

ilta09

leading technology | optimizing value

Leading Technology | Optimizing Value

Business Continuity Planning

Completing a Business Impact Assessment

Pamela Hill
Managing Director
Hyperion Global Partners

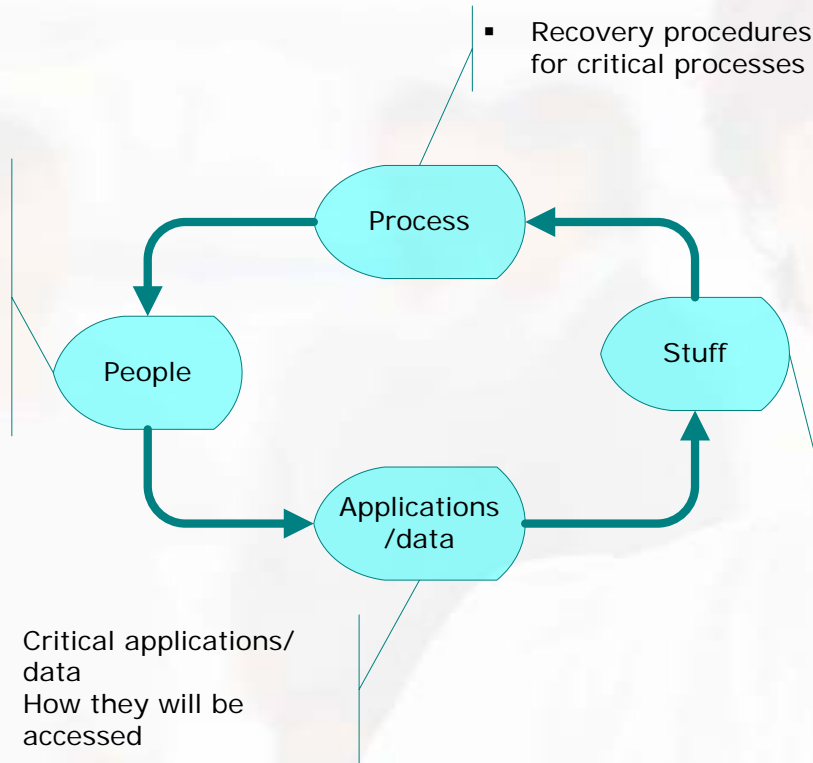
Judi Flournoy
CIO
Loeb & Loeb LLP

Business Impact Assessment

- Purpose
 - To understand how a disaster or business interruption will impact your business
 - From a business process perspective
 - From a technology perspective
 - Allows you to define recovery time/recovery point objectives (RTO/RPO)
 - Create a 360 degree view of a process
 - Technology
 - People
 - Process
 - Inputs/outputs
 - Vital records

Create a 360 View of Recovery

- Recovery team members and their back ups
- Contact information
- Where people will go to continue working
- How/when to communicate



- Critical vendors/service providers
- Records
- Supplies
- Legal specific items such as special paper for filings
- Contact information
- Passwords

BIA Process

1. Gather information

- Survey
- Face to face
- Hybrid
 - Recommend hybrid
 - Survey first
 - Follow up with interviews

2. Interviews allow you

- To push back on the “I want it all yesterday” approach many people will take
- To understand how the process is enabled by the underlying technology
- Discuss ways to work without technology for short periods of time
- Ask clarifying questions regarding inputs/outputs so you understand the process/information flow

BIA Process

- Survey questions – Discuss Example
 - Process name
 - Who does it
 - Define inputs/outputs
 - What processes, departments and people provide input
 - What processes, departments and people receive information from you/your process
 - Define underlying technology
 - What is it
 - How long can you be without it before it impacts your processes
 - How much data can you lose and reasonably expect to recover
 - This is an IT consideration - don't ask the end user this question

BIA Process

- Interview – What to Focus On
 - Describe your existing process(es)
 - How do you use technology to complete the process
 - Detail all of the underlying technology
 - Don't forget to start at the desktop
 - Local applications or how the applications are accessed
 - Security related items such as IP recognition for efilng, digital certificates, etc.
 - Understand where data are stored (even if you think you already know)

BIA Process

- Interview – what to focus on
 - Discuss how to complete the process if the office/app/data is/are unavailable
 - Discuss how to work remotely with their applications
 - Identify trends for training opportunities
 - Discuss post-disaster security considerations (e.g., won't require an RSA token following a disaster)
 - Discuss applications that are not on the remote access list (and why)
 - Be honest in your explanation of current recovery capabilities for applications and data
 - This is an opportunity to educate – use it!

BIA Process

- What to do with the information
 - Compile it into usable bite-sized documents by audience
 - Executive Team
 - Critical processes by RTO
 - Business recovery strategy (discuss sample)
 - Operations/Facilities Team
 - Workspace requirements
 - IT
 - RTO/RPO
 - Hardware/software requirements
 - Special considerations like digital certs/IP address authentication
 - HR
 - People related to processes
 - Work from home capacity

BIA Process

- What to do with the information
 - Create a list of RTO/RPO
 - Complete a gap analysis of current recovery capabilities to what users expect
 - This information tells you
 - Technical priority restore list
 - What to focus BC/DR dollars and resources on
 - What to focus people, workspace, and other resources on during a recovery

Sample Critical Apps/Services

0 – 4 Hours	1 Day	2 – 3 Days	3 – 5 Days
<ul style="list-style-type: none"> •Network •WAN •Security •Remote access •Email continuity •Mobile messaging •Phones •Documents •Contact information 	<ul style="list-style-type: none"> •Email recovery •Records •Conflicts/intake •Filings •Calendar/ docket •Lit support •Intra/extranets 	<ul style="list-style-type: none"> •Workspace •Accounts receivables 	<ul style="list-style-type: none"> •Financial systems •Cost recovery •Practice apps

BIA Process – Change Management

- On-going Analysis
 - Threat Assessment
 - Are there new threats?
 - Has your organization's vulnerability to any threat changed?
 - Would the impact of certain risks be more devastating now than previously?
 - Has the likelihood of any threat occurring increased?
 - BIA Follow up – see example
 - Any significant change in technology
 - Back end integration
 - End user interface and/or workflow
 - New applications

Free Resources

Disaster Recovery Journal

<http://www.drj.com/>

Sample plans

http://www.drj.com/index.php?option=com_content&task=view&id=259&Itemid=298

The institute for continuity management

<https://www.drii.org/>

Disaster recovery and business continuity supercast

http://searchcio.techtarget.com/generic/0,295582,sid182_gci1267493,00.html

The source for business continuity

<http://www.disaster-resource.com/>

CPM focused on convergence of business continuity, and security

<http://www.contingencyplanning.com/>

Business Continuity Links

http://www.rothstein.com/links/rothstein_recommended2.html

- Questions?

Thanks for coming!

Pamela Hill

phill@hyperiongp.com

217.778.6976

Judi Flournoy

jflournoy@loeb.com

310.282.2050