

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

Subject Area 4 – Developing Business Continuity Strategies

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

Subject Area 4 – Developing Business Continuity Strategies

Sub-Topic #3	#	What	How	Points of Reference
PLANNING & DEVELOPMENT				
Planning & Development	1	Identify and incorporate risk mitigation strategies from the output of Subject Area 2 Risk Evaluation and Control.	<ul style="list-style-type: none"> Have a full understanding of Risk Acceptance identified in Subject Area 2 and how it may affect this strategy. 	<ul style="list-style-type: none"> Subject Area 2 – Risk and Evaluation Control
	2	Ensure that a strategy exists for protecting vital records including electronic and paper	<ul style="list-style-type: none"> Identify Vital Records throughout the organization. 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. 	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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.	<p>Review the following types of recovery alternatives and be prepared to make recommendations:</p> <ul style="list-style-type: none"> • Alternative site or business facility • Cold, Warm or Hot Sites • Drop Ship/Quick ship agreements • Manual Procedures • Mitigation • Mobile Trailer • Reciprocal agreements • Work from Home <p>Note: List may not be all inclusive</p>	<ul style="list-style-type: none"> • Appendix 4.4 - Planning & Development Recovery Alternative Definitions • Appendix 4.4 - Planning & Development Recovery Alternate Strategy Matrix
Planning & Development (Cont'd)	5	Assess the feasibility of available resources and solutions for the continuity/recovery of business processes.	<ul style="list-style-type: none"> • Develop a Business Statement/Request for Proposal (RFP) which includes: <ul style="list-style-type: none"> • Review of vendors that provide 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) 	<ul style="list-style-type: none"> • Appendix 4.5 - Planning & Development – Hot Site RFP

Subject Area 4 – Developing Business Continuity Strategies

Sub-Topic #3	#	What	How	Points of Reference
PLANNING & DEVELOPMENT			<ul style="list-style-type: none"> • Develop a cost benefit analysis and an implementation timeline for each strategy. • Compare the cost ranges along with the advantages and disadvantages to implement each strategy. • Present concise and specific recommendations to management. (The cost benefit analysis should be used to justify all recommendations) • Implement solution. 	

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.ffiiec.gov/ffiiecinfobase/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/>.)