Protecting Information Assets
- Unit# 9 -

Business Continuity and Disaster Recovery Planning

Agenda

- In The News
- Business Continuity and Disaster Recovery Planning
- Test Taking Tip
- Quiz

Business Continuity

Capability to continue service delivery at acceptable levels following" natural or human-induced disaster

Source: International Standards Organization 22300:2018

Security and resilience - Vocabulary

Resiliency

"Capacity to recover quickly from difficulties

...

Antonyms:

- Vulnerability, weakness..."

Source: https://www.lexico.com/en/synonym/resilience

Disaster Context

- *Disruptions to operations can occur with or without warning*

- *Results may be predictable or unanticipated*

The first priority is always the safety of the people:
- *Employees*
- *Service and Support Staff*
- *Visitors*

```
File  Edit  Format  View  Help
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
WayneEvenson@protonmail.com
or
WayneEvenson@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk
No system is safe
```

Business Continuity Management

The **Business Continuity Plan** (BCP) is developed to help assure the organization's ability to maintain, resume, and recover the business

- *It is not just about recovering information technology capabilities*

Planning focuses on the entire enterprise's mission critical infrastructure

- People
- Processes
- Technology

To assure resilient response, organizations need…

Business Continuity Plan (BCP)

Documented procedures for recovering and resuming critical operational functions following significant disruption

…includes a Disaster Recovery Plan (DRP)

Procedures for relocating critical information systems operations to an alternative site following significant disruption

Case study: MAERSK shipping

Our Disaster Recovery Plan Goes Something Like This...
HELP! HELP!

2016 – Maersk shipping company's senior system administrators warn company that its network of 80,000+ computers was vulnerable to attack
- Windows 2000 servers and Windows XP computers overdue for replacement
- Leadership approved upgrades, but systems administrators not motivated to implement the upgrades (due to bonuses based on "uptime" and not security)
- ***No contingency planning (no Disaster Recovery Plan)***

2017, March – Microsoft issues emergency patch to update systems and protect from NotPetya, Maersk's systems not upgraded or patched to protect from NotPetya virus/malware

2017, June – NotPetya encryption attack hits Maersk's offices in Ukraine (arrived as infected e-mail attachments)
- ***Rapidly spreads through Maersk's global wide area network resulting in complete IT availability loss***
  - Active directory domain controllers (network of 150) providing login information (i.e. usernames & passwords) and access control authorization information <u>all wiped out</u>
- 1 Active Directory domain controller in Ghana unaffected due to being off the internet due to electricity blackout
- Resulting in 10-days of lost business ($300,000,000 in expenses and lost earnings)

2017, July – System upgraded (4,000 new servers, 45,000 new PC's, with 2,500 applications) and computer-based business processes restored

Availability is the focus of BCP & DRP

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for pro... pri... inf... [44...	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on...

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Business Continuity and Disaster Recovery planning focuses on Contingency Planning controls

…other controls play important roles in assuring effective contingency planning and disaster recovery!

CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Business Continuity Plan (BCP)
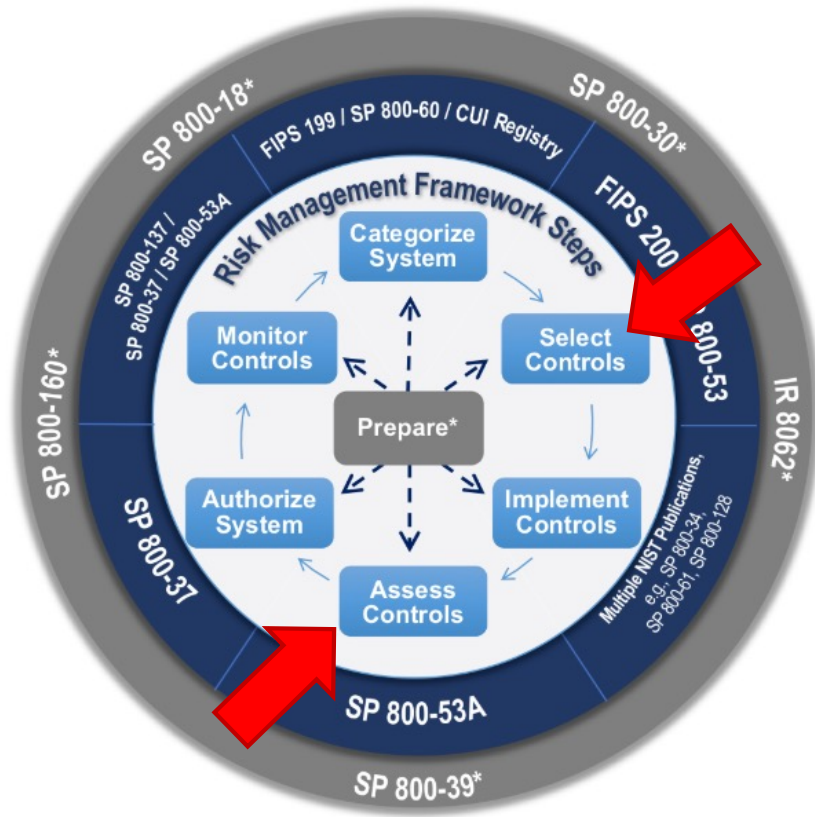
3 Phases of disaster contingency response :

1. Activation and Notification
- **i. Activation criteria**
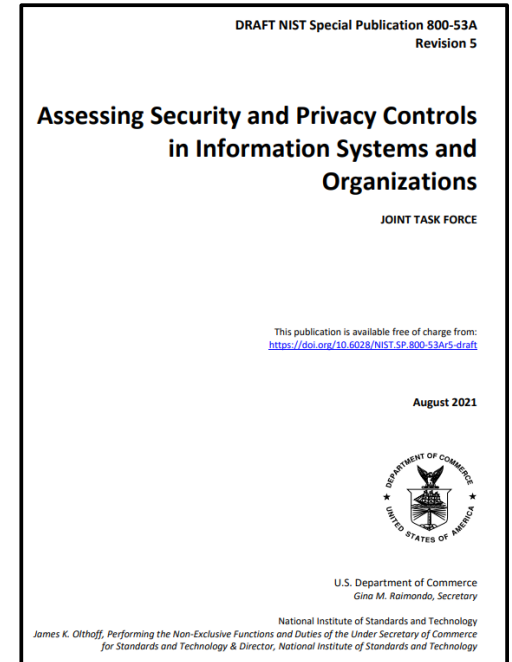- **ii. Notification procedures**
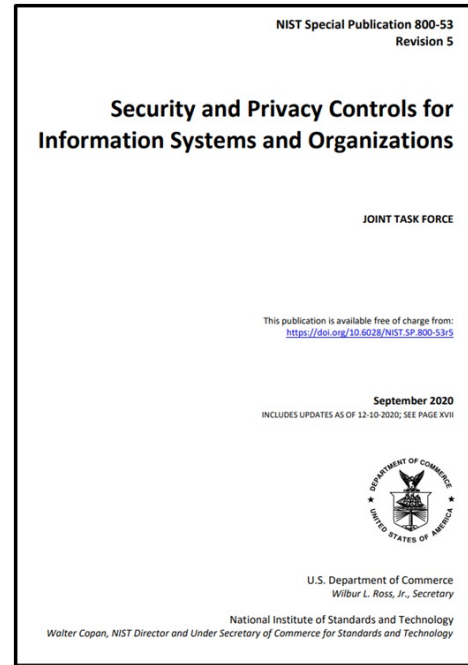- **iii. Outage assessment**

2. Recovery - Disaster Recovery Plan (DRP)
- **i. Sequence of recovery activities**
- **ii. Recovery procedures**

3. Reconstitution

Contingency Planning (CP)

CONTROL NUMBER	CONTROL NAME / CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CP-1	Policy and Procedures		x	x	x
CP-2	Contingency Plan		x	x	x
CP-2(1)	COORDINATE WITH RELATED PLANS			x	x
CP-2(2)	CAPACITY PLANNING				x
CP-2(3)	RESUME MISSION AND BUSINESS FUNCTIONS			x	x
CP-2(4)	RESUME ALL MISSION AND BUSINESS FUNCTIONS	W: Incorporated into CP-2(3).			
CP-2(5)	CONTINUE MISSION AND BUSINESS FUNCTIONS				
CP-2(6)	ALTERNATE PROCESSING AND STORAGE SITES				
CP-2(7)	COORDINATE WITH EXTERNAL SERVICE PROVIDERS				
CP-2(8)	IDENTIFY CRITICAL ASSETS				
CP-3	Contingency Training				
CP-3(1)	SIMULATED EVENTS				
CP-3(2)	MECHANISMS USED IN TRAINING ENVIRONMENTS				
CP-4	Contingency Plan Testing				
CP-4(1)	COORDINATE WITH RELATED PLANS				
CP-4(2)	ALTERNATE PROCESSING SITE				
CP-4(3)	AUTOMATED TESTING				
CP-4(4)	FULL RECOVERY AND RECONSTITUTION				
CP-4(5)	SELF-CHALLENGE				
CP-5	Contingency Plan Update				
CP-6	Alternate Storage Site				
CP-6(1)	SEPARATION FROM PRIMARY SITE				
CP-6(2)	RECOVERY TIME AND RECOVERY POINT OBJECTIVES				
CP-6(3)	ACCESSIBILITY				
CP-7	Alternate Processing Site				
CP-7(1)	SEPARATION FROM PRIMARY SITE				
CP-7(2)	ACCESSIBILITY				
CP-7(3)	PRIORITY OF SERVICE				
CP-7(4)	PREPARATION FOR USE				
CP-7(5)	EQUIVALENT INFORMATION SECURITY SAFEGUARDS				
CP-7(6)	INABILITY TO RETURN TO PRIMARY SITE				
CP-8	Telecommunications Services				
CP-8(1)	PRIORITY OF SERVICE PROVISIONS				

CONTROL NUMBER	CONTROL NAME / CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CP-8(2)	SINGLE POINTS OF FAILURE			x	x
CP-8(3)	SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS				x
CP-8(4)	PROVIDER CONTINGENCY PLAN				x
CP-8(5)	ALTERNATE TELECOMMUNICATION SERVICE TESTING				
CP-9	System Backup		x	x	x
CP-9(1)	TESTING FOR RELIABILITY AND INTEGRITY			x	x
CP-9(2)	TEST RESTORATION USING SAMPLING				

CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information System Recovery and Reconstitution	X	X	X

NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

October 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

DRAFT NIST Special Publication 800-53A
Revision 5

NIST Spec

**Assessing Securit
Controls in Feder
Systems and (**

Building Eff

Th

This

		CP-2	**CONTINGENCY PLAN**
			ASSESSMENT OBJECTIVE:
			Determine if the organization:

ASSESSMENT OBJECTIVE:

Determine if the organization:

CP-2(a)		develops and documents a contingency plan for the information system that:	
	CP-2(a)(1)		*identifies essential missions and business functions and associated contingency requirements;*
	CP-2(a)(2)	CP-2(a)(2)[1]	*provides recovery objectives;*
		CP-2(a)(2)[2]	*provides restoration priorities;*
		CP-2(a)(2)[3]	*provides metrics;*
	CP-2(a)(3)	CP-2(a)(3)[1]	*addresses contingency roles;*
		CP-2(a)(3)[2]	*addresses contingency responsibilities;*
		CP-2(a)(3)[3]	*addresses assigned individuals with contact information;*
	CP-2(a)(4)		*addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;*
	CP-2(a)(5)		*addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented;*
	CP-2(a)(6)	CP-2(a)(6)[1]	*defines personnel or roles to review and approve the contingency plan for the information system;*
		CP-2(a)(6)[2]	*is reviewed and approved by organization-defined*

an for the information system that:

and business functions and associated

overy objectives;

oration priorities;

rics;

ntingency roles;

ntingency responsibilities;

signed individuals with contact

tial missions and business functions
n disruption, compromise, or failure;

rmation system restoration without
safeguards originally planned and

nnel or roles to review and approve
cy plan for the information system;

nd approved by organization-defined
roles;

onnel (identified by name and/or by
ments to whom copies of the
istributed;

ntingency plan to organization-defined
nd organizational elements;

es with incident handling activities;

w the contingency plan for the

n with the organization-defined

information system, or environment of

	CP-2(e)[2]	*problems encountered during plan implementation, execution, and testing;*
CP-2(f)	CP-2(f)[1]	*defines key contingency personnel (identified by name and/or by role) and organizational elements to whom contingency plan changes are to be communicated;*

Identifying essential missions and business functions

An important and big topic:

- How to maintain the continued operation of the business' mission critical processes?

- Based on conducting a **Business Impact Analysis (BIA)**
  - Process of analyzing activities and the effect that a business disruption might have upon them
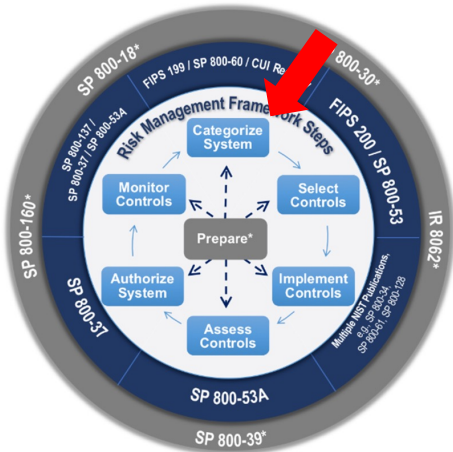
MIS 5206 Protecting Information Assets
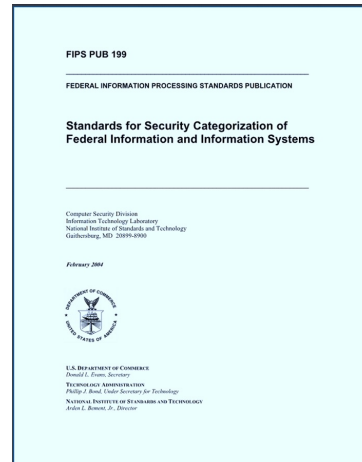
Security Objective	POTENTIAL IMPACT		
	LOW	**MODERATE**	**HIGH**
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

Business Impact Analysis (BIA) answers…

1. What are the work processes ?
2. How critical is each ?
   - *Assess impacts of not performing these activities over time;*
3. How quick do each need to be recovered?
   - *Prioritize the timeframe for resuming each activity at a specified minimum acceptable level, consider how long before the impacts of not resuming each would become unacceptable*
4. What data, applications, people, 3rd parties (e.g. suppliers, partners, …) are needed to run each critical process ?

Prerequisite for Business Impact Analysis and Disaster Recovery Planning

Good work process documentation identifying all people, data, applications, communications and information technologies needed to restore operations

Meta-level view of information processing in large enterprises

There may be 5 or 10 high-level business processes ("meta-processes"), for example:

1. *Develop product offerings*
2. *Bring product offerings to market*
3. *Acquire customer orders*
4. *Fulfill customer orders*
5. *Manage the business*
   - **For example has 6 sub-processes...**

Sherwood, J., Clark, A. and Lynas D. (2005)

"Manage the business"

Example of Top-Down Business Process Analysis
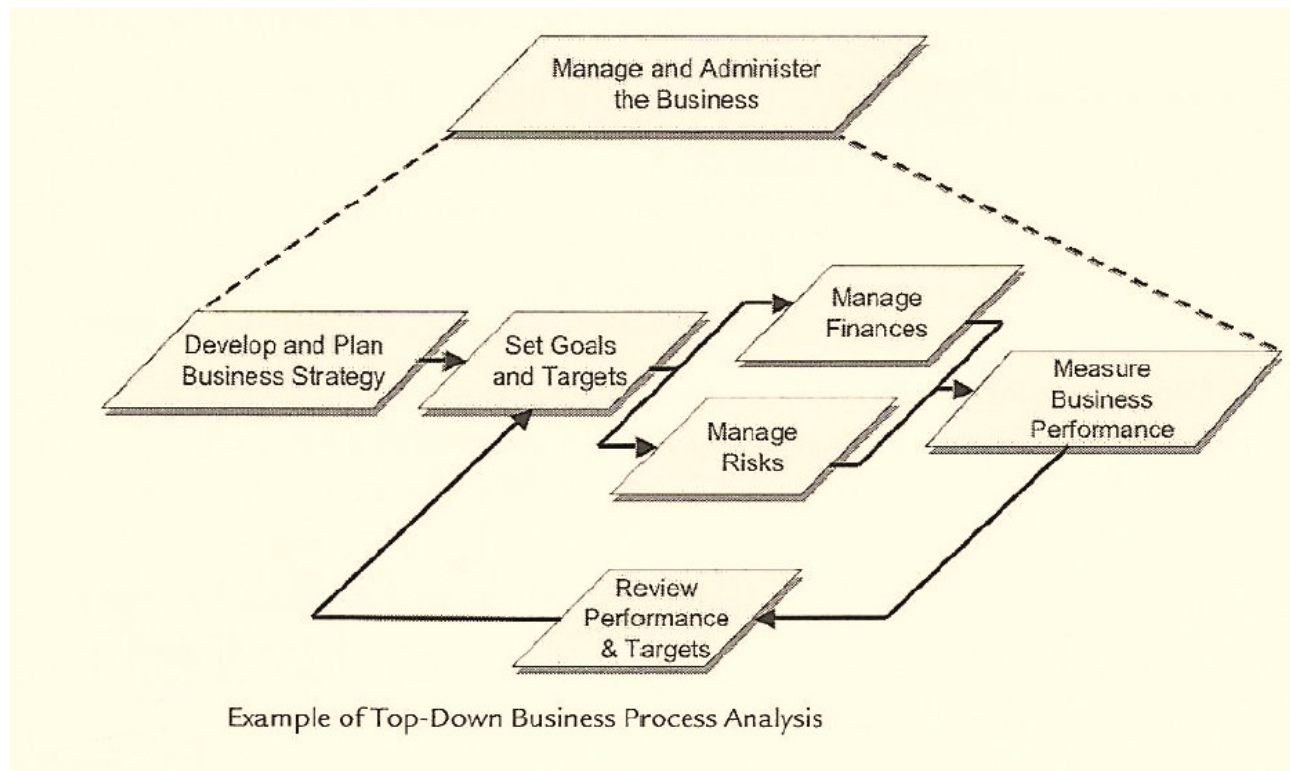
Top-down business process analysis

Also known as: Structured decomposition

Level 1: 10 Processes

Level 2: 100 Processes

Level 3: 1000 Processes

Level 4: 10,000 Processes

Multi-Level Business Process Analysis
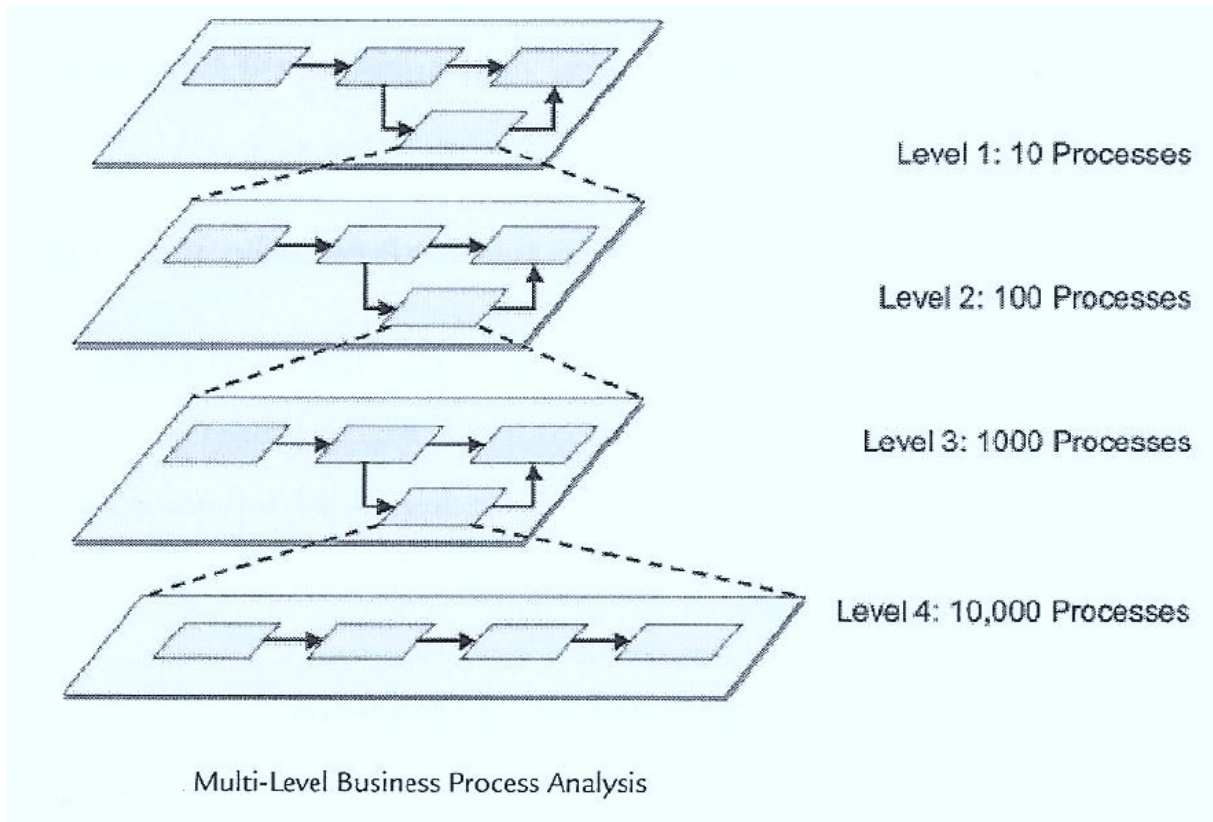
Organizations that achieve this level of detail have an excellent model for understanding their business and business continuity management

Auditing the Business Continuity Plan

Step 1

- Has the business identified and mapped their business processes?

- Have they assessed business impact of loss of each business process?

- Have they classified and ranked business processes into 3 or 4 prioritized groups?

  1. **High** (Catastrophic/Severe) – Loss of this process will result in deaths and/or destroy the business

  2. **Moderate** (Serious) – Loss will be extremely costly and cause persistent, severe damage to the business

  3. **Low** (limited) – Loss will impact the business

  4. **Other** – Damage caused by loss of this process can be absorbed

BIA – Business Impact Analysis

1. Business Process Impact Assessment

2. Functional Analysis of Processes

3. Resource Analysis of Functions

4. Threat Scenario Synthesis

5. Resilience Analysis

6. Business Continuity Planning

7. Risk Financing for Cost of Recovery
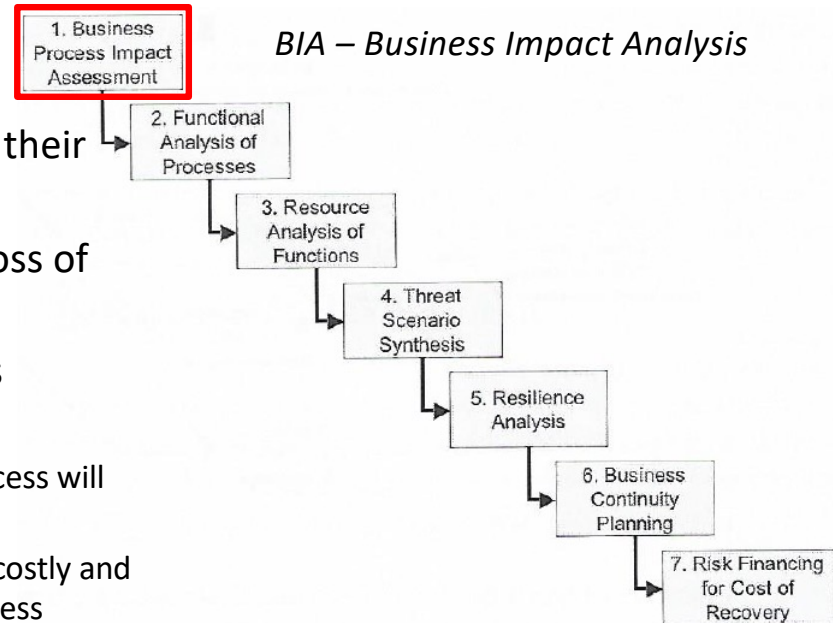
Sherwood, J., Clark, A. and Lynas D. (2005), Enterprise Security Architecture, CRC Press

Does the organization have an inventory of work processes supported by each information system ?

Example:

Service request and utility maintenance management work order information system

- City's Public Works Department
- 4 Divisions (230 employees)
  - Sewer
  - Water
  - Transportation
  - Operations

Service Request / Work Order System
"Computerized Maintenance Management System (CMMS)"

Priorities for recovery example

Public Works Dept **Operations Division**	Street Cleaning	Mow Grass
		Clean Lots
		Street Cleaning - Mechanical and Manual
		Snow Removal
		Debris Removal (Emergency Response)
		Special Pick Ups
		Leaf Removal
		Neighborhood Cleanup
	Public Property	Special Events
		Special Projects
		Building Repair
		Tree Lighting
		Electrical Repair
	Street	Potholes, Street Repair, and Resurfacing
		Special Event Blockade
	Sanitation	Catch Basin Repair
		Catch Basin Cleaning
		Garbage Collection

Auditing the Business Continuity Plan

Step 2

- Select each high and moderate impact process
- Does documentation of these important business processes exist?
- Can your analysis follow trace through all sub-processes?
  - *Down to single functional steps to discover all information systems, data and resources needed to keep this high-impact or moderate-impact process in continuous operation?*
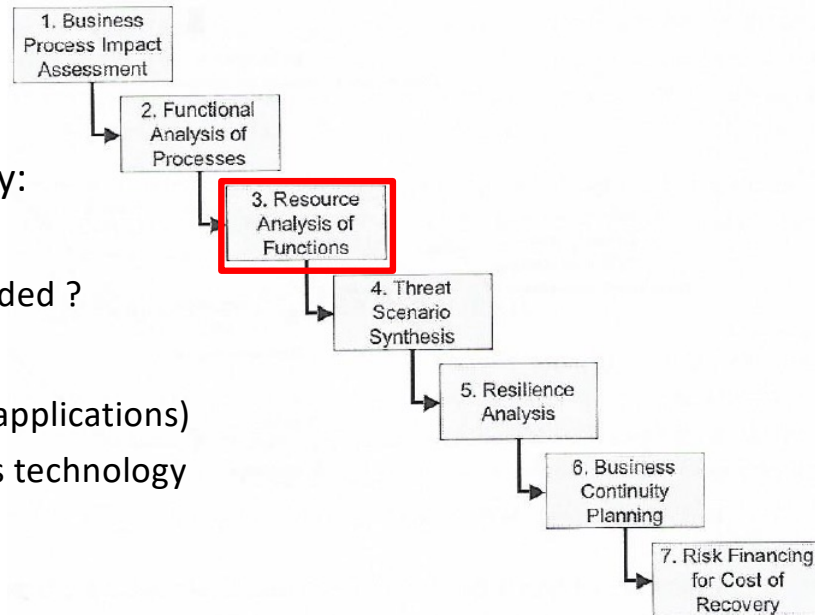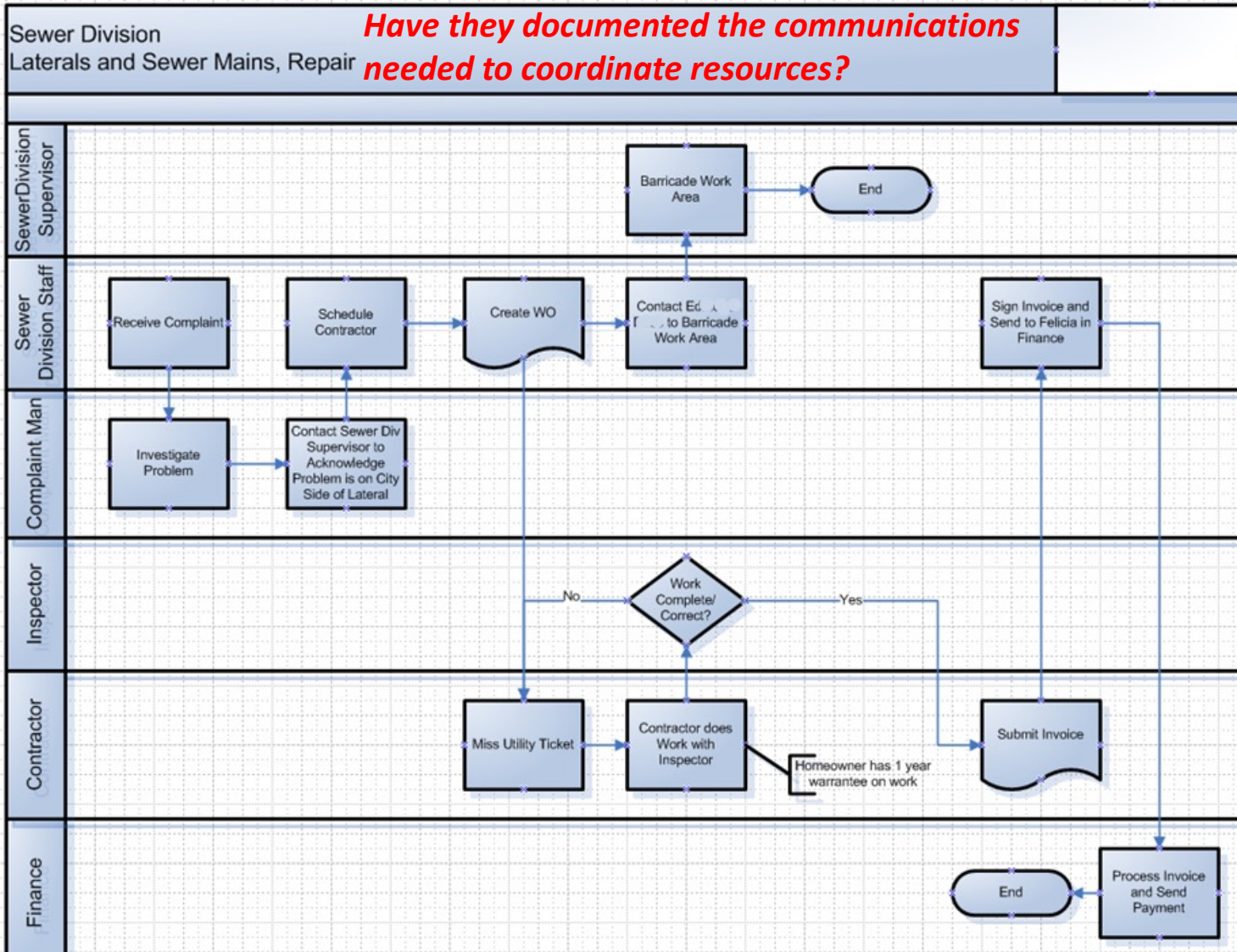
Sherwood, J., Clark, A. and Lynas D. (2005), <u>Enterprise Security Architecture,</u> CRC Press

Priorities for recovery example

Public Works Dept **Operations** **Division**	**Street Cleaning**	**Mow Grass**
		Clean Lots
		Street Cleaning - Mechanical and Manual
		Snow Removal
		Debris Removal (Emergency Response)
		Special Pick Ups
		Leaf Removal
		Neighborhood Cleanup
	Public Property	**Special Events**
		Special Projects
		Building Repair
		Tree Lighting
		Electrical Repair
		Potholes, Street Repair, and Resurfacing
		Special Event Blockade
		Catch Basin Repair
		Catch Basin Cleaning
		Garbage Collection

Operations Division
Street Cleaning - Debris Removal (Emergency Response)

Supervisor

Crew

Sewer Division
Repair & Replace Manhole (Frame and Cover)

Contributor(s) to this Process:
Michelle
Edmond

Finance

Process Invoice and Send Payment → End

Sewer Operations Supervisor

Receive Request or Complaint → Replace cover only? —Yes→ Replace Cover → End

Replace cover only? —No→

Engineering Division

Receive Call from Operations → Create WO → Schedule Contractor → Emergency?

Emergency? —Yes→
Emergency? —No (slow)→

Sign Invoice and Send to Felicia in Finance

Inspector

Meet with Contractor Before Work is Commenced

Work Complete/Correct? —No→
Work Complete/Correct? —Yes→

Sign Invoice

Contractor

Miss Utility Process → Complete Work → Send Invoice

Contractor will repair manhole frame and cover and provide traffic control, street barricades, and restore pavement after repair.

MIS 5206 Protec

Business Process Modeling

A collection of Swim Lane models document the work processes of each organizational division

Sewer Work processes

Business Process Modeling

Water work processes

Business Process Modeling

Transportation Work processes

Operations work processes

MIS 5206 Protecting Information Assets

Auditing the Business Continuity Plan

Step 3

- For each sub-process or function identified in Step 2, can you identify:
  - What resources are needed ?
  - How much of each resource is needed ?

    - People
    - Information systems (i.e. applications)
    - Data and communications technology
    - Other Equipment
    - …

1. Business Process Impact Assessment
2. Functional Analysis of Processes
3. Resource Analysis of Functions
4. Threat Scenario Synthesis
5. Resilience Analysis
6. Business Continuity Planning
7. Risk Financing for Cost of Recovery

Sherwood, J., Clark, A. and Lynas D. (2005), <u>Enterprise Security Architecture,</u> CRC Press

Have they mapped out the work processes and staff resources needed from each department?

	Work Types	Sewer Division						
		Street & Sewer	CSO System Supervisor	Chief Construction Inspector	Sewer Inspector	Construction Inspector	Complaint Person	CCTV Crew
Sewer Division — Sewer Collection	Laterals and Sewer Mains, Install (City)	■				■		
	Laterals and Sewer Mains, Install (Contractor)	■				■		
	Laterals and Sewer Mains, Repair	■			■		■	
	Manhole, Repair & Replace	■			■			
	Catch Basins, New	■			■			
	Catch Basins, Repair & Replace	■			■			
	Lamphole Repair & Replace	■			■			
	CCTV & Cleaning	■						■
	CSO Cleaning & Repairs	■	■					
	Street Repair (cave in)	■			■			
	Miss Utility Stake Outs		■	■				

Sewer Division
Laterals and Sewer Mains, Repair

SewerDivision Supervisor
- Barricade Work Area → End

Sewer Division Staff
- Receive Complaint → Schedule Contractor → Create WO → Contact Ed... ... to Barricade Work Area
- Sign Invoice and Send to Felicia in Finance

Complaint Man
- Investigate Problem
- Contact Sewer Div Supervisor to Acknowledge Problem is on City Side of Lateral

Inspector
- Work Complete/Correct? — No / Yes

Contractor
- Miss Utility Ticket → Contractor does Work with Inspector
- Homeowner has 1 year warrantee on work
- Submit Invoice

Finance
- End
- Process Invoice and Send Payment

Does the documentation enable you to understand the cross organizational business process workflows…

Sewer Division	Sewer Collection	Work Types	Operations Division																Other													
			Finance	Operations Director	Operations Center	Contractor Coordinator	Streets Crew	Street Cleaning Supervisor	Assistant Street Cleaning Supervisor	Foreman	Operations Crew	Mechanical Sweeper Crew	Street Sweeping Crew	Public Property Manager	Public Property Crew	Sewer Maintenance Supervisor	Sewer Crew	Sanitation Crew	Professional Services Consultant	Engineering Consultant	In house Contractors	Developer	L&I	GIS Technician	Fire Board	DELDOT	Delaware Dept of Natural Resources and Env.Control	Utility Contractor	DelMarva Power	City Council	Mayor	Police	Landlord
		Laterals and Sewer Mains, Install (City)	■																		■	■					■						
		Laterals and Sewer Mains, Install (Contractor)												■																			
		Laterals and Sewer Mains, Repair	■			■								■							■												
		Manhole, Repair & Replace	■											■			■				■												
		Catch Basins, New	■																		■												
		Catch Basins, Repair & Replace	■											■			■				■				■								
		Lamphole Repair & Replace	■														■																
		CCTV & Cleaning	■											■			■				■												
		CSO Cleaning & Repairs	■														■																
		Street Repair (cave in)	■																														
		Miss Utility Stake Outs																						■									

…identifying dependencies on critical paths for completing prioritized work processes

Who needs availability and access to the information?

…identifying dependencies on critical paths for completing prioritized work processes

Does the business understand resources needed to support mission critical work?

Note: Public Works tasks are often supported by staff from a number of Divisions, other City offices, and outside agencies

Does the business understand resources needed to support mission critical work?

Auditing the Business Continuity Plan

Step 4

- For each resource have they identified high-level threat scenarios that put that resource at risk?

- Have they focused on impacts, not causes?

1. Business Process Impact Assessment

2. Functional Analysis of Processes

3. Resource Analysis of Functions

4. Threat Scenario Synthesis

5. Resilience Analysis

6. Business Continuity Planning

7. Risk Financing for Cost of Recovery

Sherwood, J., Clark, A. and Lynas D. (2005), Enterprise Security Architecture, CRC Press

Auditing the Business Continuity Plan

Step 5

- For each resource/scenario combination
  - Are the current resources provided with sufficient resilience for the overall business to withstand impacts of the scenario?

- Are there any single points of failure?
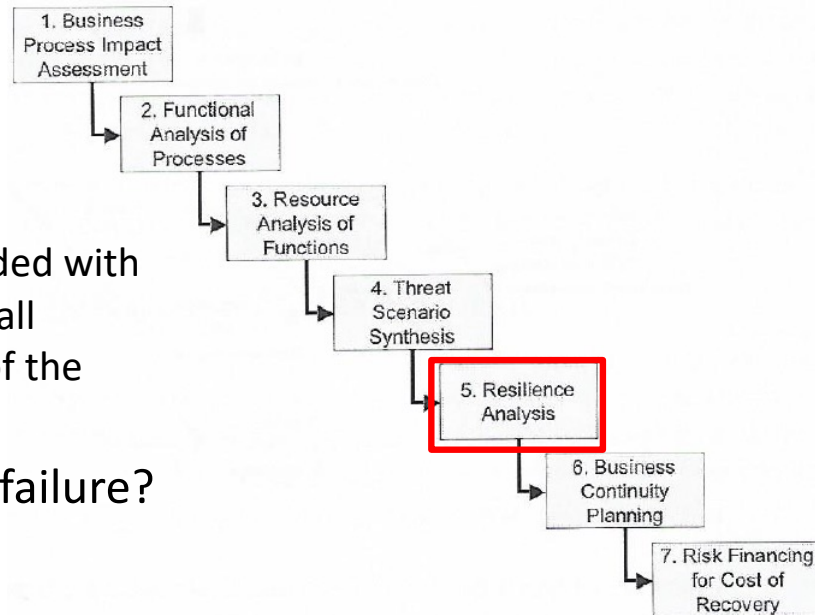
1. Business Process Impact Assessment
2. Functional Analysis of Processes
3. Resource Analysis of Functions
4. Threat Scenario Synthesis
5. Resilience Analysis
6. Business Continuity Planning
7. Risk Financing for Cost of Recovery

Sherwood, J., Clark, A. and Lynas D. (2005), Enterprise Security Architecture, CRC Press

Auditing the Business Continuity Plan

Step 6

- What additional resource protection is needed so overall business can withstand the threat scenarios?

- For example:

  – Preventive measures to avoid the threats materializing
  – Containment measures to limit the damage
  – Redundancy of resources to avoid single points of failure and to provide fallback capacity
  – Incident management plans
  – Recovery plans to resume business following an incident
  – Training and awareness

  Sherwood, J., Clark, A. and Lynas D. (2005), Enterprise Security Architecture, CRC Press


```
1. Business
Process Impact
Assessment

2. Functional
Analysis of
Processes

3. Resource
Analysis of
Functions

4. Threat
Scenario
Synthesis

5. Resilience
Analysis

6. Business
Continuity
Planning

7. Risk Financing
for Cost of
Recovery
```

CP-2	**CONTINGENCY PLAN**
	ASSESSMENT OBJECTIVE: *Determine if the organization:*

ASSESSMENT OBJECTIVE:

Determine if the organization:

CP-2(a)	develops and documents a contingency plan for the information system that:	
	CP-2(a)(1)	identifies essential missions and business functions and associated contingency requirements;
CP-2(a)(2)	CP-2(a)(2)[1]	provides recovery objectives;
	CP-2(a)(2)[2]	provides restoration priorities;
	CP-2(a)(2)[3]	provides metrics;
CP-2(a)(3)	CP-2(a)(3)[1]	addresses contingency roles;
	CP-2(a)(3)[2]	addresses contingency responsibilities;
	CP-2(a)(3)[3]	addresses assigned individuals with contact information;
CP-2(a)(4)	addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;	
CP-2(a)(5)	addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented;	
CP-2(a)(6)	CP-2(a)(6)[1]	defines personnel or roles to review and approve the contingency plan for the information system;
	CP-2(a)(6)[2]	is reviewed and approved by organization-defined personnel or roles;

	CP-2(e)[2]	problems encountered during plan implementation, execution, and testing;
CP-2(f)	CP-2(f)[1]	defines key contingency personnel (identified by name and/or by role) and organizational elements to whom contingency plan changes are to be communicated;

Business Impact Analysis (BIA) also answers

1. What are the work processes ?
2. How critical is each ?
3. What data, applications, and people are needed to run each critical process ?
4. What are the priorities for recovering information systems after disruption ?
5. For each critical IT resource, what is the :
   - **Recover time objective** (RTO):
     Maximum acceptable downtime
   - **Recovery point objective** (RPO):
     Maximum acceptable data loss (measured in time, but implies # of data records)
   - **Service delivery objective (SDO):**
     Level of services to be reached during the alternative process mode until the normal situation is restored
   - **Maximum tolerable outage (MTO):**
     Maximum time the organization can support processing in alternative mode

Auditing Recovery Plans

Have they documented:

1. Strategies, resources, timelines and dependencies?

2. Approaches to "re-initiate" crucial business functions and resume on-going operations?

Have the plans been reviewed and confirmed by function owners in the business as well as executives?

Contingency Planning (CP)

CONTROL NAME	BASELINES		
	LOW	MOD	HIGH
Contingency Planning Policy and Procedures	X	X	X
Contingency Plan	X	X	X
Contingency Training	X	X	X
Contingency Plan Testing	X	X	X
Alternative Storage Site		X	X
Alternative Processing Site		X	X
Telecommunications Services		X	X
Information System Backup	X	X	X
Information System Recovery and Reconstitution	X	X	X

CNTL NO.	CONTROL NAME Control Enhancement Name	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	Contingency Planning Policy and Procedures		X	X	X	X
CP-2	Contingency Plan		X	X	X	X
CP-2(1)	CONTINGENCY PLAN	COORDINATE WITH RELATED PLANS				X	X
CP-2(2)	CONTINGENCY PLAN	CAPACITY PLANNING					X
CP-2(3)	CONTINGENCY PLAN	RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS				X	X
CP-2(4)	CONTINGENCY PLAN	RESUME ALL MISSIONS / BUSINESS FUNCTIONS					X
	AL MISSIONS / BUSINESS					X
	SSETS				X	X
	NTS			X		X
				X	X	X
	E WITH RELATED PLANS			X		X	X
	PROCESSING SITE			X		X
		X	Incorporated into CP-2.			
	FROM PRIMARY SITE				X	X
	ME / POINT OBJECTIVES					X
					X	X
	ON FROM PRIMARY SITE				X	X
	LITY				X	X
	OF SERVICE				X	X
	TION FOR USE					X
	NT INFORMATION	X	Incorporated into CP-7.			
					X	X
	TY OF SERVICE				X	X
	POINTS OF FAILURE				X	X
	ATION OF PRIMARY /					X
	ER CONTINGENCY PLAN					X
	OR RELIABILITY /			X	X	X
					X	X
	TORATION USING					X
	E STORAGE FOR CRITICAL					X
	ION FROM UNAUTHORIZED	X	Incorporated into CP-9.			
	R TO ALTERNATE					X
	reconstitution			X	X	X
	CONSTITUTION		X	Incorporated into CP-4.			
	CONSTITUTION					X	X
CP-10(3)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	COMPENSATING SECURITY CONTROLS	X	Addressed by tailoring procedures.			
CP-10(4)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	RESTORE WITHIN TIME PERIOD					X
CP-10(5)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	FAILOVER CAPABILITY	X	Incorporated into SI-13.			

What kind of offsite alternative recovery facility do they have ?

Hot site: A geographically remote facility, fully equipped and ready to power up at a moments notice

Warm site: Includes communications components but computers are not installed – will need to be delivered and setup

Cold site: Provides only the basic environment that can be outfitted with communication, utilities and computers

Site	Cost	Hardware Equipment	Telecommunications	Setup Time
Hot Site	High	Full	Full	Short
Warm Site	Medium	Partial	Full / Partial	Medium
Cold Site	Low	None	None	Long

High Availability   Hot Site

Seconds Minutes Hours Days Weeks

Recovery Time Objective (RTO)

What kind of offsite alternative recovery facility do they have ? (continued)

Mobile site: A packaged modular processing facility mounted on transportable vehicles and kept ready to be delivered and set up at a location specified on activation

Shared site: Least expensive arrangement ("reciprocal agreements") with compatible companies who agree to host each other's employees and business functions in the event of a disaster

- *Most risky alterative - few companies maintain extra capacity and equipment suitable to host another company's business processes*
- *Better than having no plan at all*

Location of Alternate Site

Disaster recovery site should be in a different geophysical area not susceptible to same disaster as the primary operations facility

Note: even the cloud is located somewhere...
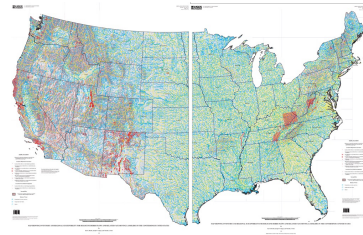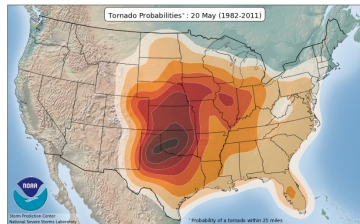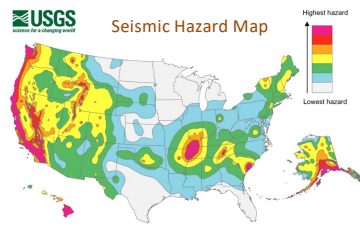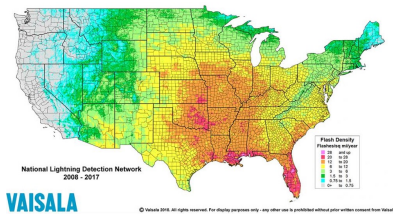
With multiple providers of:

US Long-haul High-Speed Internet Fiber Network
MIT Technology Review, 9/15/2015

Red squares show cable junctions located mostly in major population centers
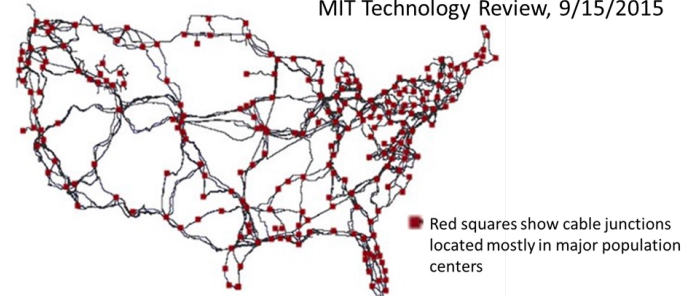
- Telecommunications
- Stable power supply
- Redundant utilities

Data backup systems and redundancies

- **Database shadowing**
- **Electronic vaulting**
- **Remote journaling**
- **Storage area network and hierarchical storage management**
- **Shared storage**
- **RAID** (Redundant Array of Independent Disks)
- **Failover clustering**
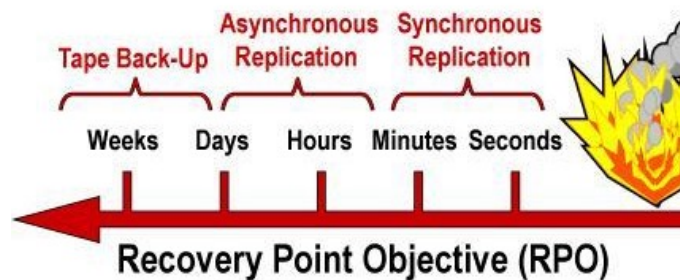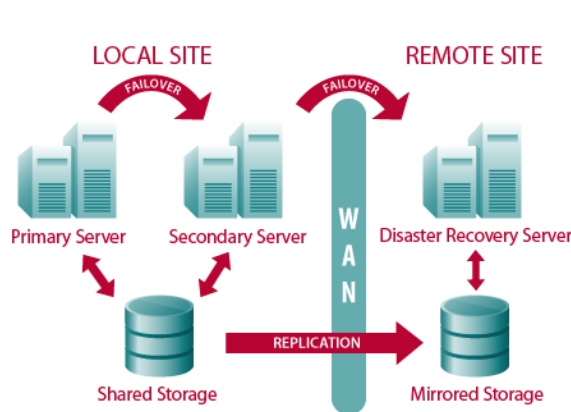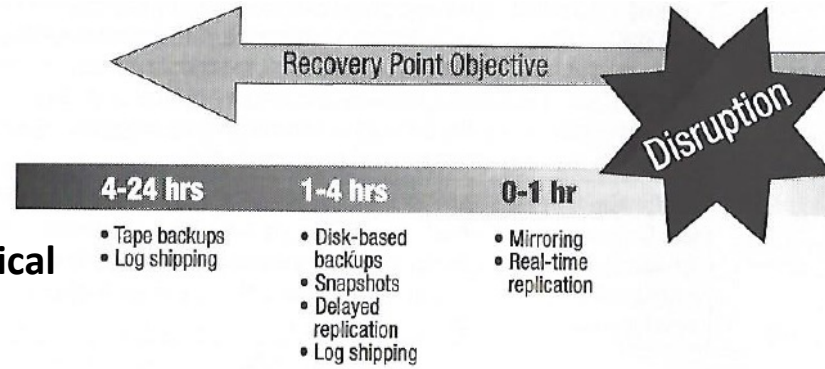
Recovery Site Options: Location strategy & Backup technology

Information System Recovery Priority	Backup / Recovery Strategy	
High priority	**Backup:** Mirrored systems and disc replication **Strategy:** Hot site	$$$
Moderate priority	**Backup:** Optical backup and WAN/VLAN replication **Strategy:** Warm or Cold site	$$
Low priority	**Backup:** Tape backup **Strategy:** Cold site	$

NIST SP 800-34 R1
Contingency Planning Guide for Federal Information Systems

Recovery Time Objective

High Availability   *Hot Site*

Seconds Minutes Hours   Days   Weeks

Facility strategy

Recovery Point Objective

Synchronous Replication   *Asynchronous Replication*   *Tape Backup*

Seconds Minutes Hours   Days   Weeks

Data backup
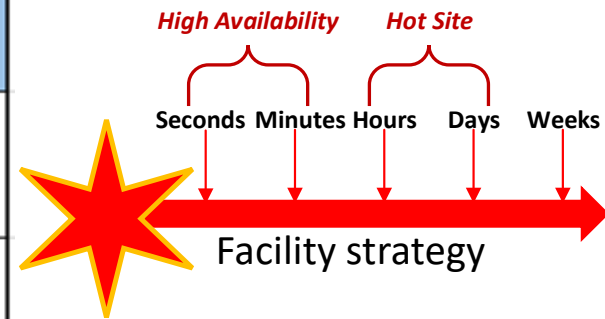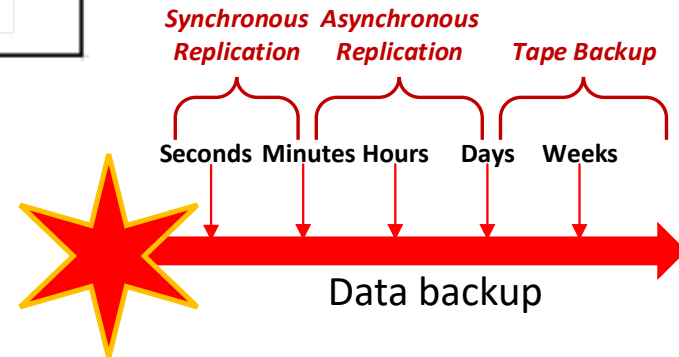
Backup Mitigation – Best Practice

Three-Two-One rule

– Make 3 copies of all mission critical software and corresponding data in 2 different formats (to run on Linux and Windows machines), with 1 copy stored off-site not connected to any network

Information System Recovery Priority	Backup / Recovery Strategy	
High priority	**Backup:** Mirrored systems and disc replication **Strategy:** Hot site	$$$
Moderate priority	**Backup:** Optical backup and WAN/VLAN replication **Strategy:** Warm or Cold site	$$
Low priority	**Backup:** Tape backup **Strategy:** Cold site	$

cheap
(money)

fast
(time)

good
(quality)

The Quality Triangle:

Pick Two

Disaster recovery time targets

Disaster recovery must be achieved within critical deadlines
- Need for careful analysis
  - Of business needs for recovery of services
  - Time-criticality of various information services

Speed of recovery must be traded off against cost
- If needed, non-stop 365 day by 24-hour service can be maintained, but it pushes the cost up very high
- Business needs and justifications must be detailed to plan disaster recovery
  - Remember: *The only goal is to create effective business continuity, whatever that needs to be*
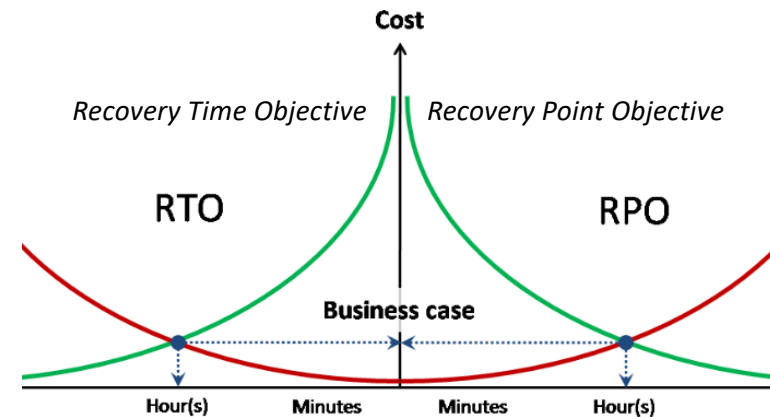
Have they classified their application systems and scheduled their restoration?

Example Classification of Applications*

Classification		Description
1	Mission Critical	Mission Critical to accomplishing the mission of the organization Can be performed only by computers No alternative manual processing capability exists Must be restored within 36 hours
2	Critical	Critical in accomplishing the work of the organization Primarily performed by computers Can be performed manually for a limited time period Must be restored starting at 36 hours and within 5 days
3	Essential	Essential in completing the work of the organization Performed by computers Can be performed manually for an extended time period Can be restored as early as 5 days, however it can take longer

* From SANS

Have they properly planned the availability of replacement software?

- In addition to data…

  - Operating systems, programs and utilities used during regular business must also be backed up regularly to the offsite facility

- An application built for a one version of an operating system, will not run if different (wrong) version of the operating system is installed at the offsite facility

  - Data is often formatted to work in a particular version of a program,

    - If that version is not available at the backup facility, it is possible that the data will not be available for use in the time of need

CP-2	CONTINGENCY PLAN
	ASSESSMENT OBJECTIVE:
	Determine if the organization:

...an for the information system that:
...and business functions and associated
...overy objectives;
...oration priorities;
...rics;
...ntingency roles;
...ntingency responsibilities;
...signed individuals with contact

...tial missions and business functions
...n disruption, compromise, or failure;
...rmation system restoration without
...safeguards originally planned and

...nnel or roles to review and approve
...ncy plan for the information system;
...nd approved by organization-defined
...roles;

...nnel (identified by name and/or by
...ements to whom copies of the
...istributed;
...ntingency plan to organization-defined
...nd organizational elements;
...es with incident handling activities;
...w the contingency plan for the
...n with the organization-defined

...information system, or environment of

ASSESSMENT OBJECTIVE:

Determine if the organization:

CP-2(a)	develops and documents a contingency plan for the information system that:		
	CP-2(a)(1)		identifies essential missions and business functions and associated contingency requirements;
	CP-2(a)(2)	CP-2(a)(2)[1]	provides recovery objectives;
		CP-2(a)(2)[2]	provides restoration priorities;
		CP-2(a)(2)[3]	provides metrics;
	CP-2(a)(3)	CP-2(a)(3)[1]	addresses contingency roles;
		CP-2(a)(3)[2]	addresses contingency responsibilities;
		CP-2(a)(3)[3]	addresses assigned individuals with contact information;
	CP-2(a)(4)		addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
	CP-2(a)(5)		addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented;
	CP-2(a)(6)	CP-2(a)(6)[1]	defines personnel or roles to review and approve the contingency plan for the information system;
		CP-2(a)(6)[2]	is reviewed and approved by organization-defined personnel or rol...

	CP-2(e)[2]	problems encountered during plan implementation, execution, and testing;
CP-2(f)	CP-2(f)[1]	defines key contingency personnel (identified by name and/or by role) and organizational elements to whom contingency plan changes are to be communicated;

Have they planned for the availability of people after disaster?

- Attention focused on backing up and restoring data and technology, often overlooks people and necessary skillsets for continuing the operation of the enterprise
- Who is responsible for calling it a "disaster" to begin DRP implementation?
- Employees may not be available after a disaster:
  - Due to death, injury, or family responsibilities
  - Business continuity committee
    - Must identify the necessary skill set for each critical task
    - Need back-up solutions (e.g. using temp agencies or cross training individuals)

Do they have Recovery Teams?

After a disaster two teams may be assembled:

1. **Recovery team**
    - – Coordinates bringing up the alternative site
    - – To be sure everyone knows what to do, tests are conducted
      - Range from troubleshooting the plan by simply walking through documents detailing the sequence of events, rehearsing the plan up to the point of actual data or resource recovery at the main site

2. **Salvage team**
    - – Assesses damage and works to bring the businesses' primary facility back on-line

BCP & DRP Templates are Available

NIST Special Publication 800-34 Rev. 1

Contingency Planning Guide for Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

May 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

TABLE OF CONTENTS

Question

Is it practical to conduct a thorough test of a Business Continuity Plan (BCP)?

- *Why might it not be practical?*
- *If it is not practical, what alternative ways can you recommend for testing a BCP?*

Disaster Recovery and Business Continuity Plans must be practiced and tested

…to be sure the plan is good, everyone is prepared, and knows what to do

Can range from:
- *Checklist review*
- *Tabletop exercise*
- *Structured walk-through*
- *Dry-Run tests*

**Common Failures in Activating
Disaster Recovery & Business Continuity Plans**

Event not identified
Plan not documented
System priorities not identified
Insufficient training
Insufficient power
Communications not in place
Unable to find passwords
Plan not up-to-date
Errors in plan

0% 10% 20% 30% 40% 50% 60% 70%

Janco Associates, Inc. (2012)
https://www.e-janco.com/PR20110304.html
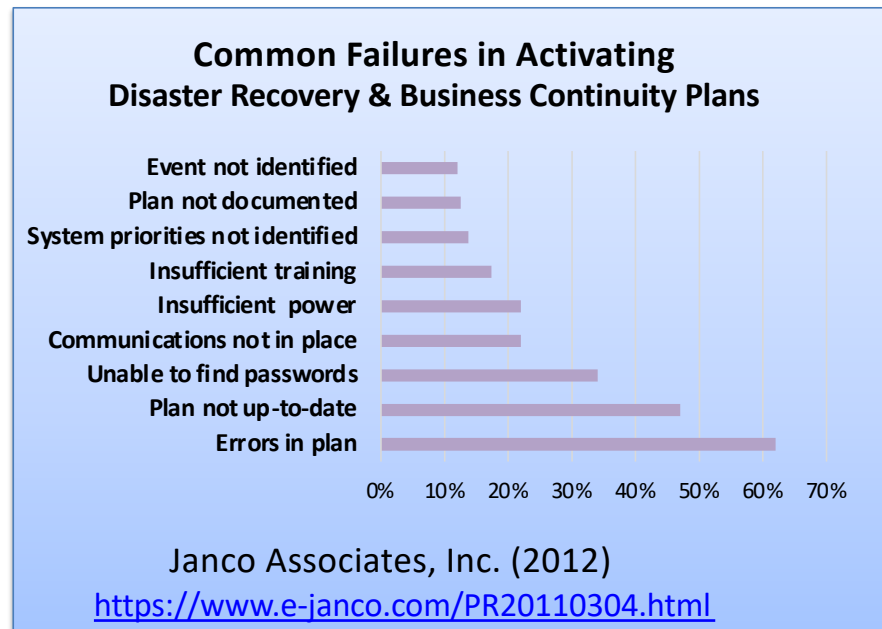
What DRP Tests have been conducted?

- **Checklist review**
  - Simplest, least labor-intensive form of testing
  - Each person has a checklist of responsibilities under the DRP
  - During testing: each person reviews his/her checklist
  - Can be done individually or as a group

- **Tabletop exercise**
  - Test facilitator descries a specific disaster scenario
  - DRP team members verbally walk through their responses to the scenario
  - Scenarios can be disseminated at the test or in advance

Exercise Your Plan

What DRP Tests have been conducted?

- **Structured walk-through**
  - More formal troubleshooting of the plan by simply walking through the documents detailing the sequence of events

- **Dry-Run tests**
  - Can be conducted on a function by function basis
  - Do not have test all functions for each cycle
  - Tests should involve actual interruptions and recoveries
  - Rehearsing the plan up to the point of actual data or resource recovery at the main site

Exercise Your Plan

Audit Focus

Areas for
IT Audit
evaluation:

Figure 3—Possible Tests/Procedures for Backup and Recovery	
Data	• Review or observe backup procedures. • Review documentation of a successful restore (within the last year). • Verify restoration personally (when risk is high or restoration is an audit objective).
Site/computers/OS	• Review the provisions of the BCP/DRP. • Review a contract (hot site, cold site, mutual aid, etc.). • Verify the ability to restore these aspects.
Applications	• Review the plan's provisions. • Review the critical applications list, including ranking. • Verify the ability to restore (personally, when risk is high or restoration is an audit objective). • Observe or inquire about the backups of application software and location.
Supplies/documentation	• Review the plan's provisions. • Observe or inquire about the provisions and location.
Recovery team	• Review the plan's provisions. • Interview one or more members of the team, and ask about roles and responsibilities. • Gain assurance that there is provision for adequate personnel for a successful restoration.

Test Taking Tip

Don't Revise Your Answer
(without a very strong reason)

- Your first answer is probably the right one

- On an exam where there is no penalty for wrong answers, you are just using time that might have gone to getting another correct answer

- If you are having second thoughts, plan to come back to that question after you have completed the entire test

1. The BEST method for assessing the effectiveness of a business continuity plan is to review the:
   a) Plans and compare them to appropriate standards
   b) Results from previous tests
   c) Emergency procedures and employee training
   d) Offsite storage and environmental controls

1. The BEST method for assessing the effectiveness of a business continuity plan is to review the:
   a) Plans and compare them to appropriate standards
   b) Results from previous tests
   c) Emergency procedures and employee training
   d) Offsite storage and environmental controls

2. With respect to business continuity strategies, an information system (IS) auditor interviews key stakeholders in an organization to determine whether they understand their roles and responsibilities. The IS auditor is attempting to evaluate the:
   a) Clarity and simplicity of the business continuity plans
   b) Adequacy of the business continuity plans
   c) Effectiveness of the business continuity plans
   d) Ability of IT and end-user personnel to respond effectively in emergencies

3. During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will PRIMARILY influence the:
   a) Responsibility for maintaining the business continuity plan
   b) Criteria for selecting a recovery site provider
   c) Recovery strategy
   d) Responsibilities of key personnel

3. During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will PRIMARILY influence the:
   a) Responsibility for maintaining the business continuity plan
   b) Criteria for selecting a recovery site provider
   c) Recovery strategy
   d) Responsibilities of key personnel

4. During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The MAJOR risk associated with this is that:
   a) Assessment of the situation may be delayed
   b) Execution of the disaster recovery plan could be impacted
   c) Notification of the media might not occur
   d) Potential crisis recognition might be ineffective

4. During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The MAJOR risk associated with this is that:
   a) Assessment of the situation may be delayed
   b) Execution of the disaster recovery plan could be impacted
   c) Notification of the media might not occur
   d) Potential crisis recognition might be ineffective

5. An organization has just completed their annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?
   a) Review and evaluate the business continuity plan for adequacy
   b) Perform a full simulation of the business continuity plan
   c) Train and educate employees regarding the business continuity plan
   d) Notify critical contacts in the business continuity plan

5. An organization has just completed their annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?
   a) Review and evaluate the business continuity plan for adequacy
   b) Perform a full simulation of the business continuity plan
   c) Train and educate employees regarding the business continuity plan
   d) Notify critical contacts in the business continuity plan

6. Integrating business continuity planning (BCP) into an IS project aids in:
   a) The retrofitting of the business continuity requirements
   b) The development of a more comprehensive set of requirements
   c) The development of a transaction flowchart
   d) Ensuring the application meets the user's needs

6. Integrating business continuity planning (BCP) into an IS project aids in:
   a) The retrofitting of the business continuity requirements
   b) The development of a more comprehensive set of requirements
   c) The development of a transaction flowchart
   d) Ensuring the application meets the user's needs

7. While observing a full simulation of the business continuity plan, an IS auditor
    notices that the notification systems within the organizational facilities could be
    severely impacted by infrastructural damage. The BEST recommendation the IS
    auditor can provide to the organization is to ensure:
    a) The salvage team is trained to use the notification system
    b) The notification system provides for the recovery of the backup
    c) Redundancies are built into the notification system
    d) The notification systems are stored in a vault

8. The activation of an enterprise's business continuity plan should be based on predetermined criteria that address the:
   a) Duration of the outage
   b) Type of outage
   c) Probability of the outage
   d) Cause of the outage

9. An organization has outsourced its wide area network (WAN) to a third-party service provider. Under these circumstances, which of the following is the PRIMARY task the IS auditor should perform during an audit of business continuity (BCP) and disaster recovery planning (DRP)?
   a) Review whether the service provider's BCP process is aligned with the organization's BCP and contractual obligations
   b) Review whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster
   c) Review the methodology adopted by the organization in choosing the service provider
   d) Review the accreditation of the third-party service provider's staff

10. An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:
    a) Alignment of the BCP with industry best practices
    b) Results of business continuity tests performed by IT and end-user personnel
    c) Off-site facility, its contents, security and environmental controls.
    d) Annual financial cost of the BCP activities versus the expected benefit of implementation of the plan

Agenda

✓ In The News

✓ Business Continuity and Disaster Recovery Planning

✓ Test Taking Tip

✓ Quiz

Protecting Information Assets
- Unit# 9 -

Business Continuity and Disaster Recovery Planning