sollievo

What Is A BIA and Why Is It Needed?

Presented by Mark Clarke, ABCP
Senior Consultant, Business Continuity Services
March 7, 2018

Topics of Discussion

- Overview of why to do a BIA
- Business Impact Analysis Definition
- Doing the BIA – Some Items to Capture
- Use of BIA Information

Sollievo I Copyright © 2018 I All Rights Reserved

sollievo

Overview

- Why do BIA?
  - Identify and Protect Assets
  - Policy
  - Management Support
  - BIA is required by regulators as part of BCP

http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_BusinessContinuityPlanning.pdf

Federal Financial Institutions Examination Council
FFIEC

Business Continuity Planning BCP
FEBRUARY 2015

Sollievo I Copyright © 2018 I All Rights Reserved

sollievo

Business Impact Analysis

Action Summary

FFIEC

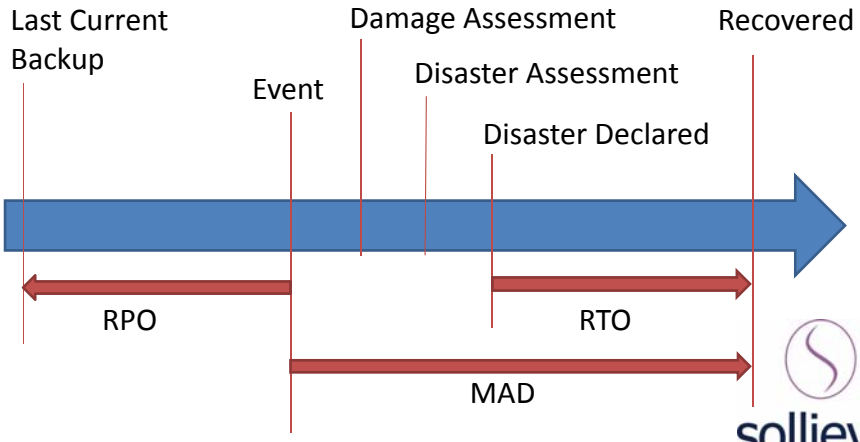
A business impact analysis (BIA) is the first step in the business continuity planning process and should include:

- Assessment and prioritization of all business functions and processes, including their interdependencies, as part of a work flow analysis;
- Identification of the potential impact of business disruptions resulting from uncontrolled, non-specific events on the institution's business functions and processes;
- Identification of the legal and regulatory requirements for the institution's business functions and processes;
- Estimation of maximum allowable downtime, as well as the acceptable level of losses, associated with the institution's business functions and processes; and
- Estimation of recovery time objectives (RTOs), recovery point objectives (RPOs), and recovery of the critical path.

Sollievo I Copyright © 2018 I All Rights Reserved

sollievo

RTO's, RPO's, & MAD's

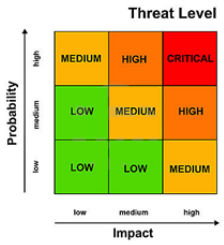


Sollievo I Copyright © 2018 I All Rights Reserved

sollievo

Assessments

- The First Step
  - Business Impact Analysis (BIA)
  - Risk Assessments



Description	Inherent Risk				Residual Risk			
	Risk (1-6)	Impact (1-6)	Score	Ranking	Risk (1-6)	Impact (1-6)	Score	Ranking
Power Failure								
Electric Internal	6	6	36	1	6	3	18	2
Electrical Vendor failure	3	6	18	3	3	3	9	4
Back-up Generators failure	6	6	36	1	4	6	24	1
Gas Leaks	3	4	12	4	3	4	12	3

Sollievo I Copyright © 2018 I All Rights Reserved

sollievo

Risk Assessment

Action Summary

FFIEC

The risk assessment is the second step in the business continuity planning process. It should include:

- Evaluating the BIA assumptions using various threat scenarios;
- Analyzing threats based upon the impact to the institution, its customers, and the financial market it serves;
- Prioritizing potential business disruptions based upon their severity, which is determined by their impact on operations and the probability of occurrence; and
- Performing a "gap analysis" that compares the existing BCP to the policies and procedures that should be implemented based on prioritized disruptions identified and their resulting impact on the institution.

Sollievo I Copyright © 2018 I All Rights Reserved

Risk Assessment

Sample Assessment Matrix

Description	Inherent Risk				Residual Risk			
	Risk (1-6)	Impact (1-6)	Score	Ranking	Risk (1-6)	Impact (1-6)	Score	Ranking
Power Failure								
Electric Internal	6	6	36	1	6	3	18	2
Electrical Vendor failure	3	6	18	3	3	3	9	4
Back-up Generators failure	6	6	36	1	4	6	24	1
Gas Leaks	3	4	12	4	3	4	12	3

Inherent Risk: The risk that exists when no controls have been put in place.

Residual Risk: The risk that remains After all efforts have been made to Mitigate or eliminate risks.

Impact		
	Quantitative	Qualitative
1 – Very Low	$ or % of dollar loss No member lost Insignificant impact on capital	No loss to reputation Negligible effect on members No regulatory consequences No service disruption
2 - Low	$$ or % of dollar loss $$ or % of revenue loss # or % of members lost Minor impact on capital	Adverse reaction by affected members Few members affected Business Disruption <1 day
3 - Moderate	$$ or % of dollar loss $$ or % of revenue loss # or % of members lost Moderate impact on capital	Adverse reaction by members Some members affected Regulatory attention Business Disruption >1 but less than 2 days
4 - High	$$ or % of dollar loss $$ or % of revenue loss # or % of members lost Significant impact on capital	Adverse reaction in news Most members affected Regulatory warning/intervention Business Disruption longer than 2 days
5 – Very High	$$ or % of dollar loss $$ or % of revenue loss # or % of members lost Catastrophic impact on capital	Loss of reputation All members affected Cease operations Cannot Recover Service

Sollievo I Copyright © 2018 I All Rights Reserved

Some Major Items to Capture

- Regulations that affect the process
- Records
- Dependencies
- Any Fines/Penalties if the process (deadlines) can't be done
- Resources needed and when
- IT backup/restoration timeframes

Sollievo I Copyright © 2018 I All Rights Reserved

Sample BIA Questions

- When will the membership be affected?
- When will they lose confidence in your organization?
- Do you have any workarounds in place for this process?
- Does your business unit RTO match with your IT capabilities?
- Do I have vendor support for this process? SLAs?
- How many people do this process?
- Is the potential for fraud higher? When?

Sollievo I Copyright © 2018 I All Rights Reserved

Who is Ultimately Responsible?

Action Summary

FFIEC

A financial institution's board and senior management are responsible for overseeing the business continuity planning process, which includes:

- Establishing policy by determining how the institution will manage and control identified risks;
- Allocating knowledgeable personnel and sufficient financial resources to properly implement the BCP;
- Ensuring that the BCP is independently reviewed and approved at least annually;
- Ensuring employees are trained and aware of their roles in the implementation of the BCP;
- Ensuring the BCP is regularly tested on an enterprise-wide basis;
- Reviewing the BCP testing program and test results on a regular basis; and
- Ensuring the BCP is continually updated to reflect the current operating environment.

sollievo

Sollievo I Copyright © 2018 I All Rights Reserved

Business Continuity Plan Development

FFIEC

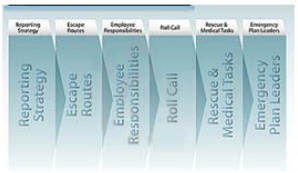
- The BIA and risk assessment represent the foundation of the BCP.
- The BCP should be written on an enterprise-wide basis, reviewed and approved by the board and senior management at least annually, and disseminated to financial institution employees for timely implementation.
- All financial institutions should develop a BCP that documents business continuity strategies and procedures to recover, resume, and maintain all critical business functions and processes.

sollievo

Sollievo I Copyright © 2018 I All Rights Reserved

Plans

- Examples of Plans
  - Emergency
  - Pandemic
  - Disaster Recovery (IT)
  - Incident Response



Sollievo I Copyright © 2018 I All Rights Reserved

sollievo

Q & A

sollievo

Contact Information

Mark Clarke, ABCP

Senior Consultant, Business Continuity Services

mclarke@sollievo.com

Toll-Free (855) 605-5664

Phone (717) 985-5300 ext. 1201

Website: www.sollievo.com

Sollievo I Copyright © 2018 I All Rights Reserved