BIA for Financial and Healthcare: How to Leverage Differences

Joe Layman, MIS, CBCP, ITIL, CRISC
Director, Business Continuity Management

Susan Zielan, CBCP
Business Resiliency Manager

AGENDA

• Introductions
• What is a BIA?
• Creating a BIA
• Ways to Capture Data
• Validating the Data
• BIA Output (RTO, RPO, MTD)
• Conclusion
OBJECTIVES

• Share our experiences / opportunities
  – Identify Business Needs → BIA Requirements
  – People, Processes, Downtime, Criticality
  – Simplify
  – Leverage differences for success
• Share resources and tools
• Ask for your ideas
• Have fun!

PARTICIPANT EXPECTATIONS

• What do you hope to learn today?
• Q/A as we go
• Use notepads for questions, if preferred.
WHAT IS A BIA?

A Process designed to prioritize business functions by assessing potential

1. Quantitative (financial) and
2. Qualitative (non-financial) impacts

that might result if an organization were to experience a business disruption.

Source: 2015 DRJ Glossary

WHAT IS A BIA?

The Business Impact Analysis provides a documented valuation process for determining continuity and recovery priorities, objects, and targets.

The evaluation process assesses the impact that a loss, interruption or disruption might have on the organization’s processes, functions and critical resources.

The BIA is the predecessor to developing the Business Continuity Plan.

Source: Private business
WHAT IS A BIA?

A process used to determine the effect of an interruption of services on each business unit and the organization as a whole.

The analysis can provide information on the short and long term effects of a disaster on such factors as profit, market share, and goodwill.

This information is requested to develop a business continuity strategy for the entire organization. The information is valuable in developing an effective Business Continuity Program.

Source: Office of Comptroller of Currency (OCC)

WHAT IS A BIA?

Summary

- A detailed study of business activities, dependencies and infrastructure.
- How the organization delivers critical products and services
- Reveals the potential impact of an incident over time
- Clarify priorities by time using RTO/RPO

Source: OCC
WHAT IS A BIA?

What is your definition?

A BIA is…….

WHY USE A BIA?

The Real Reasons

▪ Understand the cost of a business disruption
▪ Establish a foundation for developing strategies
▪ Make sound and cost effective investment decisions
▪ Ensure the continuity of a critical business function
▪ Ensure continuity of your company or entity
WHY USE A BIA?

User Pushback and Objections

- We have a single / enterprise BIA, its 5 years old
- Takes too long
- We already know the results
- Business units aren’t engaged
  - Lack of participation
  - Won’t / don’t provide meaningful data
- Management enforcement / buy-in

PROVEN METHODOLOGY

DRIII 10 Principles and Practices

1. Project Initiation and Management
2. Risk Evaluation and Control
3. Business Impact Analysis
4. Developing Business Continuity Strategies
5. Emergency Response and Operations
6. Developing and Implementing Business Continuity
7. Awareness and Training Programs
8. Exercise & Maintain Business Continuity Plans
9. Crisis Communications
10. Coordination with External Agencies
BIA OBJECTIVES

Identify

- Critical business functions and dependencies
- Financial and non-financial impacts
- Criticality of processes and applications
- Order in which processes need to be recovered
- Establish time frames for recovery
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
  - Maximum Tolerable Downtime (MTD) (BRCCI, ISO)

BUSINESS FUNCTION

Business Function vs IT (RTO/RPO) centric

- Identify all business functions
- Let the RTO/RPO identify those that are Critical
- Emphasize objectivity

Every business unit manager thinks THEIR business functions are THE MOST critical to the enterprise
RTO

Recovery Time Objective (RTO)

- The period of time within which systems, applications, or functions must be recovered after an outage.
- Includes the time required for assessment, execution and verification.

Source: 2015 DRJ Glossary

RTO

Three SLAs to manage

- Client Contracts/Regulatory – just the facts
- IT capability – the reality
- Business unit – wish list usually the shortest and least objective

Which one wins out?
Why?
RPO

Recovery Point Objective (RPO)

- The point in time to which data is restored and/or systems are recovered after an outage.

Source: 2015 DRJ Glossary

BIA Structure

BIA Data Fields

- Business Functions
- RTO
- RPO

What additional data to collect?
How do you decide?
BIA STRUCTURE

BIA Data Fields
- Department Management
- Business Functions
- Dependencies
- Number of Staff
- Vital Records – hardcopy, electronic
- Special / Unique Assets
- Number of Desktops and Laptops

Areas to consider
- People
- Processes
- Downtime
- Criticality
BIA STRUCTURE

Data gathering based on
- People
- Processes
- Downtime
- Criticality

BIA STRUCTURE: PEOPLE

People are your Greatest Asset!
Locations - Primary and alternate/backup
Urgency
- Day 1, 2, 3…
- Week 2
Capacity
25% → 50% → 75% → 100% Capacity
BIA STRUCTURE

Data gathering based on
- People
- Processes
- Downtime
- Criticality

BIA STRUCTURE: PROCESSES

Begin with Business Processes
- Business Process Name
  - Use current naming → Out with the old
- Business Process Description
  - What does it do?
  - Why is it important?
  - When does it run / frequency / peak periods
**BIA Structure: Processes**

Where do the Processes run?

- Data Center
  - Primary
  - Secondary, backup, alternate
- Subject Matter Experts (SME)
  - Who supports the processes?
  - Business as Usual (BAU) vs disruption

**BIA Structure: Processes**

Process Owners / Decision Makers

- Business Unit Owner
  - BU Knowledge
  - Decision on delivery at time of disruption
- IT Owner
  - IT Knowledge – RTO/RPO, dependencies
  - Who knows how they run → Recovery?
BIA STRUCTURE: PROCESSES

Process Q & A
Document the process during
1. Business As Usual (BAU)
2. Disruption / Outage

BIA STRUCTURE

Data gathering based on
- People
- Processes
- Downtime
- Criticality
Tolerable Downtime

- How long can the business afford to be down?
- Contractual, State or Federal Regulations

Procedures

- Do manual procedures exist?
  Yes → attach to plan
  No → create them!
BIA STRUCTURE

All fields are based on

- People
- Processes
- Downtime
- Criticality

BIA STRUCTURE: CRITICALITY

What is the impact to the Enterprise if the process can not be performed?

- Financial - Quantitative
- Contractual, Legal, Regulatory
- Non-Financial / Intangibles - Qualitative
BIA STRUCTURE: CRITICALITY

Identify Recovery Order

- Resource availability – people
- Application Dependencies
- Business Dependencies
- Specialized equipment
- Logical
CONDUCT THE BIA

Data Gathering Methods

• Survey – completed by business unit
• Interview – completed by you with business unit owners / SMEs
• Combination

CONDUCT THE BIA

Combine the Survey and Interview

• Survey may appear to save time
• Interview provides a face-to-face opportunity with BU owners
• Collect more detailed information
• Map processes, dependencies, requirements
CONDUCT THE BIA

What method works best in your organization?
Align with
- Mission Statement
- Vision Statement
- Strategy
- Financial Revenue
FINANCIAL STANDARDS

- Financial industry is highly regulated
- Frequent Audits for compliance
- Fines
- OCC
- FFEIC

OCC BIA

Every OCC auditor has their own BIA format.
- TIP: Ask your auditor to suggest (or provide) a format - save time, effort, money, frustration
- Meet audit requirements easily
OCC

Office of Comptroller of Currency, OCC
Department of the Treasury
• Risk Management Guidance

• OCC Bulletin 2013-29
  – Recommendations for third-party relationships

OCC BIA

Example

Business Unit/Department Name: 

Description of Business Unit/Department’s Purpose in the Organization: 

Name of Unit/Department’s Manager/Director: 

In the following table, list the business processes performed by the Business Unit/Department:

1.
2.
3.
4.
5.
FOCUSED BIA

8 Questions - Concentrate on identifying

1. Critical Processes or Business Functions
2. RTO
3. RPO
4. Critical Applications they rely on
5. Critical Applications RTO
6. Critical Applications RPO
7. Critical Applications RTA (actual)
   (aka Upstream Dependency Applications)
8. Other Processes or Functions they rely on
   (aka Upstream Dependencies Processes)

FOCUSED BIA BENEFITS

First BIA
- Introduction
- Brevity

Time Sensitive
- Quick training
- Data gathering

Initial Program
- Collect initial data, build up over time
- Develop user experience over time
FOCUSED BIA BENEFITS

Has anyone used a Focused BIA?

Positives -

Drawbacks -

HEALTHCARE STANDARDS

• Health Information Privacy Protection Act (HIPPA)
• Electronic Personal Health Information (ePHI)
• Center for Medicaid Services (CMS)
• Joint Commission (JC)
HEALTHCARE

Scope
- The processes and services supported
- The method of operation
- The duration or lead-time
- Fluctuations in demand – peak operating periods
- Factors not already discovered that may affect the impact or duration of an acceptable disruption (e.g. backlogs)

HEALTHCARE

Resources
- Knowledge, skills or qualifications required
- Workplace requirements – can staff work from home?
- IT applications and communications (special requirements)
HEALTHCARE

Resources
• Records – electronic or hard copy and their location
• Equipment – Information and communication technology (ICT), office equipment, manufacturing equipment
• Legal and regulatory requirements
• Components and raw materials

HEALTHCARE

Interdependencies
• Reliance on other internal processes
• Reliance on external suppliers and vendors
• Reliance on other internal processes on the outputs of the business process
WHAT ARE YOUR REQUIREMENTS?

- Discussion

BIA OUTPUT

Quickly identify Critical Business Functions

- Time sensitive
- Impacts over Time
- Objective

<table>
<thead>
<tr>
<th>Time</th>
<th>0-24 Hrs</th>
<th>48 Hrs</th>
<th>72 Hrs</th>
<th>96 Hrs</th>
<th>Over 1 Week</th>
<th>Over 1 Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>
BIA OUTPUT

Strategies considerations

- Relocation / Work Remotely
- Cross-training
- Workload transfer
- Contractors
- Vendors
- Combination

BIA COMMON MISTAKES
**BIA COMMON MISTAKES**

Consider the impact of interrupted applications rather than business functions:

The driver of a BIA is **THE BUSINESS**

1. Address the impact on the entire organization if a business function cannot be performed.
2. Address applications that the function depends on.

---

**BIA COMMON MISTAKES**

Consider applications in isolation

Business users may know which applications they rely on, however, they do not often know which other applications/infrastructure those applications rely on.

Identify the importance of applications with an understanding of the entire IT environment: servers, storage, network, infrastructure and applications as a whole.

⇒ BU owners think **THEIR APPS** are the most critical.
**BIA COMMON MISTAKES**

Pay too little attention to financial impact
- Collect financial information – and not use it
- Other Financial costs – Penalties, missed SLAs

Pay too much attention to financial impact
- Misunderstand how processes fit into the enterprise
- “Tier 0” Enterprise functions – run the company

---

**BIA COMMON MISTAKES**

**People – Adjust for Staffing**
Management assumes people will be there and doesn’t adjust for staffing when an incident occurs. Who isn’t working? Who could be working? How?

**Data – Backups, ensure Data is recoverable**
Focus on infrastructure rather than the data. Clients rely on data for products and services. Purchase new hardware at time of incident.

**Stuff – Focus on things that are not critical**
Things that are not needed right away. Focus on Business Function Criticality and Priorities
HANDOUT – TOOLS INCLUDED IN THE HANDOUTS

RECOMMENDED READING

• ISO 22317 – Guidelines for BIA
  http://www.iso.org/iso/catalogue_detail.htm?csnumber=50054

• 10 Common BIA Mistakes

• OCC Bulletin 2013-29
  Recommendations for third-party relationships

• DRJ BIA Generally Accepted Practices Analysis

• 10 Common BIA Mistakes
Questions

THANK YOU!!

- Joe Layman, MIS, ITIL, CBCP, CRISC
  Phone: (505) 401-1145
  Email: joe bcm1@gmail.com

- Susan Zielan, CBCP
  Phone: (949) 678-8620
  e-mail: snuznd5@gmail.com