DRII/BCI Professional Practice Narrative:

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

Generally Accepted Practices (GAP) Notice:

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

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 process within the organization and expectations. 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 accurate data. • Determine specific, repeatable, testable, clear, and concise questions on the BIA that will yield expected results.	Depending on the complexity and size of the organization, you may want to consider separating the risk assessment and the business impact analysis into two separate efforts. In general the smaller the organization the easier to combine them and the larger the organization the more efficient it may be to separate them.

Subject Area 3 – Business Impact Analysis				
Sub-Topic #1 **EXECUTIVE SPONSORSHIP**	**#**	**What**	**How**	**Points of Reference**
			• Be prepared to show the benefits and value of the BIA process upfront (beyond the BCP). Executive management will gain a more objective view of the threats and risks to operations. Based upon this knowledge, management can make an informed decision on the risk tolerance it will accept. • Oftentimes, there are hidden benefits in conducting a BIA initiative. Be prepared to identify and communicate these benefits to executive management. (Examples: some hidden benefits might include: Identifying outdated technologies, unrealistic spending, integration issues with other organizational groups, business process improvement, redundancy of effort, outsourcing issues) • Develop appropriate executive management reporting avenues to report status, activities, risks, constraints and bottlenecks. • Conduct abbreviated executive level workshops. • You absolutely must have executive/senior management buy-in or you will have been set-up for failure in completing a successful BIA. • 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.	

Subject Area 3 – Business Impact Analysis				
Sub-Topic #1 **EXECUTIVE SPONSORSHIP**	**#**	**What**	**How**	**Points of Reference**
	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 for a list of time critical processes/functions to focus on if there is little time to complete a detailed BIA process. Determine what executive management wants covered if time is of the essence. • Poll executive management as to any known pitfalls or issues that may impede your progress to conduct and complete the BIA process.	

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. Often, the significance of a business process/function is overlooked because there may be no direct financial impact. However, the operational impact to the organization may be just as or even more significant to the organization. Measure whatever is important to your specific organization. • Choose impact levels using the most significant peak period for each business process/function. This may be at the end of a month, quarter or year, or according to seasonal trends in the business process. • A detailed definition of each of the impact levels must be established based on the specific industry. • A scale for quantifying the operational impacts must be established in order to ensure all process/functions are measured the same. For example, a scale of 1 – 4 could be used with the following definitions: 1 = no impact, 2 = moderate impact, 3= serious impact and 4 = severe impact. Another scale example to consider would be using a Low (L), Medium (M) or High (H) Impact scale for quantifying the impacts over each time period. 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: ➢ Market Share ➢ Reputation

Sub-Topic #3 **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 jeopardize recovery efforts if employees aren't paid in a timely manner. • A contract may state penalties for missed deadlines or deliverables, or it may not be specific to the exact recourse the organization has. • Some operational impacts are intangible. If data is lost that cannot be restored, it may be an intangible impact as it can't be attached to a direct sum of money.	Examples financial impacts may include, but not be limited to: ➢ Lost revenue ➢ Property damage ➢ Deferred income ➢ Penalties and Fines ➢ Lawsuits ➢ Cost of duplicating inventory Refer to Appendix A (**ED**: Additional Reference is needed for this item.)

Sub-Topic #3 **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 force an RTO for a business process/function. Forced recovery time objectives do not take into consideration changes of roles at time of disaster and impacts to downstream business processes and/or dependencies. If a BIA tool is used that assigns an RTO based on any sort of risk rating, there must be a process in place to override an RTO upon management review. • The RTO is used by corporate support teams to assess possible recovery strategies for the business process/function. • Assume total loss to ensure an apples-to-apples comparison of impacts. At this stage of the BIA, it is a natural step for the interviewer and the interviewee to discuss possible recovery strategies. Do not launch into recovery strategy discussions at this point; consider no recovery capability exists when determining where in time the process must recover. Determine what the point in time should be for the business process to recover.	

Sub-Topic #3 **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. Determine if there is a need to separate internal dependency impact information from external dependency impact information. • Identify supply chain links to other internal departments, Information technology infrastructure (internal and external applications, systems, voice and data network data, etc.), processes, or other third parties. Examples of third parties could be vendors, business partners, customers, etc. • Consider the loss to your organization should an outsourced service provider(s) not be able to meet your business requirements. Consider any service level agreements and/or contractual requirements in place (include international contractual relationships that may exist). • What are the inflows? When is it needed? From whom does the process/function receive information, data, requests, etc.? What does the process/function depend on for the information or resources to perform the process/function?	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

Sub-Topic #3 **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.	
Sub-Topic #3 **BIA TOOLS**	6	Determine central repository for BIA data	• 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	Examples of how BIA data can be gathered: ➢ One-on-one interviews ➢ Management /supervisor workshops ➢ Conference calls ➢ Electronic (not recommended) ➢ Questionnaire

Sub-Topic #4 **BIA PROCESS**			organization as a whole. Additionally, BIA questions will be interpreted differently by each interviewee. • As appropriate, schedule a meeting with the business/function manager to collaboratively complete the BIA questionnaire. Send out BIA questionnaire in advance so that the recipients can review it with others and get complete answers. • Explain the purpose of the BIA initiative to the interviewees. Make it clear that management has no hidden agenda such as having interviewees justify their jobs via the BIA process. It is helpful to explain that every department/ employee is important to the organization. One of the objectives is for executive management to learn what business process/function is time critical should a disaster occur. • Conduct interview and complete the questionnaire. Ensure consistency in interviewee(s) understanding of questions throughout the process. • Design and conduct follow-up interviews. If information is still missing after the interview, follow-up with the interviewee and request it be provided (e.g. financial dollar impacts may need to be provided by a finance department that supports the business process/function and not readily available).	

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 and 2. the next highest level of management. • Consider the appropriateness of using a sign off form of some kind to formally indicate the appropriate level management has reviewed and approved the BIA results. • It is important to note that information contained in the approved BIA will be communicated to others with supporting roles in planning for the recovery of the process/function such as Facilities, Telecom, IT, etc.	
	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 2: Risk Evaluation and Control

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.)