Business Impact Analysis
March 25, 2021

Stephen Heath
TAP Team
Information Security
Chancellor’s Office

Contact:
• CCCCO: sheath@cccco.edu
• Business: stephen.heath@intrinium.com
• LinkedIn: https://www.linkedin.com/in/hackerhiker/
• Twitter: https://twitter.com/hackerhiker
Business Impact Analysis

Agenda

- Definition
- How to perform a BIA
- Examples and Process
- BIA vs Risk Assessment?
- Q&A
Goal

• Understand what a BIA is
• Give you the tools to complete one
• Understand how a BIA is useful in communicating to management
Business Impact Analysis

A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies.
Business Impact Analysis

A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies.
Why do a BIA?

- Identify most critical processes or services
- Assess impact over time of not performing processes or services
- Set priorities and timeframes for recovery
- Identifying dependencies
Critical processes

• The processes needed to perform the business of the organization
• Try not to focus on technology
Type of Impacts

- Lost operations time
- Delayed revenue
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties
- Dissatisfaction or defection
- Delay of new business plans
Timeframe

• How long can the process be disrupted before the impact occurs?
• How much of that impact can we tolerate?
Recovery Time Objective (RTO)

The point in time when a function or process must be recovered, before unacceptable consequences could occur
Recovery Point Objective (RPO)

The maximum acceptable amount of data loss measured in time.
Does it matter when?
Worst Case Scenario

- Worst possible time
- Worst possible impact
- Worst possible fines
Gathering the Data
Gathering the Data

Business Impact Analysis Worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution description:</td>
<td></td>
</tr>
<tr>
<td>Key roles for this solution:</td>
<td></td>
</tr>
<tr>
<td>Key vendors for the solution:</td>
<td></td>
</tr>
<tr>
<td>Key facilities for the solution:</td>
<td></td>
</tr>
</tbody>
</table>
## Collecting the Data

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Tolerable Downtime</th>
<th>Tolerable Data Loss</th>
<th>Impact</th>
<th>Upstream process dependencies</th>
<th>Downstream process dependencies</th>
<th>Technology Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send &amp; Receive Email</td>
<td>1 hour</td>
<td>0 min</td>
<td>HIGH</td>
<td>Monthly reporting, downtime alerts</td>
<td>MS Exchange, Active Directory, Internet connection</td>
<td></td>
</tr>
</tbody>
</table>
NIST 800-34 Worksheet
### Creating Priorities

<table>
<thead>
<tr>
<th>Priority</th>
<th>Solution Name</th>
<th>RTO-Reported</th>
<th>RTO-Actual</th>
<th>RPO-Reported</th>
<th>RPO-Actual</th>
<th>Upstream dependencies</th>
<th>Downstream dependencies</th>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active Directory</td>
<td>15 min</td>
<td>1 hour</td>
<td>24 hours</td>
<td>1 hour</td>
<td></td>
<td>MS Exchange</td>
<td>1 hour recovery time insufficient. Explore Azure AD.</td>
</tr>
<tr>
<td></td>
<td>Internet Connection</td>
<td>15 min</td>
<td>0 min</td>
<td>0 hours</td>
<td>0 hours</td>
<td>Vendors</td>
<td>MS Exchange, Active Directory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MS Exchange</td>
<td>1 hour</td>
<td>1 day</td>
<td>0 hours</td>
<td>1 day</td>
<td>Active Directory,</td>
<td>Internet Connection</td>
<td>1 day recovery is BAD! Explore O365.</td>
</tr>
</tbody>
</table>

---

---
Risk?
Business Impact Analysis

A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies.
“The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.”
BIA vs Risk Assessment

**Risk Assessment**
- Identify threats, assets, & vulnerabilities
- Determine likelihood, impact
- Determine controls and counter measures

**Business Impact Analysis**
- Identify critical business functions & processes
- Classify data and resources
- Determine RTO, RPO
- Determine recovery priority for BCP/DRP
BIA vs Risk Assessment

**Risk Assessment**
- What are the bad things that can happen?
- How much would they hurt?
- What am I doing to prevent them?

**Business Impact Analysis**
- What are my critical business functions?
- How long can I be without them?
- In what order do I restore them?
Risk Assessment → Business Continuity Plan → Business Impact Analysis
Business Continuity Planning

**Business Impact Analysis**
- Develop questionnaire
- Conduct workshop to instruct business function and process managers how to complete the BIA
- Receive completed BIA questionnaire forms
- Review BIA questionnaires
- Conduct follow-up interviews to validate information and fill any information gaps

**Recovery Strategies**
- Identify and document resource requirements based on BIA
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategy options
- Select recovery strategies with management approval
- Implement strategies

**Plan Development**
- Develop plan framework
- Organize recovery teams
- Develop Relocation Plans
- Write business continuity and IT disaster recovery procedures
- Document manual workarounds
- Assemble plan; validate; gain management approval

**Testing & Exercises**
- Develop testing, exercise and maintenance requirements
- Conduct training for business continuity team
- Conduct orientation exercises
- Conduct testing and document test results
- Update BCP to incorporate lessons learned from testing and exercises
Questions?