Annex A, RACI Participants in the BCM Cycle. • <u>Practitioners Guide to Business Continuity Management.</u> Chapter 8, Section 8.04, Table 15a, The IRACI Tool.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	6	Ensure that contact information, availability to the project, and supervisory approval have been obtained for those who will be involved in BC Plan development.	<ul style="list-style-type: none"> • The professional practitioner should be sufficiently familiar with the organization to build a preliminary list of contacts for the team that is needed to support the plan development process. • The team members may be process leaders or functional area managers. (Clients and/or suppliers of functional areas should be interviewed as required.) • Review/confirm team members with executive sponsor and/or senior leadership team(s) to ensure that those resources will be authorized and responsive to work on the planning effort. 	<ul style="list-style-type: none"> • <u>Practitioners Guide to Business Continuity Management</u>, Chapter 2, Section 2.09, Resource Allocation.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	7	Define project scope, schedule and reporting points and obtain management approval.	<ul style="list-style-type: none"> • Refer to assumptions and exclusions above. • Develop a succinct Power Point project outline presentation for management to review, discuss and approve. • Ensure that all supporting components of critical processes are included in the Plan, including but not limited to IT, business processes, workplace, staff, suppliers, etc. 	<ul style="list-style-type: none"> • <u>HB 221:2004, Standards Australia/Standards New Zealand, Business Continuity Management, Template 11, The BCM Checklist.</u>

Developing and Implementing BC Plans

Developing and Implementing BC Plans				
Sub Topic	#	What	How	Points of Reference

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
Gathering Data To Use for Further Analysis and Consolidation	1	Complete a risk assessment for the processes and/or areas to be included in the Plan.	<ul style="list-style-type: none"> • Identify and define all potential risks to the process/functions to include regulatory, legal, operational, technological, financial, informational and physical security. Geographic characteristics may also need to be factored in. • Define applicable treats to the enterprise: these could include such factors as areas subject to hurricanes, tornados, floods, wild fires, civil unrest, acts of terrorism, mass transportation breakdowns, utility failures, and so forth. • Assess the probability of the threat occurring • Assess the impact from the threat occurring • Quantify/qualify the treat into a risk matrix. • Identify potential mitigations to reduce, eliminate or transfer the risk. 	<ul style="list-style-type: none"> • <u>NFPA 1600:2004. Standard on Disaster/Emergency Management and Business Continuity Programs.</u> Chapter 5, Program Elements, Risk Assessment. • <u>PAS 56:2003. Guide to Business Continuity Management.</u> Section 6.3, Risk Assessment. • <u>HB 221:2004. Standards Australia/Standards New Zealand, Business Continuity Management.</u> Chapter 2.1-Developing the BCM Program, Step 2 Risk and Vulnerability Analysis. • <u>Practitioners Guide to Business Continuity Management.</u> Chapter 3, Section 3.05, Identifying Risks; Section 3.13, The Risk Assessment Checklist; and Appendix B, Sources of Risk.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	2	Utilize the completed Business Impact Analysis (BIA) to confirm all critical business processes and/or systems, Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), dependencies (vendors, internal/external suppliers) and financial impact for prolonged outages.	<ul style="list-style-type: none"> • Review/confirm with the executive sponsor and/or senior leadership team(s) as a part of the Plan development scope. • Ensure all input is documented for use later on in writing the plan and ensure any new or modified information is included with the BIA documentation. • Outline planning assumptions to give to the process owners on the scope and parameters of the planning effort. 	<ul style="list-style-type: none"> • <u>PAS 56:2003. Guide to Business Continuity Management.</u> Section 6.2, Business Impact Analysis. • <u>HB 221:2004. Standards Australia/Standards New Zealand. Business Continuity Management.</u> Chapter 2.1-Developing the BCM Program, Step 3 Business Impact Analysis. • <u>Practitioners Guide to Business Continuity Management.</u> Chapter 4, Section 4.02, Confirming Critical Business Functions; 4.06, Identify Maximum Acceptable Outage Times and Recovery Objectives; and Template 4.3, Determining the Minimum Acceptable Outage Time.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	3	Validate and/or clarify statements from senior management about the mission, vision, and goals of the process/functions being covered by the planning effort.	<ul style="list-style-type: none"> • Document mission, vision, and goals of the organization's process and functions as determined by validation process. • Confirm with business unit or process owners, or their senior managers. 	
	4	Identify mission critical processes and any other processes that support the mission critical ones and may have potential impacts on them.	<ul style="list-style-type: none"> • Write executive summary covering the mission critical processes and their dependencies on other processes, internal or external. • Review/confirm with management. • Document process flow for use in Plan validation recommendations. 	
	5	Gather additional information from management about recovery goals, preliminary Recovery Time Objectives (RTO's) and Recovery Point Objectives (RPO's) to ensure that the scope and size of the plan development effort will meet the organization's information requirements.	<ul style="list-style-type: none"> • Review/confirm RTO's and RPO's with management. • Review/confirm recovery strategies are aligned with the RTO's and RPO's, and if not, clarify and confirm the risk level exposure management is willing to take. 	<ul style="list-style-type: none"> • <u>Practitioners Guide to Business Continuity Management</u>. Chapter 4, Section 4.01, Developing Communications for the BIA and Table 5, Communication and the BIA.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	6	Establish requirements for resources and organizational commitment to complete the plan development and implementation effort.	<ul style="list-style-type: none"> • Resources will be needed to review and evaluate all data gathered prior to initiating the plan documentation process. • Resources will be needed to complete and verify the plan components. • Resources will be needed to review the finished plan. • Resources will be needed to implement the finished plan. • Resources will be needed to exercise the plan as part of implementation. • Resources will be needed to maintain the plan. 	<ul style="list-style-type: none"> • <u>HB 221:2004, Standards Australia/Standards New Zealand, Business Continuity Management</u>. Chapter 2.1-Developing the BCM Program, Step 5 Developing Resource and Interdependency Requirements; Template 5, Minimum Resource Requirements Worksheet. • <u>Practitioners Guide to Business Continuity Management</u>. Chapter 4, Section 4.03, Identify Resource Requirements; Template 4.7, Determining IT Application Dependencies.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	7	Make sure that all impacts have been analyzed and recorded if not captured by the BIA.	<ul style="list-style-type: none"> • Financial impacts • Operational impacts • Legal impacts • Regulatory impacts • Customer impacts • Regulatory compliance impacts 	<ul style="list-style-type: none"> • <u>HB 221:2004, Standards Australia/Standards New Zealand, Business Continuity Management</u>. Chapter 2.1-Developing the BCM Program, Table 1, Examples of Disruption Impacts on the Organization. • <u>Practitioners Guide to Business Continuity Management</u>. Chapter 3, Section 3.06, Analyzing Risk.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	8	Identify and itemize vital records critical to the organization to include any critical tools or processes used in the retention process.	<ul style="list-style-type: none"> • Identify policy for vital records. If policy does not exist, work with executive sponsor to develop one. • Identify Vital Records throughout the organization • Understand retention periods for vital records including electronic and paper. • Review/confirm appropriate backup and/or storage for vital records. • Review/confirm system and data back up strategies will meet the RPO from the BIA requirements for each critical system identified. • Review vital records list to ensure that all records needed for mission critical processes are covered in the back up and retention adequately to meet the RPO. • Compliance with record keeping standards needs to be maintained at time of business interruption or disaster. • Review/confirm list with management. • Keep list to use later 	<ul style="list-style-type: none"> • <u>ANSI/ARMA 5-2003, Vital Records: Identifying, Managing, and Recovering Business-Critical Records.</u>

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	9	Identify and itemize vendors critical to the organization's mission, core business processes and/or functions as validated in Step 3 above.	<ul style="list-style-type: none"> • Review/confirm list with management to include name, location, contact information and alternates to each. • Keep list to use later 	
	10	Identify key customers for whom notification will be required at time of disaster or for whom a business work-around will be essential. Include required escalation procedures and parameters.	<ul style="list-style-type: none"> • Review/confirm list of key customers with management. • Document your key customer interfaces. • Keep list to use later. 	

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
Complete Data Analysis and Consolidation for Use in Plan Content	1	Confirm that overall recovery time objectives are achievable with recovery performance capabilities.	<ul style="list-style-type: none"> • Ensure total RTO meets Plan and customer objectives. • Validate information received with exercise times. • Ensure that up and downstream processes and components align with provided RTO's 	<ul style="list-style-type: none"> • <u>PAS 56:2003. Guide to Business Continuity Management.</u> Section 6.2, Business Impact Analysis. . • <u>HB 221:2004, Standards Australia/Standards New Zealand, Business Continuity Management.</u> Chapter 2.1-Developing the BCM Program, Step 3 Business Impact Analysis • <u>Practitioners Guide to Business Continuity Management.</u> Chapter 4, Section 4.02, Confirming Critical Business Functions; 4.06, Identify Maximum Acceptable Outage Times and Recovery Objectives; and Template 4.3, Determining the Minimum Acceptable Outage Time.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	2	Confirm that overall recovery point objectives are achievable with recovery performance capabilities.	<ul style="list-style-type: none">• Ensure total RPO meets Plan and customer objectives.• Validate information received with exercise times.• Ensure that up and downstream processes and components align with provided RPO's	

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	3	Finalize personnel and resource requirements to develop and implement the plan.	<ul style="list-style-type: none"> • Develop contact list for plan development/implementation team(s). • Develop action plan such as a project plan or a Team Action Record to track and monitor status of the plan development and implementation activities, target dates, responsibility, issues, progress, and comments. 	<ul style="list-style-type: none"> • <u>HB 221:2004, Standards Australia/Standards New Zealand, Business Continuity Management</u>. Chapter 2.1-Developing the BCM Program, Step 5 Developing Resource and Interdependency Requirements; Chapter 2.2-The BCM Workbook, Template 5, Minimum Resource Requirements Worksheet. • <u>Practitioners Guide to Business Continuity Management</u>. Chapter 4, Section 4.03, Identify Resource Requirements; Chapter 6, Assessing and Collating Resource Requirements; and Appendix D, Example of Consolidated Resource Mapping.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	4	Review, clarify and understand the recovery alternatives available for each critical business function as well as cost analysis.	<p>Review/confirm selected recovery solutions such as:</p> <ul style="list-style-type: none"> • Alternative site or business facility • Warm site • Cold Site • Drop Ship/Quick ship agreements • Hot-Site Third party service providers • Manual Procedures • Mitigation • Mobile Trailer • Reciprocal agreements • Warm Site • Work from Home (telecommuting) <p>Note: See Strategies Best Practices</p>	<ul style="list-style-type: none"> • <u>PAS 56:2003. Guide to Business Continuity Management. Section 7, BCM Strategies.</u> • <u>HB 221:2004. Standards Australia/Standards New Zealand. Business Continuity Management. (Chapter 2.2-The BCM Workbook, Template 3, Strategy Development Worksheet.</u> • <u>Practitioners Guide to Business Continuity Management. Chapter 4, Template 4.6, Determining Alternate Workarounds.</u>

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	5	Consider various approaches to developing the BCP documentation and effort.	<ul style="list-style-type: none"> • Vertical integrated planning is based upon hierarchical or functional tiers with each tier mapped to the tier above and below it. • Tiers may also require to be horizontally integrated as co-processes or interdependencies. • Tiers should incorporate references to other plans relevant to the plan you are working on, such as IT, third party service providers, work area, network, etc. • Consider the operational and response issues for Plan implementation. • Include confidentiality and Plan distribution considerations in the Plan format. 	<ul style="list-style-type: none"> • <u>Practitioners Guide to Business Continuity Management</u>. Chapter 7, The Framework of Plans.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	6	Make sure a business case analysis for the recovery plan strategy has been completed and documented.	<ul style="list-style-type: none"> • This is part of the Strategies phase but should be verified as part of the Plan development and validation phases. The final strategy of mitigation or recovery should have this analysis as input and used in the strategy decision. • Make sure that the proposed solution costs are consistent with the risk adjusted loss from an event. (See Risk Assessment section above) 	
	7	Review/confirm recovery site selection and build-out requirements.	<ul style="list-style-type: none"> • Use this information to document the component recovery phase processes. Also impacts RTO. • It is possible that this particular step may require a sub-team to gather and document detailed specifications. 	

Developing and Implementing BC Plans				
Sub Topic	#	What	How	Points of Reference
	8	Define key parameters that the Plan MUST address.	<p>Key parameter may include but not limited to:</p> <ul style="list-style-type: none"> • Legal & regulatory • Contractual & Agreements • Compliance • Plan format • Plans should draw distinction between recovering workplace and personnel vs. technology • Workplace • Staffing • Recovery Procedures • Disaster analysis, definition, notification and escalation procedures. 	<ul style="list-style-type: none"> • NFPA 1600:2004. Standard on Disaster/Emergency Management and Business Continuity Programs. Section 5.7.2, Plans. • PAS 56:2003. Guide to Business Continuity Management. Section 8, Developing and Implementing BCM Plans. • HB 221:2004. Standards Australia/Standards New Zealand. Business Continuity Management. Chapter 2.2-The BCM Workbook, Template 6, Continuity Plan Worksheet. • Practitioners Guide to Business Continuity Management. Chapter 7, Section 7.03, Contents of a BCP; and Table 17, Assurance Issues and Evidence.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
Plan Documentation Components And Applying Finalized Data to Plan Content	1	Overview and Scope	<ul style="list-style-type: none"> • Include confidentiality statement and associated authority • Plans MUST honor all required "Confidentiality" • Plans should define activities for each phase of the Recovery (response, decision process, post event & pre-recovery, DR production and "back to normal") 	
	2	Assumptions	<ul style="list-style-type: none"> • Document the assumptions that went into the planning effort. • These items should clarify and define any issues related to, but not limited to, RTO, RPO, notification and recovery or mitigation 'environment', limitations or support expected. • Include any references that support the Plan implementation such as vendor BCP parameters, etc. • Identify any impact they may have on the Plan implementation. • Documentation should be understandable and actionable for 	<ul style="list-style-type: none"> • If a subscription recovery facility is used, the assumption is that the facility will be available in the event of an event requiring relocation of services.

Developing and Implementing BC Plans				
Sub Topic	#	What	How	Points of Reference
			individuals with expertise in a particular area in the event that key personnel are not available.	
	3	Exclusions	<ul style="list-style-type: none"> Clearly outline what the plan is not intended to cover. Specifically identify, with explanation of exclusion, what is excluded or supporting processes or resources not included. Identify any potential impact they may have. 	
	4	Compliance Statements	<ul style="list-style-type: none"> Document Plan components that address specific key legal and/or regulatory issues. This aids audit, reporting and compliance requirements. 	<ul style="list-style-type: none"> <u>PAS 56:2003. Guide to Business Continuity Management. Section 10.3. Audit.</u> <u>Practitioners Guide to Business Continuity Management. Chapter 9, Maintenance of a BCM, Table 17, Assurance Issues and Evidence.</u>

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	5	Teams	Document the following team information: <ul style="list-style-type: none"> • Key contacts • Reporting structure • Roles & responsibilities • Contact information including but not limited to name, address (with zip code) phones numbers, emergency contacts and alternates. • For clarity, team names should match up and downstream Plan parameters. 	
	6	Declaration & Escalation process	<ul style="list-style-type: none"> • Document the disaster identification and declaration process including but not limited to Declaration authorities and the initial Notification Procedure and/or checklist 	
	7	Supporting resources	<ul style="list-style-type: none"> • These will normally be call back lists showing personnel and contact 	

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
			information. <ul style="list-style-type: none"> • Document the up and downstream resources for each process to ensure requirements are met • Document the interface requirements for each supporting resource • Identify critical metrics (physical, timing, etc.) for each resource • Reference detailed documentation as required to minimize Plan size, especially resources with frequent changes or time constrained. Use known terminology and add a glossary as necessary • Identify each external supporting resource 	
	8	Controls	<ul style="list-style-type: none"> • Document each Plan component requiring a control point, give a brief explanation of the objective and purpose of the control, the metrics and team responsible for the control • Identify the control authority (policy, regulatory, compliance, etc., and person) as appropriate 	

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
			<ul style="list-style-type: none"> • Identify incident management (reporting, audit, budget, etc.) and tracking (inventory control, reporting, etc) controls and the associated authority and policy or regulation. 	
	9	Recovery flow	<ul style="list-style-type: none"> • If the sequencing of events can be displayed graphically, it can help to understand when different part of the plan is executed and also when resources are needed. • Develop the Plan structure to support the Process Operational and Recovery flow • Document the Plan for each sub-component and functional area to allow appropriate distribution and support required Confidentiality. • Identify up and downstream requirements and dependencies • Document any component assumptions • Use graphics as appropriate for 	

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
			clarification and for inclusion in the Plan validation process <ul style="list-style-type: none">• Identify each external supporting resource (to include supply chain).	

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	10	Plan Overviews	<p>Provide an overview of each sub-component of the overall Plan, including but not limited to:</p> <ul style="list-style-type: none"> • Command and Control • Communication plan (internal and external) • Media Interface plan (pre-scripted and approved messages) • Technology & tools plan • Workplace plan • Staffing plan • Operational procedures plan for each phase of the recovery, such as interim work-arounds • Supply chain plan dependencies and work-arounds 	<ul style="list-style-type: none"> • <u>NFPA 1600:2004. Standard on Disaster/Emergency Management and Business Continuity Programs.</u> Section 5.7.2, Plans. • <u>PAS 56:2003. Guide to Business Continuity Management.</u> Section 8, Developing and Implementing BCM Plans; and Annex B.5, Developing and Implementing BCM Plans. • <u>HB 221:2004, Standards Australia/Standards New Zealand, Business Continuity Management.</u> Chapter 2.2-The BCM Workbook, Step 6: Developing Continuity Plans; Template 6, Continuity Plan Worksheet; and Template 9: Minimum Standard for Content of BCM Plan. . • <u>Practitioners Guide to Business Continuity Management.</u> Chapter 7, Section 7.03, Contents of a BCP; and Table 17, Assurance Issues and Evidence.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
	11	Appendices	<ul style="list-style-type: none"> • Validation schedule • Key internal contacts detailed information • Vendor & suppliers detailed information • Off-site resource information (vital records, hot-site, workplace relocation, etc.) • Graphics (maps, floor & site layouts, photos, organization charts, process and recovery flow, etc) • Inventories • Sub-plan details as applicable • Reporting requirements • Event tracking requirements • Compliance requirements and references 	

Developing and Implementing BC Plans				
Sub Topic	#	What	How	Points of Reference
Follow-up Activities	1	Plan status report	<ul style="list-style-type: none"> Document a summary of the current state of the Business Continuity Program including processes included, excluded, and any open items (or planning gaps). Emphasis should be given to potential issues and the results expected with Plans as developed. 	
	2	Plan recommendations report to include but not limited to: <ul style="list-style-type: none"> Confidentiality Plan Maintenance & distribution Validation process Audit process Training requirements Awareness program Command and control 	<ul style="list-style-type: none"> This report should be guidelines for each of the aforementioned items and/or issues. Validate issues with appropriate teams and review with and obtain approval from the executive sponsor for this plan development effort. 	<ul style="list-style-type: none"> NFPA 1600:2004. Standard on Disaster/Emergency Management and Business Continuity Programs. Chapter 13, Exercises, Evaluations and Corrective Actions. PAS 56:2003. Guide to Business Continuity Management. Annex b, Section 7 – Exercising, Maintenance and Audit.

Developing and Implementing BC Plans

Sub Topic	#	What	How	Points of Reference
				<ul style="list-style-type: none"> • <u>HB 221:2004, Standards Australia/Standards New Zealand, Business Continuity Management.</u> Section 2.1, Step 8, Training, Maintaining and Testing Plans; and Template 10: Training and Testing Development Worksheet. • <u>Practitioners Guide to Business Continuity Management.</u> Chapter 9, Maintenance of BCM; Section 9.02, Performance and 9.05, The Maintenance Checklist.

Developing and Implementing BC Plans				
Sub Topic	#	What	How	Points of Reference
	3	Post-Incident Documentation	<ul style="list-style-type: none"> • Once teams have been deactivated, debrief Emergency Response, Crisis Management and Business Recovery teams. • Identify and prioritize key learnings. • Gather cost accounting detail. • Gather visual records of event, e.g. digital or hardcopy photos, newspaper reports, internal and external communications. 	

VII. Appendix

NFPA 1600:2004 Standard on Disaster/Emergency Management and Business Continuity Programs (Price: No Charge)

PAS 56:2003 Guide to Business Continuity Management (Price: £60 (approx \$114))

HB 221:2004 Standards Australia/Standards New Zealand Business Continuity Management (Price: Australian \$41.18 (approx \$32.00))

Practitioners Guide to Business Continuity Management (to be published by Standards Australia)

Federal Preparedness Circular 65: Federal Executive Continuity of Operations (COOP). June 15, 2005. (Price: No charge)

DRII/BCI Professional Practice:

- Develop and implement procedures for response and stabilizing the situation following an incident or event, including establishing and managing an Emergency Operations Center to be used as a command center during the emergency.

Generally Accepted Practices (GAP) Notice:

- This document is to serve as a repository of knowledge which is to be applied across various verticals
- This document contains a conceptual basis for Program development vs. an auditable checklist

Emergency Response and Operations				
Sub-Topic	#	What	How	Points of Reference
Corporate Sponsorship <i>(Management Commitment)</i>	1	Identify stakeholders / decision makers.	<ul style="list-style-type: none"> • Brainstorm with management team. 	SUBJECT 1: Project Initiation and Management
	2	Acquire a Senior Management Sponsor to support the program and is willing to periodically attend meetings and support related recommendations.	<ul style="list-style-type: none"> • Schedule a meeting with the CxO to 'sell' the business continuity management program concept and obtain commitment • Management Team to identify the critical areas to approach. 	Corporate Organization Chart
	3	Identify risks (natural, man-made, human, environmental, political, neighboring industries, etc.) as well as the likelihood of risk so the plan addresses the appropriate level.	<ul style="list-style-type: none"> • Conduct a formal threat assessment for the facility. • Work with local Emergency Management Agencies to identify risks. • Research the Internet for historical data. • Evaluate the risks identified in Subject Area 2 for your respective region. 	<ul style="list-style-type: none"> - SUBJECT 2: Risk Evaluation and Control - SUBJECT 3: Business Impact Analysis - Search Internet for business related white papers
	4	Identify preventative measures that can minimize the potential disaster from occurring.	<ul style="list-style-type: none"> • Review the threats and categorize by priority • Obtain approval from management / sponsors regarding the level of acceptable risk. • Indicate the various mitigation strategies for each threat. 	<ul style="list-style-type: none"> - SUBJECT 2: Risk Evaluation and Control - SUBJECT 3: Business Impact Analysis

Emergency Response and Operations				
Sub-Topic	#	What	How	Points of Reference
	5	Develop Emergency Response planning phases.	<ul style="list-style-type: none"> Involve internal partners such as Security Facilities, Life Safety, Risk Management, HR, Communications (internal and external), Legal, Finance/Accounting, Travel, Transportation or others. Also consider key external partners 	<ul style="list-style-type: none"> Corporate policies and procedures SUBJECT 9: Public Relations and Crisis Communications SUBJECT 10: Coordination with Public Authorities
	6	Develop the strategy: <ul style="list-style-type: none"> Present for approval cost benefits including the advantages / disadvantages of implementing an Emergency Response Program. Obtain formal approval for the program strategy as well as the budget 	<ul style="list-style-type: none"> Schedule a meeting with Senior Management / Sponsor to present the pros/cons, including financial information, related to implementing an Emergency Response Program. 	<ul style="list-style-type: none"> www.fema.gov/library/biz2.shtml SUBJECT 2: Risk Evaluation and Control SUBJECT 3: Business Impact Analysis SUBJECT 6: Developing Business Continuity Plans (follow same principals but with an emphasis on Emergency Response)
	7	Educate Senior Management on their Roles and Responsibilities.	<ul style="list-style-type: none"> Partner with Senior Management / Sponsor to document their roles and responsibilities. 	<ul style="list-style-type: none"> Provide Senior Management a review of the BC process as well as their roles and responsibilities SUBJECT 7: Training and Awareness

Emergency Response and Operations				
Sub-Topic	#	What	How	Points of Reference

Emergency Response and Operations

Sub-Topic	#	What	How	Points of Reference
Planning and Documenting – Emergency Response	1	Partner with the local municipalities to be included in all proposed modifications to the local emergency management process and to be notified of any federal notification received.	<ul style="list-style-type: none"> • Prior to an event, identify, notify and exchange contact data with the various municipal representatives • Conduct periodic meetings with the representatives. • Obtain management approval to conduct on-site tours so local reps can become familiar with office location. NOTE: Make prior request with officials to not 'write-up' any infractions if they are noted during the tour. 	<ul style="list-style-type: none"> - CERT (Community Emergency Response Team) - Public Health - EMA director, fire chief, mayor, etc. - SUBJECT 9: Crisis Communications - SUBJECT 10: Coordination with Public Authorities
	2	Partner with the local emergency management agencies to develop response plans for various scenarios initially targeting those identified in the Threat Assessment.	<ul style="list-style-type: none"> • Contact key representatives from the following areas • Schedule a meeting to discuss the top five, initially, identified risks. Discuss/confirm the company's response plans and how to mitigate the impact of such an event. • Present the findings to the management. • Participate in local emergency management agencies on-going meetings. • Participate in public-private forum, if available. 	<ul style="list-style-type: none"> - CERT - Police, Fire and Rescue, Health Department, Local Emergency Planning Committees, etc. - SUBJECT 2: Risk Evaluation and Control - SUBJECT 10: Coordination with Public Authorities

Emergency Response and Operations

Sub-Topic	#	What	How	Points of Reference
	3	<p>Develop an Emergency Response Team to include representation from areas such as Security, Real Estate, Business Continuity, Human Resources, Safety, Public Relations / Communications, Insurance, Internal Audit, Legal, and Business Representation.</p> <p>NOTE: This team's major objective would be to respond to the immediate emergency, making the appropriate decisions and directing supporting groups such as security personnel.</p>	<ul style="list-style-type: none"> ▪ Establish structure for Incident Management. ▪ Designate the leadership role to ensure single point of accountability for decisions. ▪ Develop roles and responsibilities. ▪ Develop tasks. ▪ Populate teams with primary, secondary, etc. designation. NOTE: Team members are to obtain management approval prior to acceptance of responsibilities. ▪ Develop escalation procedures. ▪ Develop communication flow. ▪ Develop tiered notification system, i.e., call trees, automated callouts. ▪ Designate representative(s) to participate on ICS (Incident Management System) Team. 	<ul style="list-style-type: none"> - SUBJECT 1: Project Initiation and Management - ICS / NIMS, NFPA1600 - Call trees, automated callouts
	4	Maintain team	<ul style="list-style-type: none"> ○ Conduct regular scheduled meetings ○ Update team roster ○ Conduct drills ○ Conduct educational / training session 	SUBJECT 7: Training and Awareness
		Document the process for activation and the triggers that would result in activation or alert.	<p>Develop a procedure that outlines the triggers that would result in an action or alert.</p> <ul style="list-style-type: none"> - Establish phone trees - Implement automated notification systems - Maintain contact information - Establish notification timeframes - Develop notification matrix of contact methods during and after business hours. 	
	5	Partner with the Security and Facilities Departments to ensure efficient and coordinated emergency response and communications throughout the response phase.	Develop a procedure that outlines the roles and responsibilities of staff and management during an event.	SUBJECT 1: Project Initiation and Management

Emergency Response and Operations

Sub-Topic	#	What	How	Points of Reference
	6	Establish a Command Center	Determine location(s), resources and procedures for physical and/or virtual Command Centers. - Alert point person for Command Center site(s) that it is to be activated.	
	7	Establish procedures for evacuation (both internal and external) as well as for sheltering in place.	<ul style="list-style-type: none"> • Train the appropriate teams and employees in their roles. • Establish a procedure to verify employees are accounted for • Consider special evacuation needs and visitors. • Security to take sign-in sheet to assembly point. • Ensure there are multiple assembly points (NOTE: It is not advisable to visibly mark assembly points external to the building) • Partner with neighboring businesses 	<ul style="list-style-type: none"> - SUBJECT 2: Risk Evaluation and Control - SUBJECT 7: Training and Awareness - Partner with internal and external authorities to ensure compliance with local codes and ordinances
	8	Consider additional safety training opportunities in such areas as fire extinguisher training, CPR/First Aid/AED training, etc.	<ul style="list-style-type: none"> • Ensure training provided is in alignment with your municipalities and legal requirements. • May need to consult with the Legal Department, HR (special needs employees), and Health & Safety. 	SUBJECT 7: Training and Awareness SUBJECT 10: Coordination with Public Authorities
	9	Identify and acquire emergency supplies for Emergency Response Team.	Issue the following to the ER Team: <ul style="list-style-type: none"> - Vests - Walkie-talkies - Clipboards, etc. - Periodically inventory and replace expired items 	www.fema.gov

Emergency Response and Operations				
Sub-Topic	#	What	How	Points of Reference
	10	Identify and acquire emergency supplies, food, and resources (hardware, software, etc.) for Command Center – everyday and disaster specific based upon the risks identified in Threat Assessment.	<ul style="list-style-type: none"> - Obtain supplies - Periodically inventory and replace expired items - Store at Command Center in accessible secured location 	American Red Cross Readiness Kit (www.arc.org)
	11	Develop and document methodology for communicating to employees during an incident. Include processes for when employees are at work as well as after hours.	<p>Consider implementing an automated notification system.</p> <ul style="list-style-type: none"> - Develop scripts based on Threat Assessment to be customized at time of event. - Establish hotline for employees. <ul style="list-style-type: none"> - One-way status line (without ability for caller to leave message); OR - Status Line with capability for caller to leave a message. <p>Update the status line on a periodic basis. Implement an awareness campaign. Document communication plan.</p>	<p>Contact Lists Automated notification system www.fema.gov [research re communication with employees]</p> <ul style="list-style-type: none"> - Publish hotline number on company intranet, and/or labels affixed to employee badges. - See Subject Area #7 – Training & Awareness

Emergency Response and Operations				
Sub-Topic	#	What	How	Points of Reference
Documenting an Emergency Response Plan	1	Establish Crisis Command Centers	Establish one or more, appropriate to your environment: primary, secondary, on-site, off-site, virtual, etc.	[Discussion Point for next meeting] Right now all of our examples are one word, would like to see references to Appendices that would include detailed examples, such as: types of command centers (live, virtual...), list of members of ER team and their respective roles. www.fema.gov
	2			

Emergency Response and Operations				
Sub-Topic	#	What	How	Points of Reference
	3			
	4			
	5			

Emergency Response and Operations				
Sub-Topic	#	What	How	Points of Reference
Exercising the Emergency Response Plan	1	Identify the appropriate exercise type to implement (i.e., Note: there could be hand-offs in place of an exercise.	[Be consistent w/verbiage – obtain types from DRII re types] – could be a hand-off	
	2	Conduct emergency response exercises utilizing realistic scenarios.		
	3	When developing a full-scale exercise, ensure to involve external participants (i.e. local officials, vendors, customers, etc.).		
	4	Increase the level of simulation over time (i.e., orientation, drills, tabletop, intra-departmental, etc.) and exercise various plans annually.		
	5	Ensure primaries and alternates are involved within the exercises.		
	6	Document key findings from the exercise.		
	7	Periodically distribute key findings report to business owners until resolutions are complete.		
	8	Incorporate any significant changes resulting from the exercise and update the plan accordingly.		

DRII/BCI Professional Practice Narrative:

- Determine and guide the selection of alternative business recovery operating strategies for recovery of business and information technologies within the recovery time objective, while maintaining the organization’s critical functions.

Generally Accepted Practices (GAP) Notice:

- This document is to serve as a repository of knowledge which is to be applied across various verticals
- This document contains a conceptual basis for Program development vs. an auditable checklist

Developing Business Continuity Strategies

	Item #	What	How	Points of Reference
Corporate Sponsorship (Obtaining Management Approval)	1	Develop or utilize an existing reporting process to ensure management is provided with frequent status reports throughout the strategy development process.	<ul style="list-style-type: none"> • Dialog with Management on reporting process within the organization and expectations. • Develop or utilize an existing reporting format that is meaningful to direct management including status, next period activities, risks, constraints and potential problems. 	Subject Area 1 – Project Initiation and Management.
	2	Senior management (particularly chief executive, financial and operational officers) should review the developed strategy(s) taking into consideration acceptable risk exposures.	<ul style="list-style-type: none"> • When selecting a strategy review the risk assessment(s) to ensure there are no conflicts. • Summarize risks and continuity timelines and present to Senior Management with project timelines for approval of strategies that are developed. 	Subject Area 2 – Risk and Evaluation Control Subject Area 3 – Business Impact Analysis Others – Vulnerability and Privacy Assessments.
	3	Obtain Senior Management approval for strategies.	<ul style="list-style-type: none"> • Request approval of strategy from direct manager. • Seek advice on content for next approval level. • Put together appropriate content change for next approval level. • Repeat until final approval is achieved at the Senior Management Level. 	

Developing Business Continuity Strategies

	Item #	What	How	Points of Reference
Pre-Planning	1	Review all critical business processes and/or systems, RTO, RPO, dependencies (vendors, internal/external suppliers) and financial impact for prolonged outages.	<ul style="list-style-type: none"> Utilize the information in the BIA ensuring that new critical processes and/or systems are identified. 	Subject Area 3 – Business Impact Analysis
	2	Continuity Planners and Business Managers need to understand potential impact of all relevant laws, industry regulations and government codes.	<ul style="list-style-type: none"> Determine responsibility for maintaining current knowledge of laws, regulations etc. within the various organizational functions within the company such as: Fire Safety, Risk Management, Legal (General Counsel), and Audit etc. Establish a structure for transference of information with the various organizational functions. 	www.disasterrecovery.com/drlegislation_chart.htm (partial list of legislative requirements)
	3	Continuity Planners and Business Managers *should be aware of the kinds of audits or other reporting requirements to which they might be subjected. * Depending upon liability “should” may be a “must”.	<ul style="list-style-type: none"> Determine who has responsibility for Audit and Information Technology/Security within the organization. Understand from these departments the types of audits that they/the organization is subject to. Build bridges with these departments to maintain currency of information. 	<ul style="list-style-type: none"> Internal Audit External Audit Regulatory Requirements (Ie; Basel, Sarbanes Oxley Act (SOX), Health Information Protection Act (HIPA), Health Insurance Portability and Accountability Act (HIPPA), etc.)
	4	Review Assumptions to ensure they align with new emerging threats.	<ul style="list-style-type: none"> Review “Worst Case Scenario” for which these strategies might apply. Ensure location, human resources issues; environmental risks, customer/supplier chains, etc. are taken into consideration when developing the strategy(s). 	<ul style="list-style-type: none"> Subject Area 1 – Project Initiation and Management. Subject Area 2 – Risk and Evaluation Control Subject Area 3 – Business Impact Analysis

Developing Business Continuity Strategies

	Item #	What	How	Points of Reference
Planning & Development	1	Identify and incorporate risk mitigation strategies from the output of Subject Area 2 Risk Evaluation and Control.	<ul style="list-style-type: none"> • Have a full understanding of Risk Acceptance identified in Subject Area 2 and how it may affect this strategy. 	<ul style="list-style-type: none"> • Subject Area 2 – Risk and Evaluation Control
	2	Ensure that a strategy exists for protecting vital records including electronic and paper	<ul style="list-style-type: none"> • Identify Vital Records throughout the organization • Understand retention periods for vital records including electronic and paper. • Define key aspects for backup and/or storage of vital records such as location, method and security. • Ensure that senior management accepts the program for vital records retention. • Develop system and data back up strategies that will meet the RPO from the BIA requirements for each critical system identified. 	<ul style="list-style-type: none"> • Subject Area 3 – Business Impact Analysis • Record Retention Requirements for your industry/state/country • Archive Requirements for your industry/state/country • Third Party Vendors
	3	Identify the internal and/or external continuity resources and solutions that meet the business requirements.	<ul style="list-style-type: none"> • Review internal resources (ie: Multiple locations with like business functions & technology) • Search out external business resources using processes such as RFI, Queries, Professional Organizations, etc. 	<ul style="list-style-type: none"> • Third Party Vendors

Developing Business Continuity Strategies

	Item #	What	How	Points of Reference
Planning & Development (Cont'd)	4	Identify and understand the spectrum of available recovery alternatives available for each critical business function.	Review the following types of recovery alternatives and be prepared to make recommendations: <ul style="list-style-type: none"> • Alternative site or business facility • Cold, Warm or Hot Sites • Drop Ship/Quick ship agreements • Manual Procedures • Mitigation • Mobile Trailer • Reciprocal agreements • Work from Home Note: List may not be all inclusive	<ul style="list-style-type: none"> • Appendix 4.4 - Planning & Development Recovery Alternative Definitions • Appendix 4.4 - Planning & Development Recovery Alternate Strategy Matrix
Planning & Development (Cont'd)	5	Assess the feasibility of available resources and solutions for the continuity/recovery of business processes.	<ul style="list-style-type: none"> • Develop a Business Statement/Request for Proposal (RFP) which includes: <ul style="list-style-type: none"> • Review of vendors that provide 	<ul style="list-style-type: none"> • Appendix 4.5 - Planning & Development – Hot Site RFP

Developing Business Continuity Strategies

	Item #	What	How	Points of Reference
			<p>critical goods & services to your business</p> <ul style="list-style-type: none"> • Priority clause • Guarantee of delivery clause • Redundancy capabilities • Alternate staff • Work-arounds • Surge capacities (ie: cross training of critical resources, stock-piling of critical supplies) • Minimum hardware requirements • Networking requirements (from alternate locations to home site) <ul style="list-style-type: none"> • Develop a cost benefit analysis and an implementation timeline for each strategy. • Compare the cost ranges along with the advantages and disadvantages to implement each strategy. • Present concise and specific recommendations to management. (The cost benefit analysis should be used to justify all recommendations) • Implement solution. 	

DRII/BCI Professional Practice Narrative:

- Identify the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts. Establish critical functions, their recovery priorities, and interdependencies so that recovery time objective(s) and recovery point objective(s) can be set.

Generally Accepted Practices (GAP) Notice:

- This document is to serve as a repository of knowledge which is to be applied across various verticals
- This document contains a conceptual basis for Program development vs. an auditable checklist

Business Impact Analysis				
	#	What	How	Points of Reference
I - Executive Sponsorship (Obtain Management Approval)	1-1	Gain executive management buy-in	<p>Dialog with management on communication process within the organization and expectations. Consider setting expectations with regulators, auditors (internal and external), executive management, "The Board of Directors", business unit managers, state government departments, a BCP steering committee.</p> <ul style="list-style-type: none"> • Make sure that the project scope statement sets forth the terms, timeframe for completion, guidelines for determining the types of questions to ask on the BIA and the value/benefit of the data collected. Ensure that all stakeholders, employees, regulators, auditors, managers, those funding the BIA, are in agreement over the ultimate value of the BIA questions, expectations are agreed upon and how results will be used to move forward in the process. • Ensure the success of the project initiative; detail a process that will involve stakeholders and document agreed upon expected results. Typically BIA results are used to validate funding of a recovery strategy and/or recovery solution(s). • Ask executive management at what level will the BIA process gain the most accurate data. • Determine specific, repeatable, testable, clear, and concise questions on the BIA that will yield expected results. • Be prepared to show the benefits and value of the BIA process upfront (beyond the BCP). Executive management will gain a more objective view of the threats and risks to operations. Based upon this knowledge, management can make an informed decision on the risk tolerance it will accept. • Oftentimes, there are hidden benefits in conducting a BIA initiative. Be prepared to identify and communicate these benefits to executive management. (Examples: some hidden benefits might include: Identifying outdated technologies, unrealistic spending, integration issues with other organizational groups, business process improvement, redundancy of effort, outsourcing issues) 	Depending on the complexity and size of the organization, you may want to consider combining the risk assessment and the business impact analysis.

Business Impact Analysis				
	#	What	How	Points of Reference
			<ul style="list-style-type: none"> • Develop appropriate executive management reporting avenues to report status, activities, risks, constraints and bottlenecks. • Conduct abbreviated executive level workshops. • You absolutely must have executive/senior management buy-in or you will have been set-up for failure in completing a successful BIA. 	
	1-2	Request executive level support be communicated for the BIA initiative	<ul style="list-style-type: none"> • Consider writing a sample memo for executive management explaining the BIA initiative and their support of it. Emphasize that the BIA is the cornerstone, the foundation that all recovery strategies will be based on and the importance to obtain the highest quality results (i.e. both accurate and timely) that gives a fair representation of the impacts to the organization at all levels. • Recommend to executive management both the audience and the appropriate level to distribute the BIA support memo. • Offer to attend staff meetings to explain the BIA initiative if appropriate. • Consider using the organization's intranet website and other communication vehicles in support of the BIA initiative. 	
II - Understand the Organization	2-1	Identify business processes / functions	<ul style="list-style-type: none"> • For each part of your organization, request updated organizational charts (if in existence), workflow diagrams, basically any documentation that may assist in understanding the organizational structure. • When determining how best to conduct the BIA interviews, stay as close to the organization of management currently in place (i.e. follow the organizational chart that accurately reflects the division of responsibilities). Determine if it makes good business sense to conduct BIAs through a geographical analysis depending on the types and number of buildings, at a departmental level, and/or at a process/function level. • The term process is often used synonymously with the word function. In general, a BIA is completed for each business process/function. Where processes/functions provide distinctly different products, services, or outputs, separate BIAs may be appropriate especially if operational and financial impacts of a loss will be significantly different for each process. (For example, a separate BIA should be completed for Revenue Billing, Remittance Processing, Telemarketing, etc.) • Consider the appropriateness of polling executive management for a list of time critical processes/functions to focus on if there is little time to complete a detailed BIA process. Determine what executive management wants covered if time is of the essence. • Poll executive management as to any known pitfalls or issues that may impede your progress to conduct and complete the BIA process. 	

Business Impact Analysis

	#	What	How	Points of Reference
III - BIA Tools	3-1	Design a custom tailored business impact analysis questionnaire	<ul style="list-style-type: none"> • Spend time upfront to customize the BIA for the organization. Design a questionnaire that is written specifically for the organization keeping in mind its business language and culture. Update a prior BIA for the organization based on previous learnings. • The BIA is not an exercise in “Yes” and “No” answers; the purpose is to draw information from the source that is useful to the BIAs stated objectives. • Consider the purpose for requesting information on the BIA questionnaire and then re-consider possible related subsequent follow-up questions. Avoid continually going back and asking for data from BIA participants. • Identify the impact categories that are important and peculiar to your specific organization. Assess your current industry setting when custom tailoring your BIA questionnaire. • Consistently use the same timeframes to measure impacts over time for both financial and operational impacts. By using the same time measurements, it allows BIA results to be consistently compared across the organization. • Be consistent with the scale used to measure impacts to the organization. • It is important to capture both the quantitative (i.e. tangible) and the qualitative (i.e. intangible) impacts to the organization. • If one on one and/or face to face interviews are conducted, guidelines should be provided and reviewed with the BIA team before BIA interviews are conducted. • Lobby not to add questions to the BIA questionnaire that support another management initiative if it is inappropriate to do so (avoid scope creep). 	

Business Impact Analysis

	#	What	How	Points of Reference
	3-2	Determine the operational impact over time of a disruption to each process/function	<ul style="list-style-type: none"> • It is important to quantify the operational impacts to an organization resulting from a business process/function being unavailable. Often, the significance of a business process/function is overlooked because there may be no direct financial impact. However, the operational impact to the organization may be just as or even more significant to the organization. Measure whatever is important to your specific organization. • Choose impact levels using the most significant peak period for each business process/function. This may be at the end of a month, quarter or year, or according to seasonal trends in the business process. • A detailed definition of each of the impact levels must be established based on the specific industry. • A scale for quantifying the operational impacts must be established in order to ensure all process/functions are measured the same. For example, a scale of 1 – 4 could be used with the following definitions: 1 = no impact, 2 = moderate impact, 3= serious impact and 4 = severe impact. Another scale example to consider would be using a Low (L), Medium (M) or High (H) Impact scale for quantifying the impacts over each time period. • Where possible, contracted service level agreements and any associated penalties should be identified, along with legal or regulatory penalties. Force majeure clauses should be reviewed as part of the review. • Consider SOX- Section 409 Material event) can also be used to gain CXO (i.e. CEO, CFO, CIO,) level support for initiative. 	<p>Examples of tangible impacts may include, but not be limited to:</p> <ul style="list-style-type: none"> ➤ Legal/Regulatory/Contractual ➤ Operational ➤ Customer Service (Internal and/or External customers) ➤ Financial <p>Examples of intangible impacts may include, but not be limited to:</p> <ul style="list-style-type: none"> ➤ Market Share ➤ Reputation

Business Impact Analysis

	#	What	How	Points of Reference
	3-3	Determine the financial impact over time of a disruption to each process/function	<ul style="list-style-type: none"> • Financial impacts to the organization as a result of process unavailability can be directly or indirectly applied to each process/function. The BIA seeks to identify both direct and indirect financial impacts. Measure whatever is important to your specific organization. • Choose impact levels using the most significant peak period for each business process/function. This may be at the end of a month, quarter or year, or according to seasonal trends in the business process. • The same time periods used to measure operational impacts should be used to measure the financial impacts. If you do not consistently use the same timeframes to measure impacts, it makes it impossible to compare BIA results consistently across the organization. • A scale for quantifying the financial impact over each time period must be established based on the organization's size and the specific industry. • Determine if the financial impacts over time are cumulative. • Determine the cumulative financial impact for each category of financial impacts. • Consider the many types of revenue loss for the organization as some revenue may not truly be a loss. Consider revenue loss measurements versus revenue that is truly deferred income. • Financial impacts vary by industry; do not overlook favorable trends (intangible impacts). • Make sure that financial impacts to downstream processes are not recorded and double counted in the financial cost to the organization. • Identify the intangible impacts that make up the significant risks and exposures to the organization. One intangible impact may be that the organization will lose employees and jeopardize recovery efforts if employees aren't paid in a timely manner. • A contract may state penalties for missed deadlines or deliverables, or it may not be specific to the exact recourse the organization has. • Some operational impacts are intangible. If data is lost that cannot be restored, it may be an intangible impact as it can't be attached to a direct sum of money. 	<p>. Examples financial impacts may include, but not be limited to:</p> <ul style="list-style-type: none"> ➤ Lost revenue ➤ Property damage ➤ Deferred income ➤ Penalties and Fines ➤ Lawsuits ➤ Cost of duplicating inventory <p>Refer to Appendix A</p>
	3-4	Determine recovery time objectives (RTOs)	<ul style="list-style-type: none"> • Based upon the financial and operational impacts, determine the RTO. The RTO is the period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. Similar Terms: Maximum allowable downtime. • Determine the minimum acceptable level of operations that are required for this business process/function within the RTO. For example, if the RTO is 4-7 days, 	

Business Impact Analysis

	#	What	How	Points of Reference
			<p>does this business process/function need to be restored at 100% of production capability? Could the business process/function be recovered in stages? Ask how long can the organization live with the process at less than a normal production capacity (i.e. a reduced level of operations while in recovery mode? Could 50% of the production capability be recovered in 4-7 days and the remaining 50% be recovered in 31+ days? Remember also that in a disaster situation, it is not a business as usual environment.</p> <ul style="list-style-type: none"> • A BIA tool should never force an RTO for a business process/function. Forced recovery time objectives do not take into consideration changes of roles at time of disaster and impacts to downstream business processes and/or dependencies. If a BIA tool is used that assigns an RTO based on any sort of risk rating, there must be a process in place to override an RTO upon management review. • The RTO is used by corporate support teams to assess possible recovery strategies for the business process/function. • Assume total loss to ensure an apples to apples comparison of impacts. At this stage of the BIA, it is a natural step for the interviewer and the interviewee to discuss possible recovery strategies. Do not launch into recovery strategy discussions at this point; consider no recovery capability exists when determining where in time the process must recover. Determine what the point in time should be for the business process to recover. • RTOs should be supported by the operational and financial impacts and ratings. If the RTO is not supported by the impact ratings, then the cause must be determined (i.e. Did you miss something? Do roles change at time of disaster?) The RTO must pass a reality check by several levels in the organization. Be prepared to backup the RTO with the impacts and the ratings assigned. 	

Business Impact Analysis

	#	What	How	Points of Reference
	3-5	Determine both internal and external business dependencies	<ul style="list-style-type: none"> • Consider the most appropriate method to document both internal and external dependencies. Determine if there is a need to separate internal dependency impact information from external dependency impact information. • Identify supply chain links to other internal departments, Information technology infrastructure (internal and external applications, systems, voice and data network data, etc.), processes, or other third parties. Examples of third parties could be vendors, business partners, customers, etc. • Consider the loss to your organization should an outsourced service provider(s) not be able to meet your business requirements. Consider any service level agreements and/or contractual requirements in place (include international contractual relationships that may exist). • What are the inflows? When is it needed? From whom does the process/function receive information, data, requests, etc.? What does the process/function depend on for the information or resources to perform the process/function? • What are the outflows? When is it needed? Whom does the business process/function provide information to? What do others depend on from this business process/function? • As part of the BIA, it is important to understand what happens to your organization if a source the business process relies on is unavailable for any reason. Measure how fast and severe the impact is (i.e., operational impact). These exposures or gaps should be addressed as part of the Risk Assessment and risk mitigation process. • Consider completing business process maps to document the inflows and outflows. 	<p>Examples of internal and/or external business dependencies include, but are not limited to providers of:</p> <ul style="list-style-type: none"> ➤ Forms ➤ Raw materials ➤ Sub assembly points ➤ Inventory ➤ Courier service ➤ Customer service
	3-6	Determine central repository for BIA data	<ul style="list-style-type: none"> • Determine how BIA data will be used ongoing. Consider reporting requirements for your organization ongoing. • Determine where to house BIA data and how to update data ongoing (i.e. via a database, a spreadsheet, a specific software package, etc.). 	

Business Impact Analysis

	#	What	How	Points of Reference
IV - BIA Process	4-1	Gather BIA information using the most appropriate method for your organization.	<ul style="list-style-type: none"> • Prior to kicking off the BIA process, those individuals responsible for conducting the business impact analysis should jointly review the BIA process to: <ol style="list-style-type: none"> 1. Ensure the BIA is interpreted properly; it is important for those involved in gathering/conducting the BIA to mutually understand the questions being asked on the BIA questionnaire. BIA questions can be interpreted differently within the BIA team members. The joint review will help to eliminate any misunderstanding of the data that needs to be collected. 2. Review the message to convey (such as the importance of the BIA to the organization) and the interview techniques that are to be used to gather the data needed to complete the BIA. • Prior to gathering the BIA data, consider sending out the BIA questionnaire and questionnaire guidelines (i.e. how to interpret each question on the BIA). Questionnaires that are sent out and completed without the assistance of a Business Continuity Professional will yield results that cannot be reasonably compiled and compared (i.e. rather than gathering an apples to apples comparison, the results compare more like apples to tractors). Individual managers may not know the impact they have on the organization as a whole. Additionally, BIA questions will be interpreted differently by each interviewee. • As appropriate, schedule a meeting with the business/function manager to collaboratively complete the BIA questionnaire. Send out BIA questionnaire in advance so that the recipients can review it with others and get complete answers. • Explain the purpose of the BIA initiative to the interviewees. Make it clear that management has no hidden agenda such as having interviewees justify their jobs via the BIA process. It is helpful to explain that every department/ employee is important to the organization. One of the objectives is for executive management to learn what business process/function is time critical should a disaster occur. • Conduct interview and complete the questionnaire. Ensure consistency in interviewee(s) understanding of questions throughout the process. • Design and conduct follow-up interviews. If information is still missing after the interview, follow-up with the interviewee and request it be provided (e.g. financial dollar impacts may need to be provided by a finance department that supports the business process/function and not readily available). 	<p>Examples of how BIA data can be gathered:</p> <ul style="list-style-type: none"> ➤ One-on-one interviews ➤ Management /supervisor workshops ➤ Conference calls ➤ Electronic (not recommended)

Business Impact Analysis				
	#	What	How	Points of Reference
V - BIA Findings	5-1	Obtain approval for individual BIA results	<ul style="list-style-type: none"> Depending on the size and complexity of your organization, consider the appropriate level(s) of approval for the BIA results. For example, it may be appropriate for some organizations to obtain at least two levels of approval for the BIA results that involve both 1. the business process owner/manager and 2. the next highest level of management. Consider the appropriateness of using a sign off form of some kind to formally indicate the appropriate level management has reviewed and approved the BIA results. It is important to note that information contained in the approved BIA will be communicated to others with supporting roles in planning for the recovery of the process/function such as Facilities, Telecom, IT, etc. 	
	5-2	Prepare analysis of BIA results	<ul style="list-style-type: none"> Consolidate the individual BIA information to determine the organizational priorities for recovery over time. The recovery time objectives should drive the priorities for business process recovery including its technical components. Define report format. 	
VI - Gain Management Approval of BIA results	6-1	Obtain executive management approval of BIA summary and recovery prioritizations	<ul style="list-style-type: none"> Consider the most appropriate manner to gain approval of the BIA results. Consider for your organization if it is appropriate to circulate the BIA results by meeting with each executive manager individually to present results, or distributing written draft results to each line of business manager. Gain approval of BIA results from all appropriate levels of management before presenting the final results to the executives as a group. Develop a final summary presentation that easily shows the priorities for recovery and the RTOs to management. Determine what type of formal sign-off is required to move to the next phase of planning. Be prepared to answer detailed BIA questions from the executive managers (have the detailed BIA questionnaire results available should a detailed question arise) 	
	6-2	Prepare executive management presentation	<ul style="list-style-type: none"> A summary report is prepared and presented to executive management. The presentation should be a formality at this point. There should be absolutely no surprises on the summary presentation for executive management. Executive management should clearly be able to understand the impacts to the organization should processes/functions be unavailable; this data will support the recovery time objectives required by the process/function. 	
	6-3	Be prepared to discuss next steps	<ul style="list-style-type: none"> BIA data can quickly become outdated. Once the BIA results and priorities for recovery are approved, it is extremely important to act quickly and begin work on developing recovery strategies. 	

Business Impact Analysis

	#	What	How	Points of Reference
VII - BIA Life Cycle	7-1	Determine BIA review and update requirements.	<ul style="list-style-type: none"> • Determine how often BIA results need to be reviewed for the organization (i.e. annually, semi-annually, etc). There may be legal and/or regulatory requirements that dictate how often a BIA must be reviewed and updated. Consider if your organization is required by any internal or external auditing authority to complete specific tasks and any associated timeframes for completion. • Depending on your organization's dynamics, consider implementing a tickler system to ensure updates occur as planned. • Communicate BIA review cycle to executive management and other management levels as appropriate. • Determine audit trail for updates and a records retention schedule. 	

DRII/BCI Professional Practice Narrative:

- Determine the events and external surroundings that can adversely affect the organization and its facilities with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.

Generally Accepted Practices (GAP) Notice:

- This document is to serve as a repository of knowledge which is to be applied across various verticals
- This document contains a conceptual basis for Program development vs. an auditable checklist

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Identify Potential Risks to the Organization / Loss Potentials	1	Identify exposures from both internal and external sources, which may include: <ul style="list-style-type: none"> • Natural, man-made, technological, or political • Accidental vs. intentional • Internal vs. external • Controllable risks vs. those beyond the organization's control • Events with prior warnings vs. those with no prior warnings 	<ul style="list-style-type: none"> • Research past disasters in geographical area • Research past disasters in industry • Research past disasters in related industries • Research past disasters internally within organization • Utilize Business Impact Analysis (BIA) discussion / development for internal functions • Identify interdependencies to other organizations, systems, etc. • Research past disasters within your interdependent organizations <ul style="list-style-type: none"> – geographical, industry, related industries, and internal) – connectivity, communication, security • Prepare analysis grid showing the threats, risks, controllable factors (internal/external, accidental/intentional, with/without warning, controllable/uncontrollable) 	<ul style="list-style-type: none"> • Federal Emergency Management Agency (FEMA) website • State Emergency Management Organization websites • Local Police and Fire Departments • Business Continuity Publications • Newspapers • Internal Company Records • Building Management • Internal Interview Sessions (leading to BIA development) • Third-Party Disclosures (leading to BIA development) • Analysis Grid Example (Develop)

Risk Evaluation and Control

Sub-Topic	#	What	How	Points of Reference
	2	Determine the probability of the above events	<ul style="list-style-type: none"> • Validate credibility of information sources • Determine impacts to the organization • Research available historical probability factors • Analyze historical probability against degree of environmental change (e.g. increased threat of terrorism today may require adjustment to historical probability) • Analyze mitigating controls in place • Determine additional controls that could be implemented • Analyze probability that each identified threat could occur • Analyze probability of impact occurring as a result of each of the identified threats • Analyze effectiveness of current and potential mitigating controls 	<ul style="list-style-type: none"> • Federal Emergency Management Agency (FEMA) website • State Emergency Management Organizations • Local Police and Fire Departments • Business Continuity Publications • Newspapers • Internal Company Records • Internal Interview Sessions (leading to BIA development) • Third-Party Disclosures (leading to BIA development)

Risk Evaluation and Control

Sub-Topic	#	What	How	Points of Reference
	3	Develop methods of information gathering	<ul style="list-style-type: none"> • Partner with Internal Audit to learn of existing risks • Partner with local emergency management agency for a historical impact to business addresses • Network with local Business Continuity Planners • Research the FEMA website for declared disasters in the area • Research the “neighbors” in the general vicinity (may be indirectly impacted by potential chemical hazards, political targets, etc.) • Map nearest “transportation highways” to business location (e.g. auto, train, flight paths) • Identify single points of failure (e.g. gas, water, electricity, fiber cable, critical vendors) • Subscribe to Business Continuity publications • Sign-up for FEMA and State Emergency Management newsletters • Arrange for visiting speakers from local organizations • Attend Business Continuity seminars 	<ul style="list-style-type: none"> • FEMA Website/newsletters • State Emergency Management website/newsletters • Networking meetings • Seminars/presentations • Local Business Continuity Organizations • Business Continuity publications • Local Police / Fire Department / Utility Companies • Highway Departments • Internal Audit

Risk Evaluation and Control

Sub-Topic	#	What	How	Points of Reference
	4	Develop a method to evaluate probability vs. severity	Assess and incorporate the following elements into a method customized for the organization involved: <ul style="list-style-type: none"> • Determine current annual loss potential associated with each identified risk • Determine frequency factor (no. times per year) for each risk • Multiply annual loss potential by the frequency factor to determine annual loss exposure (ALE) • Determine likelihood of simultaneous risks occurring • Determine total simultaneous loss exposure • Determine effectiveness of mitigating controls with reducing or eliminating risk (recalculate ALE as if controls were all in place) • Determine costs of mitigating controls • Determine recovery requirements • Determine expected recovery time using actual test experience (preferred), industry experiences, or expert estimations • Adjust ALE to show loss for expected recovery time with and without suggested controls in place 	<ul style="list-style-type: none"> • Probability formula from DRII training materials • Internal Cost/Benefit guidelines and practices • Actual cost figures • Subject Matter Expert (SME) Estimations • ISO 7799 Standards Methodology • Auditor Organization Standards & Process • Federal (e.g. FFIEC)

Risk Evaluation and Control

Sub-Topic	#	What	How	Points of Reference
	5	Establish ongoing support of evaluation process	<ul style="list-style-type: none"> • Prepare costs/benefit statement • Prepare qualitative loss statement, e.g. potential for loss of life • Prepare executive presentation summarizing analysis results and source information • Demonstrate validity of presented information with test results, industry experiences, etc. • Obtain upper management championship of effort 	<ul style="list-style-type: none"> • Internal Cost/Benefit guidelines and practices • Internal Presentation guidelines and practices • Subject Matter Expert (SME) Estimations and Support • Certification as Business Continuity Planner • Knowledge of industry standards / best practices
	6	Identify relevant regulatory and/or legislative issues	<ul style="list-style-type: none"> • Consult Legal department and/or outside counsel • Consult internal Compliance officers • Consult internal Business Area management • Research federal rules and regulations for industry • Research state rules and regulations for industry 	<ul style="list-style-type: none"> • Internal/external Legal Council • Internal Compliance Officers • Federal and State websites

Risk Evaluation and Control

Sub-Topic	#	What	How	Points of Reference
------------------	----------	-------------	------------	----------------------------

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Determine the Organization's Specific Exposures to Loss Potentials	1	Establish process to assess identified loss potential	Develop method to estimate loss potential that considers: <ul style="list-style-type: none"> • Value of assets • Value of labor and opportunity costs • Frequency and duration estimates of each threat category • Mitigation effects of existing safeguards Review exposure information	<ul style="list-style-type: none"> • Internal Accounting / Finance Department • Internal Risk Management Department • Insurance Contacts / Information • Building Management • Local / County Emergency Management • FEMA • Local Police / Fire, Homeland Security
	2	Categorize exposures: <ul style="list-style-type: none"> • Primary exposures the organization may face (e.g. hurricane) • Secondary / collateral events that could materialize because of such exposures (e.g. wind damage, roof collapse) 	Create an exposure categorization table with two sections – primary exposures and secondary / collateral events that lists: <ul style="list-style-type: none"> • Exposure Name and / or Cause • Loss Potential – Single Occurrence • Loss Potential – Annual Exposure 	<ul style="list-style-type: none"> • Internal Accounting / Finance Department • Internal Risk Management Department • Insurance Contacts / Information
	3	Rank exposures	Identify potential losses: <ul style="list-style-type: none"> • Staff • Facility • Area • Data • Telecommunications • Channels of distribution Prioritize exposure categorization table by ranking and sorting by: <ul style="list-style-type: none"> • Exposures most likely to occur • Exposures with greatest impact (worst case) 	<ul style="list-style-type: none"> • Internal Accounting / Finance Department • Internal Risk Management Department • Insurance Contacts / Information

Risk Evaluation and Control

Sub-Topic	#	What	How	Points of Reference
Identify Controls and Safeguards to Prevent and/or Mitigate the Effect of the Loss Potential	1	Environmental Controls	Identify: <ul style="list-style-type: none"> • Physical Access (buildings, rooms, grounds) • Geographic Location (incidents) • Utilities 	<ul style="list-style-type: none"> • Building Management • FFIEC Guidelines – Federal Financial Institutions Examination Council • Auditors Organizations (Auditnet.org) • Internal Audit • National Institute of Standards and Technology • Risk Management Organizations
		Technical Controls	Identify: <ul style="list-style-type: none"> • Data Security • Network Security • Quality Assurance (ongoing controls) • Data & Media Administration • Assets (physical inventory) 	<ul style="list-style-type: none"> • Information Systems Audit and Control Association • National Institute of Standards and Technology • Auditor Organizations (Auditnet.org) • Internal Audit
		Operational Controls	Identify: <ul style="list-style-type: none"> • Strategic Business Objectives • Policies • Procedures • Administration • Legal / Regulatory Requirements • Key Personnel (personnel roles) • Supply Chain (Vendors) • Federal Authorities • State Authorities • Local Authorities • Industry Standards (audit methods) 	<ul style="list-style-type: none"> • FFIEC Guidelines – Federal Financial Institutions Examination Council • Auditors Organizations (Auditnet.org) • Internal Audit • Risk Management Organizations • National Institute of Standards and Technology

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	4	Reputation Controls	Identify: <ul style="list-style-type: none"> • Media Sources • Internal Communications • External Communications 	<ul style="list-style-type: none"> • DisasterCenter.com • Risk Management Organizations • Internal Audit • Internal PR / HR Departments
	5	Effectiveness	Identify: <ul style="list-style-type: none"> • Impacts of recommended mitigation options: <ul style="list-style-type: none"> – Testing Options – Risk Assumption – Risk Avoidance – Risk Limitations – Risk Transference 	<ul style="list-style-type: none"> • National Institute of Standards and Technology • Internal Audit

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Identify, Evaluate, Select, and Use Appropriate Risk Analysis Methodologies and Tools, and Expertise Needed	1	Identify alternative risk analysis methodologies, tools, and sources of internal and external expertise	Type of measurement: <ul style="list-style-type: none"> • Qualitative methodologies / tools • Quantitative methodologies / tools Type of process: <ul style="list-style-type: none"> • Manual Process • Interview <ul style="list-style-type: none"> - In person - Videoconference - Teleconference Automated Process - Email Combination of manual and automated	<ul style="list-style-type: none"> • NIST SP 800-30 Risk Management Guide for Information Technology Systems • FISCAM, PP. 16, 17, 18 • ISO 17799 – Assessing Security Risks, p. IX. • www/bettermanagement.com/risk analysis • RiskWatch • RiskPac • Identify existing data/analysis
	2	Evaluate alternative risk analysis methodologies, tools, and sources of internal and external expertise	Evaluate advantages and disadvantages of options: <ul style="list-style-type: none"> • Reliability / confidence factor • Basis of mathematical formulas used 	<ul style="list-style-type: none"> • Product/service references • Industry publications • External expertise / actuarial guidance

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	3	Select appropriate methodology, tool(s), and external expertise needed for organization-wide implementation	<ul style="list-style-type: none"> Identify target population for data collection Identify any specific requirements, e.g. regulatory, financial, etc. 	<ul style="list-style-type: none"> Internal legal counsel Internal / external audit
	4	Use appropriate methodology, tool(s), and outside expertise to develop risk analysis	Conduct analysis of data collection based on methodology chosen	<ul style="list-style-type: none"> Utilize and enhance risk assessment performed in prior steps (see above)

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Identify and Implement Information-Gathering Activities	1	Develop a strategy consistent with business issues and organizational policy	<ul style="list-style-type: none"> Establish support (tone from the top) Decide what areas, groups and locations will be covered. Determine breadth and depth of information to be gathered. Confirm consistency with organizational policy. Determine storage location, access control, and update frequency 	<ul style="list-style-type: none"> Board of Directors Corporate Champion Legal Financial Internal Audit
	2	Develop a strategy that can be managed across business divisions and organizational locations	<ul style="list-style-type: none"> Determine collection criteria: <ul style="list-style-type: none"> Business unit down to base level Location centric include all businesses. Allow for reorganization and location changes. Are there single points of failure that need special attention? 	<ul style="list-style-type: none"> Corporate Champion Business Unit Managers Site Managers Business Continuity Program Office
	3	Develop risk assessment form	<ul style="list-style-type: none"> Develop clear concise format. Allow for some flexibility Ensure that each area is self-explanatory. Create toolkit / cover package to explain each area. Ensure distribution method is consistent. 	<ul style="list-style-type: none"> Business Continuity Program Office Business Managers Key Stakeholders Sample of participants

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	4	Create organization-wide methods of information collection and distribution	<ul style="list-style-type: none"> • Deliver and follow-up - forms and questionnaires • Schedule interviews with appropriate individuals at the Business level, with additional follow-ups as needed • Conduct cross-group or large-group meetings for data gathering. Determine status meeting schedule. • Ensure appropriate individuals are committed to conduct documentation review. • Analyze to ensure that the process supports data collected, not a predetermined outcome. 	<ul style="list-style-type: none"> • Business Continuity Program Office • Business Managers • Key Stakeholder • Sample of participants
	5	Conduct formal risk assessment	<ul style="list-style-type: none"> • Update forms and questionnaires early in the process if deficiencies are determined • Use a consistent process for interviews; do not vary from the questionnaire without updating and re-interviewing earlier participants • Conduct group meetings as needed. Status meetings on predetermined schedule. • Perform consistent documentation review of input. Determine areas for further research / follow-up. 	<ul style="list-style-type: none"> • Corporate Champion • Business Unit Managers • Site Managers • Program Office • Business Managers • Key Stakeholder • Other named participants
	6	Document risk assessment findings.	<ul style="list-style-type: none"> • Analyze and publish, as scheduled, top level and detailed results supported by forms and interviews. • Store accumulated information as outlined in Section 1 	<ul style="list-style-type: none"> • Board of Directors • Corporate Champion • Legal • Financial • Internal Audit

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Evaluate the Effectiveness of Controls and Safeguards	1	Develop communications flow with other internal departments / divisions and external service providers	<ul style="list-style-type: none"> Identify control assessment team members both internal and external Review types of controls in place—physical and procedural Review goal of the control—deter or lessen the loss Discuss actual experience and test result findings associated with each control 	<ul style="list-style-type: none"> Business Management Internal Suppliers Internal Risk Management Compliance Officers Technical staff External Vendors
	2	Establish business continuity service level agreements for both supplier and customer organizations and groups within and external to the organization	<ul style="list-style-type: none"> Review BIAs to determine service levels required to meet the stated RTO's and other requirements Perform cost/benefit associated with meeting defined standards Discuss cost/benefit results with business management Agree upon standards to be delivered and penalties for non-performance Document and sign formal service level agreement Setup process to monitor service level performance 	<ul style="list-style-type: none"> Business Management Internal Suppliers Legal Counsel Compliance Officers Internal Risk Management Legal Regulatory Requirements External Vendors Technical staff
	3	Develop preventive and pre-planning options	<ul style="list-style-type: none"> Identify gaps in control process and available options to close them Complete Cost / benefit for options <ul style="list-style-type: none"> Capital investment Maintenance Costs Benefit derived Training required Determine implementation priorities, procedures, and control Develop test plan and remediation process Audit functions and responsibilities 	<ul style="list-style-type: none"> Business Management Internal Suppliers Internal Risk Management Technical staff External Vendors Internal Audit Legal Counsel Compliance Officers

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	4	Understand options for risk management and selection of appropriate or cost-effective response, i.e. risk avoidance, transfer, or acceptance of risk	<ul style="list-style-type: none"> • Develop security practices • Identify methods to minimize the effects of the loss potential • Brief participants, ensuring they understand their objectives and reporting structure • Develop interface with suppliers and utilities 	<ul style="list-style-type: none"> • Business Management • Internal Suppliers • Internal Risk Management • Technical staff • External Vendors • Internal Audit • Legal Counsel • Compliance Officers
	5	Develop recommendations for improved backup and restoration procedures	<ul style="list-style-type: none"> • Review above defined controls, gaps, costs and benefits • Develop a recommendations document based on the above information • Partner with internal and external resources to validate and refine the recommendations document 	<ul style="list-style-type: none"> • Legal counsel • Internal Risk Management • Internal Audit • Legal / regulatory requirements • Industry sources • Records management vendor • Business process owners • Business process staff

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Identify and Evaluate Risks, Controls, and Mitigation	1	Establish disaster scenarios based on risks to which the organization is exposed	Develop disaster scenarios based on the following criteria: <ul style="list-style-type: none"> • Magnitude of severity (e.g. ability to perform business) • Critical dates / times 	<ul style="list-style-type: none"> • DRII.org

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Alternatives	2	Evaluate risks	Classify risks according to relevant criteria, including: <ul style="list-style-type: none"> • Risks under the organization's control • Risks beyond the organization's control • Exposures with prior warnings (e.g. tornadoes, hurricanes) • Exposures with no prior warnings (e.g. earthquakes, terrorist attacks) 	<ul style="list-style-type: none"> • FFIEC Guidelines – Federal Financial Institutions Examination Council • Auditors Organizations (Auditnet.org) • National Institute of Standards and Technology
	3	Evaluate impact of risks and exposures on those factors essential for conducting business operations	<ul style="list-style-type: none"> • Availability of personnel • Availability of information technology • Availability of communications technology • Availability of external capabilities (vendors, insurance, etc.) 	<ul style="list-style-type: none"> • Internal personnel
	4	Re-evaluate previously identified controls	<ul style="list-style-type: none"> • Categorize controls <ul style="list-style-type: none"> - Preventive - Reactive • Calculate impacts of controls based on previous risks and exposures analysis • Recommend changes to controls if necessary <ul style="list-style-type: none"> - Partner with Internal Audit - Recommend implementation of a BCP oversight committee. 	<ul style="list-style-type: none"> • Internal Audit

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	5	Evaluate controls and recommend changes, if necessary, to reduce impact due to risks and exposures	<ul style="list-style-type: none"> • Preventive controls to inhibit impact exposures (e.g. passwords, smoke detectors, and firewalls) • Reactive controls to compensate for impact of exposures (e.g. hot sites) • Incorporate business continuity / disaster recovery procedures in all change management requests within the IT / IS environment • During plan implementation, implement such formats as checklists, etc., so that business continuity teams can operate efficiently and effectively. (Avoid thick procedures that would be viewed as overwhelming during an event, and, possibly, discarded when needed most) • Partner with Internal Audit to highlight the need-to-resolve issues • Recommend implementation of an oversight committee to approve and review an on-going business continuity program 	<ul style="list-style-type: none"> • Internal Audit

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Security	1	Identify the organization's possible security exposures	Identify the specific categories of risk which may affect the organization: <ul style="list-style-type: none"> • Physical security of all premises, internal and external • Information security, including computer room and media storage area; on site and off site • Communications security, including voice and data communications • Network security, including Intranet and Internet • Personnel security 	<ul style="list-style-type: none"> • Legal counsel • Internal Risk Management • Internal audit • Legal / regulatory requirements • Industry sources • Business process owners • Business process staff

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	2	Evaluate existing security controls and procedures	Review: <ul style="list-style-type: none"> • Industry Standards • Vendor security recommendations • Corporate policies / rules compliance • Internal Audit guidelines • Conduct controlled tests, where applicable, e.g.: <ul style="list-style-type: none"> – Site inspections – Penetration – External audit (e.g. SAS70) 	<ul style="list-style-type: none"> • Legal counsel • Internal Risk Management • Internal audit • Legal / regulatory requirements • Industry sources • Security application vendor • Business process owners • Business process staff
	3	Develop recommendations for improved security controls and procedures	Partner with the Risk Management Department and Internal Audit to develop recommendations and conduct on-going security reviews to prevent potential situations from. <ul style="list-style-type: none"> • As part of 'design in process', include risk reduction, mitigation and business controls. • Ensure implementation teams complete efforts as described. • Provide for continuous auditing (self-audit and Internal Audit) 	<ul style="list-style-type: none"> • Legal counsel • Internal Risk Management • Internal Audit • Legal / regulatory requirements • Industry sources • Business process owners • Business process staff

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Vital Records Management	1	Identify vital record needs in the organization, including paper and electronic records	<ul style="list-style-type: none"> • Agree on definition of vital records (e.g. those records required by a business to stay in business) • Review or create the organization's Records Retention Schedule to identify administrative and operational vital records • Determine frequency of data backups / replication • Identify special issues and needs concerning paper and electronic vital records (e.g. email-related vital records) • Calculate retention periods, and location / disposition timeframes • Identify timeframes for retention • Identify the need for tightly controlled disposition / destruction methods • Consider the potential need for long-term preservation • Identify records retrieval / recovery needs and processes • Identify the right media for storage • Identify the optimal storage environment • Identify technologies / equipment needed to retrieve records (e.g. tape / microfilm) 	<ul style="list-style-type: none"> • Business process owners • Business process staff • Legal counsel • Internal Risk Management • Technical staff • Internal records management department • Records management vendor

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	2	Evaluate existing backup and restoration procedures for vital records	<ul style="list-style-type: none"> • Evaluate the existence and viability of the organization's Records Retention Program and Records Retention Schedule • Review the current vital records management program and documentation <ul style="list-style-type: none"> – Completeness – Accuracy – Maintenance – Appropriate and effective distribution – Periodic training – Periodic exercise of procedures – Offsite storage of current vital records inventory and procedures, including emergency operating information and procedures • Assess the level of adherence to the vital records management program and its overall effectiveness from a technical and business standpoint • Evaluate potential threats to vital records • Evaluate strategies for protecting vital records 	<ul style="list-style-type: none"> • Business managers • Legal counsel • Internal Risk Management • Internal Audit • Legal / regulatory requirements • Industry sources • Internal records management department • Technical staff • Records management vendor • NFPA • NARA (National Archives and Records Administration)

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	3	Develop recommendations for improved backup and restoration procedures	<ul style="list-style-type: none"> • Develop a recommendations document based on the above information • Partner with internal and external resources to validate and refine the recommendations document 	<ul style="list-style-type: none"> • Legal counsel • Internal Risk Management • Internal Audit • Legal / regulatory requirements • Industry sources • Internal records management • Records management vendor • Business process owners • Business process staff • Technical staff

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Document and Present Findings	1	Document findings	<ul style="list-style-type: none"> • Consolidate findings into a single document • Prepare an high-level summary report for presentation to executive management • Consider presentation of findings from a marketing standpoint – define and sell the value of the findings and recommendations 	<ul style="list-style-type: none"> • Internal Risk Management • Internal Audit • Legal counsel

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	2	Present findings and advise management on feasible, cost-effective security measures required to prevent / reduce vital records and security-related risks and exposures	<ul style="list-style-type: none"> • Develop a presentation that clearly summarizes the results and the information in the high-level summary report • Consider meeting with each senior manager individually before presenting the final results to the executives as a group. • Schedule and present findings and recommendations to prevent / reduce vital records and security-related risks and exposures to executive management team • Be prepared to answer detailed questions from the senior managers (take the detailed results to the meeting as a backup) • Obtain formal sign-off and approval to move to the next phase of planning and implementation 	<ul style="list-style-type: none"> • Internal Risk Management • Internal Audit • Legal counsel

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Document Risk Acceptance	1	Determine, and agree on, the cost of downtime	<ul style="list-style-type: none"> • Identify the business process • Identify the method used to measure cost of interruption. <ul style="list-style-type: none"> – Is human life at risk? – Is revenue lost? – Is revenue delayed? – Is there a cost for additional resources needed to recover? – Are there legal or regulatory issues? – Are there contract requirements? – Could penalties be assessed? 	<ul style="list-style-type: none"> • Business process owners • Business process staff • Recovery staff • Legal Counsel • Contracting Office • Internal Finance / Accounting

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	2	Ensure that service level agreements are documented and considered, in terms of interdependencies (e.g. clients, vendors, key business units)	<ul style="list-style-type: none"> Identify relationships to other processes, business units, etc. Determine the level of criticality for each interdependent relationship. Verify the presence or absence of service level agreements for each relationship. Determine if the service level agreements are adequate to meet the time requirements for the business process. Determine if there are contract provisions affecting the conduct of the business process. 	<ul style="list-style-type: none"> Service Level Agreements Customers of business process Technical Staff Contracting Office
	3	Develop a risk prioritization grid that maps out the business risk and technical risks	<ul style="list-style-type: none"> Identify the risk to the business process Associate the technical risks to the business process. Rate the technical risks for likelihood and criticality. Rate the recommendations for ease of fix. Identify the level of cost for each fix. Rank the risks according to criticality, then ease of fix under each business risk. Rate recommendations for comparative cost: low, moderate; high. Set priorities based on level of risk and cost. Develop a corrective action plan. 	<ul style="list-style-type: none"> NIST SP 800-30 Risk Management Guide for Information Technology Systems Test results, when available

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
	4	Discuss with executives and ensure that they document accepted risks	<ul style="list-style-type: none"> • Document the risk to the business process and the cost/time to remediate. • Review the each documented risk and determine if it will be addressed or accepted. • If action is to be taken, develop a corrective action plan. • If no action is to be taken, document the decision by <ul style="list-style-type: none"> – Email – Signature – Risk Acknowledgement Database Update 	<ul style="list-style-type: none"> • Business Process Owners • Technical Staff • Operating/processing staff • Internal Risk Management • Internal Finance / Accounting • Executive management

Risk Evaluation and Control				
Sub-Topic	#	What	How	Points of Reference
Implement Backup, Restoration, and Security-related Measures and Procedures	1	Implement, or assist with implementation of, security measures approved by management	<ul style="list-style-type: none"> • Review corrective action plans • Identify key contacts • Verify your role in the implementation <ul style="list-style-type: none"> – Level of authority – Watchdog – Reporting – Vendor liaison 	<ul style="list-style-type: none"> • Gap analysis authors • Facilities Management • Technical Staff • Legal Counsel • Other Internal Experts
	2	Implement, or assist with implementation of, backup and restoration procedures for the organization's vital records approved by management	<ul style="list-style-type: none"> • Review gap analysis • Identify areas requiring improvement • Verify that recommendations will meet the identified need • Verify your role in implementation <ul style="list-style-type: none"> – Level of authority – Watchdog – Reporting – Vendor liaison 	<ul style="list-style-type: none"> • Gap analysis authors • Technical Staff • Records Management Team • External Records Management Advisor • Legal Counsel • Other internal experts

DRII/BCI Professional Practice Narrative:

- Establish the need for a Business Continuity Plan (BCP), including obtaining management support and organizing and managing the BCP project to completion. (This includes defining the problem; communicating the need for a BCP; developing budget requirements; identifying Planning Team(s) and Action Plans; and developing project management and documentation requirements.)

Generally Accepted Practices (GAP) Notice:

- This document is to serve as a repository of knowledge which is to be applied across various verticals
- This document contains a conceptual basis for Program development vs. an auditable checklist

Project Initiation and Management				
Sub-Topic	#	What	How	Points of Reference
Initiate	1	Define the need for Business Continuity.	<ul style="list-style-type: none"> ▪ Research and compile facts showing possible risks to the enterprise. 	<ul style="list-style-type: none"> ▪ Past Audit Comments ▪ Regulatory obligations ▪ Legal obligations ▪ Past disasters ▪ Best practices publications (white papers, banking circulars, etc...) ▪ Relevant regulatory Industry trade bodies ▪ Consulting recommendations

Project Initiation and Management

Sub-Topic	#	What	How	Points of Reference
	2	Identify the purpose and goals for the BC initiative.	<ul style="list-style-type: none"> ▪ Determine the BC focus by building a business case to identify readiness requirements ▪ Define high level roles and responsibilities across the business units impacted by the BC initiative. ▪ Obtain a high level understanding of corporate environment including products and services ▪ If available, review existing BC materials to leverage previous work 	<ul style="list-style-type: none"> ▪ Best practices publications (such as those used within the Information Security and or Project Management best practices) ▪ Cost Benefit Analysis Doc (including actual cost of past outages as well as the impact of brand damage and other concerns discovered in defining the need). ▪ Organization Charts ▪ Mission Statements ▪ Key documents such as: evacuation procedures, medical emergency, crisis mgmt and Y2K docs ▪ Service Level Agreement (SLA) document ▪ Customer Expectations document
	3	Gain buy-in and commitment for meeting goals.	<ul style="list-style-type: none"> ▪ Guide leadership (sponsors) in defining objectives, policies and critical success factors ▪ Communicate the purpose and goals with stakeholders (eg... Board of Directors, Regions, Sr. Mgmt, etc...) and receive feedback and initial approval. ▪ Identify and communicate project risks 	<ul style="list-style-type: none"> ▪ Project proposals ▪ Statements of work ▪ Cost benefit analysis docs ▪ Business Case

Project Initiation and Management				
Sub-Topic	#	What	How	Points of Reference
	4	Establish a governance structure	<ul style="list-style-type: none"> ▪ Identify Steering committee roles and responsibilities ▪ Develop supporting documentation required for the initiative ▪ Receive funding and approval to move forward ▪ Establish / review BC policy ▪ Identify need for BC Standards and definition of terminology ▪ Set decision-making protocol and issue escalation policies relative to continuity issues ▪ Gain agreement on overall timescales 	<ul style="list-style-type: none"> ▪ Mission Statement ▪ Critical Success Factor doc ▪ Conflicting priorities ▪ Portfolio / program management standards
	5	Provide awareness	<ul style="list-style-type: none"> ▪ Establish Project Communications plan 	<ul style="list-style-type: none"> ▪ BC website ▪ Debriefings ▪ Brownbag lunches ▪ Employee input

Project Initiation and Management				
Sub-Topic	#	What	How	Points of Reference
Plan	1	Establish a steering committee.	<ul style="list-style-type: none"> ▪ Identify and engage a team of affected managers to oversee project progress and to resolve issues. ▪ Establish project milestone review and approval protocol ▪ Establish the framework required to measure project success 	<ul style="list-style-type: none"> ▪ Project Status report template ▪ Project Issues and risk logs ▪ Project schedules ▪ Project plan template

Project Initiation and Management

Sub-Topic	#	What	How	Points of Reference
	2	Develop the project plan.	<ul style="list-style-type: none"> ▪ Adjust project documentation to reflect final decisions and approvals ▪ Define project deliverables and related activities ▪ List tasks and estimate effort and duration ▪ Assign project team members to tasks ▪ Set milestones ▪ Document project scope control ▪ Document project risks ▪ Develop project risk mitigation 	<ul style="list-style-type: none"> ▪ Work breakdown structure doc ▪ Project proposals ▪ Statements of work ▪ Cost benefit analyzes ▪ High-level project plan ▪ Work plans ▪ Scope control processes ▪ Change Control Procedures
	3	Determine project cost tracking	<ul style="list-style-type: none"> ▪ Establish methods to track project assets and expenses, ▪ Establish resource tracking and reporting procedures. 	<ul style="list-style-type: none"> ▪ Budget reports, Inventory and acquisition logs ▪ Time sheets
	4	Determine the project environment.	<ul style="list-style-type: none"> ▪ Determine the need for additions or changes to tools and supplies, such as acquiring or upgrading planning software ▪ Establish documentation storage and access procedures 	<ul style="list-style-type: none"> ▪ Version control procedures ▪ Security environment ▪ Confidentiality policies ▪ Change Control Procedures ▪ Documentation Management ▪ Information Handling Standards
	5	Determine training requirements	<ul style="list-style-type: none"> ▪ Schedule training on the use of new software (as required) ▪ Provide BC training ▪ 	<ul style="list-style-type: none"> ▪ Personnel skills inventory ▪ Documentation standards and guidelines ▪ Plan Templates

Project Initiation and Management				
Sub-Topic	#	What	How	Points of Reference
	6	Develop project success metrics	<ul style="list-style-type: none"> ▪ Refine the critical success factors ▪ Develop and implement measurements 	<ul style="list-style-type: none"> ▪ Critical success factors ▪ Project health measurements ▪ Checklist for Project Documentation ▪ Project Score Card ▪ PM Standards Compliance Audit Guide
	7	Develop the awareness program	<ul style="list-style-type: none"> ▪ Establish and validate components and delivery methods 	<ul style="list-style-type: none"> ▪ SUBJECT AREA 7: Awareness and Training Programs

Project Initiation and Management				
Sub-Topic	#	What	How	Points of Reference

Project Initiation and Management

Sub-Topic	#	What	How	Points of Reference
Execute	1	Conduct a Project Kick-off.	<ul style="list-style-type: none"> ▪ Facilitate a meeting with the team members to communicate the project mission and plan. ▪ Review assignments, work schedules and milestones. ▪ Set guidelines for rules of operations and progress review 	<ul style="list-style-type: none"> ▪ Status reports ▪ Issues and risk logs ▪ Project Escalation procedures ▪ Documentation Standards and Guidelines ▪ Information Handling Standards ▪ Change Control Procedures ▪ Documentation Management
	2	Implement Interim Life Safety Plan	<ul style="list-style-type: none"> ▪ Ensure the existence of an emergency only plan and develop one if needed ▪ Ensure emergency management awareness across enterprise 	<ul style="list-style-type: none"> ▪ SUBJECT AREA 5: Emergency Response and Operations ▪ SUBJECT AREA 7: Awareness and Training Programs
	3	Manage Risk Assessment	<ul style="list-style-type: none"> ▪ Assign representatives from in-scope organizational areas ▪ Use project controls to ensure success 	<ul style="list-style-type: none"> ▪ SUBJECT AREA 2: Risk Evaluation and Control
	4	Conduct a Risk Awareness Campaign	<ul style="list-style-type: none"> ▪ Work with governance body to implement policy changes ▪ Educate personnel on purpose and importance of updated preventative measures 	<ul style="list-style-type: none"> ▪ SUBJECT AREA 7: Awareness and Training Programs

Project Initiation and Management				
Sub-Topic	#	What	How	Points of Reference
	5	Manage Business Impact Analysis	<ul style="list-style-type: none"> ▪ Assign representatives from in-scope organizational areas ▪ Use project controls to ensure success 	<ul style="list-style-type: none"> ▪ SUBJECT AREA 3: Business Impact Analysis
	6	Develop BC Strategy and Standards	<ul style="list-style-type: none"> ▪ Assign representatives from in-scope organizational areas ▪ Use project controls to ensure success 	<ul style="list-style-type: none"> ▪ SUBJECT AREA 4: Developing Business Continuity Management Strategies
	7	Implement BC Solutions	<ul style="list-style-type: none"> ▪ Assign representatives from in-scope organizational areas ▪ Use project controls to ensure success 	<ul style="list-style-type: none"> ▪ SUBJECT AREA 5: Emergency Response and Operations ▪ SUBJECT AREA 6: Developing and Implementing Business Continuity and Crisis Management Plans ▪ SUBJECT AREA 9: Crisis Communications ▪ SUBJECT AREA 10: Coordination with External Agencies

Project Initiation and Management

Sub-Topic	#	What	How	Points of Reference
	8	Develop and execute a BC awareness program	<ul style="list-style-type: none"> • Assign representatives from in-scope organizational areas • Use project controls to ensure success 	<ul style="list-style-type: none"> • SUBJECT AREA 7: Awareness and Training Programs
	9	Develop and Exercise Planning Teams	<ul style="list-style-type: none"> • Assign representatives from in-scope organizational areas • Use project controls to ensure success 	<ul style="list-style-type: none"> • SUBJECT AREA 8: Maintaining and Exercising BC Plans

Project Initiation and Management				
Sub-Topic	#	What	How	Points of Reference
Control	1	Manage project scope	<ul style="list-style-type: none"> ▪ Document additional BC risks and needs not included in the original purpose and goals. ▪ Manage changes to areas of focus ▪ Escalate project scope concerns to the steering committee ▪ Manage to the tasks within the project plan 	<ul style="list-style-type: none"> ▪ Change control procedures ▪ Project mission statement ▪ Critical Success Factors ▪ Project Plan (including timeline) ▪ Budget reports ▪ Other planning materials
	2	Manage project issues	<ul style="list-style-type: none"> ▪ Identify and track project issues ▪ Manage project issues ▪ Escalate project issues to stakeholders as warranted, identifying either closure or escalation to risk status 	<ul style="list-style-type: none"> ▪ Risk logs ▪ Project mission, success factors and other planning materials ▪ Issue logs
	3	Manage project risks	<ul style="list-style-type: none"> ▪ Identify and track project risks. ▪ Develop resolutions to risks by adjusting project plans and assignments ▪ Mitigate/reduce the likelihood of an uncertain event either negatively or positively impacting the project ▪ Manage project issues ▪ Escalate project risk concerns to the steering committee 	<ul style="list-style-type: none"> ▪ Risk logs ▪ Budget reports ▪ Project mission, success factors and other planning materials ▪ Issue logs
	4	Manage deliverable quality	<ul style="list-style-type: none"> ▪ Ensure documentation standards and guidelines are followed ▪ Manage acceptance of deliverables 	<ul style="list-style-type: none"> ▪ Documentation standards and guidelines ▪ Acceptance and sign-off

Project Initiation and Management				
Sub-Topic	#	What	How	Points of Reference
	5	Conduct PM Standards Audit	<ul style="list-style-type: none"> ▪ Evaluate actual project plans as they compare to original deliverable definitions and estimates ▪ Develop recommendations for project improvements to meet critical success factors 	<ul style="list-style-type: none"> ▪ Project schedule ▪ Project success metrics ▪ Critical success factors ▪ Project health measurements ▪ Standards for project documentation ▪ Project Score Card ▪ PM Standards Compliance Audit Guide
	6	Measure progress against project success metrics	<ul style="list-style-type: none"> ▪ Evaluate actual project plans as they compare to original deliverable definitions and estimates ▪ Develop recommendations for project improvements ▪ Document and communicate progress ▪ Review previously agreed upon metrics to ensure compliance to SLAs, CSFs, etc... 	<ul style="list-style-type: none"> ▪ Project metrics ▪ Project score card ▪ Status reports

Project Initiation and Management				
Sub-Topic	#	What	How	Points of Reference

Project Initiation and Management

Sub-Topic	#	What	How	Points of Reference
Close	1	Evaluate project manager performance	<ul style="list-style-type: none"> ▪ Audit PM performance based on requirements as identified in the Portfolio Program Mgmt Standards 	<ul style="list-style-type: none"> ▪ Project schedule ▪ Project success metrics ▪ Critical success factors ▪ Project health measurements ▪ Standards for project documentation ▪ Project Score Card ▪ PM Standards Compliance Audit Guide
	2	Conduct Project lessons learned	<ul style="list-style-type: none"> ▪ Collect steering committee feedback ▪ Facilitate project team session ▪ Recommend improvements to project management methodology 	<ul style="list-style-type: none"> ▪ Issues logs ▪ Project schedules ▪ Project metrics, score cards and status reports
	3	Close Project	<ul style="list-style-type: none"> ▪ Archive project deliverables ▪ Announce project success 	