

**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

| <b>Subject Area 2 – Risk Evaluation and Control</b> |          |             |            |                            |
|---|----------|-------------|------------|----------------------------|
| <b>Sub-Topic #1</b>                                 | <b>#</b> | <b>What</b> | <b>How</b> | <b>Points of Reference</b> |
| <b>ID RISK / LOSS<br/>POTENTIAL</b>                 |          |             |            |                            |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #1<br>ID RISK / LOSS<br>POTENTIAL                           | # | What  | How   | Points of Reference  |
|---|---|---|---|--|
| <b>Identify Potential Risks to the Organization / Loss Potentials</b> | 1 | Identify exposures from both internal and external sources, which may include: <ul style="list-style-type: none"> <li>• Natural, man-made, technological, or political</li> <li>• Accidental vs. intentional</li> <li>• Internal vs. external</li> <li>• Controllable risks vs. those beyond the organization’s control</li> <li>• Events with prior warnings vs. those with no prior warnings</li> </ul> | <ul style="list-style-type: none"> <li>• Research past disasters in geographical area</li> <li>• Research past disasters in industry</li> <li>• Research past disasters in related industries</li> <li>• Research past disasters internally within organization</li> <li>• Utilize Business Impact Analysis (BIA) discussion / development for internal functions</li> <li>• Identify interdependencies to other organizations, systems, etc.</li> <li>• Research past disasters within your interdependent organizations               <ul style="list-style-type: none"> <li>– geographical, industry, related industries, and internal)</li> <li>– connectivity, communication, security</li> </ul> </li> <li>• Prepare analysis grid showing the threats, risks, controllable factors (internal / external, accidental / intentional, with / without warning, controllable / uncontrollable)</li> </ul> | <ul style="list-style-type: none"> <li>• Federal Emergency Management Agency (FEMA) website</li> <li>• State Emergency Management Organization websites</li> <li>• Local Police and Fire Departments</li> <li>• Business Continuity Publications</li> <li>• Newspapers</li> <li>• Internal Company Records</li> <li>• Building Management</li> <li>• Internal Interview Sessions (leading to BIA development)</li> <li>• Third-Party Disclosures (leading to BIA development)</li> <li>• Analysis Grid Example (Develop)</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #1<br>ID RISK / LOSS<br>POTENTIAL | # | What  | How   | Points of Reference  |
|---|---|---|---|--|
|   | 2 | Determine the probability of the above events | <ul style="list-style-type: none"> <li>• Validate credibility of information sources</li> <li>• Determine impacts to the organization</li> <li>• Research available historical probability factors</li> <li>• Analyze historical probability against degree of environmental change (e.g. increased threat of terrorism today may require adjustment to historical probability)</li> <li>• Analyze mitigating controls in place</li> <li>• Determine additional controls that could be implemented</li> <li>• Analyze probability that each identified threat could occur</li> <li>• Analyze probability of impact occurring as a result of each of the identified threats</li> <li>• Analyze effectiveness of current and potential mitigating controls</li> </ul> | <ul style="list-style-type: none"> <li>• Federal Emergency Management Agency (FEMA) website</li> <li>• State Emergency Management Organizations</li> <li>• Local Police and Fire Departments</li> <li>• Business Continuity Publications</li> <li>• Newspapers</li> <li>• Internal Company Records</li> <li>• Internal Interview Sessions (leading to BIA development)</li> <li>• Third-Party Disclosures (leading to BIA development)</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #1<br>ID RISK / LOSS<br>POTENTIAL | # | What                                     | How  | Points of Reference   |
|---|---|--|--|---|
|   | 3 | Develop methods of information gathering | <ul style="list-style-type: none"> <li>• Partner with Internal Audit to learn of existing risks</li> <li>• Partner with local emergency management agency for a historical impact to business addresses</li> <li>• Network with local Business Continuity Planners</li> <li>• Research the FEMA website for declared disasters in the area</li> <li>• Research the “neighbors” in the general vicinity (may be indirectly impacted by potential chemical hazards, political targets, etc.)</li> <li>• Map nearest “transportation highways” to business location (e.g. auto, train, flight paths)</li> <li>• Identify single points of failure (e.g. gas, water, electricity, fiber cable, critical vendors)</li> <li>• Subscribe to Business Continuity publications</li> <li>• Sign-up for FEMA and State Emergency Management newsletters</li> <li>• Arrange for visiting speakers from local organizations</li> <li>• Attend Business Continuity seminars</li> </ul> | <ul style="list-style-type: none"> <li>• FEMA Website/newsletters</li> <li>• State Emergency Management website/newsletters</li> <li>• Networking meetings</li> <li>• Seminars/presentations</li> <li>• Local Business Continuity Organizations</li> <li>• Business Continuity publications</li> <li>• Local Police / Fire Department / Utility Companies</li> <li>• Highway Departments</li> <li>• Internal Audit</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #1<br>ID RISK / LOSS<br>POTENTIAL | # | What  | How   | Points of Reference   |
|---|---|---|---|---|
|   | 4 | Develop a method to evaluate probability vs. severity | <p>Assess and incorporate the following elements into a method customized for the organization involved:</p> <ul style="list-style-type: none"> <li>• Determine current annual loss potential associated with each identified risk</li> <li>• Determine frequency factor (no. times per year) for each risk</li> <li>• Multiply annual loss potential by the frequency factor to determine annual loss exposure (ALE)</li> <li>• Determine likelihood of simultaneous risks occurring</li> <li>• Determine total simultaneous loss exposure</li> <li>• Determine effectiveness of mitigating controls with reducing or eliminating risk (recalculate ALE as if controls were all in place)</li> <li>• Determine costs of mitigating controls</li> <li>• Determine recovery requirements</li> <li>• Determine expected recovery time using actual test experience (preferred), industry experiences, or expert estimations</li> <li>• Adjust ALE to show loss for expected recovery time with and without suggested controls in place</li> </ul> | <ul style="list-style-type: none"> <li>• Probability formula from DRII training materials</li> <li>• Internal Cost/Benefit guidelines and practices</li> <li>• Actual cost figures</li> <li>• Subject Matter Expert (SME) Estimations</li> <li>• ISO 7799 Standards Methodology</li> <li>• Auditor Organization Standards &amp; Process</li> <li>• Federal (e.g. FFIEC)</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #1<br>ID RISK / LOSS<br>POTENTIAL | # | What   | How   | Points of Reference  |
|---|---|--|---|--|
|   | 5 | Establish ongoing support of evaluation process        | <ul style="list-style-type: none"> <li>• Prepare costs/benefit statement</li> <li>• Prepare qualitative loss statement, e.g. potential for loss of life</li> <li>• Prepare executive presentation summarizing analysis results and source information</li> <li>• Demonstrate validity of presented information with test results, industry experiences, etc.</li> <li>• Obtain upper management championship of effort</li> </ul> | <ul style="list-style-type: none"> <li>• Internal Cost/Benefit guidelines and practices</li> <li>• Internal Presentation guidelines and practices</li> <li>• Subject Matter Expert (SME) Estimations and Support</li> <li>• Certification as Business Continuity Planner</li> <li>• Knowledge of industry standards / best practices</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |
|   | 6 | Identify relevant regulatory and/or legislative issues | <ul style="list-style-type: none"> <li>• Consult Legal department and/or outside counsel</li> <li>• Consult internal Compliance officers</li> <li>• Consult internal Business Area management</li> <li>• Research federal rules and regulations for industry</li> <li>• Research state rules and regulations for industry</li> </ul>  | <ul style="list-style-type: none"> <li>• Internal/external Legal Council</li> <li>• Internal Compliance Officers</li> <li>• Federal and State websites</li> </ul>  |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #2<br><b>DETERMINE EXPOSURE TO LOSS</b>                         | # | What   | How  | Points of Reference  |
|---|---|--|--|--|
| <b>Determine the Organization's Specific Exposures to Loss Potentials</b> | 1 | Establish process to assess identified loss potential  | Develop method to estimate loss potential that considers: <ul style="list-style-type: none"> <li>• Value of assets</li> <li>• Value of labor and opportunity costs</li> <li>• Frequency and duration estimates of each threat category</li> <li>• Mitigation effects of existing safeguards</li> </ul> Review exposure information | <ul style="list-style-type: none"> <li>• Internal Accounting / Finance Department</li> <li>• Internal Risk Management Department</li> <li>• Insurance Contacts / Information</li> <li>• Building Management</li> <li>• Local / County Emergency Management</li> <li>• FEMA</li> <li>• Local Police / Fire, Homeland Security</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |
|   | 2 | Categorize exposures: <ul style="list-style-type: none"> <li>• Primary exposures the organization may face (e.g. hurricane)</li> <li>• Secondary / collateral events that could materialize because of such exposures (e.g. wind damage, roof collapse)</li> </ul> | Create an exposure categorization table with two sections – primary exposures and secondary / collateral events that lists: <ul style="list-style-type: none"> <li>• Exposure Name and / or Cause</li> <li>• Loss Potential – Single Occurrence</li> <li>• Loss Potential – Annual Exposure</li> </ul>                             | <ul style="list-style-type: none"> <li>• Internal Accounting / Finance Department</li> <li>• Internal Risk Management Department</li> <li>• Insurance Contacts / Information</li> </ul>  |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #2<br>DETERMINE<br>EXPOSURE<br>TO LOSS | # | What           | How  | Points of Reference   |
|--|---|----------------|--|---|
|  | 3 | Rank exposures | <p>Identify potential losses:</p> <ul style="list-style-type: none"> <li>• Staff</li> <li>• Facility</li> <li>• Area</li> <li>• Data</li> <li>• Telecommunications</li> <li>• Channels of distribution</li> </ul> <p>Prioritize exposure categorization table by ranking and sorting by:</p> <ul style="list-style-type: none"> <li>• Exposures most likely to occur</li> <li>• Exposures with greatest impact (worst case)</li> </ul> | <ul style="list-style-type: none"> <li>• Internal Accounting / Finance Department</li> <li>• Internal Risk Management Department</li> <li>• Insurance Contacts / Information</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #3<br>CONTROLS & SAFEGUARDS TO MITIGATE   | # | What                   | How   | Points of Reference   |
|---|---|------------------------|---|---|
| <b>Identify Controls and Safeguards to Prevent and/or Mitigate the Effect of the Loss Potential</b> | 1 | Environmental Controls | Identify: <ul style="list-style-type: none"> <li>• Physical Access (buildings, rooms, grounds)</li> <li>• Geographic Location (incidents)</li> <li>• Utilities</li> </ul>   | <ul style="list-style-type: none"> <li>• Building Management</li> <li>• FFIEC Guidelines – Federal Financial Institutions Examination Council</li> <li>• Auditors Organizations (Auditnet.org)</li> <li>• Internal Audit</li> <li>• National Institute of Standards and Technology</li> <li>• Risk Management Organizations</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |
|   | 2 | Technical Controls     | Identify: <ul style="list-style-type: none"> <li>• Data Security</li> <li>• Network Security</li> <li>• Quality Assurance (ongoing controls)</li> <li>• Data &amp; Media Administration</li> <li>• Assets (physical inventory)</li> </ul> | <ul style="list-style-type: none"> <li>• Information Systems Audit and Control Association</li> <li>• National Institute of Standards and Technology</li> <li>• Auditor Organizations (Auditnet.org)</li> <li>• AS/NZS4360:2004 Risk Management</li> <li>• Internal Audit</li> </ul>  |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #3<br>CONTROLS &<br>SAFEGUARDS<br>TO MITIGATE | # | What                 | How  | Points of Reference  |
|---|---|----------------------|--|--|
|   | 3 | Operational Controls | Identify: <ul style="list-style-type: none"> <li>• Strategic Business Objectives</li> <li>• Policies</li> <li>• Procedures</li> <li>• Administration</li> <li>• Legal / Regulatory Requirements</li> <li>• Key Personnel (personnel roles)</li> <li>• Supply Chain (Vendors)</li> <li>• Federal Authorities</li> <li>• State Authorities</li> <li>• Local Authorities</li> <li>• Industry Standards (audit methods)</li> </ul> | <ul style="list-style-type: none"> <li>• FFIEC Guidelines – Federal Financial Institutions Examination Council</li> <li>• Auditors Organizations (Auditnet.org)</li> <li>• Internal Audit</li> <li>• Risk Management Organizations</li> <li>• National Institute of Standards and Technology</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |
|   | 4 | Reputation Controls  | Identify: <ul style="list-style-type: none"> <li>• Media Sources</li> <li>• Internal Communications</li> <li>• External Communications</li> </ul>  | <ul style="list-style-type: none"> <li>• DisasterCenter.com</li> <li>• Risk Management Organizations</li> <li>• Internal Audit</li> <li>• Internal PR / HR Departments</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul>   |
|   | 5 | Effectiveness        | Identify: <ul style="list-style-type: none"> <li>• Impacts of recommended mitigation options:                             <ul style="list-style-type: none"> <li>– Testing Options</li> <li>– Risk Assumption</li> <li>– Risk Avoidance</li> <li>– Risk Limitations</li> <li>– Risk Transference</li> </ul> </li> </ul>  | <ul style="list-style-type: none"> <li>• National Institute of Standards and Technology</li> <li>• Internal Audit</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul>  |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #4   | # | What  | How  | Points of Reference  |
|--|---|---|--|--|
| <b>RISK ANALYSIS<br/>METHODOLOGY<br/>&amp; TOOLS</b>   |   |   |  |  |
| <b>Identify, Evaluate, Select, and Use Appropriate Risk Analysis Methodologies and Tools, and Expertise Needed</b> | 1 | Identify alternative risk analysis methodologies, tools, and sources of internal and external expertise     | Type of measurement: <ul style="list-style-type: none"> <li>• Qualitative methodologies / tools</li> <li>• Quantitative methodologies / tools</li> </ul> Type of process: <ul style="list-style-type: none"> <li>• Manual Process</li> <li>• Interview                             <ul style="list-style-type: none"> <li>- In person</li> <li>- Videoconference</li> <li>- Teleconference</li> </ul> </li> </ul> Automated Process - Email<br>Combination of manual and automated | <ul style="list-style-type: none"> <li>• NIST SP 800-30 Risk Management Guide for Information Technology Systems</li> <li>• FISCAM, pp. 16, 17, 18</li> <li>• ISO/IEC 27002:2005 – Assessing Security Risks, pg. IX.</li> <li>• <a href="http://www.bettermanagement.com/risk-analysis">http://www.bettermanagement.com/risk-analysis</a></li> <li>• RiskWatch</li> <li>• RiskPac</li> <li>• Identify existing data/analysis</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |
|  | 2 | Evaluate alternative risk analysis methodologies, tools, and sources of internal and external expertise     | Evaluate advantages and disadvantages of options: <ul style="list-style-type: none"> <li>• Reliability / confidence factor</li> <li>• Basis of mathematical formulas used</li> </ul>   | <ul style="list-style-type: none"> <li>• Product/service references</li> <li>• Industry publications</li> <li>• External expertise / actuarial guidance</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul>  |
|  | 3 | Select appropriate methodology, tool(s), and external expertise needed for organization-wide implementation | <ul style="list-style-type: none"> <li>• Identify target population for data collection</li> <li>• Identify any specific requirements, e.g. regulatory, financial, etc.</li> </ul>   | <ul style="list-style-type: none"> <li>• Internal legal counsel</li> <li>• Internal / external audit</li> </ul>  |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #4<br>RISK ANALYSIS<br>METHODOLOGY<br>& 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 | <ul style="list-style-type: none"> <li>• Utilize and enhance risk assessment performed in prior steps (see above)</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #5<br>INFORMATION<br>GATHERING<br>ACTIVITIES         | # | What  | How   | Points of Reference   |
|--|---|---|---|---|
| <b>Identify and Implement Information-Gathering Activities</b> | 1 | Develop a strategy consistent with business issues and organizational policy                  | <ul style="list-style-type: none"> <li>• Establish support (tone from the top)</li> <li>• Decide what areas, groups and locations will be covered.</li> <li>• Determine breadth and depth of information to be gathered.</li> <li>• Confirm consistency with organizational policy.</li> <li>• Determine storage location, access control, and update frequency</li> </ul>                    | <ul style="list-style-type: none"> <li>• Board of Directors</li> <li>• Corporate Champion</li> <li>• Legal</li> <li>• Financial</li> <li>• Internal Audit</li> </ul>              |
|  | 2 | Develop a strategy that can be managed across business divisions and organizational locations | <ul style="list-style-type: none"> <li>• Determine collection criteria:                             <ul style="list-style-type: none"> <li>– Business unit down to base level</li> <li>– Location centric include all businesses.</li> </ul> </li> <li>• Allow for reorganization and location changes.</li> <li>• Are there single points of failure that need special attention?</li> </ul> | <ul style="list-style-type: none"> <li>• Corporate Champion</li> <li>• Business Unit Managers</li> <li>• Site Managers</li> <li>• Business Continuity Program Office</li> </ul>   |
|  | 3 | Develop risk assessment form  | <ul style="list-style-type: none"> <li>• Develop clear concise format.</li> <li>• Allow for some flexibility</li> <li>• Ensure that each area is self-explanatory.</li> <li>• Create toolkit / cover package to explain each area.</li> <li>• Ensure distribution method is consistent.</li> </ul>  | <ul style="list-style-type: none"> <li>• Business Continuity Program Office</li> <li>• Business Managers</li> <li>• Key Stakeholders</li> <li>• Sample of participants</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #5<br>INFORMATION<br>GATHERING<br>ACTIVITIES | # | What  | How   | Points of Reference  |
|--|---|---|---|--|
|  | 4 | Create organization-wide methods of information collection and distribution | <ul style="list-style-type: none"> <li>• Deliver and follow-up - forms and questionnaires</li> <li>• Schedule interviews with appropriate individuals at the Business level, with additional follow-ups as needed</li> <li>• Conduct cross-group or large-group meetings for data gathering. Determine status meeting schedule.</li> <li>• Ensure appropriate individuals are committed to conduct documentation review.</li> <li>• Analyze to ensure that the process supports data collected, not a predetermined outcome.</li> </ul> | <ul style="list-style-type: none"> <li>• Business Continuity Program Office</li> <li>• Business Managers</li> <li>• Key Stakeholder</li> <li>• Sample of participants</li> </ul>   |
|  | 5 | Conduct formal risk assessment  | <ul style="list-style-type: none"> <li>• Update forms and questionnaires early in the process if deficiencies are determined</li> <li>• Use a consistent process for interviews; do not vary from the questionnaire without updating and re-interviewing earlier participants</li> <li>• Conduct group meetings as needed. Status meetings on predetermined schedule.</li> <li>• Perform consistent documentation review of input. Determine areas for further research / follow-up.</li> </ul>   | <ul style="list-style-type: none"> <li>• Corporate Champion</li> <li>• Business Unit Managers</li> <li>• Site Managers</li> <li>• Program Office</li> <li>• Business Managers</li> <li>• Key Stakeholder</li> <li>• Other named participants</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #5<br>INFORMATION<br>GATHERING<br>ACTIVITIES | # | What                               | How  | Points of Reference  |
|--|---|------------------------------------|--|--|
|  | 6 | Document risk assessment findings. | <ul style="list-style-type: none"> <li>• Analyze and publish, as scheduled, top level and detailed results supported by forms and interviews.</li> <li>• Store accumulated information as outlined in Section 1</li> </ul> | <ul style="list-style-type: none"> <li>• Board of Directors</li> <li>• Corporate Champion</li> <li>• Legal</li> <li>• Financial</li> <li>• Internal Audit</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #6   | #        | What   | How   | Points of Reference   |
|--|----------|--|---|---|
| <b>EVALUATE CONTROLS &amp; SAFEGUARDS</b>                    |          |  |   |   |
| <b>Evaluate the Effectiveness of Controls and Safeguards</b> | <b>1</b> | Develop communications flow with other internal departments / divisions and external service providers   | <ul style="list-style-type: none"> <li>• Identify control assessment team members both internal and external</li> <li>• Review types of controls in place—physical and procedural</li> <li>• Review goal of the control—deter or lessen the loss</li> <li>• Discuss actual experience and test result findings associated with each control</li> </ul>  | <ul style="list-style-type: none"> <li>• Subject Area 1: Project Initiation and Management</li> <li>• Business Management</li> <li>• Internal Suppliers</li> <li>• Internal Risk Management</li> <li>• Compliance Officers</li> <li>• Technical staff</li> <li>• External Vendors</li> </ul>  |
|  | <b>2</b> | Establish business continuity service level agreements for both supplier and customer organizations and groups within and external to the organization | <ul style="list-style-type: none"> <li>• Review Business Impact Assessment (BIAs) to determine service levels required to meet the stated Recovery Time Objectives (RTO's) and other requirements</li> <li>• Perform cost/benefit associated with meeting defined standards</li> <li>• Discuss cost/benefit results with business management</li> <li>• Agree upon standards to be delivered and penalties for non-performance</li> <li>• Document and sign formal service level agreement</li> <li>• Setup process to monitor service level performance</li> </ul> | <ul style="list-style-type: none"> <li>• Subject Area 3: Business Impact Analysis</li> <li>• Business Management</li> <li>• Internal Suppliers</li> <li>• Legal Counsel</li> <li>• Compliance Officers</li> <li>• Internal Risk Management</li> <li>• Legal Regulatory Requirements</li> <li>• External Vendors</li> <li>• Technical staff</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #6<br><br>EVALUATE<br>CONTROLS &<br>SAFEGUARDS | # | What   | How   | Points of Reference   |
|--|---|--|---|---|
|  | 3 | Develop preventive and pre-planning options  | <ul style="list-style-type: none"> <li>• Identify gaps in control process and available options to close them</li> <li>• Complete Cost / benefit for options                             <ul style="list-style-type: none"> <li>- Capital investment</li> <li>- Maintenance Costs</li> <li>- Benefit derived</li> <li>- Training required</li> </ul> </li> <li>• Determine implementation priorities, procedures, and control</li> <li>• Develop test plan and remediation process</li> <li>• Audit functions and responsibilities</li> </ul> | <ul style="list-style-type: none"> <li>• Business Management</li> <li>• Internal Suppliers</li> <li>• Internal Risk Management</li> <li>• Technical staff</li> <li>• External Vendors</li> <li>• Internal Audit</li> <li>• Legal Counsel</li> <li>• Compliance Officers</li> </ul>  |
|  | 4 | Understand options for risk management and selection of appropriate or cost-effective response, i.e. risk avoidance, transfer, or acceptance of risk | <ul style="list-style-type: none"> <li>• Develop security practices</li> <li>• Identify methods to minimize the effects of the loss potential</li> <li>• Brief participants, ensuring they understand their objectives and reporting structure</li> <li>• Develop interface with suppliers and utilities</li> </ul>   | <ul style="list-style-type: none"> <li>• Business Management</li> <li>• Internal Suppliers</li> <li>• Internal Risk Management</li> <li>• Technical staff</li> <li>• External Vendors</li> <li>• Internal Audit</li> <li>• Legal Counsel</li> <li>• Compliance Officers</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #6                                      | # | What   | How  | Points of Reference   |
|---|---|--|--|---|
| <b>EVALUATE<br/>CONTROLS &amp;<br/>SAFEGUARDS</b> | 5 | Develop recommendations for improved backup and restoration procedures | <ul style="list-style-type: none"> <li>• Review above defined controls, gaps, costs and benefits</li> <li>• Develop a recommendations document based on the above information</li> <li>• Partner with internal and external resources to validate and refine the recommendations document</li> </ul> | <ul style="list-style-type: none"> <li>• Legal counsel</li> <li>• Internal Risk Management</li> <li>• Internal Audit</li> <li>• Legal / regulatory requirements</li> <li>• Industry sources</li> <li>• Records management vendor</li> <li>• Business process owners</li> <li>• Business process staff</li> <li>• Australian Standards Practitioners Guide to Business Continuity HB292: 2006</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #7  | #        | What   | How   | Points of Reference   |
|---|----------|--|---|---|
| <b>EVALUATE RISKS, CONTROLS &amp; MITIGATION ALTERNATIVES</b> | <b>1</b> | Establish disaster scenarios based on risks to which the organization is exposed                     | Develop disaster scenarios based on the following criteria: <ul style="list-style-type: none"> <li>• Magnitude of severity (e.g. ability to perform business)</li> <li>• Critical dates / times</li> </ul>  | <ul style="list-style-type: none"> <li>• DRII.org</li> </ul>  |
|   | <b>2</b> | Evaluate risks   | Classify risks according to relevant criteria, including: <ul style="list-style-type: none"> <li>• Risks under the organization’s control</li> <li>• Risks beyond the organization’s control</li> <li>• Exposures with prior warnings (e.g. tornadoes, hurricanes)</li> <li>• Exposures with no prior warnings (e.g. earthquakes, terrorist attacks)</li> </ul> | <ul style="list-style-type: none"> <li>• FFIEC Guidelines – Federal Financial Institutions Examination Council</li> <li>• Auditors Organizations (Auditnet.org)</li> <li>• National Institute of Standards and Technology</li> <li>• AS/NZS4360:2004 Risk Management</li> </ul> |
|   | <b>3</b> | Evaluate impact of risks and exposures on those factors essential for conducting business operations | <ul style="list-style-type: none"> <li>• Availability of personnel</li> <li>• Availability of information technology</li> <li>• Availability of communications technology</li> <li>• Availability of external capabilities (vendors, insurance, etc.)</li> </ul>  | <ul style="list-style-type: none"> <li>• Internal personnel</li> <li>• AS/NZS4360:2004 Risk Management</li> <li>•</li> </ul>  |
|   | <b>4</b> | Re-evaluate previously identified controls   | <ul style="list-style-type: none"> <li>• Categorize controls                             <ul style="list-style-type: none"> <li>- Preventive</li> <li>- Reactive</li> </ul> </li> <li>• Calculate impacts of controls based on previous risks and exposures analysis</li> <li>• Recommend changes to controls if necessary</li> </ul>                           | <ul style="list-style-type: none"> <li>• Internal Audit</li> </ul>  |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #7  | # | What   | How   | Points of Reference  |
|---|---|--|---|--|
| <b>EVALUATE RISKS, CONTROLS &amp; MITIGATION ALTERNATIVES</b> |   |  | <ul style="list-style-type: none"> <li>- Partner with Internal Audit</li> <li>- Recommend implementation of a BCP oversight committee.</li> </ul>   |  |
|   | 5 | Evaluate controls and recommend changes, if necessary, to reduce impact due to risks and exposures | <ul style="list-style-type: none"> <li>• Preventive controls to inhibit impact exposures (e.g. passwords, smoke detectors, and firewalls)</li> <li>• Reactive controls to compensate for impact of exposures (e.g. hot sites)</li> <li>• Incorporate business continuity / disaster recovery procedures in all change management requests within the IT / IS environment</li> <li>• 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)</li> <li>• Partner with Internal Audit to highlight the need-to-resolve issues</li> <li>• Recommend implementation of an oversight committee to approve and review an on-going business continuity program</li> </ul> | <ul style="list-style-type: none"> <li>• Internal Audit</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #8<br>SECURITY | # | What  | How   | Points of Reference  |
|--------------------------|---|---|---|--|
| <b>Security</b>          | 1 | Identify the organization's possible security exposures | Identify the specific categories of risk which may affect the organization: <ul style="list-style-type: none"> <li>• Physical security of all premises, internal and external</li> <li>• Information security, including computer room and media storage area; on site and off site</li> <li>• Communications security, including voice and data communications</li> <li>• Network security, including Intranet and Internet</li> <li>• Personnel security</li> </ul> | <ul style="list-style-type: none"> <li>• Legal counsel</li> <li>• Internal Risk Management</li> <li>• Internal audit</li> <li>• Legal / regulatory requirements</li> <li>• Industry sources</li> <li>• Business process owners</li> <li>• Business process staff</li> </ul>  |
|                          | 2 | Evaluate existing security controls and procedures      | Review: <ul style="list-style-type: none"> <li>• Industry Standards</li> <li>• Vendor security recommendations</li> <li>• Corporate policies / rules compliance</li> <li>• Internal Audit guidelines</li> <li>• Conduct controlled tests, where applicable, e.g.:                             <ul style="list-style-type: none"> <li>– Site inspections</li> <li>– Penetration</li> <li>– External audit (e.g. SAS70)</li> </ul> </li> </ul>                          | <ul style="list-style-type: none"> <li>• Legal counsel</li> <li>• Internal Risk Management</li> <li>• Internal audit</li> <li>• Legal / regulatory requirements</li> <li>• Industry sources</li> <li>• Security application vendor</li> <li>• Business process owners</li> <li>• Business process staff</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #8<br>SECURITY | # | What  | How   | Points of Reference   |
|--------------------------|---|---|---|---|
|                          | 3 | Develop recommendations for improved security controls and procedures | <p>Partner with the Risk Management Department and Internal Audit to develop recommendations and conduct on-going security reviews to prevent potential situations from.</p> <ul style="list-style-type: none"> <li>• As part of 'design in process', include risk reduction, mitigation and business controls.</li> <li>• Ensure implementation teams complete efforts as described.</li> <li>• Provide for continuous auditing (self-audit and Internal Audit)</li> </ul> | <ul style="list-style-type: none"> <li>• Legal counsel</li> <li>• Internal Risk Management</li> <li>• Internal Audit</li> <li>• Legal / regulatory requirements</li> <li>• Industry sources</li> <li>• Business process owners</li> <li>• Business process staff</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #9                    | #        | What  | How  | Points of Reference  |
|---------------------------------|----------|---|--|--|
| <b>VITAL RECORDS MANAGEMENT</b> |          |   |  |  |
| <b>Vital Records Management</b> | <b>1</b> | Identify vital record needs in the organization, including paper and electronic records | <ul style="list-style-type: none"> <li>• Agree on definition of vital records (e.g. those records required by a business to stay in business)</li> <li>• Review or create the organization's Records Retention Schedule to identify administrative and operational vital records</li> <li>• Determine frequency of data backups / replication</li> <li>• Identify special issues and needs concerning paper and electronic vital records (e.g. email-related vital records)</li> <li>• Calculate retention periods, and location / disposition timeframes</li> <li>• Identify timeframes for retention</li> <li>• Identify the need for tightly controlled disposition / destruction methods</li> <li>• Consider the potential need for long-term preservation</li> <li>• Identify records retrieval / recovery needs and processes</li> <li>• Identify the right media for storage</li> <li>• Identify the optimal storage environment</li> <li>• Identify technologies / equipment needed to retrieve records (e.g. tape / microfilm)</li> </ul> | <ul style="list-style-type: none"> <li>• Business process owners</li> <li>• Business process staff</li> <li>• Legal counsel</li> <li>• Internal Risk Management</li> <li>• Technical staff</li> <li>• Internal records management department</li> <li>• Records management vendor</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #9                    | #        | What  | How   | Points of Reference   |
|---------------------------------|----------|---|---|---|
| <b>VITAL RECORDS MANAGEMENT</b> | <b>2</b> | Evaluate existing backup and restoration procedures for vital records | <ul style="list-style-type: none"> <li>• Evaluate the existence and viability of the organization's Records Retention Program and Records Retention Schedule</li> <li>• Review the current vital records management program and documentation                             <ul style="list-style-type: none"> <li>– Completeness</li> <li>– Accuracy</li> <li>– Maintenance</li> <li>– Appropriate and effective distribution</li> <li>– Periodic training</li> <li>– Periodic exercise of procedures</li> <li>– Offsite storage of current vital records inventory and procedures, including emergency operating information and procedures</li> </ul> </li> <li>• Assess the level of adherence to the vital records management program and its overall effectiveness from a technical and business standpoint</li> <li>• Evaluate potential threats to vital records</li> <li>• Evaluate strategies for protecting vital records</li> </ul> | <ul style="list-style-type: none"> <li>• Business managers</li> <li>• Legal counsel</li> <li>• Internal Risk Management</li> <li>• Internal Audit</li> <li>• Legal / regulatory requirements</li> <li>• Industry sources</li> <li>• Internal records management department</li> <li>• Technical staff</li> <li>• Records management vendor</li> <li>• NFPA (National Fire Protection Association)</li> <li>• NARA (National Archives and Records Administration)</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #9<br><br>VITAL<br>RECORDS<br>MANAGEMENT | # | What   | How   | Points of Reference  |
|--|---|--|---|--|
|  | 3 | Develop recommendations for improved backup and restoration procedures | <ul style="list-style-type: none"> <li>• Develop a recommendations document based on the above information</li> <li>• Partner with internal and external resources to validate and refine the recommendations document</li> </ul> | <ul style="list-style-type: none"> <li>• Legal counsel</li> <li>• Internal Risk Management</li> <li>• Internal Audit</li> <li>• Legal / regulatory requirements</li> <li>• Industry sources</li> <li>• Internal records management</li> <li>• Records management vendor</li> <li>• Business process owners</li> <li>• Business process staff</li> <li>• Technical staff</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #10                          | #        | What   | How  | Points of Reference   |
|--|----------|--|--|---|
| <b>DOCUMENT &amp; PRESENT FINDINGS</b> | <b>1</b> | Document findings  | <ul style="list-style-type: none"> <li>• Consolidate findings into a single document</li> <li>• Prepare an high-level summary report for presentation to executive management</li> <li>• Consider presentation of findings from a marketing standpoint – define and sell the value of the findings and recommendations</li> </ul>  | <ul style="list-style-type: none"> <li>• Internal Risk Management</li> <li>• Internal Audit</li> <li>• Legal counsel</li> </ul> |
| <b>Document and Present Findings</b>   | <b>2</b> | Present findings and advise management on feasible, cost-effective security measures required to prevent / reduce vital records and security-related risks and exposures | <ul style="list-style-type: none"> <li>• Develop a presentation that clearly summarizes the results and the information in the high-level summary report</li> <li>• Consider meeting with each senior manager individually before presenting the final results to the executives as a group.</li> <li>• Schedule and present findings and recommendations to prevent / reduce vital records and security-related risks and exposures to executive management team</li> <li>• Be prepared to answer detailed questions from the senior managers (take the detailed results to the meeting as a backup)</li> <li>• Obtain formal sign-off and approval to move to the next phase of planning and implementation</li> </ul> | <ul style="list-style-type: none"> <li>• Internal Risk Management</li> <li>• Internal Audit</li> <li>• Legal counsel</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #11<br>DOCUMENT<br>RISK<br>ACCEPTANCE | # | What  | How   | Points of Reference   |
|---|---|---|---|---|
| <b>Document Risk Acceptance</b>                 | 1 | Determine, and agree on, the cost of downtime   | <ul style="list-style-type: none"> <li>• Identify the business process</li> <li>• Identify the method used to measure cost of interruption.                             <ul style="list-style-type: none"> <li>– Is human life at risk?</li> <li>– Is revenue lost?</li> <li>– Is revenue delayed?</li> <li>– Is there a cost for additional resources needed to recover?</li> <li>– Are there legal or regulatory issues?</li> <li>– Are there contract requirements?</li> <li>– Could penalties be assessed?</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Business process owners</li> <li>• Business process staff</li> <li>• Recovery staff</li> <li>• Legal Counsel</li> <li>• Contracting Office</li> <li>• Internal Finance / Accounting</li> </ul> |
|   | 2 | Ensure that service level agreements are documented and considered, in terms of interdependencies (e.g. clients, vendors, key business units) | <ul style="list-style-type: none"> <li>• Identify relationships to other processes, business units, etc.</li> <li>• Determine the level of criticality for each interdependent relationship.</li> <li>• Verify the presence or absence of service level agreements for each relationship.</li> <li>• Determine if the service level agreements are adequate to meet the time requirements for the business process.</li> <li>• Determine if there are contract provisions affecting the conduct of the business process.</li> </ul>   | <ul style="list-style-type: none"> <li>• Service Level Agreements</li> <li>• Customers of business process</li> <li>• Technical Staff</li> <li>• Contracting Office</li> </ul>  |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #11<br>DOCUMENT<br>RISK<br>ACCEPTANCE | # | What   | How  | Points of Reference   |
|---|---|--|--|---|
|   | 3 | Develop a risk prioritization grid that maps out the business risk and technical risks | <ul style="list-style-type: none"> <li>• Identify the risk to the business process</li> <li>• Associate the technical risks to the business process.</li> <li>• Rate the technical risks for likelihood and criticality.</li> <li>• Rate the recommendations for ease of fix.</li> <li>• Identify the level of cost for each fix.</li> <li>• Rank the risks according to criticality, then ease of fix under each business risk.</li> <li>• Rate recommendations for comparative cost: low, moderate; high.</li> <li>• Set priorities based on level of risk and cost.</li> <li>• Develop a corrective action plan.</li> </ul> | <ul style="list-style-type: none"> <li>• NIST SP 800-30 Risk Management Guide for Information Technology Systems</li> <li>• Test results, when available</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #11<br>DOCUMENT<br>RISK<br>ACCEPTANCE | # | What   | How   | Points of Reference   |
|---|---|--|---|---|
|   | 4 | Discuss with executives and ensure that they document accepted risks | <ul style="list-style-type: none"> <li>• Document the risk to the business process and the cost/time to remediate.</li> <li>• Review the each documented risk and determine if it will be addressed or accepted.</li> <li>• If action is to be taken, develop a corrective action plan.</li> <li>• If no action is to be taken, document the decision by                             <ul style="list-style-type: none"> <li>– Email</li> <li>– Signature</li> <li>– Risk Acknowledgement Database Update</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Business Process Owners</li> <li>• Technical Staff</li> <li>• Operating/processing staff</li> <li>• Internal Risk Management</li> <li>• Internal Finance / Accounting</li> <li>• Executive management</li> </ul> |

## Subject Area 2 – Risk Evaluation and Control

| Sub-Topic #12  | #        | What   | How   | Points of Reference  |
|--|----------|--|---|--|
| <b>BACKUP,<br/>RESTORATION<br/>&amp; SECURITY<br/>MEASURES</b> | <b>1</b> | Implement, or assist with implementation of, security measures approved by management  | <ul style="list-style-type: none"> <li>• Review corrective action plans</li> <li>• Identify key contacts</li> <li>• Verify your role in the implementation                             <ul style="list-style-type: none"> <li>– Level of authority</li> <li>– Watchdog</li> <li>– Reporting</li> <li>– Vendor liaison</li> </ul> </li> </ul>  | <ul style="list-style-type: none"> <li>• Gap analysis authors</li> <li>• Facilities Management</li> <li>• Technical Staff</li> <li>• Legal Counsel</li> <li>• Other Internal Experts</li> </ul>  |
|  | <b>2</b> | Implement, or assist with implementation of, backup and restoration procedures for the organization's vital records approved by management | <ul style="list-style-type: none"> <li>• Review gap analysis</li> <li>• Identify areas requiring improvement</li> <li>• Verify that recommendations will meet the identified need</li> <li>• Verify your role in implementation                             <ul style="list-style-type: none"> <li>– Level of authority</li> <li>– Watchdog</li> <li>– Reporting</li> <li>– Vendor liaison</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Gap analysis authors</li> <li>• Technical Staff</li> <li>• Records Management Team</li> <li>• External Records Management Advisor</li> <li>• Legal Counsel</li> <li>• Other internal experts</li> </ul> |

## 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](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>.)