Business Continuity
Part 2
Converting Risk Assessments to Risk Mitigation Activities to Business Recovery Plans

Howard Pierpont
Intel Corporation
Hillsboro, OR
Jan 2005
Intel strives to prevent injury to employees, guests and neighbors; protect Intel's assets from damage or loss; and minimize the effects of any incident so that they do not compromise Intel's ability to achieve its mission. Intel recognizes that a wide variety of disasters (natural and human-caused) or failures (physical and information systems) can occur. Although these incidents cannot always be avoided even where preventative measures have been taken, through effective planning we can reduce both the duration and severity of any event that does occur.

To accomplish our goals of preventing injury, protecting assets, and minimizing the impact of any incident, Intel operations incorporate Business Continuity as a core business practice. Business Continuity is an integral approach to doing business that promotes safety as a core value while providing reasonable assurance we can respond to emergencies and keep our core business running during times of unexpected events or disasters.
Examples of Threat Categories

- Natural Disasters
- People Issues
- Major on-site issues
- Major off-site issues
- Product
- Computing Infrastructure
- Suppliers
- Customers
- Governments
- Partners/Allies
Examples of Impact Categories

- People
- Computing
- Physical
- Logistic
- Financial
- Customer
- Legal
- Indirect
COO, CEO and CFO support in place

• Need to ensure all areas were considered
  – Employees
  – Customers
  – Stockholders
  – Investment community

• Every Intel organization must make Business Continuity a core business practice

• Quantify, where possible, the loss impact from both a business interruption (number of days) and a financial standpoint (dollars).

• A sum of money was set aside for immediate upgrades to vulnerable areas

• Use funds rapidly and wisely as they may be withdrawn

• Additional funding to come from business with needs
Top Level Support

Safety and Security Initiative

- Senior VP with ability to call on any Business Unit if needed
  - Physical Security including employee access
  - Communication
  - Safety and Security Task Force (SSTF) Core competencies
  - Business Continuity Program Office (BCPO)
  - Keep the message consistent and programs on time line

- BCPO Management
  - Sr Manager, 3 BC Coaches, 1 webmaster, 1 Comms Manager, 1 Support / Course Dev
  - Create toolkits, presentations, common methods, common reporting
  - Coaches took the message through out the Business units
    - Every Intel organization must make Business Continuity a core business practice
    - Quantify, where possible, the loss impact from both a business interruption (number of days) and a financial standpoint (dollars).

- Run the process in less than 12 months to sustaining
Key BC Questions:
*Is your organization ready....*
*Could your organization answer these questions?*

- Do you understand your core business vulnerabilities or potential failure points during a major extended crisis?
- Do you have emergency management structures and defined roles & responsibilities in place to respond to a crisis?
- Do you know your key support groups and suppliers BC plans? Are your plans in alignment so you would be able to continue operations?
- Do you know how to contact key individuals required to respond to the crisis in your organization through a variety of channels including non-working hours?
BC Planning Process

- Identify Risks
- Determine Impact
- Develop Risk Mitigation Strategies
- Determine Areas needing BC plans

Respond to Disasters as Needed

Conduct Drills & Exercises
Conduct Self-Assessment

Analyze Risk

Test Response

Prepare Response

Mitigate Risks
Prepare Plans
- Business Recovery
- Emergency Response

Develop Risk Mitigation Strategies
Risk Analysis and Mitigation Planning
BC Planning Process

Prepare

Test Response

Analyze Risk

Identify Risks
Determine Impact
Develop Risk Mitigation Strategies
Determine Areas needing BC plans

Prepare Response

Mitigate Risks
Prepare Plans
- Business Recovery
- Emergency Response

Conduct Drills & Exercises
Conduct Self-Assessment

Respond to Disasters as Needed
Risk & Impact Assessment: Getting Started

- Pick a format
- Make it universal for the group
- Ensure that you can ‘roll up the data’

**Basic Information:**
- Organization
- Owner
- Date and Revision Number
- Approving Body and Approval Date

**Core Business Function**
- Typically 3-5 May be more or less

**Supporting Business Processes**
- Typically 3-5 May be more or less
Risk & Impact Assessment

• For each Supporting Business Function indicate:
  – Critical Links with other organizations
  – In place Controls
  – Are the current Controls Effective
  – Impacts / Failures and Single Points of Failure [SPoF]
  – Impact Severity – H/M/L – Models uses 3 could be 5 or 10
  – Likelihood of Occurrence – H/M/L - Model Uses 3
  – Mitigation Required / Desired

• Complete for each Business Function
• Validate assumptions with Support Groups
• Subject Matter Expert / Content Expert has Worksheet reviewed and agreed to by management
• Peer Reviews
Project Organization Model

Sponsor

BC Champion

Business Unit Lead
  - Content Expert
  - Content Expert
  - Content Expert

Business Unit Lead
  - Content Expert
  - Content Expert
  - Content Expert

Business Unit Lead
  - Content Expert
  - Content Expert
  - Content Expert

BC Program Office

BC Coach

Support Groups
  - IT
  - Quality
  - HR
  - Legal
  - Facilities
  - Others
Project Organization Model

Sponsor

BC Champion

Business Unit Lead
- Content Expert
- Content Expert
- Content Expert

Business Unit Lead
- Content Expert
- Content Expert
- Content Expert

Business Unit Lead
- Content Expert
- Content Expert
- Content Expert

Support Groups
- IT
- Quality
- HR
- Legal
- Facilities
- Others

BC Program Office

BC Coach
Project Organization Model

Sponsor

BC Champion

Business Unit Lead
- Content Expert
- Content Expert
- Content Expert

Business Unit Lead
- Content Expert
- Content Expert
- Content Expert

Business Unit Lead
- Content Expert
- Content Expert
- Content Expert

Support Groups
- IT
- Quality
- HR
- Legal
- Facilities
- Others

BC Program Office

BC Coach
Risk & Impact Assessment

- **Business Unit Lead:**
  - Conducts Peer reviews
  - Look for commonality of issues
  - Assist in Prioritizing mitigation efforts
  - Obtain Business unit Management ‘buy-in’

- **Re-validate assumptions with Support Groups**

- **Business Unit Peer reviews**
  - Reviews conducted by BC Champion
  - Look for commonality of issues
  - Assist in Prioritizing mitigation efforts
  - Obtain Business unit Management ‘buy-in’

- **Report out prepared**
- **Recommended mitigation efforts presented**
- **Formalize plan creation**
Develop Risk Mitigation Strategies

- Based on the risk analysis, determine which actions provide the best cost-benefit ratio with regards to risk reduction.

- Examples of Risk Mitigation Include:
  - Building backup or redundant information systems
  - Moving to lower risk manufacturing locations and logistics channels
  - Duplicating IP (designs, source code, etc.)
  - Pre-qualifying alternate suppliers
  - Distributing unique or critical path manufacturing processes to multiple sites
## Risk Assessment Outcome Chart

<table>
<thead>
<tr>
<th>Severity</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>1.4</td>
<td>1.1</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td>1.5</td>
<td>1.2</td>
</tr>
<tr>
<td>High</td>
<td>1.6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Likelihood**:
  - Low
  - Medium
  - High
Severity

Low

Medium

High

Likelihood

Low

Medium

High

Move High/High Low/Low

Risk Assessment Outcome Goal
Mitigate Risks
Emergency Response and
Disaster Recovery Plans
BC Planning Process

- Respond to Disasters as Needed
- Conduct Drills & Exercises
- Conduct Self-Assessment

1. Identify Risks
2. Determine Impact
3. Develop Risk Mitigation Strategies
4. Determine Areas needing BC plans

5. Mitigate Risks
   - Prepare Plans
   - Business Recovery
   - Emergency Response

6. Prepare Response
7. Analyze Risk
8. Test Response
Develop Disaster Recovery Plans

- Based on the Risk Mitigation Actions, determine the extent to which critical functions need to be covered in Disaster Recovery Plans (DRP).

- The DRP is the process of developing advance arrangements and procedures that enable an organization to respond to a disaster and resume the critical business functions within a predetermined period of time, minimize the amount of loss, and repair or replace the damaged facilities as soon as possible.*

* Disaster Recovery Institute
Disaster Recovery

- Threat/Disaster IMPACT
- Emergency Response
  - 0-3 Days
  - 0-60 Days
- Disaster Recovery
- Normal Business Operations

Emergency Response Plan(s)
Disaster Recovery Plan(s)
Business Recovery Plan

- Overview
  - Plan Author(s) and Preparing Organization
  - Recovery Strategy
  - Recovery Plan Scope
  - Plan Objectives
  - Recovery Team Contact Lists
  - Recovery Team Roles and Responsibilities
  - Recovery Team Location
  - Communication Channels

- Business Recovery Trigger Points
  - Recovery Time Objective (RTO) Requirements
  - Recovery Plan Authorization & Activation Triggers
Business Recovery Plan

- Critical Recovery Information
  - Business Recovery Plan Checklist
  - Business Recovery Priorities
  - Job Descriptions
  - Travel Coordination
  - Offsite Storage Information
  - Keys, Electronic Codes and Passwords
  - Vendors/Suppliers

- Business Recovery Procedures
  - Recovery Procedures
  - Recovery Procedures for Group/Function/Process
Business Recovery Plan

- Restoring Functional / Normal Operations
  - Criteria for Returning to Functional / Normal Operations
  - Normal Operations Startup
  - Post-Mortem Event

- Plan Maintenance Procedures
  - Plan Review and Update Process
  - Business Recovery Plan Distribution Procedures
  - Revision History
Business Recovery Plan

- **Trigger points**
  - Helps determine the appropriate response for different events

- **Recovery time goals**
  - Will help drive prioritization of activities

- **Critical Information**
  - Checklists for crisis teams
  - Priorities for recovery sequences
  - Information storage – where can critical data and information be found.
  - Documentation, resource lists

- **Recovery Procedures**
  - Criteria for returning to normal operations
BC Planning Process

Respond to Disasters as Needed

Conduct Drills & Exercises
Conduct Self-Assessment

Test Response

Analyze Risk

Prepare Response

Identify Risks
Determine Impact
Develop Risk Mitigation Strategies
Determine Areas needing BC plans

Mitigate Risks
Prepare Plans
- Business Recovery
- Emergency Response
Drills, Exercises and Self-Assessment

• An untested plan is only paper
  – Multiple types of tests and exercises
  – Should include first line and secondary players
  – The more you test the better the response
  – Conduct after action or post mortem report
  – Assign action items and follow up through closure
  – Update plans and redistribute
  – Prepare management report on activities

• Self-Assessment
  – Common questionnaire to be completed by representatives from each group
  – Provides benchmark for further improvement
BC Planning Process

1. **Analyze Risk**
   - Identify Risks
   - Determine Impact
   - Develop Risk Mitigation Strategies
   - Determine Areas needing BC plans

2. **Prepare Response**
   - Mitigate Risks
   - Prepare Plans
     - Business Recovery
     - Emergency Response

3. **Test Response**
   - Conduct Drills & Exercises
   - Conduct Self-Assessment

4. **Respond to Disasters as Needed**
Business Continuity: Summary

- Assess Risks and drive Risk Mitigation Activities
- Ensure Readiness
  - Drive Disaster Recovery Plan creation/updates
  - Coordinate with supporting organizations and internal customers
  - Coordinate with external suppliers of materials and services
- Test Readiness
  - Conduct drills/testing of plans