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.)

Expert / Distinguished Reviewer: Mike Cannon, CBCP, CPMP, CIA, CSP, CISA (Review Completed - 3/112015)

Subject Area 1 – Project Initiation and Management				
Sub-Topic #1: INITIATE	**#**	**What**	**How**	**Points of Reference**
	1	Define the need for Business Continuity.	• Research and compile facts showing possible risks to the enterprise.	• Past audit comments • Regulatory obligations • Legal obligations • Past incidents • Best practices publications (white papers, banking circulars, etc…) • Relevant regulatory/ industry trade bodies • Consulting recommendations • Benchmarking data

Subject Area 1 – Project Initiation and Management				
Sub-Topic #1: INITIATE	**#**	**What**	**How**	**Points of Reference**
	2	Identify the purpose and goals for the BC initiative.	• Review, finalize and submit for approval a business case that identifies BC 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. • Draft a project proposal / charter. • Draft a Business Continuity Management Policy	• Subject Area 6 • 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 management and other emergency management plans • Service Level Agreement (SLA) • Customer expectations / requirement specs

Subject Area 1 – Project Initiation and Management				
Sub-Topic #1: INITIATE	**#**	**What**	**How**	**Points of Reference**
	3	Gain buy-in and commitment for meeting goals.	• Identify Sponsors. • Guide leadership (sponsors) in defining objectives, policies and critical success factors. • Communicate the purpose and goals with stakeholders (e.g.... Board of Directors, Regions, Sr. Mgmt, etc…) and receive feedback and initial approval. • Identify high-level project targets and timeframes. • Identify and communicate project risks. • Gain approval of draft proposal / charter.	• Statements of work • Cost benefit analysis documentation • Business Case • Critical Success Factors (CSF)
	4	Establish a governance structure.	• Identify Steering committee roles and responsibilities. • Identify, review and approve 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.	• Mission Statement • Documentation of Critical Success Factors • Conflicting priorities • Portfolio / program management standards

Subject Area 1 – Project Initiation and Management				
Sub-Topic #1: INITIATE	**#**	**What**	**How**	**Points of Reference**
	5	Provide awareness of overall project.	• Establish Project Communications plan.	• BC website • Debriefings • Brownbag lunches • Employee input • Intranet • Town Hall meetings • Administration communication process • Quarterly newsletters

Subject Area 1 – Project Initiation and Management				
Sub-Topic #2 PLAN	**#**	**What**	**How**	**Points of Reference**
	1	Establish a steering committee.	• 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.	• Project status report template • Project issues and risk logs • Project schedule • Project plan
	2	Develop the project plan.	• 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.	• Work breakdown structure document • Project proposals • Statements of work • Cost benefit analyzes • High-level project plan • Work plans • Scope control processes • Change control procedures • Table Of Contents for Project Management Body of Knowledge (PMBOK)

Subject Area 1 – Project Initiation and Management				
Sub-Topic #2 **PLAN**	**#**	**What**	**How**	**Points of Reference**
	3	Determine project cost tracking.	• Establish methods to track project assets and expenses. • Establish resource tracking and reporting procedures.	• Budget reports, Inventory and acquisition logs • Time sheets • Table Of Contents for Project Management Body of Knowledge (PMBOK)
	4	Determine the project environment.	• Determine the need for additions or changes to tools and supplies, such as acquiring or upgrading planning software. • Establish documentation storage and access procedures.	• Change control procedures • Security environment • Confidentiality policies • Documentation management standards • Information handling standards • Table Of Contents for Project Management Body of Knowledge (PMBOK)
	5	Determine training requirements.	• Schedule training on the use of new software (as required). • Provide general BC training. • Provide BCP Tool training. • Provide BCP Roles and Responsibility overview. • Provide in-depth BC training as applicable.	• Personnel skills inventory • Documentation management standards • Project Plan • Subject Area 7: Awareness and Training Programs

Subject Area 1 – Project Initiation and Management				
Sub-Topic #2 PLAN	**#**	**What**	**How**	**Points of Reference**
	6	Develop project success metrics.	• Refine the critical success factors. • Develop and implement measurements.	• Critical Success Factors • Project health measurements • Project documentation checklist • Project score card • PM standards compliance audit guide • Table Of Contents for Project Management Body of Knowledge (PMBOK)
	7	Develop the awareness program.	• Establish and validate components and delivery methods.	• Subject Area 7: Awareness and Training Programs

Subject Area 1 – Project Initiation and Management				
Sub-Topic #3 **EXECUTE**	**#**	**What**	**How**	**Points of Reference** (
	1	Conduct a Project Kick-off.	• 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.	• Status reports • Issues and risk logs • Project escalation procedures • Information handling standards • Change control procedures • Documentation management standards • Table Of Contents for Project Management Body of Knowledge (PMBOK)
	2	Implement Interim Life Safety Plan.	• Ensure the existence of an emergency only plan and develop one if needed. • Ensure emergency management awareness across enterprise.	• Subject Area 5: Emergency Response and Operations • Subject Area 7: Awareness and Training Programs
	3	Manage Risk Assessment.	• Assign representatives from in-scope organizational areas. • Use project controls to ensure success.	• Subject Area 2: Risk Evaluation and Control
	4	Conduct a Risk Awareness Campaign.	• Work with governance body to implement policy changes. • Educate personnel on purpose and importance of updated preventive measures.	• Subject Area 7: Awareness and Training Programs

Subject Area 1 – Project Initiation and Management				
Sub-Topic #3 **EXECUTE**	**#**	**What**	**How**	**Points of Reference** (
	5	Manage Business Impact Analysis.	• Assign representatives from in-scope organizational areas. • Use project controls to ensure success.	• Subject Area 3: Business Impact Analysis
	6	Develop BC Strategy and Standards.	• Assign representatives from in-scope organizational areas. • Use project controls to ensure success.	• Subject Area 4: Developing Business Continuity Management Strategies
	7	Implement BC Solutions.	• Assign representatives from in-scope organizational areas. • Use project controls to ensure success.	• 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
	8	Develop and execute a BC awareness program.	• Assign representatives from in-scope organizational areas. • Use project controls to ensure success.	• Subject Area 7: Awareness and Training Programs

Subject Area 1 – Project Initiation and Management				
Sub-Topic #3 **EXECUTE**	**#**	**What**	**How**	**Points of Reference** (
	9	Develop and Exercise Planning Teams.	• Assign representatives from in-scope organizational areas. • Use project controls to ensure success.	• Subject Area 7: Awareness and Training Programs • Subject Area 8: Maintaining and Exercising BC Plans

Subject Area 1 – Project Initiation and Management				
Sub-Topic #4 CONTROL	**#**	**What**	**How**	**Points of Reference**
	1	Manage project scope.	• 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.	• Change control procedures • Project mission statement • Critical Success Factors • Project Plan • Budget reports • Other planning materials
	2	Manage project issues.	• Identify and track project issues • Manage project issues • Escalate project issues to stakeholders as warranted, identifying either closure or escalation to risk status	• Risk / Issue logs • Project mission, success factors and other planning materials
	3	Manage project risks.	• 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.	• Risk logs • Budget reports • Project mission, success factors and other planning materials • Issue logs
	4	Manage deliverable quality.	• Ensure documentation standards and guidelines are followed. • Manage acceptance of deliverables.	▪ Documentation management standards ▪ Acceptance and sign-off

Subject Area 1 – Project Initiation and Management				
Sub-Topic #4 CONTROL	**#**	**What**	**How**	**Points of Reference**
	5	Conduct PM Standards Audit.	• Evaluate actual project plans as they compare to original deliverable definitions and estimates. • Develop recommendations for project improvements to meet critical success factors.	• Project Plan schedule • Project success metrics • Critical Success Factors • Project health measurements • Documentation Management Standards • Project Score Card • PM standards compliance audit guide • Table Of Contents for Project Management Body of Knowledge (PMBOK)
	6	Measure progress against project success metrics.	• 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, Critical Success Factors, etc…	• Project metrics • Project Score Card • Status reports

Subject Area 1 – Project Initiation and Management				
Sub-Topic #5 CLOSE	**#**	**What**	**How**	**Points of Reference**
	1	Evaluate project manager performance.	• Audit PM performance based on requirements as identified in the Portfolio Program Management Standards.	• Project Plan schedule • Project success metrics • Critical success factors • Project health • Documentation management standards • Project Score Card • PM standards compliance audit guide
	2	Conduct Project Lessons Learned.	• Collect steering committee feedback. • Facilitate project team session. • Recommend improvements to project management methodology.	• Project Plan • Issues logs • Project Plan schedule • Project metrics, score cards and status reports
	3	Close Project.	• Archive project deliverables. • Announce project success.	

External References: Standards, Guidelines & National Practice Publications

ANSI / ARMA 5-2010 – Vital Records: Identifying, Managing, and Recovering Business-Critical Records. ARMA International, August 2010. ISBN: 978-1-931786-87-4. (Source: http://www.arma.org/.)

ANSI / NFPA 1600:2013 – Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association, March 2013. ISBN: 978-145590602-4 (Source: http://www.nfpa.org.)

AS/NZS 5050; 2010 – Business Continuity – Managing Disruption-Related Risk. Standards Australia /Standards New Zealand, June 2010. ISBN: 978 0-7337-9615-9. Source: http://www.saiglobal.com.)

BS 22301: 2012 – Societal Security – Business Continuity Management Systems – Requirements. BSI Business Information, November 2012. ISBN: 978-981-4353-38-0. (Source: http://www.bsi-global.com.)

PMBOK: June 2013 – Project Management Body of Knowledge, 2013 Edition. Project Management Institute. ISBN-13:893-7485908328 ISBN:10: 1935589679 Edition: 5th. (Source: http://www.pmi.org.)

SS 540: 2008 – Singapore Standard for Business Continuity Management – Standardization Department, SPRING Singapore, 2008. ISBN: 978-9814154833. Source: http://www.spring.gov.sg.)

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

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #1 **ID RISK / LOSS POTENTIAL**	**#**	**What**	**How**	**Points of Reference**

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #1 **ID RISK / LOSS POTENTIAL**	**#**	**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: • 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	• 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 – 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)	• 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) • AS/NZS4360:2004 Risk Management

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #1 **ID RISK / LOSS POTENTIAL**	**#**	**What**	**How**	**Points of Reference**
	2	Determine the probability of the above events	• 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	• 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) • AS/NZS4360:2004 Risk Management

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #1 **ID RISK / LOSS POTENTIAL**	**#**	**What**	**How**	**Points of Reference**
	3	Develop methods of information gathering	• 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	• 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

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #1 **ID RISK / LOSS POTENTIAL**	**#**	**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: • 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	• 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) • AS/NZS4360:2004 Risk Management

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #1 **ID RISK / LOSS POTENTIAL**	**#**	**What**	**How**	**Points of Reference**
	5	Establish ongoing support of evaluation process	• 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	• 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 • AS/NZS4360:2004 Risk Management
	6	Identify relevant regulatory and/or legislative issues	• 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	• Internal/external Legal Council • Internal Compliance Officers • Federal and State websites

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #2 **DETERMINE EXPOSURE TO LOSS**	**#**	**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: • 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	• Internal Accounting / Finance Department • Internal Risk Management Department • Insurance Contacts / Information • Building Management • Local / County Emergency Management • FEMA • Local Police / Fire, Homeland Security • AS/NZS4360:2004 Risk Management
	2	Categorize exposures: • 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: • Exposure Name and / or Cause • Loss Potential – Single Occurrence • Loss Potential – Annual Exposure	• Internal Accounting / Finance Department • Internal Risk Management Department • Insurance Contacts / Information

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #2 **DETERMINE EXPOSURE TO LOSS**	**#**	**What**	**How**	**Points of Reference**
	3	Rank exposures	Identify potential losses: • Staff • Facility • Area • Data • Telecommunications • Channels of distribution Prioritize exposure categorization table by ranking and sorting by: • Exposures most likely to occur • Exposures with greatest impact (worst case)	• Internal Accounting / Finance Department • Internal Risk Management Department • Insurance Contacts / Information

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #3 **CONTROLS & SAFEGUARDS TO MITIGATE**	**#**	**What**	**How**	**Points of Reference**
Identify Controls and Safeguards to Prevent and/or Mitigate the Effect of the Loss Potential	**1**	Environmental Controls	Identify: • Physical Access (buildings, rooms, grounds) • Geographic Location (incidents) • Utilities	• Building Management • FFIEC Guidelines – Federal Financial Institutions Examination Council • Auditors Organizations (Auditnet.org) • Internal Audit • National Institute of Standards and Technology • Risk Management Organizations • AS/NZS4360:2004 Risk Management
	2	Technical Controls	Identify: • Data Security • Network Security • Quality Assurance (ongoing controls) • Data & Media Administration • Assets (physical inventory)	• Information Systems Audit and Control Association • National Institute of Standards and Technology • Auditor Organizations (Auditnet.org) • AS/NZS4360:2004 Risk Management • Internal Audit

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #3 **CONTROLS & SAFEGUARDS TO MITIGATE**	**#**	**What**	**How**	**Points of Reference**
	3	Operational Controls	Identify: • 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)	• FFIEC Guidelines – Federal Financial Institutions Examination Council • Auditors Organizations (Auditnet.org) • Internal Audit • Risk Management Organizations • National Institute of Standards and Technology • AS/NZS4360:2004 Risk Management
	4	Reputation Controls	Identify: • Media Sources • Internal Communications • External Communications	• DisasterCenter.com • Risk Management Organizations • Internal Audit • Internal PR / HR Departments • AS/NZS4360:2004 Risk Management
	5	Effectiveness	Identify: • Impacts of recommended mitigation options: – Testing Options – Risk Assumption – Risk Avoidance – Risk Limitations – Risk Transference	• National Institute of Standards and Technology • Internal Audit • AS/NZS4360:2004 Risk Management

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #4 **RISK ANALYSIS METHODOLOGY & TOOLS**	**#**	**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: • Qualitative methodologies / tools • Quantitative methodologies / tools Type of process: • Manual Process • Interview - In person - Videoconference - Teleconference Automated Process - Email Combination of manual and automated	• NIST SP 800-30 Risk Management Guide for Information Technology Systems • FISCAM, pp. 16, 17, 18 • ISO/IEC 27002:2005 – Assessing Security Risks, pg. IX. • http://www.bettermanagement.com/risk analysis • RiskWatch • RiskPac • Identify existing data/analysis • AS/NZS4360:2004 Risk Management
	2	Evaluate alternative risk analysis methodologies, tools, and sources of internal and external expertise	Evaluate advantages and disadvantages of options: • Reliability / confidence factor • Basis of mathematical formulas used	• Product/service references • Industry publications • External expertise / actuarial guidance • AS/NZS4360:2004 Risk Management
	3	Select appropriate methodology, tool(s), and external expertise needed for organization-wide implementation	• Identify target population for data collection • Identify any specific requirements, e.g. regulatory, financial, etc.	• Internal legal counsel • Internal / external audit

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #4 **RISK ANALYSIS METHODOLOGY & TOOLS**	**#**	**What**	**How**	**Points of Reference**
	4	Use appropriate methodology, tool(s), and outside expertise to develop risk analysis	Conduct analysis of data collection based on methodology chosen	• Utilize and enhance risk assessment performed in prior steps (see above)

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #5 **INFORMATION GATHERING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
Identify and Implement Information-Gathering Activities	**1**	Develop a strategy consistent with business issues and organizational policy	• 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	• Board of Directors • Corporate Champion • Legal • Financial • Internal Audit
	2	Develop a strategy that can be managed across business divisions and organizational locations	• Determine collection criteria: – 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?	• Corporate Champion • Business Unit Managers • Site Managers • Business Continuity Program Office
	3	Develop risk assessment form	• 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.	• Business Continuity Program Office • Business Managers • Key Stakeholders • Sample of participants

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #5 **INFORMATION GATHERING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
	4	Create organization-wide methods of information collection and distribution	• 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.	• Business Continuity Program Office • Business Managers • Key Stakeholder • Sample of participants
	5	Conduct formal risk assessment	• 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.	• Corporate Champion • Business Unit Managers • Site Managers • Program Office • Business Managers • Key Stakeholder • Other named participants • AS/NZS4360:2004 Risk Management

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #5 **INFORMATION GATHERING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
	6	Document risk assessment findings.	• Analyze and publish, as scheduled, top level and detailed results supported by forms and interviews. • Store accumulated information as outlined in Section 1	• Board of Directors • Corporate Champion • Legal • Financial • Internal Audit

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #6 **EVALUATE CONTROLS & SAFEGUARDS**	**#**	**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	• 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	• Subject Area 1: Project Initiation and Management • 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	• Review Business Impact Assessment (BIAs) to determine service levels required to meet the stated Recovery Time Objectives (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	• Subject Area 3: Business Impact Analysis • Business Management • Internal Suppliers • Legal Counsel • Compliance Officers • Internal Risk Management • Legal Regulatory Requirements • External Vendors • Technical staff

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #6 **EVALUATE CONTROLS & SAFEGUARDS**	**#**	**What**	**How**	**Points of Reference**
	3	Develop preventive and pre-planning options	• Identify gaps in control process and available options to close them • Complete Cost / benefit for options - Capital investment - Maintenance Costs - Benefit derived - Training required • Determine implementation priorities, procedures, and control • Develop test plan and remediation process • Audit functions and responsibilities	• Business Management • Internal Suppliers • Internal Risk Management • Technical staff • External Vendors • Internal Audit • Legal Counsel • Compliance Officers
	4	Understand options for risk management and selection of appropriate or cost-effective response, i.e. risk avoidance, transfer, or acceptance of risk	• 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	• Business Management • Internal Suppliers • Internal Risk Management • Technical staff • External Vendors • Internal Audit • Legal Counsel • Compliance Officers • AS/NZS4360:2004 Risk Management

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #6 **EVALUATE CONTROLS & SAFEGUARDS**	**#**	**What**	**How**	**Points of Reference**
	5	Develop recommendations for improved backup and restoration procedures	• 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	• Legal counsel • Internal Risk Management • Internal Audit • Legal / regulatory requirements • Industry sources • Records management vendor • Business process owners • Business process staff • Australian Standards Practitioners Guide to Business Continuity HB292: 2006

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #7 **EVALUATE RISKS, CONTROLS & MITIGATION ALTERNATIVES**	**#**	**What**	**How**	**Points of Reference**
Identify and Evaluate Risks, Controls, and Mitigation Alternatives	**1**	Establish disaster scenarios based on risks to which the organization is exposed	Develop disaster scenarios based on the following criteria: • Magnitude of severity (e.g. ability to perform business) • Critical dates / times	• DRII.org
	2	Evaluate risks	Classify risks according to relevant criteria, including: • 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)	• FFIEC Guidelines – Federal Financial Institutions Examination Council • Auditors Organizations (Auditnet.org) • National Institute of Standards and Technology • AS/NZS4360:2004 Risk Management
	3	Evaluate impact of risks and exposures on those factors essential for conducting business operations	• Availability of personnel • Availability of information technology • Availability of communications technology • Availability of external capabilities (vendors, insurance, etc.)	• Internal personnel • AS/NZS4360:2004 Risk Management •
	4	Re-evaluate previously identified controls	• Categorize controls - Preventive - Reactive • Calculate impacts of controls based on previous risks and exposures analysis • Recommend changes to controls if necessary	• Internal Audit

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #7 **EVALUATE RISKS, CONTROLS & MITIGATION ALTERNATIVES**	**#**	**What**	**How**	**Points of Reference**
			- Partner with Internal Audit - Recommend implementation of a BCP oversight committee.	
	5	Evaluate controls and recommend changes, if necessary, to reduce impact due to risks and exposures	• 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	• Internal Audit

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #8 **SECURITY**	**#**	**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: • 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	• Legal counsel • Internal Risk Management • Internal audit • Legal / regulatory requirements • Industry sources • Business process owners • Business process staff
	2	Evaluate existing security controls and procedures	Review: • Industry Standards • Vendor security recommendations • Corporate policies / rules compliance • Internal Audit guidelines • Conduct controlled tests, where applicable, e.g.: – Site inspections – Penetration – External audit (e.g. SAS70)	• Legal counsel • Internal Risk Management • Internal audit • Legal / regulatory requirements • Industry sources • Security application vendor • Business process owners • Business process staff

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #8 **SECURITY**	**#**	**What**	**How**	**Points of Reference**
	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. • 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)	• Legal counsel • Internal Risk Management • Internal Audit • Legal / regulatory requirements • Industry sources • Business process owners • Business process staff

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #9 **VITAL RECORDS MANAGEMENT**	**#**	**What**	**How**	**Points of Reference**
Vital Records Management	**1**	Identify vital record needs in the organization, including paper and electronic records	• 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)	• Business process owners • Business process staff • Legal counsel • Internal Risk Management • Technical staff • Internal records management department • Records management vendor

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #9 **VITAL RECORDS MANAGEMENT**	**#**	**What**	**How**	**Points of Reference**
	2	Evaluate existing backup and restoration procedures for vital records	• 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 – 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	• Business managers • Legal counsel • Internal Risk Management • Internal Audit • Legal / regulatory requirements • Industry sources • Internal records management department • Technical staff • Records management vendor • NFPA (National Fire Protection Association) • NARA (National Archives and Records Administration)

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #9 **VITAL RECORDS MANAGEMENT**	**#**	**What**	**How**	**Points of Reference**
	3	Develop recommendations for improved backup and restoration procedures	• Develop a recommendations document based on the above information • Partner with internal and external resources to validate and refine the recommendations document	• 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

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #10 **DOCUMENT & PRESENT FINDINGS**	**#**	**What**	**How**	**Points of Reference**
Document and Present Findings	**1**	Document findings	• 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	• Internal Risk Management • Internal Audit • Legal counsel
	2	Present findings and advise management on feasible, cost-effective security measures required to prevent / reduce vital records and security-related risks and exposures	• 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	• Internal Risk Management • Internal Audit • Legal counsel

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #11 **DOCUMENT RISK ACCEPTANCE**	**#**	**What**	**How**	**Points of Reference**
Document Risk Acceptance	**1**	Determine, and agree on, the cost of downtime	• Identify the business process • Identify the method used to measure cost of interruption. – 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?	• Business process owners • Business process staff • Recovery staff • Legal Counsel • Contracting Office • Internal Finance / Accounting
	2	Ensure that service level agreements are documented and considered, in terms of interdependencies (e.g. clients, vendors, key business units)	• 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.	• Service Level Agreements • Customers of business process • Technical Staff • Contracting Office

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #11 **DOCUMENT RISK ACCEPTANCE**	**#**	**What**	**How**	**Points of Reference**
	3	Develop a risk prioritization grid that maps out the business risk and technical risks	• 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.	• NIST SP 800-30 Risk Management Guide for Information Technology Systems • Test results, when available

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #11 **DOCUMENT RISK ACCEPTANCE**	**#**	**What**	**How**	**Points of Reference**
	4	Discuss with executives and ensure that they document accepted risks	• 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 – Email – Signature – Risk Acknowledgement Database Update	• Business Process Owners • Technical Staff • Operating/processing staff • Internal Risk Management • Internal Finance / Accounting • Executive management

Subject Area 2 – Risk Evaluation and Control				
Sub-Topic #12 **BACKUP, RESTORATION & SECURITY MEASURES**	**#**	**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	• Review corrective action plans • Identify key contacts • Verify your role in the implementation – Level of authority – Watchdog – Reporting – Vendor liaison	• 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	• Review gap analysis • Identify areas requiring improvement • Verify that recommendations will meet the identified need • Verify your role in implementation – Level of authority – Watchdog – Reporting – Vendor liaison	• Gap analysis authors • Technical Staff • Records Management Team • External Records Management Advisor • Legal Counsel • Other internal experts

External References: Standards, Guidelines & National Practice Publications

ANSI / ARMA 5-2003 – Vital Records: Identifying, Managing, and Recovering Business-Critical Records. ARMA International, March 2003. (ISBN: 1-931786-12-7. Source: http://www.arma.org/.)

ANSI / NFPA 1600:2007 – Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association, March 2007. (Source: http://www.nfpa.org.)

AS/NZS 4360:2004 – Risk Management. Standards Australia /Standards New Zealand, August 2004. (ISBN: 0-7337-5904-1. Source: http://www.saiglobal.com.)

BS 25999-1: 2006 – Business Continuity Management – Part 1: Code of Practice. BSI Business Information, November 2006. (ISBN: 0 580 49601 5. Source: http://www.bsi-global.com.)

Business Continuity Guideline, A Practical Approach to Emergency Preparedness, Crisis Management, and Disaster Recovery. ASIS International, 2005. (Source: http://www.asisonline.org/guidelines/guidelinesbc.pdf.)

Federal Information System Controls Audit Manual (FISCAM), January 1999. GAO. (Source: http://www.gao.gov/special.pubs.)

FEMA 141: Emergency Management Guide for Business and Industry. FEMA, October 1993. (Source: http://www.fema.gov/pdf/library/bizindst.pdf.)

FFIEC – Business Continuity Planning Booklet. Federal Financial Institutions Examination Council (FFIEC), March 2003. (Source: http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf.)

HB 292: 2006 – Practitioners Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7472-5. Source: http://www.saiglobal.com.)

HB 293: 2006 – Executive Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7488-1. Source: http://www.saiglobal.com.)

ISO/IEC 27002:2005 (ISO/IEC 17799:2005) – Information Technology Security Techniques - Code of Practice for Information Security Management. International Standards Organization, June 2005. (Source: http://www.iso.org.)

ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements. International Standards Organization, October 2005. (Source: http://www.27001.com/.)

NARA – Primer on Disaster Preparedness, Management, and Response for Paper-Based Materials. National Archives and Records Administration (NARA), October 1993.
(Source: http://www.archives.gov/preservation/emergency-prep/disaster-prep-primer.pdf.)

NIST 800-30 – Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST), July 2002. (SP 800-30. Source: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.)

PMBOK: 2004 – Project Management Body of Knowledge, 2004 Edition. Project Management Institute.
(ISBN: 1-930699-45-X. Source: http://www.pmi.org.)

RiskWatch - RiskWatch Information Security product Suite includes software for vulnerability assessments, risk analyses and compliance reviews of information systems specifically for ISO/IEC 27002:2005), GLBA-FFIEC, HIPAA, and SOX.
(Source: http://www.riskwatch.com/.)

TR 19: 2005 – Technical Reference for Business Continuity Management. SPRING Singapore, 2005.
(ISBN: 981-4154-13-X. Source: http://www.spring.gov.sg.)

DRII/BCI Professional Practice Narrative:
Identify the impacts resulting from the interruption of business processes/functions over time on normal operations and techniques that can be used to quantify and qualify such impacts. Establish the criticality of functions, their recovery priorities, and interdependencies to set recovery time objective(s) and recovery point objective(s).

Expert / Distinguished Reviewer: Barney Pelant, MBCP (Review Completed – 10/1/2014)

Subject Area 3 – Business Impact Analysis				
Sub-Topic #1 **EXECUTIVE SPONSORSHIP**	**#**	**What**	**How**	**Points of Reference**
Executive Sponsorship	1	Gain executive management buy-in	• Dialog with management on communication processes and expectations within the organization. Consider setting expectations with executive management, "The Board of Directors", business unit managers, regulators, auditors (internal and external), state government departments and the BCP steering committee as appropriate. • 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 relevant 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 value and time sensitivity of business processes/functions, and with this knowledge, can make informed decisions on the investment to make in recovery strategies.	The risk assessment and business impact analysis should be two separate efforts. This is because the premises and purposes of these two efforts are different, and combining them can unnecessarily corrupt the findings of the BIA study.

Subject Area 3 – Business Impact Analysis				
Sub-Topic #1 **EXECUTIVE SPONSORSHIP**	**#**	**What**	**How**	**Points of Reference**
			• There are often 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) • 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 be set up for failure in completing a successful BIA. • 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. • Give examples of what might happen if the company does NOT conduct a BIA.	
	2	Request executive level support be communicated for the BIA initiative	• 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.	

Subject Area 3 – Business Impact Analysis				
Sub-Topic #2 **UNDERSTAND THE ORGANIZATION**	**#**	**What**	**How**	**Points of Reference**
UNDERSTAND THE ORGANIZATION	1	Identify business processes / functions	• 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 to reduce the depth of the BIA study, rather than the scope, 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.	

Subject Area 3 – Business Impact Analysis				
Sub-Topic #3 **BIA TOOLS**	**#**	**What**	**How**	**Points of Reference**
BIA TOOLS	1	Design a custom tailored business impact analysis questionnaire	• 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. • Define report format. (Moved from Section 5-2) • 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).	

Subject Area 3 – Business Impact Analysis				
Sub-Topic #3 **BIA TOOLS**	**#**	**What**	**How**	**Points of Reference**
BIA TOOLS	2	Determine the operational impact over time of a disruption to each process/function	• It is important to quantify the operational impacts to an organization resulting from a business process/function being unavailable. The significance of a business process/function is often 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 and levels of importance to your organization. • 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. Another scale example might be, Essential, Necessary Desirable. • 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.	Examples of tangible impacts may include, but not be limited to: ➢ Legal/ Regulatory/ Contractual ➢ Operational ➢ Customer Service (Internal and/or External customers) ➢ Financial Examples of intangible impacts may include, but not be limited to: ➢ Reputation ➢ Management Control ➢ Employee Morale

BIA TOOLS	3	Determine the financial impact over time of a disruption to each process/function	• 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 disrupt business processes/functions 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.	Examples of potential financial impacts include, but may not be limited to: ➢ Lost revenue ➢ Deferred income ➢ Penalties and Fines ➢ Lawsuits Refer to Appendix A

BIA TOOLS	4	Determine recovery time objectives (RTOs), Maximum Allowable Downtime/Outage (MAD/MAO) and Recovery Point Objective (RPO)	• 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, 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. • A BIA tool should never assign an RTO for a business process/function based on the worst possible time for an interruption of that business process/function to occur. The actual recovery time objectives following an interruption do not take into consideration the time of disaster and impacts to downstream business processes and/or dependencies. A BIA tool should not assign an RTO based on any sort of risk rating. • The RTO is used by corporate support teams to assess possible recovery strategies for the business process/function. • 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.	

BIA TOOLS	5	Determine both internal and external business dependencies	• 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. • Each company should explicitly spell out their MAD, RTO and RPO definitions. e.g. Is the RTO from the incident until applications are 'up'; or from the declaration until systems are turned over to users; or is it from incident until customer information is current? • Consider the most appropriate method to document both internal and external dependencies. Internal dependency impact information should be separate 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?	Examples of internal and/or external business dependencies include, but are not limited to providers of: ➢ Forms ➢ Raw materials ➢ Sub assembly points ➢ Inventory ➢ Courier service ➢ Customer service

BIA TOOLS	5	Determine both internal and external business dependencies	• 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.	
BIA TOOLS	6	Determine central repository for BIA data	• Determine the appropriate confidentiality level, access and handling of BIA data within your organization. • 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.). • Ensure that the BIA data and artifacts be stored in a secure, backed up environment.	

Subject Area 3 – Business Impact Analysis				
Sub-Topic #4 **BIA PROCESS**	**#**	**What**	**How**	**Points of Reference**
BIA PROCESS	1	Gather BIA information using the most appropriate method for your organization.	• Ensure that all participants receive proper training and understand the value, importance and need for the BIA. • Prior to kicking off the BIA process, those individuals responsible for conducting the business impact analysis should jointly review the BIA process to: 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. • Consider partnering your business/function managers with their IT counterparts during the data gathering process as the quality of the information gathered with them together will almost always be better than the data gathered from them separately. • 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	Examples of how BIA data can be gathered: ➢ One-on-one interviews ➢ Management /supervisor workshops ➢ Conference calls ➢ Electronic ➢ Questionnaire

BIA PROCESS			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 business process/function sensitivity 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).	

Subject Area 3 – Business Impact Analysis				
Sub-Topic #5 **BIA FINDINGS**	**#**	**What**	**How**	**Points of Reference**
BIA Findings	1	Obtain approval for individual BIA results	• 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 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.	
	2	Prepare analysis of BIA results	• 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.	

Subject Area 3 – Business Impact Analysis				
Sub-Topic #6 **GAIN MGT APPROVAL OF BIA RESULTS**	**#**	**What**	**How**	**Points of Reference**
Gain Management Approval of BIA results	1	Obtain executive management approval of BIA summary and recovery prioritizations	• 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)	
	2	Prepare executive management presentation	• 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.	
	3	Be prepared to discuss next steps	• 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.	Subject Area 4: Developing Business Continuity Strategies

Subject Area 3 – Business Impact Analysis				
Sub-Topic #7 **BIA LIFECYCLE**	**#**	**What**	**How**	**Points of Reference**
BIA Life Cycle	1	Determine BIA review and update requirements.	• 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.	

External References: Standards, Guidelines & National Practice Publications

ANSI / NFPA 1600:2007 – Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association, March 2007. (Source: http://www.nfpa.org.)

AS/NZS 4360:2004 – Risk Management. Standards Australia /Standards New Zealand, August 2004. (ISBN: 0-7337-5904-1. Source: http://www.saiglobal.com.)

BS 25999-1: 2006 – Business Continuity Management – Part 1: Code of Practice. BSI Business Information, November 2006. (ISBN: 0 580 49601 5. Source: http://www.bsi-global.com.)

Federal Information System Controls Audit Manual (FISCAM), January 1999. GAO. (Source: http://www.gao.gov/special.pubs.)

FEMA 141: Emergency Management Guide for Business and Industry. FEMA, October 1993. (Source: http://www.fema.gov/pdf/library/bizindst.pdf.)

FEMA IS-700: An Introduction to the National Incident Management System (NIMS). FEMA Independent Study Program. (Source: http://www.training.fema.gov/emiWeb/IS/is700.asp.)

FFIEC – Business Continuity Planning Booklet. Federal Financial Institutions Examination Council (FFIEC), March 2003. (Source: http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf.)

Federal Information System Controls Audit Manual. General Accounting Office (GAO), July 1999. (Source: http://www.gao.gov/special.pubs/mgmtpln.pdf)

HB 292: 2006 – Practitioners Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7472-5. Source: http://www.saiglobal.com.)

HB 293: 2006 – Executive Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7488-1. Source: http://www.saiglobal.com.)

ISO/IEC 27002:2005 (ISO/IEC 17799:2005) – Information Technology Security Techniques - Code of Practice for Information Security Management. International Standards Organization, June 2005. (Source: http://www.iso.org.)

ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements. International Standards Organization, October 2005. (Source: http://www.27001.com/.)

NARA – Primer on Disaster Preparedness, Management, and Response for Paper-Based Materials. National Archives and Records Administration (NARA), October 1993.
(Source: http://www.archives.gov/preservation/emergency-prep/disaster-prep-primer.pdf.)

NIST 800-30 – Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST), July 2002. (SP 800-30. Source: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.)

Open for Business, Disaster Planning Toolkit for Small to Mid-Sized Business Owners. Institute for Business and Home Safety (IBHS), January 2005. (Source: http://www.ibhs.org/docs/OpenForBusiness.pdf.)

PMBOK: 2004 – Project Management Body of Knowledge, 2004 Edition. Project Management Institute.
(ISBN: 1-930699-45-X. Source: http://www.pmi.org.)

RiskWatch - RiskWatch Information Security product Suite includes software for vulnerability assessments, risk analyses and compliance reviews of information systems specifically for ISO/IEC 27002:2005), GLBA-FFIEC, HIPAA, and SOX.
(Source: http://www.riskwatch.com/.)

TR 19: 2005 – Technical Reference for Business Continuity Management. SPRING Singapore, 2005.
(ISBN: 981-4154-13-X. Source: http://www.spring.gov.sg.)

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

Subject Area 4 – Developing Business Continuity Strategies

Sub-Topic #1 CORPORATE SPONSORHSIP	#	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.	• 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.	• 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.	• 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	

Subject Area 4 – Developing Business Continuity Strategies				
Sub-Topic #2 **PRE-PLANNING**	**#**	**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.	• 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.	• 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/drlegistation_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".	• 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.	• Internal Audit • External Audit • Regulatory Requirements (i.e., 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.	• 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).	• Subject Area 1 – Project Initiation and Management. • Subject Area 2 – Risk and Evaluation Control • Subject Area 3 – Business Impact Analysis

Subject Area 4 – Developing Business Continuity Strategies				
Sub-Topic #3 **PLANNING & DEVELOPMENT**	**#**	**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.	• Have a full understanding of Risk Acceptance identified in Subject Area 2 and how it may affect this strategy.	• Subject Area 2 – Risk and Evaluation Control
	2	Ensure that a strategy exists for protecting vital records including electronic and paper	• Identify Vital Records throughout the organization. NOTE: Vital records as defined by your 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.	• ANSI / ARMA 5-2003 – Vital Records: Identifying, Managing, and Recovering Business-Critical Records. • 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.	• Review internal resources (ie: Multiple locations with like business functions & technology) • Search out external business resources using tactics such as Requests for Information (RFI), Queries, Professional Organization reviews etc.	• Third Party Vendors

Subject Area 4 – Developing Business Continuity Strategies				
Sub-Topic #3 **PLANNING & DEVELOPMENT**	**#**	**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: • 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	• 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.	• Develop a Business Statement/Request for Proposal (RFP) which includes: • Review of vendors that provide critical goods & services to your business • 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)	• Appendix 4.5 - Planning & Development – Hot Site RFP

Subject Area 4 – Developing Business Continuity Strategies				
Sub-Topic #3 **PLANNING & DEVELOPMENT**	**#**	**What**	**How**	**Points of Reference**
			• 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.	

External References: Standards, Guidelines & National Practice Publications

ANSI / ARMA 5-2003 – Vital Records: Identifying, Managing, and Recovering Business-Critical Records. ARMA International, March 2003. (ISBN: 1-931786-12-7. Source: http://www.arma.org/.)

ANSI / NFPA 1600:2007 – Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association, March 2007. (Source: http://www.nfpa.org.)

AS/NZS 4360:2004 – Risk Management. Standards Australia /Standards New Zealand, August 2004. (ISBN: 0-7337-5904-1. Source: http://www.saiglobal.com.)

BS 25999-1: 2006 – Business Continuity Management – Part 1: Code of Practice. BSI Business Information, November 2006. (ISBN: 0 580 49601 5. Source: http://www.bsi-global.com.)

Crisis Communications Handbook. Jane's Information Group, January 2005. (ISBN: 0-7106-2596-0. Source: http://catalog.janes.com/catalog/public/index.cfm.)

FFIEC – Business Continuity Planning Booklet. Federal Financial Institutions Examination Council (FFIEC), March 2003. (Source: http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf.)

HB 292: 2006 – Practitioners Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7472-5. Source: http://www.saiglobal.com.)

HB 293: 2006 – Executive Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7488-1. Source: http://www.saiglobal.com.)

ISO/IEC 27002:2005 (ISO/IEC 17799:2005) – Information Technology Security Techniques - Code of Practice for Information Security Management. International Standards Organization, June 2005. (Source: http://www.iso.org.)

NIST 800-30 – Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST), July 2002. (SP 800-30. Source: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.)

Open for Business, Disaster Planning Toolkit for Small to Mid-Sized Business Owners. Institute for Business and Home Safety (IBHS), January 2005. (Source: http://www.ibhs.org/docs/OpenForBusiness.pdf.)

TR 19: 2005 – Technical Reference for Business Continuity Management. SPRING Singapore, 2005. (ISBN: 981-4154-13-X. Source: http://www.spring.gov.sg.)

DRII/BCI Professional Practice Narrative:

- Develop and implement procedures to respond to and stabilize the situation following an incident or event. This includes identifying and developing emergency response procedures; identifying command and control requirements and procedures; and defining strategy for salvage and restoration.

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

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #1 **CORPORATE SPONSORSHIP**	**#**	**What**	**How**	**Points of Reference**
Corporate Sponsorship *(Management Commitment)*	1	Identify stakeholders / decision makers.	• Brainstorm with senior management team.	• Subject Area 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.	• 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.	• Work with internal partners (i.e. Risk Management, Audit, Corporate Security, Facilities (Real Estate), Building Management) • 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.	• Subject Area 2: Risk Evaluation and Control • Subject Area 3: Business Impact Analysis • Search Internet for business related white papers

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #1 **CORPORATE SPONSORSHIP**	**#**	**What**	**How**	**Points of Reference**
	4	Identify preventative measures that can minimize the potential disaster from occurring.	• 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. • Short –term vs long-term strategies to reduce and eliminate risks	• Subject Area 2: Risk Evaluation and Control • Subject Area 3: Business Impact Analysis
	5	Develop Emergency Response planning phases.	• Involve internal partners such as Security, Facilities (Real Estate), Life Safety, Risk Management, HR, Communications (internal and external), Legal, Finance/Accounting, Travel, Transportation or others. Also consider key external partners	• Corporate policies and procedures • Subject Area 9: Public Relations and Crisis Communications • Subject Area 10: Coordination with Public Authorities
	6	Develop the strategy: - 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	• Schedule a meeting with Senior Management / Sponsor to present the pros/cons, including financial information, related to implementing an Emergency Response Program.	• www.fema.gov/library/biz2.shtm • Subject Area 2: Risk Evaluation and Control • Subject Area 3: Business Impact Analysis • Subject Area 6: Developing Business Continuity Plans (follow same principals but with an emphasis on Emergency Response)

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #1 **CORPORATE SPONSORSHIP**	**#**	**What**	**How**	**Points of Reference**
	7	Educate Senior Management on their Roles and Responsibilities.	• Partner with Senior Management / Sponsor to document their roles and responsibilities.	• Provide Senior Management a review of the BC process as well as their roles and responsibilities • Subject Area 7: Training and Awareness

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #2 **PLANNING & DOCUMENTING EMERGENCY RESPONSE**	**#**	**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.	• 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. • Model off local ICS	• CERT (Community Emergency Response Team) • Public Health • EMA director, fire chief, mayor, etc. • Subject Area 9: Crisis Communications • Subject Area 10: Coordination with Public Authorities • ICS (Incident Command System)
	2	Partner with the local emergency management agencies to develop response plans for various scenarios initially targeting those identified in the Threat Assessment.	• Contact key representatives from the organizations listed under Points of Reference. • 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.	• CERT (Community Emergency Response Team) • Police, Fire and Rescue, Health Department, Local Emergency Planning Committees, etc. • Subject Area 2: Risk Evaluation and Control • Subject Area 10: Coordination with Public Authorities

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #2 **PLANNING & DOCUMENTING EMERGENCY RESPONSE**	**#**	**What**	**How**	**Points of Reference**
	3	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. 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.	• 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.	• Subject Area 1: Project Initiation and Management • ICS / NIMS, NFPA1600 • Call trees, automated callouts
	4	Maintain team	• Conduct regular scheduled meetings • Update team roster • Conduct drills • Conduct educational / training session	• Subject Area 7: Training and Awareness

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #2 **PLANNING & DOCUMENTING EMERGENCY RESPONSE**	**#**	**What**	**How**	**Points of Reference**
	5	Document the process for activation and the triggers that would result in activation or alert. - Imminent vs pending - Stages of crisis	Develop a procedure that outlines the triggers that would result in an action or alert. - Implement automated notification systems - Maintain contact information - Establish notification timeframes - Develop notification matrix of contact methods during and after business hours - Establish phone trees	• NOAA (National Oceanic & Atmospheric Administration) • WHO (World Health Organization)
	6	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 Area 1: Project Initiation and Management
	7	Establish a Command Center	Determine location(s), resources and procedures for physical and/or virtual Command Centers. - Determine point person for Command Center site(s) that it is to be activated.	

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #2 **PLANNING & DOCUMENTING EMERGENCY RESPONSE**	**#**	**What**	**How**	**Points of Reference**
	8	Establish procedures for evacuation (both internal and external) as well as for sheltering in place.	• Train the appropriate teams and employees in their roles. • Establish procedures to account for employees and visitors. • Consider special evacuation needs.. • 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 (i.e. churches, other businesses). • Pattern with building management.	• Subject Area 2: Risk Evaluation and Control • Subject Area 7: Training and Awareness • Partner with internal and external authorities to ensure compliance with local codes and ordinances
	9	Consider additional safety training opportunities in such areas as fire extinguisher training, CPR/First Aid/AED training, etc.	• 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.	• CERT (Community Emergency Response Team) • Red Cross • Subject Area 7: Training and Awareness • Subject Area 10: Coordination with Public Authorities

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #2 **PLANNING & DOCUMENTING EMERGENCY RESPONSE**	**#**	**What**	**How**	**Points of Reference**
	10	Identify and acquire emergency supplies for Emergency Response Team.	Issue the following to the ER Team: - Vests - Walkie-talkies - Clipboards, etc. - Periodically inventory and replace expired items - Bull Horn	• www.fema.gov
	11	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.	• Obtain supplies • Periodically inventory and replace expired items • Store at Command Center in accessible secured location • Partner with supply chain (internal and/or external)	• American Red Cross Readiness Kit (www.arc.org)

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #2 **PLANNING & DOCUMENTING EMERGENCY RESPONSE**	**#**	**What**	**How**	**Points of Reference**
	12	Develop and document methodology for communicating to employees during an incident. Include processes for when employees are at work as well as after hours.	• Consider implementing an automated notification system. • Develop scripts based on Threat Assessment to be customized at time of event. • Establish hotline for employees. - One-way status line (without ability for caller to leave message); OR - Status Line with capability for caller to leave a message. • Update the status line on a periodic basis. • Implement an awareness campaign. • Document communication plan. • Partner with Corporate Communications for approval of scripts • Identify spokesperson	• Contact Lists • Automated notification system • www.fema.gov • Publish hotline number on company intranet, and/or labels affixed to employee badges. • See Subject Area 7 – Training & Awareness

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #3 **DOCUMENTING AN EMERGENCY RESPONSE PLAN**	**#**	**What**	**How**	**Points of Reference**
Documenting an Emergency Response Plan	1	Establish Crisis Command Centers	Establish one or more centers, appropriate to your environment: primary, secondary, on-site, off-site, virtual, etc.	• www.fema.gov
	2			
	3			
	4			
	5			

Subject Area 5 – Emergency Response and Operations				
Sub-Topic #4 **EXERCISING THE EMERGENCY RESPONSE**	**#**	**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.		
	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.		

External References: Standards, Guidelines & National Practice Publications

ANSI / NFPA 1600:2007 – Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association, March 2007. (Source: http://www.nfpa.org.)

BS 25999-1: 2006 – Business Continuity Management – Part 1: Code of Practice. BSI Business Information, November 2006. (ISBN: 0 580 49601 5. Source: http://www.bsi-global.com.)

Community Emergency Response Teams (CERT). https://www.citizencorps.gov/cert/

FEMA 141: Emergency Management Guide for Business and Industry. FEMA, October 1993. (Source: http://www.fema.gov/pdf/library/bizindst.pdf.)

FEMA IS-700: An Introduction to the National Incident Management System (NIMS). FEMA Independent Study Program. (Source: http://www.training.fema.gov/emiWeb/IS/is700.asp.)

HB 292: 2006 – Practitioners Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7472-5. Source: http://www.saiglobal.com.)

HB 293: 2006 – Executive Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7488-1. Source: http://www.saiglobal.com.)

Open for Business, Disaster Planning Toolkit for Small to Mid-Sized Business Owners. Institute for Business and Home Safety (IBHS), January 2005. (Source: http://www.ibhs.org/docs/OpenForBusiness.pdf.)

TR 19: 2005 – Technical Reference for Business Continuity Management. SPRING Singapore, 2005. (ISBN: 981-4154-13-X. Source: http://www.spring.gov.sg.)

Subject Area #6
Developing and Implementing BC Plans
March 10, 2008

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

Subject Area 6 – Developing and Implementing BC Plans				
Sub Topic #1 **PRE-PLANNING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
Pre-Planning Activities	1	Ensure that an executive sponsor is assigned with oversight and budget authority for plan development and implementation.	• Identify the highest level of management with oversight for the business process, function, or technology being covered by the continuity plan. • Request a person at that level be directly appointed or designate a direct report to sponsor development of the business continuity plan(s). ❑ Executive officers such as the CFO, CIO, and market Presidents / Executives are the preferred sponsors. • Meet with executive sponsor. Review the planning process, expected deliverables, resource requirements, and communication flow for status reporting.	• **Subject Area #1 : Project Initiation and Management** • NFPA 1600:2007. Chapter 4, Program Management. • HB 221:2004. Introduction and Chapter 2.1-Developing the BCM Program, Step 1: Commencement. • HB 292: 2006. Chapter 2, Commencement of BCM; and Section 2.3, Gaining the Commitment of Management, Section 2.6, Gaining the Commitment of Others. • BS 25999-1:2006, Chapter 5 (BCM Programme Management) • NIST SP 800-34: 2002, Contingency Planning for Information Technology Systems.)

Subject Area 6 – Developing and Implementing BC Plans				
Sub Topic #1 **PRE-PLANNING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
			• Determine how, when and by what means they wish to be informed of issues, completion milestones, cost, and progress in plan development.	
	2	Ensure that a business continuity policy is defined.	• The business continuity planning process should be guided by a policy for the organization as a whole. • Areas to be addressed in the Business Continuity Policy include: ❑ Purpose ❑ Goals ❑ Scope ❑ Triggers & Activation ❑ Implementation Process ❑ Compliance Requirements ❑ Glossary • The policy should be applicable across the enterprise. It should also provide high-level directives and implementation requirements for next-level organizations.	• NFPA 1600:2007. Chapter 4 (Program Management). • BS 25999-1:2006. Section 4 (The Business Continuity Policy) • HB 221:2004, Introduction and Chapter 2.1 (Developing the BCM Program, Step 1: Commencement) • HB 292: 2006, Chapter 2 (Commencement of BCM) • Federal Executive Branch Continuity of Operations (COOP), FPC-65, June 15, 2005 • NIST SP 800-34: 2002, Contingency Planning for Information Technology Systems.)

Subject Area 6 – Developing and Implementing BC Plans				
Sub Topic #1 **PRE-PLANNING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
			• Where one does not exist, the executive sponsor should form a team with representatives from key departments to determine the organization's business continuity goals and the process that will be used to achieve them. • The Business Continuity Policy is usually written by a team including representatives from: ❑ Legal ❑ Human Resources ❑ Finance ❑ Risk Management ❑ Business Continuity ❑ key lines of business	
	3	Define, clarify, and develop sponsor communication.	• Communication with sponsors should update them on key issues and milestones in plan development. • If the organization does not have a pre-defined format for progress reports, confer with the sponsor, or designee, to determine what information needs to be included in the communication, how often it	• Subject Area 1. Project initiation and Management • HB 292: 2006. Section 2.6, Gaining the Commitment of Others; and Section 2.13, The Commencement Checklist.

Subject Area 6 – Developing and Implementing BC Plans				
Sub Topic #1 **PRE-PLANNING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
			should be provided, and what methods should be used to present the information • Topics to consider in the sponsor's status report include: o progress on plan completion o major obstacles to plan completion and action needed to overcome them o requests for approval to change scope, budget and / or scheduled completion dates • Appropriate reviews / approvals for planning effort and content may be established using a RACI table. o RACI tables listing the reporting requirements along with the names of those responsible (R), accountable (A), consulted (C), and informed (I) in the process.	
	4	Define scope of activity required to develop the Business Continuity Plan(s).	• Determine which locations, operations and departments business continuity plans will be developed for. (The BIA can be used to determine this.)	• HB 221:2004, Introduction, and Chapter 2.1- Developing the BCM Program, Step 1: Commencement.

Subject Area 6 – Developing and Implementing BC Plans				
Sub Topic #1 **PRE-PLANNING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**

			• Identify key assumptions the business continuity plans are based on.
			• Identify any locations, operations, and departments not being included in the planning process, as determined from interviews with executive management.
			• Develop list of all plans required to ensure integrated recovery of business and technology infrastructure.
			  ❑ Business functions are recovered using the business continuity plans which are developed by the business departments.
			  ❑ Technology infrastructure is recovered using the Disaster Recovery Plan, which is developed by the Information Technology.
			• Incorporate above information into a statement of scope and present to executive sponsor for formal signoff.
				• HB 292: 2006, Chapter 2, Commencement of BCM; and Section 2.7, Establishing the Infrastructure of BCM.
				• NIST SP 800-34: 2002, Contingency Planning for Information Technology.

Subject Area 6 – Developing and Implementing BC Plans				
Sub Topic #1 **PRE-PLANNING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**

	5	Review the organizational structure and identify those in the management hierarchy who will have overall responsibility for business continuity plan development at each level of the organization.	• Identify executive and management owners for all mission-critical business activities.
			  ❑ Mission critical activities are usually those that cannot be delayed or deferred.
			  ❑ They are activities considered vital to the organization's survival.
			• Identify managers of operations and support functions with dependencies on these mission-critical activities.
				• HB 221:2004, Chapter 8, Section 8.04, Identifying Stakeholders and their needs, and Section 8.5, Using IRACI.

	6	Identify team members to be involved in the development of each business continuity plan.	• The Business Continuity team should include
			  ❑ Executive Sponsor
			  ❑ Line-of-Business Leaders
			  ❑ Department Heads and/ or Functional Managers
			  ❑ Process Leaders / Owners
			  ❑ Representatives from Mission-Critical Vendors and / or Suppliers
			• The Business Continuity Team should be lead by a Project Manager.
				• HB 221:2004, Chapter 2, Section 2.09, Resource Allocation.
				• Federal Executive Branch Continuity of Operations (COOP), FPC-65, June 15, 2005.

Subject Area 6 – Developing and Implementing BC Plans				
Sub Topic #1 **PRE-PLANNING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
			• The Project Manager should review team composition to ensure each member has sufficient resources to complete the work assigned. Consider: ❑ Availability ❑ Bandwidth ❑ Technical Expertise ❑ Knowledge of the Business	
	7	Obtain formal approval of executive sponsor for project scope, schedule, resources and metrics. This information is usually contained in a document called the Project Plan or Project Charter.	• Develop the document that identifies: ❑ Project Goal and Objectives ❑ Project Description ❑ Project Scope ▪ Include outsourced and contract support services as well as those provided internally (e.g. IT) ❑ Project Resources ▪ Staffing for plan development, implementation, and maintenance ▪ Tools & Equipment ❑ Business Case ❑ Metrics	• HB 221:2004, Template 11, The BCM Checklist. • Subject Area 3: Business Impact Analysis • HB 221:2004, Chapter 2.1- Developing the BCM Program, Step 5 Developing Resource and Interdependency Requirements; Template 5, Minimum Resource Requirements Worksheet. • HB 292: 2006, Chapter 4, Section 4.4, Identify Resource

Subject Area 6 – Developing and Implementing BC Plans				
Sub Topic #1 **PRE-PLANNING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
			❑ Communications, including project reporting schedule ❑ Project Timeline • Develop forms and templates required to track and monitor status of development and implementation activities, target dates, issue resolution and overall progress of the project. • Develop a presentation to review key elements of Project Plan / Project Charter with the Executive Sponsor and key members of the management team. • Obtain Executive Sponsor's approval.	Requirements; Template for Determining IT Application Dependencies. • FPC 65: 2002, Federal Preparedness Circular, Federal Executive Branch Continuity of Operations (COOP).
	8	Develop plan format and content guidelines.	• Develop Table of Contents, templates and format samples for the business continuity plans. • Identify level of detail required to complete the plan.	
	9	Assemble plan development and implementation teams.	• Develop contact list for plan development and implementation team(s).	• HB 221:2004, Chapter 2.1-Developing the BCM Program, Step 5 Developing Resource and Interdependency Requirements; Chapter 2.2-The BCM Workbook, Template 5,

Subject Area 6 – Developing and Implementing BC Plans				
Sub Topic #1 **PRE-PLANNING ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
				Minimum Resource Requirements Worksheet. • HB 292: 2006, Chapter 4, Section 4.4, Identify Resource Requirements; Chapter 6, Assessing and Collating Resource Requirements; and Appendix G, Example of Consolidated Resource Mapping.

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #2 **GATHERING DATA**	**#**	**What**	**How**	**Points of Reference**
Review Data Needed for Plan Development	1	Review risk assessment and/or Business Impact Analysis to validate which business functions and/or processes should be included in the plan.	• Define threats to the business and its critical functions, e.g.: ❑ hurricane ❑ tornado ❑ flood ❑ wild fire ❑ civil unrest ❑ acts of terrorism ❑ mass transportation breakdowns ❑ utility failures, etc. • Assess the impact of these treats. Areas of impact may include: ❑ regulatory ❑ legal ❑ operations ❑ technology ❑ financial ❑ information and data ❑ physical plant, ❑ brand and image ❑ Regulatory compliance impacts	• NFPA 1600:2007. Chapter 5, 5.3 Risk Assessment. • PAS 56:2003. Guide to Business Continuity Management. Section 6.3, Risk Assessment. • HB 221:2004 Chapter 2.1-Developing the BCM Program, Step 2 Risk and Vulnerability Analysis. • HB 292: 2006, Chapter 3, Section 3.05, Identifying Risks; Section 3.13, The Risk Assessment Checklist; and Appendix B, Sources of Risk. • NIST SP 800-34: 2002, Contingency Planning for Information Technology Systems.) • Subject Area 3: Business Impact Analysis

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #2 **GATHERING DATA**	**#**	**What**	**How**	**Points of Reference**
			• Assess probability using a percentage if known. • If not known, use a scale of 1-3 or 1-5 to rate likelihood of occurrence on a scale of low to high, or on rate of occurrence in a 5, 10, 25 or 50 year timeframe • Assess impact using a dollar value to estimate short and long-term financial loss. • If not known, use a scale of 1-3 or 1-5 to estimate severity of impact on the organization's reputation, its ability to meet regulatory/compliance requirements and its ability to meet contractual obligations. • Calculate the risk. Risk = Probability * Impact ❑ Note: Where impact is seasonal or varies with time, use 'worst case' value, i.e. maximum impact. • Incorporate results into a Risk Matrix. • Prioritize business continuity plan development based on risk.	• HB 221:2004, Standards Chapter 2.1- Developing the BCM Program, Table 1, Examples of Disruption Impacts on the Organization. • HB 292: 2006, Chapter 3, Section 3.6, Analyzing Risk.

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #2 **GATHERING DATA**	**#**	**What**	**How**	**Points of Reference**

	2	➢ Utilize the Business Impact Analysis (BIA) to determine recovery goals, objectives and timeframes to be addressed in the business continuity plan(s).	• Identify and review information contained in the BIA with management team to determine which recovery goals, objectives and timeframes need to be addressed., including but not limited to:
			  all critical business processes and/or systems,
			  Recovery Time Objectives (RTOs),
			  Recovery Point Objectives (RPOs),
			  dependencies (vendors, internal/external suppliers) and
			  cost of operation and recovery during prolonged outages.
			• If any changes are needed, obtain approval from management team and document those changes in the BIA.
			• Identify most appropriate strategy and/or combination of strategies to recover the people, processes, and supporting technology critical to the business. These strategies may include:
			  Alternative site or business facility
			  Warm site
			  Cold Site
				• Subject Area 3: Business Impact Analysis
				• BS 25999-1. Chapter 6 (Understanding the Organization).
				• HB 221:2004. Standards, Chapter 2.1-Developing the BCM Program, Step 3 Business Impact Analysis.
				• HB 292: 2006. Chapter 4, Section 4.3, Confirming Critical Business Functions; 4.7, Identify Maximum Acceptable Outage Times and Recovery Objectives; and 4.11, The BIA Checklist.
				• NIST SP 800-34: 2002, Contingency Planning for Information Technology Systems.

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #2 **GATHERING DATA**	**#**	**What**	**How**	**Points of Reference**
			▯ Drop Ship/Quick ship agreements ▯ Hot-Site Third party service providers ▯ Manual Procedures ▯ Mitigation ▯ Mobile Trailer ▯ Reciprocal agreements ▯ Warm Site ▯ Work from Home (telecommute) • Review recovery strategy with management team. • If changes are needed, document them in business continuity plan goals, objectives and assumptions.	
	3	Document the dependencies with all processes identified as mission critical.	• Identify dependencies between critical processes and support functions. • Document internal and external dependencies required to achieve the recovery objectives, including: ❑ Hardware and software infrastructure ❑ LAN, WAN and telecommunications	• Subject Area 1: Project Initiation and Management • Subject Area 3: Business Impact Analysis

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #2 **GATHERING DATA**	**#**	**What**	**How**	**Points of Reference**
			❑ Vendor and 3rd party products or services ❑ Products and services produced internally ❑ Personnel and facilities • Develop a document that summarizes, or illustrates, the dependencies between mission-critical activities and the processes required to support them. • Include dependencies on other departments internal to the organization as well as those that are external. This summary should ❑ State the Recovery Goal ❑ Review Critical Processes and Dependencies ❑ Identify the Recovery Goal for each Critical Process ❑ Identify the Strategy (or Combination of Strategies) Selected to Meet that Goal	
	4	Identify and list vital records critical to business recovery.	• Identify Vital Records required for recovery. • Identify retention periods for vital	• ANSI / ARMA 5-2003. • Subject Area 3: Business Impact

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #2 **GATHERING DATA**	**#**	**What**	**How**	**Points of Reference**
		Vital Records (as defined by the ANSI/ARMA Vital Records Standard) contain information necessary to □ continue operation or survival of an organization immediately following a crisis □ recreate the organization's legal and financial status □ preserve the rights and obligations of stakeholders, including employees, customers, investors, and citizens.	records including electronic and paper. • Review vital records backup, storage, and retrieval process to ensure consistency with RTO and RPO needs of the business. • Develop list of vital records required by business continuity plan. • Review and update periodically as part of routine plan maintenance.	Analysis • ANSI / ARMA 5-2003
	5	Identify and itemize vendors critical to the organization's mission, core business processes and/or functions as validated in Step 3 above.	• Develop list of vendors and contractors whose services will be required by the business continuity plan. • Review and validate list with management team. • Include name, location, primary and backup contacts for each vendor / contractor on the list. • Review and update periodically as part of routine plan maintenance.	• Subject Area 3: Business Impact Analysis

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #2 **GATHERING DATA**	**#**	**What**	**How**	**Points of Reference**
	6	Identify key customers who will require notification when the business continuity plan is activated.	• Develop list of key customers to be notified when the business continuity plan is activated. • Review/confirm list with management team. • Include name, location, primary and backup contacts for each customer on the list. • Review and update periodically as part of routine plan maintenance.	• Subject Area 3: Business Impact Analysis
	7	Document processes required to achieve Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Note: other phrases which are consistent with RTO are Maximum Acceptable Outage Time (MAO) and Maximum Down Time. Maximum Acceptable Outage (MAO) is the maximum amount of time a system can be unavailable before its loss will compromise the organization's objectives or survival.	• Document tasks and activities required to achieve recovery objectives and timeframes for completion.	• Subject Area 3: Business Impact Analysis • HB 292: 2006. Chapter 4, Section 4.2, Developing Communications for the BIA and Table on Communication and the BIA.

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #3 **DOCUMENTATION & APPLYING DATA TO PLAN**	**#**	**What**	**How**	**Points of Reference**
Plan Documentation Components **And** **Applying Finalized Data to Plan Content**	1	Define key areas that MUST be addressed in the Plan.	Plans must address the organization's: • Legal & Regulatory Requirements • Contractual Obligations • Work Area Recovery Requirements • IT and Telecommunication System Recovery Requirements • Staffing • Recovery Procedures • Disaster analysis, definition, notification and escalation procedures • Backups and alternate worksites.	• NFPA 1600 : 2007, Section 5.8.3, Plans. • PAS 56:2003. Guide to Business Continuity Management. Section 8, Developing and Implementing BCM Plans. • HB 221:2004 Chapter 2.2-The BCM Workbook, Template 6, Continuity Plan Worksheet. • HB 292: 2006, Chapter 7, Section 7.3, Contents of Plans: Specific), and Table on Assurance Issues and Evidence.
	2	General	• Identify plan and plan contents as "Confidential". • If plan is for government or defense departments, apply appropriate security classifications to each section of the document. • Documentation should be understandable and actionable by individuals with expertise in a particular area in the event that key personnel are not available.	

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #3 **DOCUMENTATION & APPLYING DATA TO PLAN**	**#**	**What**	**How**	**Points of Reference**
	3	Assumptions	• Document the assumptions that business continuity plan and recovery is based on. ❑ For example, 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. • Assumptions should clearly define ❑ RTO, RPO, and MAO ❑ availability of recovery site or alternate work environment ❑ notification and response times of support required to implement the business continuity plan.	
	4	Exclusions	• Identify which activities are not covered by the business continuity plan. • Identify, with explanation of reason for doing so, which support processes and resources are specifically excluded from the business continuity plan. • Review exclusions with the management team and obtain approval to develop the plan with these exclusions.	

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #3 **DOCUMENTATION & APPLYING DATA TO PLAN**	**#**	**What**	**How**	**Points of Reference**
	5	Compliance Statements	• Identify any compliance requirements associated with development, maintenance and implementation of the plan. • Flag items in the plan which address key legal and/or regulatory requirements. (This aids audit, reporting and compliance requirements.)	• BS 25999-2 : 2007 Section 5.1 (Internal Audit) • HB 292: 2006, Chapter 9, Maintenance of BCM, Table on Assurance Issues and Evidence. • Federal Executive Branch Continuity of Operations (COOP), FPC-65, June 15, 2005.
	6	Teams	Identify team members, roles, responsibilities and contact information for all teams involved in implementing the plan, including but not limited to: • Names of team leads, members and alternates • Reporting structure • Definition of roles & responsibilities • Contact information including address (with zip code), primary and backup phone numbers in case of emergency,	• Subject Area 4: Developing Business Continuity Strategies
	7	Declaration & Escalation	• Document the disaster notification and declaration process including but not limited to ❑ Plan activation	

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #3 **DOCUMENTATION & APPLYING DATA TO PLAN**	**#**	**What**	**How**	**Points of Reference**
			❑ Team activation ❑ Disaster Declaration authority ❑ Team notification and call-out procedure(s) ❑ Call Trees	
	8	Supporting Resources	• Identify each supporting resource • Identify which upstream and which downstream resources are required for the plan to meet its recovery objectives • Identify the interface requirements for each supporting resource ❑ Identify critical metrics (physical, timing, etc.) for each resource • Reference external documents by title, section and page number as needed to balance plan detail with overall document size. • Use terminology commonly known by members of the business continuity team • Define any terms not commonly known in a glossary and include as appendix material to the plan.	• Subject Area 3: Business Impact Analysis • Subject Area 4: Developing Business Continuity Strategies

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #3 **DOCUMENTATION & APPLYING DATA TO PLAN**	**#**	**What**	**How**	**Points of Reference**
	9	Controls	• Document recovery activities and Plan components requiring controls. • Explain objective and purpose of the control. Identify metrics and team member responsible for implementing the control(s) • Identify and/or cite authority (policy, regulatory, compliance, etc., and person) requiring the control • Identify incident management and controls required during plan implementation. For example: ❑ Expense reporting and signature authority limits ❑ Inventory control and tracking	
	10	Recovery Process Flow	• If the sequence of events in the business continuity plan can be displayed graphically, it will help to illustrate when different parts of the plan are executed and when resources are needed. • Identify upstream and downstream dependencies ❑ Upstream dependencies are defined by the organization's need fore goods and services in	

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #3 **DOCUMENTATION & APPLYING DATA TO PLAN**	**#**	**What**	**How**	**Points of Reference**
			recovering its mission-critical business activities and implementing the plan. ❑ Downstream dependencies are defined by the need of clients, customers, and others requiring goods and services from the organization. • Identify each external supporting resource (to include supply chain) • Use product and process flows, graphics, and illustrations as needed to identify the sequence of activities in plan implementation. • Validate product and process flows with the management team to ensure they are accurate and consistent with the business activities being recovered.	
	11	Plan and Sub-Plan Organization	• Where necessary to simplify or segregate the work required for the recovery of mission-critical activities, complex plans and recovery procedures may be broken into sub plans that can be executed by individual teams. • Each sub plan should provide specific information for its team(s) and define their procedures for:	• Subject Area 4: Developing Business Continuity Strategies • Subject Area 5: Emergency Response and Operations • Subject Area 9: Public relations and Crisis Coordination • NFPA 1600 : 2007.

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #3 **DOCUMENTATION & APPLYING DATA TO PLAN**	**#**	**What**	**How**	**Points of Reference**
			❑ Notification and Activation ❑ Command and Control ❑ Internal Communication (e.g. employees and members of the organization) ▪ This should include a set of pre-scripted and pre-approved messages for scenarios most likely to cause business interruption. ❑ External Communication (e.g. Media and the press) ▪ This should include a set of pre-scripted and pre-approved messages for scenarios most likely to cause business interruption. ❑ Recovery of technology infrastructure & tools plan ❑ Recovery of work area ❑ Recovery of staff and human resources ❑ Recovery of mission critical operations, including workarounds	Section 5.8.3, Plans. • BS 25999-2 : 2007. Section 4.3 (Developing and Implementing a BCM Response). • HB 221 : 2004, 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. · • HB 292 : 2006, Chapter 7, Writing the Plan, Section 7.2, Contents of Plans: Generic, and Section 7.3, Contents of Plans: Specific, and Table on Assurance Issues and Evidence.

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #3 **DOCUMENTATION & APPLYING DATA TO PLAN**	**#**	**What**	**How**	**Points of Reference**
			❑ Recovery from supply chain disruption	
	12	Appendix Material	• Plans and sub plans may require additional material for ease of reference in plan implementation. This includes information related to: ❑ Validation schedule ❑ Key contacts ❑ Lists of vendors and suppliers ❑ Off-site locations and vendor contacts for ▪ retrieval of vital records ▪ activation of hot-site, alternate workplaces and facilities where personnel will relocate ❑ Graphics that will assist in plan implementation including: ▪ maps ▪ floor & site layouts, ▪ photos ▪ organization charts, ▪ process and recovery flows	

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #3 **DOCUMENTATION & APPLYING DATA TO PLAN**	**#**	**What**	**How**	**Points of Reference**
			❑ Inventories of equipment and supplies ❑ Requirements for ▪ Expense reporting and record keeping ▪ Event tracking ▪ Regulatory and legal compliance.	

Subject Area 6: Developing and Implementing BC Plans				
Sub Topic #4 **FOLLOW-UP ACTIVITIES**	**#**	**What**	**How**	**Points of Reference**
Plan Maintenance and Update **(i.e. Continuous Improvement)**	1	Perform scheduled and/or unscheduled plan review • Scheduled reviews are conducted annually or bi-annually • Unscheduled reviews are conducted as major changes occur in product, process, personnel, and/or facilities	• Schedule regular review of plans and recovery procedures. • Schedule audit of recovery and continuity plans. • Document changes to plans and sub plans.	• BS 25999-2 : 2007. Section 6.2 (Continual Improvement)
	2	Post-Incident Documentation	• Once teams have deactivated, debrief Emergency Response, Crisis Management and Business Continuity teams. • Review status reports and gather data. • 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.	

External References: Standards, Guidelines & National Practice Publications

ANSI / ARMA 5-2003 – Vital Records: Identifying, Managing, and Recovering Business-Critical Records. ARMA International, March 2003. (ISBN: 1-931786-12-7. Source: http://www.arma.org/.)

ANSI / NFPA 1600:2007 – Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association, March 2007. (Source: http://www.nfpa.org.)

AS/NZS 4360:2004 – Risk Management. Standards Australia /Standards New Zealand, August 2004. (ISBN: 0-7337-5904-1. Source: http://www.saiglobal.com.)

BS 25999-1: 2006 – Business Continuity Management – Part 1: Code of Practice. BSI Business Information, November 2006. (ISBN: 0 580 49601 5. Source: http://www.bsi-global.com.)

BS 25999-2: 2007 – Business Continuity Management – Part 2: Specification. BSI Business Information, November 2007. (ISBN: 978-0-580-59913-2. Source: http://www.bsi-global.com.)

Business Continuity Guideline, A Practical Approach to Emergency Preparedness, Crisis Management, and Disaster Recovery. ASIS International, 2005. (Source: http://www.asisonline.org/guidelines/guidelinesbc.pdf.)

Federal Information System Controls Audit Manual (FISCAM), January 1999. GAO. (Source: http://www.gao.gov/special.pubs.)

FFIEC – Business Continuity Planning Booklet. Federal Financial Institutions Examination Council (FFIEC), March 2003. (Source: http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf.)

Federal Information System Controls Audit Manual. General Accounting Office (GAO), July 1999. (Source: http://www.gao.gov/special.pubs/mgmtpln.pdf)

HB 292: 2006 – Practitioners Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7472-5. Source: http://www.saiglobal.com.)

HB 293: 2006 – Executive Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7488-1. Source: http://www.saiglobal.com.)

ISO/IEC 27002:2005 (ISO/IEC 17799:2005) – Information Technology Security Techniques - Code of Practice for Information Security Management. International Standards Organization, June 2005. (Source: http://www.iso.org.)

ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements. International Standards Organization, October 2005. (Source: http://www.27001.com/.)

NARA – Primer on Disaster Preparedness, Management, and Response for Paper-Based Materials. National Archives and Records Administration (NARA), October 1993.
(Source: http://www.archives.gov/preservation/emergency-prep/disaster-prep-primer.pdf.)

NIST 800-30 – Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST), July 2002. (SP 800-30. Source: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.)

Open for Business, Disaster Protection and Recovery Planning Toolkit for Small to Mid-Sized Business Owners. Institute for Business and Home Safety (IBHS), 2007. (Source: http://www.disastersafety.org/business_protection/.)

PAS 56: 2003. Guide to Business Continuity Management.
(NOTE: This document has been replaced by BS25999 Business Continuity Management)

PMBOK: 2004 – Project Management Body of Knowledge, 2004 Edition. Project Management Institute.
(ISBN: 1-930699-45-X. Source: http://www.pmi.org.)

RiskWatch - RiskWatch Information Security product Suite includes software for vulnerability assessments, risk analyses and compliance reviews of information systems specifically for ISO/IEC 27002:2005), GLBA-FFIEC, HIPAA, and SOX.
(Source: http://www.riskwatch.com/.)

TR 19: 2005 – Technical Reference for Business Continuity Management. SPRING Singapore, 2005.
(ISBN: 981-4154-13-X. Source: http://www.spring.gov.sg.)

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

Subject Area 7 – Awareness and Training				
Sub-Topic #1 **TRAINING & AWARENESS**	**#**	**What**	**How**	**Points of Reference**

Subject Area 7 – Awareness and Training				
Sub-Topic #1 **TRAINING & AWARENESS**	**#**	**What**	**How**	**Points of Reference**
Training and Awareness	1	Establish objectives and components of Corporate BCM Awareness and Training Program	• 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

Subject Area 7 – Awareness and Training				
Sub-Topic #1 **TRAINING & AWARENESS**	**#**	**What**	**How**	**Points of Reference**
	2	Identify Functional Awareness and Training requirements	• 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	Subject Area 6: Developing Business Continuity Strategies Network Reliability Interoperability Council (NRIC) Standard

Subject Area 7 – Awareness and Training				
Sub-Topic #1 **TRAINING & AWARENESS**	**#**	**What**	**How**	**Points of Reference**
	3	Develop Awareness and Training Methodology	• Determine who target audience is • Determine if Training Materials will be the same for all audiences • Determine if Training should be put on LAN for easy access (e.g. Lotus Notes Database) • Determine if Training is Mandatory or Volunteer (recommend making it mandatory like Anti-Money Laundering or Code Of Ethics training) • 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	• 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	

Subject Area 7 – Awareness and Training				
Sub-Topic #1 **TRAINING & AWARENESS**	**#**	**What**	**How**	**Points of Reference**
	5	Identify external Awareness and Training Opportunities	• 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	• Lessons learned from previous tests and exercises and actual incidents should be built into the testing cycle • Keep apprised of industry trends for BC Training Programs	Subject Area 8: Maintaining and Exercising Plans
	7	Develop and Deliver various types of Training Programs (i.e. Computer based, classroom, test-based and instructional guides and templates	• 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	Subject Area 8: Maintaining and Exercising Plans

Subject Area 7 – Awareness and Training				
Sub-Topic #1 **TRAINING & AWARENESS**	**#**	**What**	**How**	**Points of Reference**
	8	Develop Awareness Programs (i.e. Management, Team Members, New Employee Orientation and current employee refresher program)	• 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 Awareness 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	

Subject Area 7 – Awareness and Training				
Sub-Topic #1 **TRAINING & AWARENESS**	**#**	**What**	**How**	**Points of Reference**
	9	Identify Other Opportunities for Education	• Attend conferences/meetings of the following: ➢ 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.

External References: Standards, Guidelines & National Practice Publications

ANSI / NFPA 1600:2007 – Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association, March 2007. (Source: http://www.nfpa.org.)

BS 25999-1: 2006 – Business Continuity Management – Part 1: Code of Practice. BSI Business Information, November 2006. (ISBN: 0 580 49601 5. Source: http://www.bsi-global.com.)

Business Continuity Guideline, A Practical Approach to Emergency Preparedness, Crisis Management, and Disaster Recovery. ASIS International, 2005. (Source: http://www.asisonline.org/guidelines/guidelinesbc.pdf.)

FEMA 141: Emergency Management Guide for Business and Industry. FEMA, October 1993. (Source: http://www.fema.gov/pdf/library/bizindst.pdf.)

FEMA IS-700: An Introduction to the National Incident Management System (NIMS). FEMA Independent Study Program. (Source: http://www.training.fema.gov/emiWeb/IS/is700.asp.)

HB 292: 2006 – Practitioners Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7472-5. Source: http://www.saiglobal.com.)

HB 293: 2006 – Executive Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7488-1. Source: http://www.saiglobal.com.)

ISO/IEC 27002:2005 (ISO/IEC 17799:2005) – Information Technology Security Techniques - Code of Practice for Information Security Management. International Standards Organization, June 2005. (Source: http://www.iso.org.)

ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements. International Standards Organization, October 2005. (Source: http://www.27001.com/.)

Open for Business, Disaster Planning Toolkit for Small to Mid-Sized Business Owners. Institute for Business and Home Safety (IBHS), January 2005. (Source: http://www.ibhs.org/docs/OpenForBusiness.pdf.)

TR 19: 2005 – Technical Reference for Business Continuity Management. SPRING Singapore, 2005. (ISBN: 981-4154-13-X. Source: http://www.spring.gov.sg.)

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

Subject Area 8 – Maintaining and Exercising BC Plans				
Sub-Topic #1 **MAINTAINING QUALITY REVIEW PROGRAM**	**#**	**What**	**How**	**Points of Reference**
Maintaining – Quality Review Program	1	Reference Subject Area 6		
	2	Minimum requirement of corporate standard plan content and frequency of updates.	• Understand what your corporate and regulatory standards are.	
	3	Plan component review: • Review contact info at least quarterly • Review requirements at least semi-annually • Review procedures at least annually	• Require each location review plan components periodically.	
	4	Make other reviews when organizational changes require, including workarea and physical environments.	• Incorporate major organizational changes into plan	
	5	Ensure consistency with plan content guidelines established in Plan Development practice.	• Review plan to ensure consistency with other content guidelines.	

Subject Area 8 – Maintaining and Exercising BC Plans				
Sub-Topic #1 **MAINTAINING QUALITY REVIEW PROGRAM**	**#**	**What**	**How**	**Points of Reference**
	6	Management reporting – status of comparison to standards.	• Report findings to senior management and issues to BRC.	• Sample Heat map/reporting examples.
	7	Change Management Processes (address proactive and reactive points).	• Integrate IT DRP and BCP with existing change management processes, and SDLC efforts. • Identify Change Management triggers.	• Organizations Program Mgmt guidelines. • Organization's System Development Lifecycle (SLDC) framework.
	8	Base any quality requirements on existing regulations (e.g., audit, legal, ISO, SOX, HIPAA, FINRA).	• Consider all existing regulations governing your organization and build quality requirements around them	

Maintaining and Exercising BC Plans				
Sub-Topic #2 EXERCISING	**#**	**What**	**How**	**Points of Reference**
Exercising	1	Develop exercise strategies.	• Identify and define objectives for overall exercise program.	• To be assessed on a strategic basis.
	2	Develop exercise objectives and scope.	• Consider all risks when developing exercise. • Identify and document testing approaches and types to be used (phased walkthrough, simulation procedural, etc.…)	
	3	Identify pre-planning steps as per test type.	• Define "outcome"/ ultimate deliverable for test.	
	4	Use scorecard to grade objectives – scoring mechanism to grade objectives.	• Develop a scorecard to grade objectives. • Identify measurements to success.	
	5	Conduct exercise.		
	6	Manage/track exercise actions.	• Develop a process to track actions to confirm closure.	

Maintaining and Exercising BC Plans				
Sub-Topic #2 EXERCISING	**#**	**What**	**How**	**Points of Reference**
	7	Publish post-mortem issues tracking and summary.	• Identify issues resulting from test, assignments for resolutions, and target completion dates.	

Maintaining and Exercising BC Plans				
Sub-Topic #3 **DISCUSSION BASED EXERCISES**	**#**	**What**	**How**	**Points of Reference**
Exercising – Discussion-based	1	Execute an interactive walkthrough of a documented plan	• Discuss scenario against documented plan	
	2	Hold tabletop exercises to facilitate the understanding of policy, roles & responsibilities, response and recovery approach and priorities	• Bring critical functions into a conference room to discuss response to a scenario	
	3	Execute with individual business units (aka departments)	• Develop a scenario for a single business unit	
	4	Execute with several units together as a joint exercise	• Develop a scenario for multiple business units	

Maintaining and Exercising BC Plans				
Sub-Topic #3 **OPERATION BASED EXERCISES**	**#**	**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	• Exercise the documented notification process	
	2	Hold relocation exercises	• Move critical functions to planned recovery location to validate location is acceptable	
	2a	Functional	• Technology: O/S restore: restore systems or applications without interfaces. Business: Single business units or particular processes (functions).	
	2b	Integrated	• 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.	

Maintaining and Exercising BC Plans				
Sub-Topic #3 **OPERATION BASED EXERCISES**	**#**	**What**	**How**	**Points of Reference**
	2c	Comprehensive	• Technology: All systems & components of the production site. Business: All units from same site validating capabilities for all functions for a given risk tier.	

External References: Standards, Guidelines & National Practice Publications

ANSI / NFPA 1600:2007 – Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association, March 2007. (Source: http://www.nfpa.org.)

BS 25999-1: 2006 – Business Continuity Management – Part 1: Code of Practice. BSI Business Information, November 2006. (ISBN: 0 580 49601 5. Source: http://www.bsi-global.com.)

Business Continuity Guideline, A Practical Approach to Emergency Preparedness, Crisis Management, and Disaster Recovery. ASIS International, 2005. (Source: http://www.asisonline.org/guidelines/guidelinesbc.pdf.)

FEMA 141: Emergency Management Guide for Business and Industry. FEMA, October 1993. (Source: http://www.fema.gov/pdf/library/bizindst.pdf.)

HB 292: 2006 – Practitioners Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7472-5. Source: http://www.saiglobal.com.)

HB 293: 2006 – Executive Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7488-1. Source: http://www.saiglobal.com.)

ISO/IEC 27002:2005 (ISO/IEC 17799:2005) – Information Technology Security Techniques - Code of Practice for Information Security Management. International Standards Organization, June 2005. (Source: http://www.iso.org.)

ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements. International Standards Organization, October 2005. (Source: http://www.27001.com/.)

Open for Business, Disaster Planning Toolkit for Small to Mid-Sized Business Owners. Institute for Business and Home Safety (IBHS), January 2005. (Source: http://www.ibhs.org/docs/OpenForBusiness.pdf.)

TR 19: 2005 – Technical Reference for Business Continuity Management. SPRING Singapore, 2005. (ISBN: 981-4154-13-X. Source: http://www.spring.gov.sg.)

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, social media, etc.)

Expert / Distinguished Reviewer: Gwen Shintani, MBCP, MBCI (Review Completed - 9/10/2014)

Subject Area 9 – Public Relations and Crisis Coordination				
Sub-Topic #1 PLANNING	**#**	**What**	**How**	**Point of Reference**
Assessment	1	Research and document previous incidents and or existing processes to conduct gap and determine next steps	• Identify experience level necessary.	
			• Identify requirements and potential liabilities based on gap analysis.	
			• Identify existing processes and plans.	
			• Identify Industry best practices and lessons learned.	
			• Identify vulnerabilities	
Planning	1	Ensure the company's Communications Department has identified key resources designated to initiate crisis communications with employees, business partners, vendors, the public, government and external media (including social media).	• Have senior management identify any additions or deletions of key resources. • Consider including: government, employees, customers, media / Communications Department, business partners, vendors, social media, etc. • Obtain senior management approval on sponsorship for designated and trained internal resources.	• Stakeholder listing (company, rep. name, primary and alternate contact information, etc.) • Implement standard sign-off forms or agreements as evidence of approval.
	2	Develop objectives and individual commitments.	• Identify accountabilities and measurements to success.	• Subject Area 1: Project Initiation & Managment
	3	Identify Industry Professional Practices, media, local, state and federal agencies.	• Reach out to focus groups to gain insights into various organizations. • Message mapping to identify data points • Contact and engage external/first responders, inviting them to participate	• Association of Contingency Planners (www.acp-international.org), • DRII (www.drii.org)

Subject Area 9 – Public Relations and Crisis Coordination				
Sub-Topic #2 DEVELOP	**#**	**What**	**How**	**Point of Reference**
Develop	1	Develop Crisis Communication Plans with internal personnel (management, staff, response teams, etc.)	• Obtain contact (during and after business hours) information for personnel. • Establish notification lists for Senior Management. • Establish notification lists for Crisis Management teams. • Call tree update. • Establish notification lists for internal departments. • Establish notification lists for other response teams. • Identify backup for each item noted above.	
	2	Document procedures and identify tools to manage relationships and communications process with external partners: business partners, governmental agencies, vendors, social media, etc.	• 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.	

Subject Area 9 – Public Relations and Crisis Coordination				
Sub-Topic #2 **DEVELOP**	**#**	**What**	**How**	**Point of Reference**
	3	Develop Crisis Communication Plans with the Media (including Social Media)	• 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. • Develop methods of communication (notification). • Message alert process. • Conference numbers developed.	
	4	Develop an Awareness and Education Program for Staff and Management	• 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. • Continued re-enforcement of updates with employees (check in process, critical data, etc…).	• Subject Area 7: Awareness and Training

Subject Area 9 – Public Relations and Crisis Coordination				
Sub-Topic #2 **DEVELOP**	**#**	**What**	**How**	**Point of Reference**
	5	Establish communication methods (i.e., 800 number, website, pager distribution lists, conference lines, social media, sms, automated call system, etc.)	• Develop and distribute awareness and training related to communication methods. • 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.	

Subject Area 9 – Public Relations and Crisis Coordination				
Sub-Topic #3 **IMPLEMENT**	**#**	**What**	**How**	**Point of Reference**
Implement	1	Contain media personnel during an event.	• Work with physical security and management to direct media personnel to designated location(s).	
	2	Educate employees to direct media inquiries to the Communications Department.	• Print and distribute memo instructing employees to direct any media inquires to the PR Department	
	3	Rollout of process as defined.	• TBD	

Subject Area 9 – Public Relations and Crisis Coordination				
Sub-Topic #4 EXERCISE	**#**	**What**	**How**	**Point of Reference**
Exercise	1	Develop Exercise	• Determine participants. • Schedule times and locations.	• Subject Area 8: Maintaining and Exercising BC Plans
	2	Facilitate Exercise	• Monitor the progress and keep everyone on a time schedule.	• Subject Area 8: Maintaining and Exercising BC Plans
	3	Involve appropriate external parties during exercise events.	• Extend invitations to department representatives to participate in the exercise. • Carefully select the time during the event to involve the media, if at all.	• Subject Area 8: Maintaining and Exercising BC Plans

Subject Area 9 – Public Relations and Crisis Coordination				
Sub-Topic #5 MAINTAIN	**#**	**What**	**How**	**Point of Reference**
Maintain	1	• Identify objectives and plans required for update.	• Establish document change control to record Crisis Communication Plan changes.	• HB292:2006- Practitioners Guide to Business Continuity Management.

External References: Standards, Guidelines & National Practice Publications

ANSI / NFPA 1600:2004 – Standard on Disaster Management and Business Continuity Programs. National Fire Protection Association, January 2004. (Source: http://www.nfpa.org.)

BS 25999-1: 2006 – Business Continuity Management – Part 1: Code of Practice. BSI Business Information, November 2006. (ISBN: 0 580 49601 5. Source: http://www.bsi-global.com.)

Business Continuity Guideline, A Practical Approach to Emergency Preparedness, Crisis Management, and Disaster Recovery. ASIS International, 2005. (Source: http://www.asisonline.org/guidelines/guidelinesbc.pdf.)

Crisis Communications Handbook. Jane's Information Group, January 2005.
(ISBN: 0-7106-2596-0. Source:

FFIEC – Business Continuity Planning Booklet. Federal Financial Institutions Examination Council (FFIEC), March 2003. (Source: http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf.)

HB 292: 2006 – Practitioners Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7472-5. Source: http://www.saiglobal.com.)

HB 293: 2006 – Executive Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7488-1. Source: http://www.saiglobal.com.)

Open for Business, Disaster Planning Toolkit for Small to Mid-Sized Business Owners. Institute for Business and Home Safety (IBHS), January 2005. (Source: http://www.ibhs.org/docs/OpenForBusiness.pdf.)

TR 19: 2005 – Technical Reference for Business Continuity Management. SPRING Singapore, 2005.
(ISBN: 981-4154-13-X. Source: http://www.spring.gov.sg.)

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

Subject Area 10 – 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 Department of Homeland Security (US), emergency management, fire, police, public utilities and your local & nationally elected public officials.	• 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.	Examples of groups and individuals to know: • 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 • National Security Terrorism organization.

Subject Area 10 – Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	2	Understand potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to your location and industry	• 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 • Know regulations and courses that may be required to obtain access to cordoned off areas – need to be credentialed	Examples of when this knowledge may be important: • 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 Examples of organizations: • EHMA-East Harris County Manufacturers Association • LEPC-Local Emergency Planning Committee • Industry associations • Area support groups ○ Building & "block" associations • Neighborhood Associations Lobbying points of reference: • Direct and association lobbying efforts • Zoning commissions • Appraisal District Boards • Water supply boards

Subject Area 10 – 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).	• 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.	Match expertise with requirement • PIO (Public Information Officer) • PR (Public Relations Officer) • Technical staff interface • Fire team • Hazmat team • Facilities support Example groups include: • Area councils • Local Emergency Planning Committee (LEPC) • Volunteers Active During Disaster (VOAD) • Citizen Emergency Response Team (CERT) Note: Lists are not all inclusive
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.	• 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	• ICS (Incident Command System) forms • Process flow charts • Communication interface forms • Staffing forms • Contact lists • Chemical descriptions & affects • Forms required for 3rd party Security Firms NOTE: A reference to NIIMS can also be provided.

Subject Area 10 – 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.	• 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.	• 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 Public authority groups examples: • Fire • Police or Deputy Police • National Guard Volunteer and non-Profit group examples: • Volunteer fire • CERT-Citizen Emergency Response Team • LEPC-Local Emergency Planning Committee • The ARC • Salvation Army • Baptist men Public-private incident management partnership examples: http://www.mnisac.org/ https://www.chicagofirst.org/ http://www.pittsburghcoalitionforsecurity.org/ http://www.bensbusinessforce.org http://mnisac.org/Partnerships-Homeland-Security.htm

Subject Area 10 – 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.	• 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.	Examples of sources to monitor include: • NWS (National Weather Service) email service • - Website "Alert" pages • Court (legal system) notifications through business journals, website, etc. 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 Local Metro traffic cameras (Houston) http://www.houstontranstar.org/
Preparedness	7	Ensure information that may be required immediately by public authorities during an incident is readily available.	• 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.	Examples of information required: • 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 Note: List is not all inclusive

Subject Area 10 – Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	8	Document the levels of support available to your organization's response and recovery Plan.	• 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. • Determine how next of kin notification will be addressed.	• 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.	• 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 ingress and egress issues such as timing with other business, etc.	Examples of access issues: • "All clear" parameters • Evacuation and return routes • Official escape and return routes of personal and commercial roadways, waterways and airway • Special transport routes (chemical, size, etc.) Note: List is not all inclusive
Preparedness	10	Identify and document organizational and other resources potentially available in support of public authorities and other organizations.	• 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	Examples of supporting resources: • CERT-Citizen Emergency Response Team • Sea ports • EOC Centers -Emergency (or Joint) Operation Centers

Subject Area 10 – Coordination with External Agencies				
Sub-Topic	**#**	**What**	**How**	**Points of Reference**
			validation scenarios. • Include information gathered in internal risk assessment and mitigation processes • 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.	• Evacuation support centers • Fire facilities • Hospitals, • Key vendors, • LEPC-Local Emergency Planning Committee resources • Television & Radio stations • National Guard • Police • Red Cross • Supply warehouses • United Way • Salvation Army • Baptist Men **Share item examples:** • 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

Subject Area 10 – Coordination with External Agencies				
Sub-Topic	**#**	**What**	**How**	**Points of Reference**
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 risk assessment process.	• 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. • 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.	Examples studies, assessments etc.: • Flood plain maps • Risk assessments • Monitoring systems • Road extensions • Bridge capacities • Land use studies • Debris Management Examples of where to obtain information: • Department of Transportation (DOT) • Environmental Protection Agency (EPA) • Regional Councils (HGAC Houston Galveston Area Council) • Googleearth.com • Floodsmart.gov Note: List is not all inclusive

Subject Area 10 – Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	12	Document organizations staff members that may be a member of a public authority or support group.	• 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	Public authority groups examples: • Fire • Police or Deputy Police • National Guard or any military affiliation Volunteer and non-Profit group examples: • Volunteer fire • CERT-Citizen Emergency Response Team • LEPC-Local Emergency Planning Committee • Salvation Army • Baptist men • Defense Force - Note: List is not all inclusive
Preparedness	13	Document local and regional supporting infrastructure resources.	• 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: • Roadmaps • Contour maps • Pipelines • Waterlines • Power plants and grids • Communication lines & hubs • Railroads • Bridges • Water and fuel supplies • Airports
Preparedness	14	Obtain a copy of and review the Emergency Operations Procedures of the Local Authorities,	• 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: • Fire • Police • Transportation department • HAZMAT

Subject Area 10 – Coordination with External Agencies

Sub-Topic	#	What	How	Points of Reference
Preparedness	15	Participate in local Emergency Management, Business Continuity and other organizations that support your industry.	• 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: • 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
Preparedness	16	Utilize an accepted standard of incident command format that interfaces with local/regional/etc. authorities and their implementation.	• 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.	• National Incident Management System (NIMS) • Incident Command System (ICS) forms
Preparedness	17	Review public authority and 3rd party support activities with industry peers & other company offices.	• 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	• Association of Contingency Planners

Subject Area 10 – Coordination with External Agencies				
Sub-Topic	**#**	**What**	**How**	**Points of Reference**
Preparedness	18	Determine requirements to participate in National Programs.	• 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	• 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 Note: List is not all inclusive

Subject Area 10 – 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.	• 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.	Examples of sources to monitor: 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 • Pacific Disaster Center http://www.pdc.org/core_rva.php • Houston area Metro http://www.houstontranstar.org/
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.	• Assign event documentation responsibility • Maintain effective documentation forms and process • Include gathered documentation in the internal response, emergency and recovery procedures and operational procedures.	• ICS (Incident Command System) forms • Process flow charts (RTO, RPO, etc.) • Communication interface forms • Staffing forms • Contact and contacted lists • Procedure changes & issues occurring

Subject Area 10 – 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.	• 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: • 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.	• 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: • Hazardous material spills • Fires • Bomb threats • Construction activities • Unusual (visible) activities

Subject Area 10 – 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	• 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 • Obtain check lists of what authorities will review to prevent liability issues	Training examples to consider: • 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 Exercise examples to consider: • Fire drills • Terrorist drills • Hazardous material drills • Evacuation drills • Emergency Operations Center (EOC). Note: Lists are not all inclusive
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.	• 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 • Obtain check lists of what authorities will review to prevent liability issues	Training to consider sharing includes: • Documentation validations Certification process • Table-tops • Walk-throughs • Component validations • Equipment maintenance procedures Note: List is not all inclusive

Subject Area 10 – 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.	• 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: • Newspapers • Trade and association newsletters • Television and radio announcements • Websites of the public authority and participating organizations Note: List is not all inclusive
Training/Exercise & Awareness	4	Notify and include authorities in organizational exercises where applicable.	• 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.	• Up coming exercises • Fire Drills

Subject Area 10 – 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.	• 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: • 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.	• 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	• Exercises • Fire Drills • Actual events
Post Event or Exercise	3	Participate in post event public discussions and round-tables.	• 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 • Prepare by reviewing released event information • Monitor local papers, etc. to determine when & where information will be released.	• Forums • Workshops • Conferences • Networking events

Subject Area 10 – Coordination with External Agencies				
	#	**What**	**How**	**Points of Reference**
Post Event or Exercise	4	Coordinate future internal exercises and objectives with local authorities.	• 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	

External References: Standards, Guidelines & National Practice Publications

ANSI / NFPA 1600:2007 – Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association, March 2007. (Source: http://www.nfpa.org.)

BS 25999-1: 2006 – Business Continuity Management – Part 1: Code of Practice. BSI Business Information, November 2006. (ISBN: 0 580 49601 5. Source: http://www.bsi-global.com.)

Business Continuity Guideline, A Practical Approach to Emergency Preparedness, Crisis Management, and Disaster Recovery. ASIS International, 2005. (Source: http://www.asisonline.org/guidelines/guidelinesbc.pdf.)

Crisis Communications Handbook. Jane's Information Group, January 2005. (ISBN: 0-7106-2596-0. Source: http://catalog.janes.com/catalog/public/index.cfm.)

FEMA 141: Emergency Management Guide for Business and Industry. FEMA, October 1993. (Source: http://www.fema.gov/pdf/library/bizindst.pdf.)

FEMA IS-700: An Introduction to the National Incident Management System (NIMS). FEMA Independent Study Program. (Source: http://www.training.fema.gov/emiWeb/IS/is700.asp.)

HB 292: 2006 – Practitioners Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7472-5. Source: http://www.saiglobal.com.)

HB 293: 2006 – Executive Guide to Business Continuity Management. Standards Australia /Standards New Zealand, June 2006. (ISBN: 0-7337-7488-1. Source: http://www.saiglobal.com.)

Open for Business, Disaster Planning Toolkit for Small to Mid-Sized Business Owners. Institute for Business and Home Safety (IBHS), January 2005. (Source: http://www.ibhs.org/docs/OpenForBusiness.pdf.)

TR 19: 2005 – Technical Reference for Business Continuity Management. SPRING Singapore, 2005. (ISBN: 981-4154-13-X. Source: http://www.spring.gov.sg.)