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

April 8, 2021

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

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

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

Solution Name:	
Solution Function:	
Solution Owner:	

Item	Description
Solution description:	
Key roles for this solution:	
Key vendors for the solution:	
Key facilities for the solution:	

Collecting the Data

	Tolerable			_	_	_	
Process Name	Downtin *	Data Los	Impact 💌	Upstream process dependencies 💌	Downstream process dependencies 🔻	Technology Dependencies	×
					CROSS CONTRACTOR OF THE PROPERTY OF THE PROPER	MS Exchange, Active Directory, Internet	
Send & Receive Email	1 hour	0 min	HIGH		Monthly reporting, downtime alerts	connection	
			- with the		A THE SHALL HAVE AND SHEET AND A SHEET		

NIST 800-34 Worksheet



Creating Priorities

	RTO-	RTO-	RPO-	RPO-			
Priority Solution Name	Reported	Actual	▼ Reported	Actual	 Upstream dependencies 	Downstream dependencies	Findings
Active Directory	15 min	1 hour	24 hours	1 hour		MS Exchange	1 hour recovery time insufficient. Explore Azure AD.
Internet Connection	15 min	0 min	0 hours	0 hours	Vendors	MS Exchange, Active Directory	
					Active Directory,		
MS Exchange	1 hour	1 day	0 hours	1 day	Internet Connection		1 day recovery is BAD! Explore O365.
		11					
			-				

Risk?



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



1 : possibility of loss or injury: PERIL

"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?



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 BIAs
- 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?

