



“Minding Your Business”

The Need for Completing a Mission and
Corporate Business Impact Analysis
(BIA)

Topics

- Contingency Planning / Business Impact Analysis / Return on Investment
 - High Noon
- What's in it for ME?
- What is a BIA and steps
- Templates and Collection of Information
- Fictional Example of BIA
- Summary



Contingency Planning

DILBERT

By Scott Adams



KPMG – Rich Archer

ISCP

Plan	Purpose	Scope	Plan Relationship
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering information system(s).	Addresses single or multiple information systems recovery at the current or, if appropriate alternate location.	Information system(s)-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP .

ISCP

- Systems / Networks are vital to mission/business processes.
- What is the priority to recover?
- *IT contingency planning normally applies to systems, and provides:*
 - *The steps needed to recover critical processes*
 - *At an existing or new location*

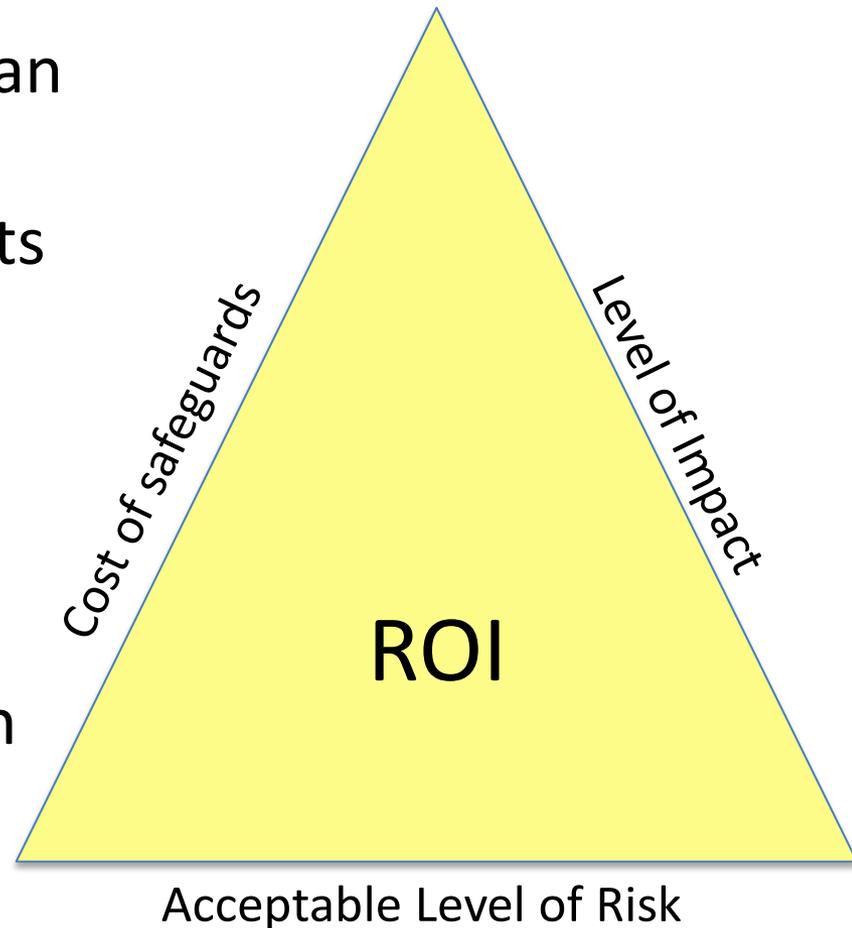


Steps to Developing ISCP

- 1. Develop the contingency planning policy statement.**
- 2. Conduct the business impact analysis (BIA).***
- 3. Identify preventive controls.**
- 4. Create contingency strategies.**
- 5. Develop an information system contingency plan.**
- 6. Ensure plan testing, training, and exercises.**
- 7. Ensure plan maintenance.**

What is a BIA?

- The second (**FIRST**) step in formulating a Contingency Plan
- A BIA is a way of measuring potential risks and the impacts to mission / business operations
- It helps you determine how much time, resources and money are necessary to adequately safeguard mission operations
- BIA facts help in justifying additional resources



Frame of Reference

- You are in the spotlight
- How a BIA might be performed

In the working world...

– Boss, I need:

- 12 new servers
- 3 cots products for... (monitoring, automating, etc...)
- Tapes
- Offsite storage
- 2 additional staff



You Are In The Spotlight

- Admin walks into Boss's office
 - We're down!
- Boss's response: WHAT!!!!
 - *What is wrong?*
 - *How long will we be out?*
 - *What's the impact of the outage?*
 - \$, People, Legal, Fines and etc
 - *At what point will we be able to restored to?*
- *Can you complete your mission / business?*



If you could do it over again...

- You are in the spotlight
- How to address the boss' frame of reference
 - Purpose (why are we here)
 - Problems & impacts
 - Solutions & recommendations
 - Risk/cost based decision based on mission
 - DOCUMENTED & APPROVED



What Is The BIA Purpose?

- What can hurt us and what's the impact?
 - Measure the impact in dollars
 - Mission or business goals / objectives
 - Regulatory / Legal actions / Fines
 - Personnel (criticality of position)
 - DOE Mission / Reputation
 - Prioritize resources for mission critical functions



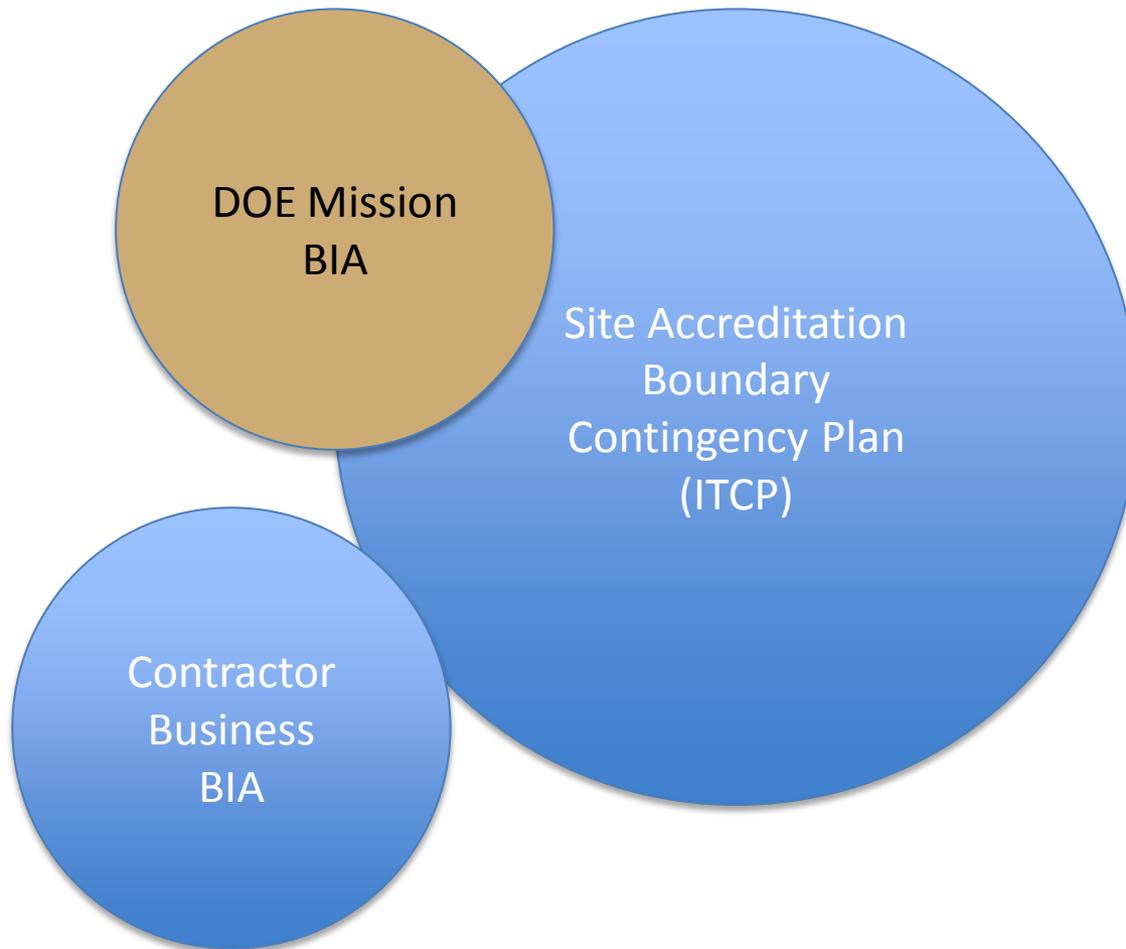
Key Words



- **Maximum Tolerable Downtime (MTD)**
 - *The MTD represents the total amount of time **federal leaders/managers** are willing to accept for a mission/business process outage or disruption and includes all impact considerations*
- **Repair Time Objective (RTO)**
 - *RTO defines the maximum amount of time that a system resource can remain unavailable before there is an **unacceptable impact** on other system resources, supported mission business processes, and the MTD.*
- **Repair Point Objective (RPO)**
 - *The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be **recovered** (given the most recent backup copy of the data) after an outage.*

ISCP BIA

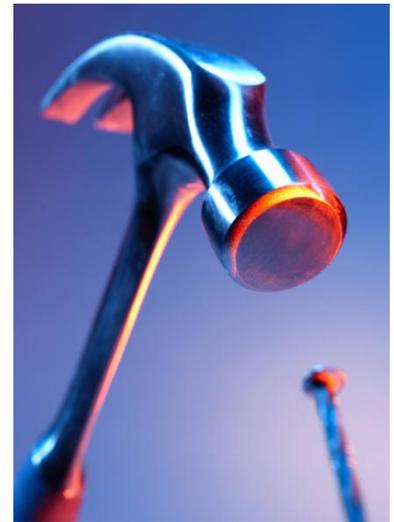
- This is about performing the DOE Mission – Not corporate business. (Although you need both)



- DOE Mission
- Auditors evaluate DOE
- Corp is separate
- Can be overlap

Word of Advice

- ***Use an independent mediator to facilitate the BIA***
- There can be emotions and EGOS involved
 - “Mines more important than yours”
 - “I’ll lose resources if the group doesn’t look important”
 - “We have to do this by computer”
 - “We have no manual procedures”
- Benefit from mediators “experience”
 - What’s reasonable
 - What’s responsible



BIA Steps

- The basic 3 step process for completing a BIA include:
 1. Determine mission/business function then determine your requirements.
 2. Identify requirements & resources.
 3. Identify recovery priorities for IT systems that support the resources and meet the requirements.



BIA Steps

- Determine mission/business function. In other words, what work are you performing for DOE?
 - Moving Dirt, waste, etc...
 - D&D
 - other



BIA Process Overview

Business Process	Potential Impact	Max Tolerable Downtime	System Part	Recovery Time Objective	Categorization Levels			M o d e r a t e
HR Process Invoice	Operations- More than 1000 People Affected	336 Hours	Applic Server	36 hours	Confid Mod	Integ Mod	Avail Low	
Eng Ship Material	Mission and Payment	120 Hours	DBMS Server	36 hours	Confid Mod	Integ Mod	Avail Low	
IT	Operations More than 1000 People	72 Hours	Applic Server	36 hours	Confid Mod	Integ Mod	Avail Mod	
H&S People	Operations More than 1000 People	8 Hours	Applic Server	36 hours	Confid Mod	Integ Mod	Avail Mod	

- Could you fill in this diagram from your current Contingency Plan?
- How do you collect this information?

Can You Answer These Questions?

What are your contract requirements?

What laws must you follow?

Are there fines for missing dates, milestones, etc?

What regulations must you follow?

Others?

Outage Impact and Impact Severity Thresholds	Threshold Criteria
Low , Moderate or High	Personnel- Mission – Financial – Regulatory – Reputation –

Examples of Outage Impact Metrics

Outage Impact and Impact Severity Thresholds	Threshold Criteria
Low	Personnel- No threat to personnel Mission – Minimal, manual methods suffice for 30 to 45 days Financial – Less than \$50K to recover Regulatory – Less than \$50K Reputation – Slight damage to DOE
Moderate	Personnel – Some justifiable threat to personnel Mission-Moderate, some degree of manual but not sustainable to meet mission Financial – Over \$150K to recover Regulatory – Greater than \$100K but less than \$1M Reputation – Moderate damage to DOE
High	Personnel-Significant threat to personnel Mission –High, disables ability to conduct mission or protect personnel Financial – Over \$250K to recover Regulatory – Over \$1M Reputation – Resulting incident makes DOE mission difficult

**Not DOE Standards

BIA Steps

- Identify resource requirements.
 - What are the key groups and IT components that support the mission and help meet the requirements?
 - What do you need to get the job done?

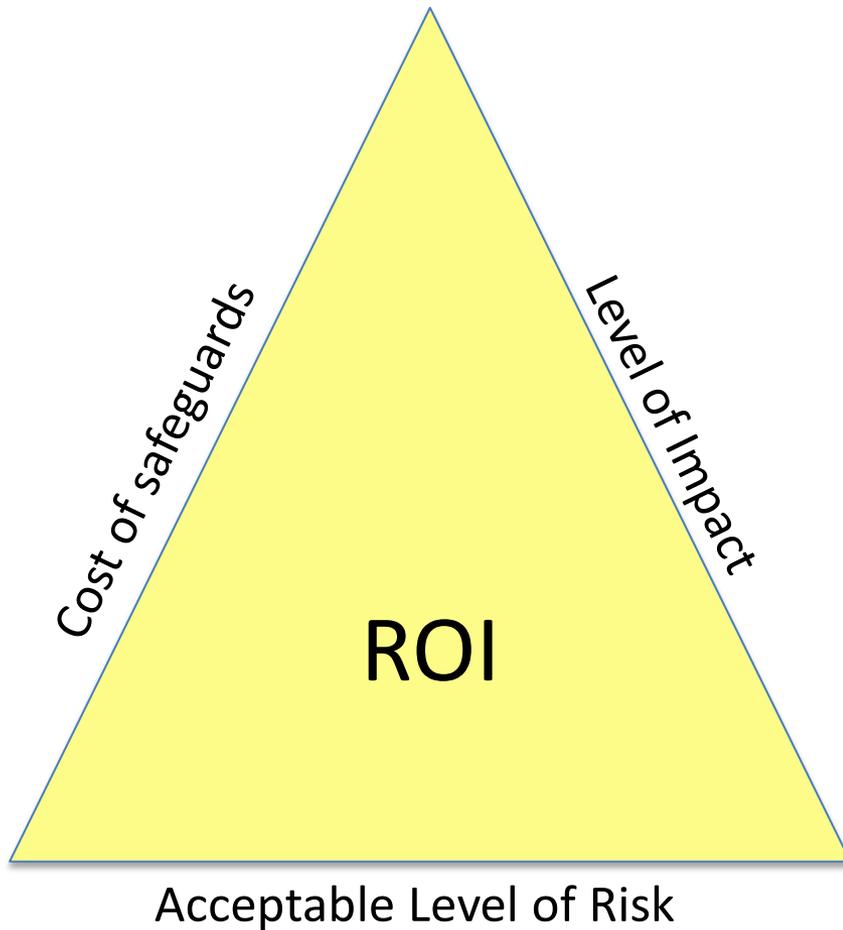
Mission or Business Process Groups	Server or Component	Consist of	Recovery Time Objective
HR	Application 1	Server A	24 hours to repair or replace
IT	All support	All Server	8 hours to repair or replace
Project Controls	Application 3	Server C & D	48 hours to repair or replace
Safety	Application 4 & 5	Server E	12 hours to repair or replace

BIA Steps

- Identify recovery priorities for IT systems that support the resources.
 - You can't have Safety, HR or Project controls without IT infrastructure
 - List of what is needed and the order its needed in.

Mission or Business Process Groups	Server or Component	Consist of	Recovery Time Objective
HR (3 rd)	Application 1	Server A	24 hours to repair or replace
IT (1 st)	All support	All Server	8 hours to repair or replace
Project Controls (4 th)	Application 3	Server C & D	48 hours to repair or replace
Safety (2 nd)	Application 4 & 5	Server E	12 hours to repair or replace

ROI

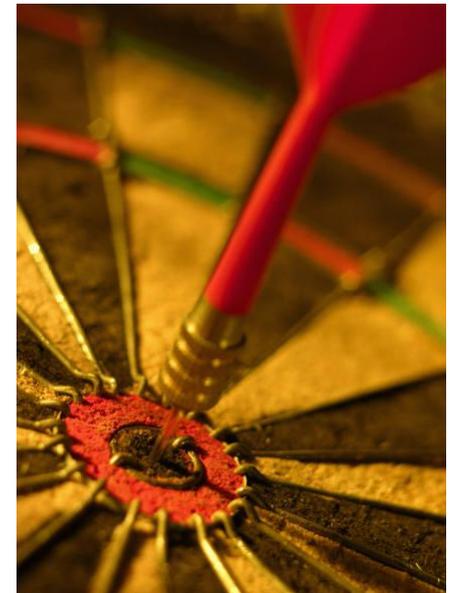


- Can adjust the ROI to the acceptable levels of risk or impact based on DOE mission goals
- Based on Fact
- Make staff justify their purchases



BIA Summary

- BIA is a way of measuring potential risk to DOE mission operations
- The BIA shows ROI
- The BIA tells us where to invest our resources
- A BIA can assist us in justifying resources





Any Questions?