

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

In The News

Nishant Shah says

OCTOBER 14, 2022 AT 12:42 AM

Air gap is a concept of storage and backup that aims at segregating production systems from the backup data location. This helps in preventing malware from reaching the backup site and locking up the data.

However, most companies today store backup data digitally which requires logical air gaps through the use of access controls to isolate secondary sites from the production and primary backup sites. Backups are still vulnerable to getting infected so there is also a certain need for using anomaly detection.

The bottom line is that air gapped systems can be a valuable protection against security threats, including from ransomware, but they are not invulnerable to infection, corruption and human errors.

So, as with all data protection measures, they are best used as part of a suite of security measures.

In The News

Pranavi Yadalam Sekhar says

OCTOBER 17, 2022 AT 10:26 PM

Businesses in Canada Warned Not to Overlook Cybersecurity As Recession Looms

KPMG International's Global CEO Outlook Survey asked CEOs what keeps them up at night. Cybersecurity ranked seventh behind economy, regulatory issues and disruptive technologies. Those who said they were "underprepared" for a cyber-attack jumped three-fold. 75% of large companies agree that cybersecurity is a strategic business imperative. Small and medium-sized businesses feel more prepared to handle a cyber-attack, according to a survey by KPMG in Canada.

More than half of SMBs have said they have been victims of cybercrime in the past year. Almost 8 in 10 SMBs say building a cybersecurity culture is just as important as building technological controls.

In The News

Interview: Microsoft Shares Its Experience of Migrating Data in Times of Cyber Warfare

Microsoft's EMEA chief security advisor Sarah Armstrong-Smith warned about the surge of cyber-risks that organizations are facing today, during Big Data London on September 22, 2022. This acceleration is due, she said, to the conjunction of an increased threat following the war in Ukraine on the one hand, and accelerating digital transformation on the other, with generalized hybrid working, a massive acceleration of cloud migration and the convergence between IT, OT and IoT networks.

"In Teams alone, we went from 17m active users before the pandemic to over 250m today, and 2bn minutes of collaboration every day," she counted in front of the audience.

Infosecurity Magazine asked her how Big Tech, and particularly Microsoft, could help companies overcome these challenges while minimizing security risks.

Sarah Armstrong-Smith: With the war in Ukraine, we started to see companies that become a lot more cognizant about the distribution of data. In times of peace, everyone tries to keep their data as close to them as possible. Now, we see a lot more customers, particularly larger enterprises, wanting to be able to move their data fast, not just in the cloud but sometimes out of the country. Also, they want to know exactly where all their applications are hosted, even when it's in the cloud – both because regulators are getting stricter, asking them for transparency and to be able to accelerate the migration when needed.

As a leading provider of cloud services, with Azure, Microsoft 365 and Dynamics, we have over 220 data centers and we use AIOps, utilizing machine learning capability to constantly monitor those data centers.

In The News

Sunam Rijal says

OCTOBER 18, 2022 AT 11:21 AM

Shocking data loss and disaster recovery statistics

<https://www.comparitech.com/data-recovery-software/disaster-recovery-data-loss-statistics/>

This article provides some statistics related to data loss and disaster recovery such as

- >ransomware attacks cause an average of 16.2 days of downtime,
- >average cost of downtime is \$1410 per minute,
- >more than 51% of small and medium sized businesses don't have an IRP in place.
- > Average time to identify data breach is 287 days.
- > After paying ransom amount, only 8% of victims recover all of their data.
- > Average ransomware victim loses around 35% of their data

This article also talks about DRP, the tips for an effective DRP and causes of data loss

In The News

Mengqi Xiong says

OCTOBER 18, 2022 AT 5:24 PM

When suspicious or abnormal activities are found, the Security Operation Center (SOC) will give an alarm and can respond quickly to reduce the potential impact and severity of security incidents. Without SOC, organizations lack real-time visibility of threats, which hinders their ability to protect business-critical assets and effectively manage information risks. The work of network security standards and compliance is constantly promoting the development of security products and practices. Security operations have begun to change from passive to active, and the network security system has been built from four dimensions defense, detection, response, and prediction. The concept of a "closed loop" for security operations has also been formed accordingly.

The modern security operation center can realize the global monitoring and real-time analysis of cloud files and process behaviors at the system kernel level, effectively bypassing the Anti-reconnaissance capability of malicious programs; It can also mine malicious threats that cannot be identified in the blacklist based on program behavior analysis to achieve active interception. Through the integration and correlation of external threats and internal threats, the severity is defined based on forming high-quality security analysis warnings. For example, from suspicious IP addresses and associations to visited users, from suspicious users to their applications, databases, or relevant sensitive files, etc., the behavior sequence of malicious acts can be determined in the time dimension, and the related threat location can be further carried out. SOC must take a more proactive approach to discover previously unknown threats or unmitigated persistent threats in its cloud infrastructure. Because complex high-level persistent threats can be hidden for weeks or even months, modern SOC teams must be trained to supplement the deficiencies of the automation system and search for hidden malware or attackers by finding suspicious activity patterns.

In The News

Asha Kunchakarra says

OCTOBER 19, 2022 AT 4:02 PM

Keystone Health, a Pennsylvania based healthcare system provider, suffered a major data breach exposing the protected health information (PHI) of close to a quarter million people. They noticed an incident on August 19th when there was an interference with Keystone IT systems. Threat actors were lurking in the organization's systems for three weeks. Some of the files contained patient information, including names, SSN, and clinical information. The breach has impacted over 235,000 people. Threat actors often target hospitals since most healthcare organizations have scant cybersecurity budgets and are extremely sensitive to downtime. They also store extremely sensitive data making it valuable in the hands of threat actors. A survey was conducted which resulted in saying that ransomware attacks against healthcare have become so frequent that some insurers either refuse to take in hospitals or leave the market.

In The News

Asha Kunchakarra says

OCTOBER 19, 2022 AT 4:02 PM

Keystone Health, a Pennsylvania based healthcare system provider, suffered a major data breach exposing the protected health information (PHI) of close to a quarter million people. They noticed an incident on August 19th when there was an interference with Keystone IT systems. Threat actors were lurking in the organization's systems for three weeks. Some of the files contained patient information, including names, SSN, and clinical information. The breach has impacted over 235,000 people. Threat actors often target hospitals since most healthcare organizations have scant cybersecurity budgets and are extremely sensitive to downtime. They also store extremely sensitive data making it valuable in the hands of threat actors. A survey was conducted which resulted in saying that ransomware attacks against healthcare have become so frequent that some insurers either refuse to take in hospitals or leave the market.

In The News

Frank Kofi Kpotivi says

OCTOBER 19, 2022 AT 8:51 PM

Indian Energy Company Tata Power's IT Infrastructure Hit By Cyber Attack

Tata Power Company Limited, India's largest integrated power company, on Friday confirmed it was targeted by a cyber attack.

The intrusion on IT infrastructure impacted "some of its IT systems," the company said in a filing with the National Stock Exchange (NSE) of India.

CyberSecurity

It further said it has taken steps to retrieve and restore the affected machines, adding it put in place security guardrails for customer-facing portals to prevent unauthorized access.

The Mumbai-based electric utility company, part of the Tata Group conglomerate, did not disclose any further details about the nature of the attack, or when it took place.

That said, cybersecurity firm Recorded Future in April disclosed attacks mounted by China-linked adversaries targeting Indian power grid organizations.

The network intrusions were said to have been aimed at "at least seven Indian State Load Despatch Centres (SLDCs) responsible for carrying out real-time operations for grid control and electricity dispatch within these respective states."

In The News

Wei Zhang says

OCTOBER 19, 2022 AT 10:19 PM

Digital Natives Are Undermining Corporate Security – Report

Ernst & Young, a consultancy giant, suggests that digital natives are more likely than digital migrants to ignore security practices. While 76 percent of respondents believe they understand cybersecurity, more than half of Gen Z and 42 percent of millennials say they will ignore mandatory updates for as long as possible, compared with 31 percent of digital immigrants. Younger workers are also more likely to use the same passwords for both their work and personal accounts. Perhaps because of growing up in the digital age and being exposed to a large amount of information every day, digital natives have a weak awareness of information security protection.

In The News

Elizaveta Ibeme says

OCTOBER 19, 2022 AT 10:58 PM

Police tricks DeadBolt ransomware out of 155 decryption keys

DeadBolt attack targeted Qnap Nas owners since January 2022 through ransomware attacks. During this time users received a message that their data has been encrypted and payment of 0.05 BTC is needed to receive a decryption key. The attackers kindly note that users are not targeted and the main purpose of this attack is to catch the attention of Qnap. Another message is addressed to Qnap as a company offering to provide the universal decryption key for 50 BTC and detail on how to page this zero-day vulnerability for 10 BTC. Luckily, Dutch police were able to retrieve the decryption keys for 90% of all reported incidents. The police made ransomware payments with minimal fees during a high traffic period of use for Bitcoin. The police received the decryption keys and then canceled the transactions before Bitcoin was able to register them. After the police were able to retrieve decryption keys without paying, DeadBolt set up a two-factor verification, that confirms that the Bitcoin transaction is completed before providing the decryption key. Ransomware attacks will persist as long as users and companies are willing to pay the ransom. Not all ransomware attacks are being reported and/or investigated.

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

Source: ISO 22301:2012

Societal security – Business continuity management systems - Requirements

...includes a Disaster Recovery Plan (DRP)

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

Case study: MAERSK shipping

- 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 all wiped out
 - 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	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

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information Systems

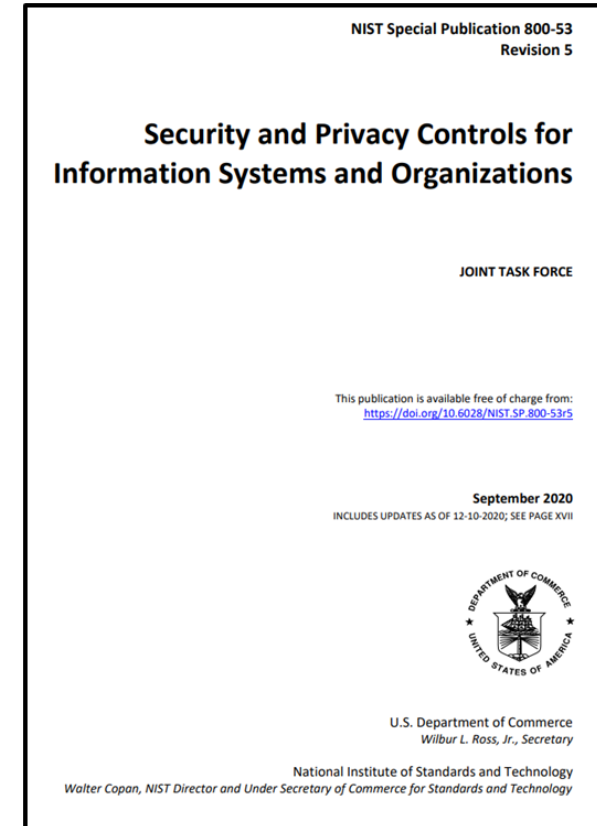
	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations,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

	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.

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



Business Continuity Plan (BCP)

3 Phases of disaster contingency response :

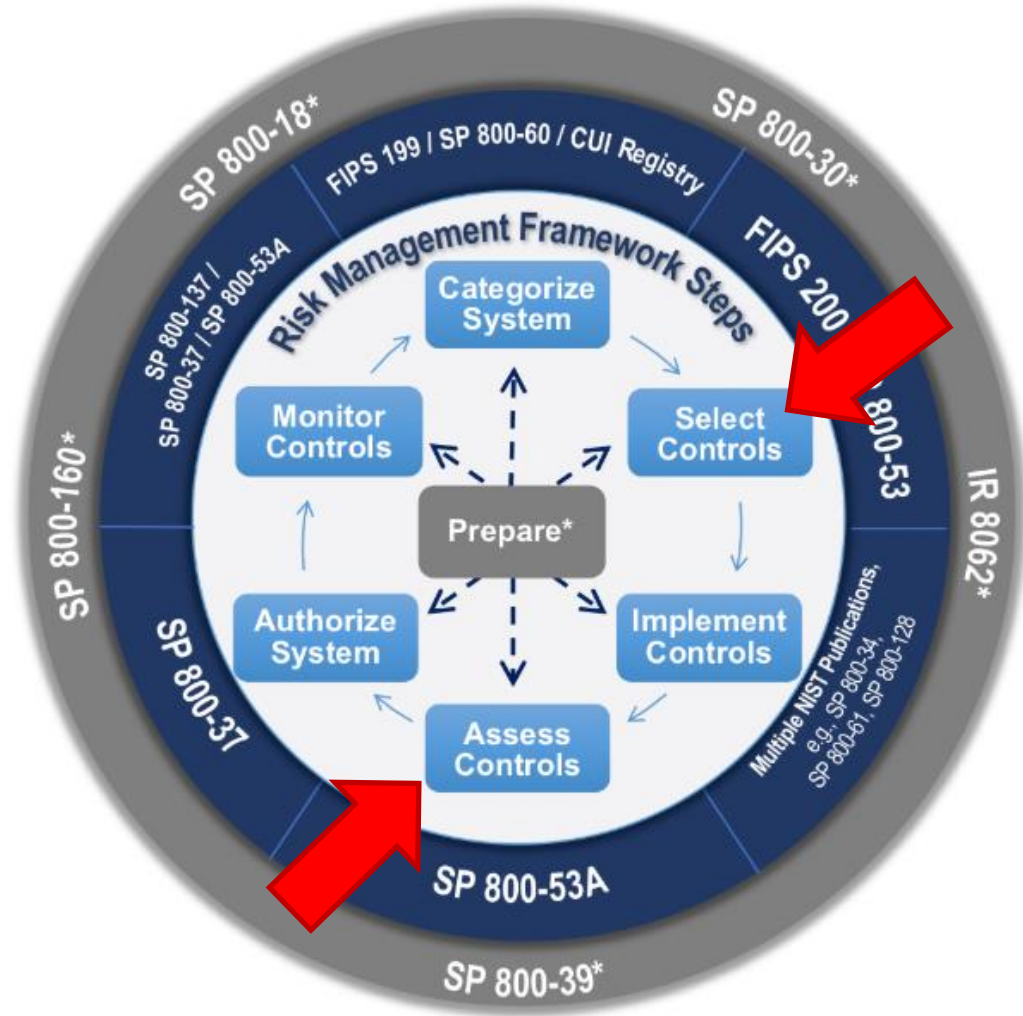
1. Activation and Notification

- 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




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


DRAFT NIST Special Publication 800-53A
 Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53Ar5-draft>

August 2021



U.S. Department of Commerce
 Gina M. Raimondo, Secretary

National Institute of Standards and Technology
 James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

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

Contingency Planning (CP)

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES			CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES																																										
			LOW	MOD	HIGH				LOW	MOD	HIGH																																								
CP-1	Policy and Procedures		x	x	x	CP-8(2)	SINGLE POINTS OF FAILURE			x	x																																								
CP-2	Contingency Plan		x	x	x	CP-8(3)	SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS				x																																								
CP-2(1)	COORDINATE WITH RELATED PLANS			x	x	CP-8(4)	PROVIDER CONTINGENCY PLAN				x																																								
CP-2(2)	CAPACITY PLANNING				x	CP-8(5)	ALTERNATE TELECOMMUNICATION SERVICE TESTING																																												
CP-2(3)	RESUME MISSION AND BUSINESS FUNCTIONS			x	x	CP-9	System Backup		x	x	x																																								
CP-2(4)	RESUME ALL MISSION AND BUSINESS FUNCTIONS		W: Incorporated into CP-2(3).			CP-9(1)	TESTING FOR RELIABILITY AND INTEGRITY			x	x																																								
CP-2(5)	CONTINUE MISSION AND BUSINESS FUNCTIONS				x	CP-9(2)	TEST RESTORATION USING SAMPLING				x																																								
CP-2(6)	ALTERNATE PROCESSING AND STORAGE SITES		<div style="text-align: center;"> <h2>CONTROL NAME</h2> <table border="1" style="margin: auto;"> <thead> <tr> <th rowspan="2"></th> <th colspan="3">BASELINES</th> </tr> <tr> <th>LOW</th> <th>MOD</th> <th>HIGH</th> </tr> </thead> <tbody> <tr> <td>Contingency Planning Policy and Procedures</td> <td>X</td> <td>X</td> <td>X</td> </tr> <tr> <td>Contingency Plan</td> <td>X</td> <td>X</td> <td>X</td> </tr> <tr> <td>Contingency Training</td> <td>X</td> <td>X</td> <td>X</td> </tr> <tr> <td>Contingency Plan Testing</td> <td>X</td> <td>X</td> <td>X</td> </tr> <tr> <td>Alternative Storage Site</td> <td></td> <td>X</td> <td>X</td> </tr> <tr> <td>Alternative Processing Site</td> <td></td> <td>X</td> <td>X</td> </tr> <tr> <td>Telecommunications Services</td> <td></td> <td>X</td> <td>X</td> </tr> <tr> <td>Information System Backup</td> <td>X</td> <td>X</td> <td>X</td> </tr> <tr> <td>Information System Recovery and Reconstitution</td> <td>X</td> <td>X</td> <td>X</td> </tr> </tbody> </table> </div>				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			
	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																																																
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																																																		

CP-2	CONTINGENCY PLAN
	ASSESSMENT OBJECTIVE: <i>Determine if the organization:</i>

ASSESSMENT OBJECTIVE:
Determine if the organization:

NIST Spec

Assessing Security Controls in Federal Systems and (Building Eff

TR

This

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

*in for the information system that:
and business functions and associated
covery 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;
tingency plan to organization-defined
nd organizational elements;
es with incident handling activities;
v the contingency plan for the
1 with the organization-defined
information system, or environment of*

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

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 ?

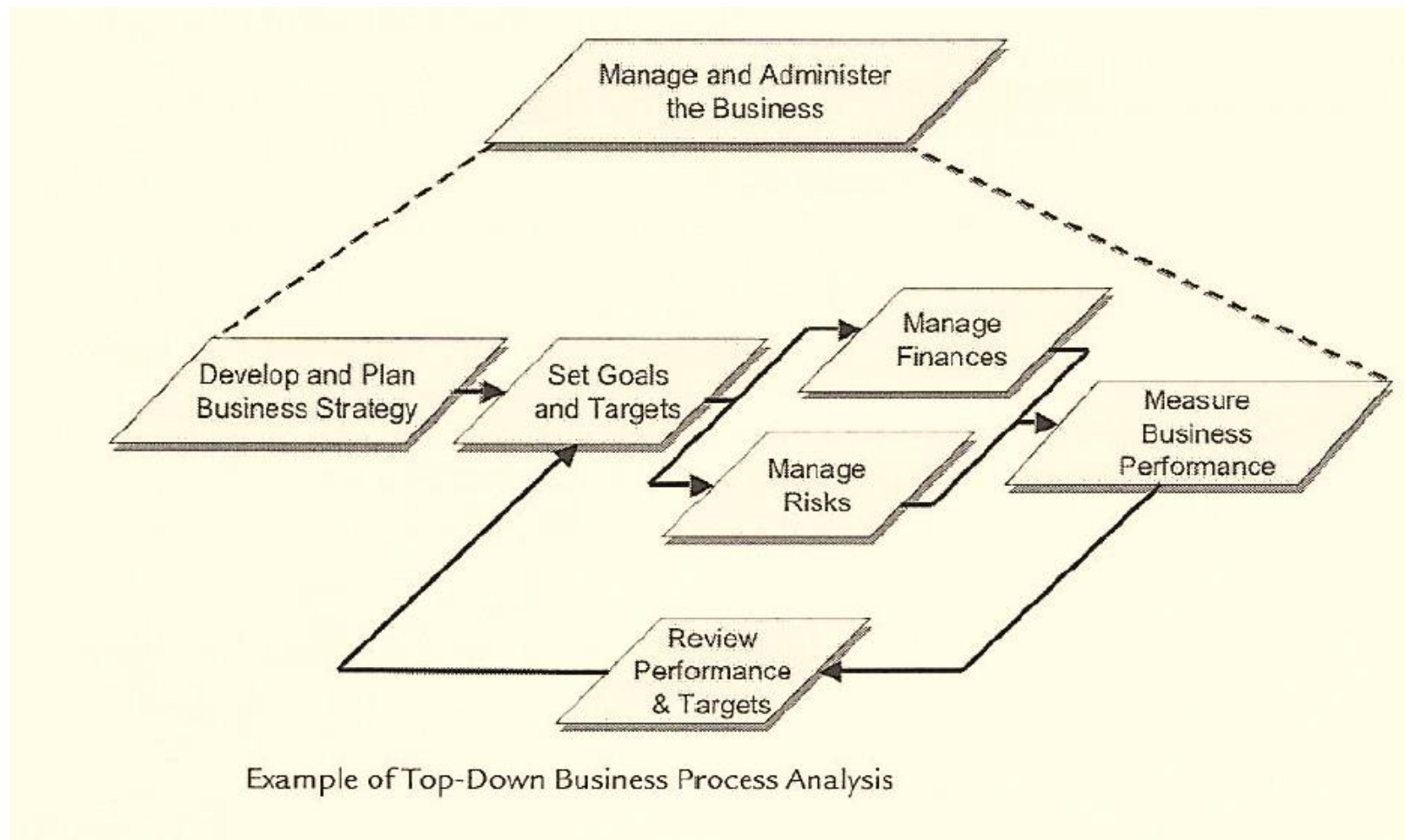
Meta-level view of information processing in large enterprises

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...*

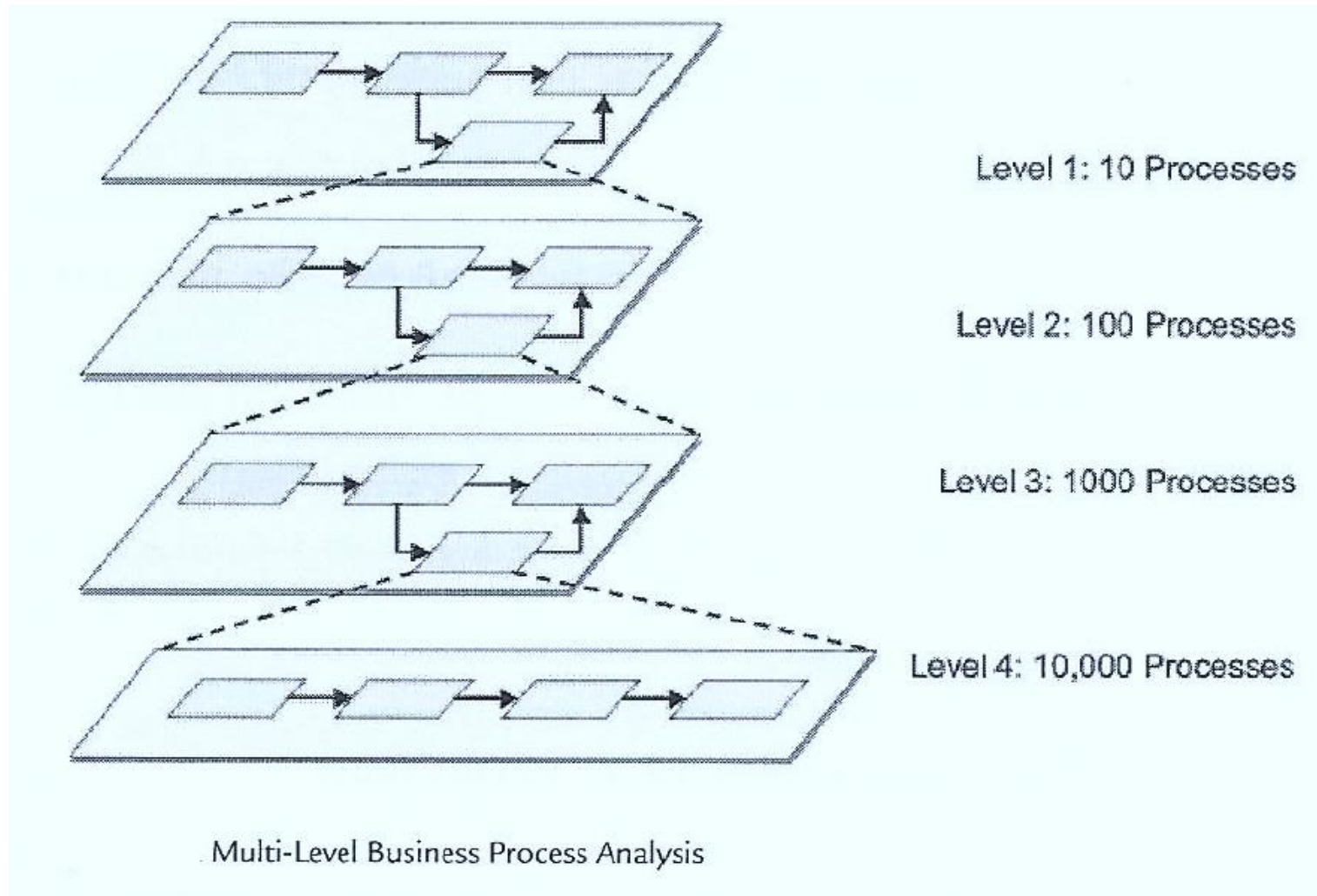
Sherwood, J., Clark, A. and Lynas D. (2005)

“Manage the business”



Top-down business process analysis

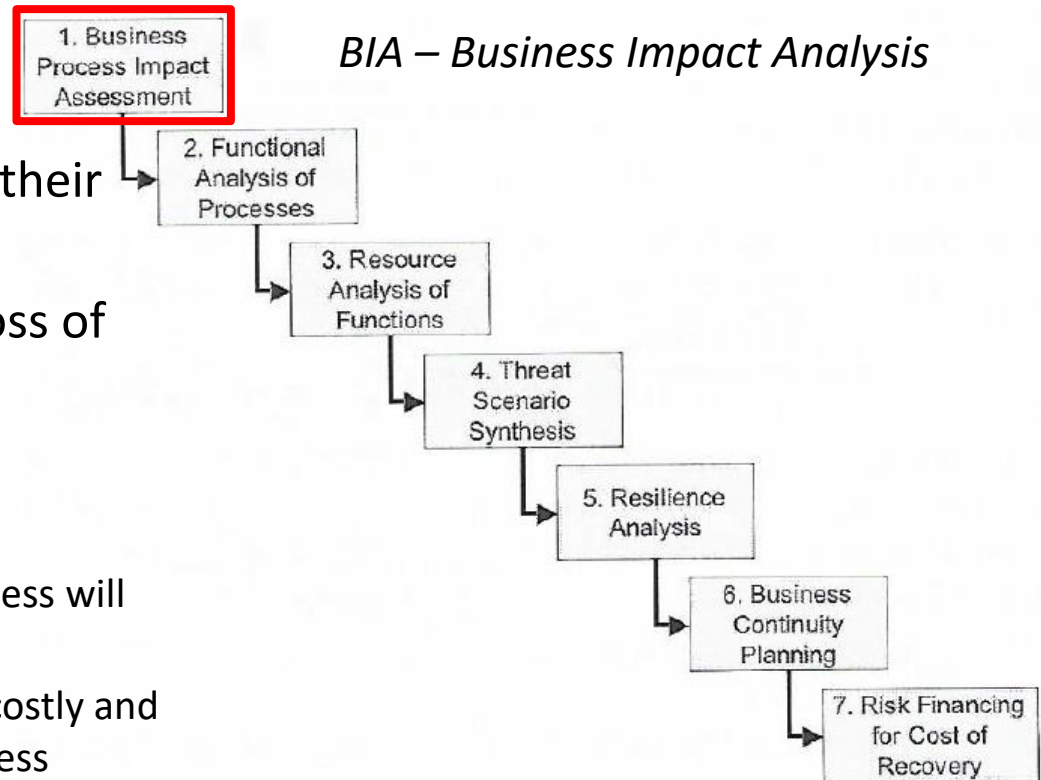
Also known as: *Structured decomposition*



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



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 ?

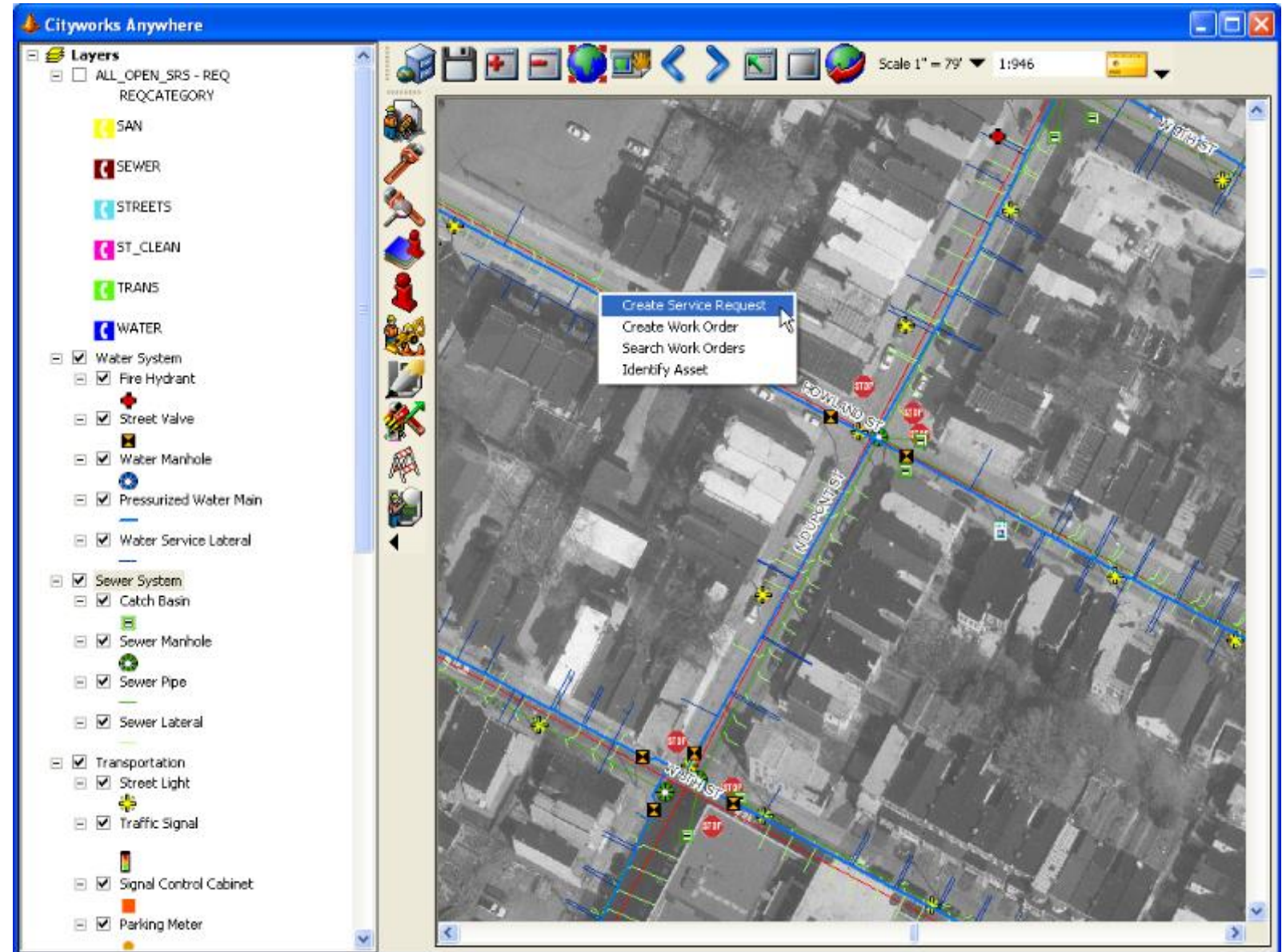
Example:

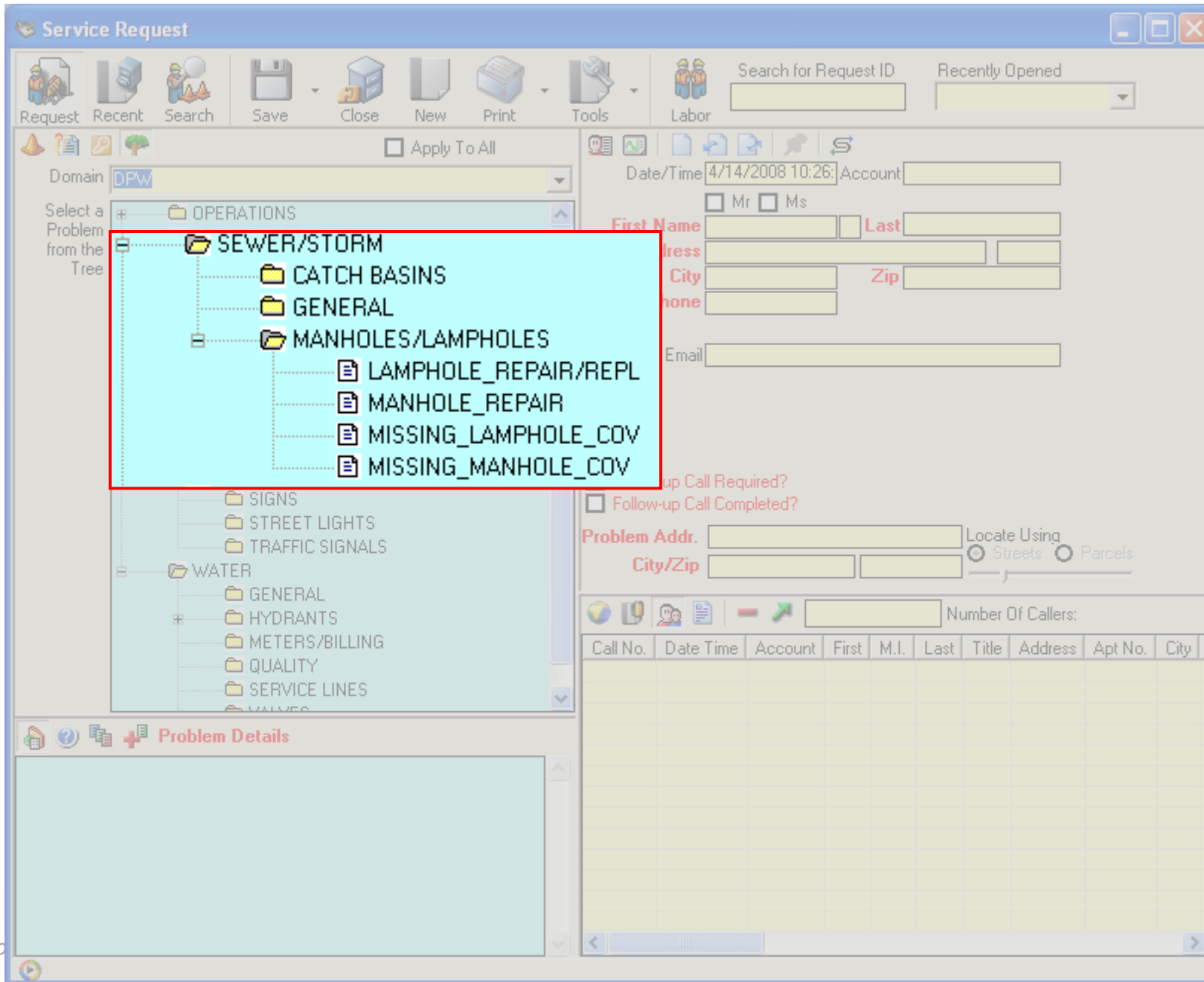
Service request and utility maintenance management work order information system

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

Service Request / Work Order System

“Computerized Maintenance Management System (CMMS)”





Service Request # 29438 MANHOLE_REPAIR / Manhole Needs Repair

Request Recent Search Save Close New Print Tools Labor

Search for Request ID: Recently Opened:

Apply To All

Problem Type **MANHOLE_REPAIR**
 Description Manhole Needs Repair

ID/Status: OPEN

Priority/Division: SEWER

Initiated By: ADMIN, CITYWORKS 4/14/2008 11:03:01 AM

Submit To: 4/14/2008 11:03:01 AM

Opened By: 4/14/2008 11:02:52 AM

Dispatch To: 4/14/2008 11:02:52 AM

Opened By:

Pri Comp. Date:

Closed By:

Is the Investigation Complete?

Is This Incident an Emergency?

Is a Work Order Needed?

Cancel

Work Order:

Work Order Description:

Project:

Problem Details

Date/Time: 4/14/2008 11:03: Account: 014624

Mr Ms

First Name: Last:

Address:

City: Zip:

Phone:

Email:

Follow-up Call Required?

Follow-up Call Completed?

Problem Addr.: Locate Using: Streets Parcels

City/Zip:

Number of Callers: 1

Call No.	Date Time	Account	First	M.I.	Last	Title	Address
29423	4/14/2008 11:03:01 AM	014624	BEN		SMITH		514 N WASHINGTON ST

Cityworks Anywhere

Scale 1" = 79' 1:946

Layers

- ALL_OPEN_SRS - REQ
 - REQCATEGORY
 - SAN
 - SEWER
 - STREETS
 - ST_CLEAN
 - TRANS
 - WATER
 - Water System
 - Fire Hydrant
 - Street Valve
 - Water Manhole
 - Pressurized Water Main
 - Water Service Lateral
 - Sewer System
 - Catch Basin
 - Sewer Manhole
 - Sewer Pipe
 - Sewer Lateral
 - Transportation
 - Street Light
 - Traffic Signal
 - Signal Control Cabinet
 - Parking Meter

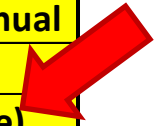
Map Content:

- SAN #27145 MISSED_RECYCLING
- SEWER #29438 MANHOLE_REPAIR
- SAN #2429 MISSED_RECYCLING
- ST_CLEAN #29019 SPECIAL_PICK_UP
- SAN #27122 MISSED_RECYCLING
- INDUCENT ST
- SEWER #27225 OTHER_SANITATION
- SAN #23265 MISSED_RECYCLING
- SAN #23471 MISSED_RECYCLING
- SAN #23252 MISSED_RECYCLING
- SAN #23754 MISSED_RECYCLING
- W 1ST ST

Toolbar: Includes icons for layers, pan, zoom, and other GIS functions.

Priorities for recovery example

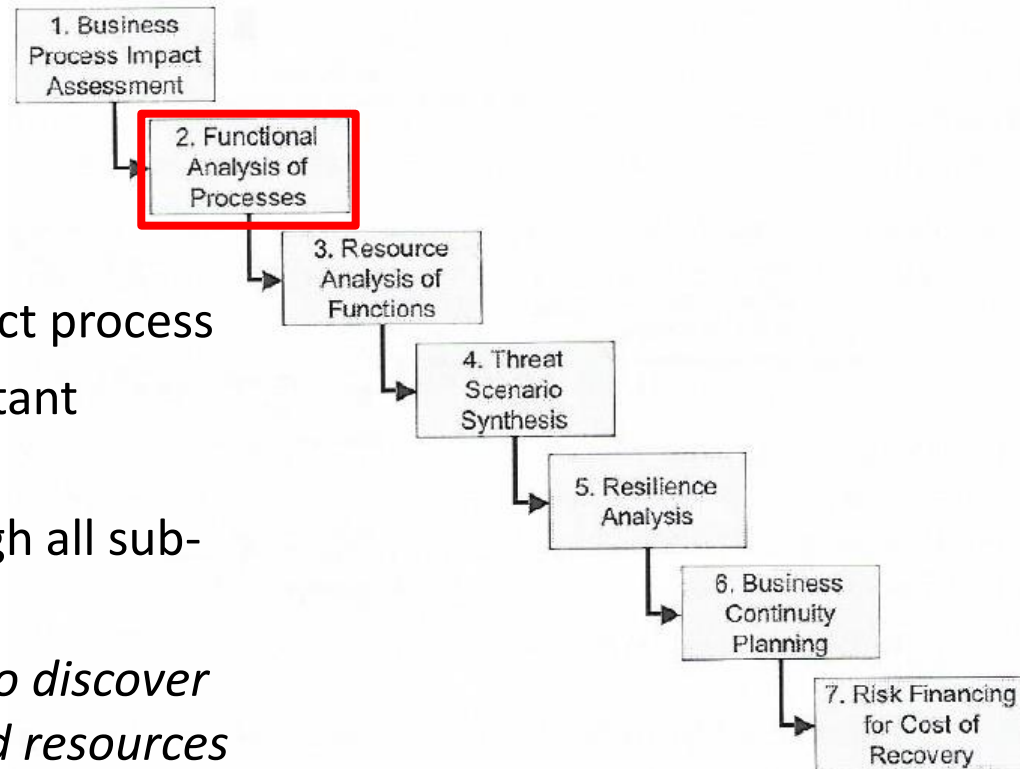
Public Works Dept Operations Division	Street Cleaning	Mow Grass
		Clean Lots
		Street Cleaning - Mechanical and Manual
		Snow Removal
		Debris Removal (Emergency Response)
		Special Pick Ups
		Leaf Removal
		Neighborhood Cleanup
	Public Property	Special Events
		Special Projects
		Building Repair
		Tree 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

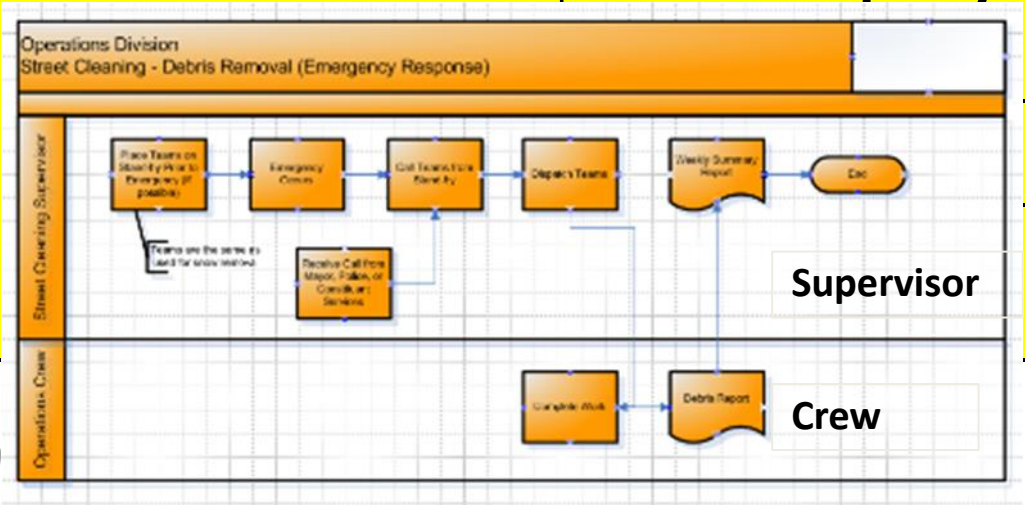
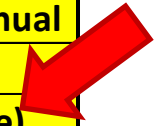
Step 2

- 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?*



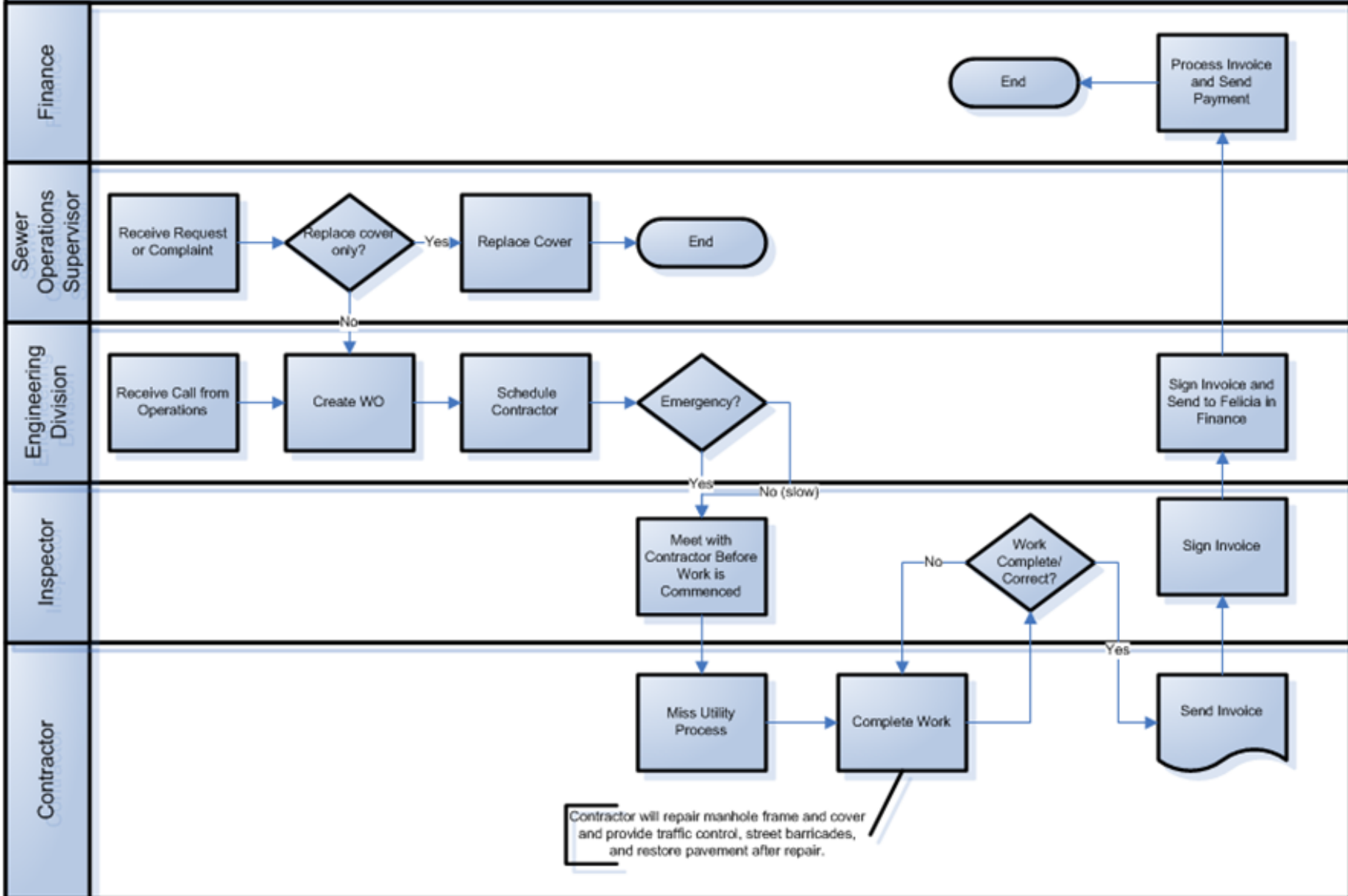
Priorities for recovery example

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	

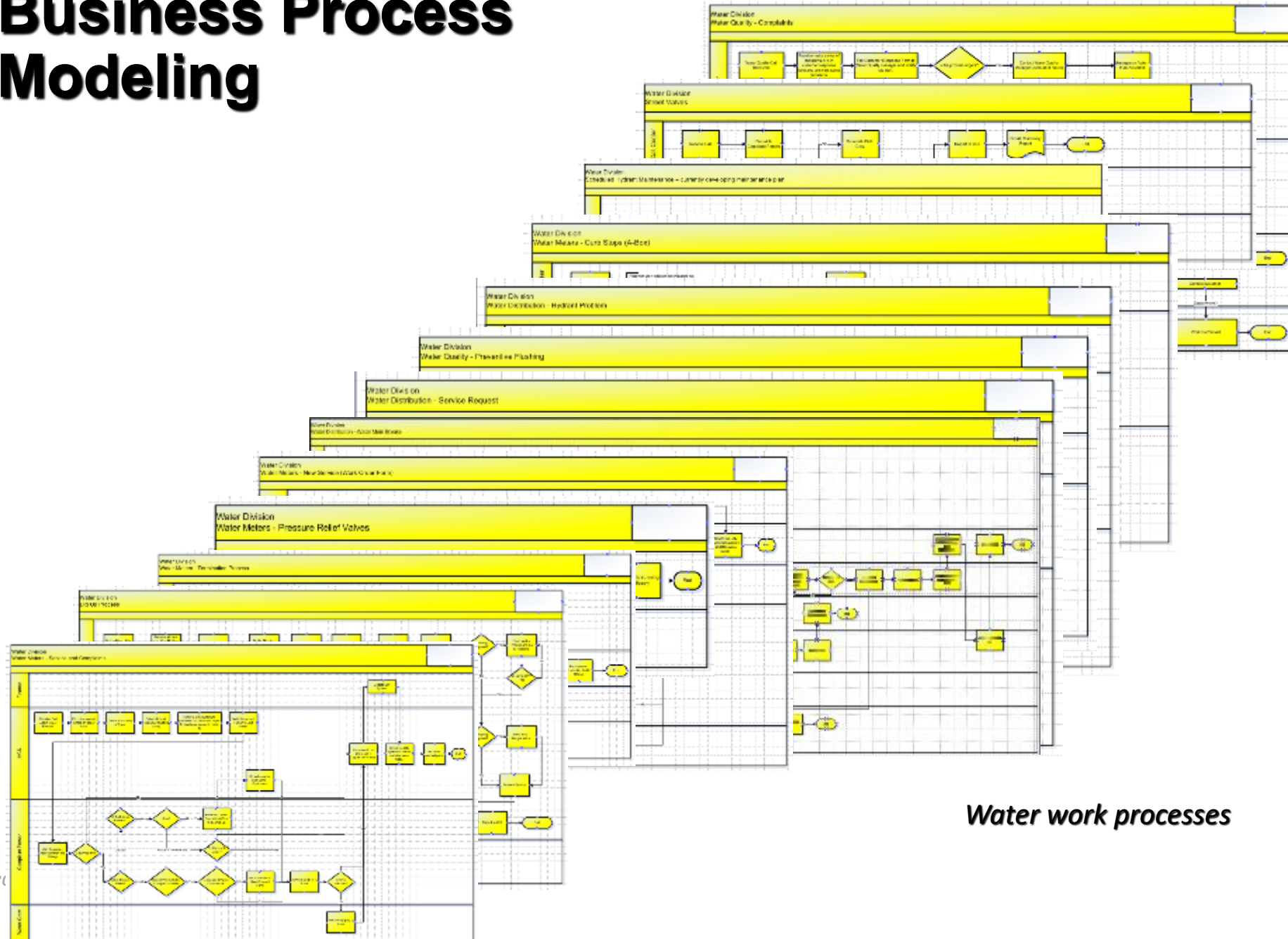


Sewer Division
 Repair & Replace Manhole (Frame and Cover)

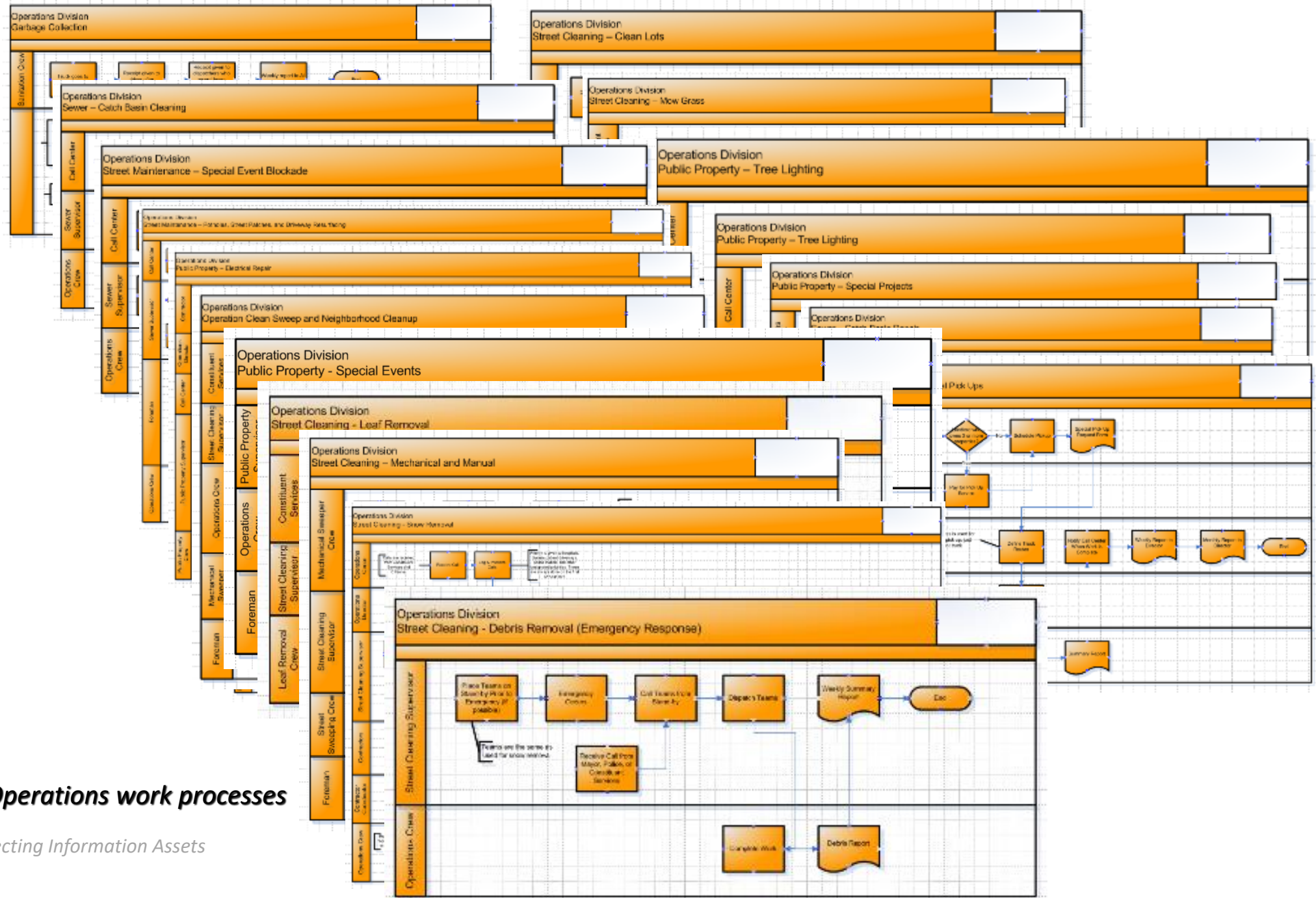
Contributor(s) to this Process:
 Michelle
 Edmond



Business Process Modeling



Water work processes

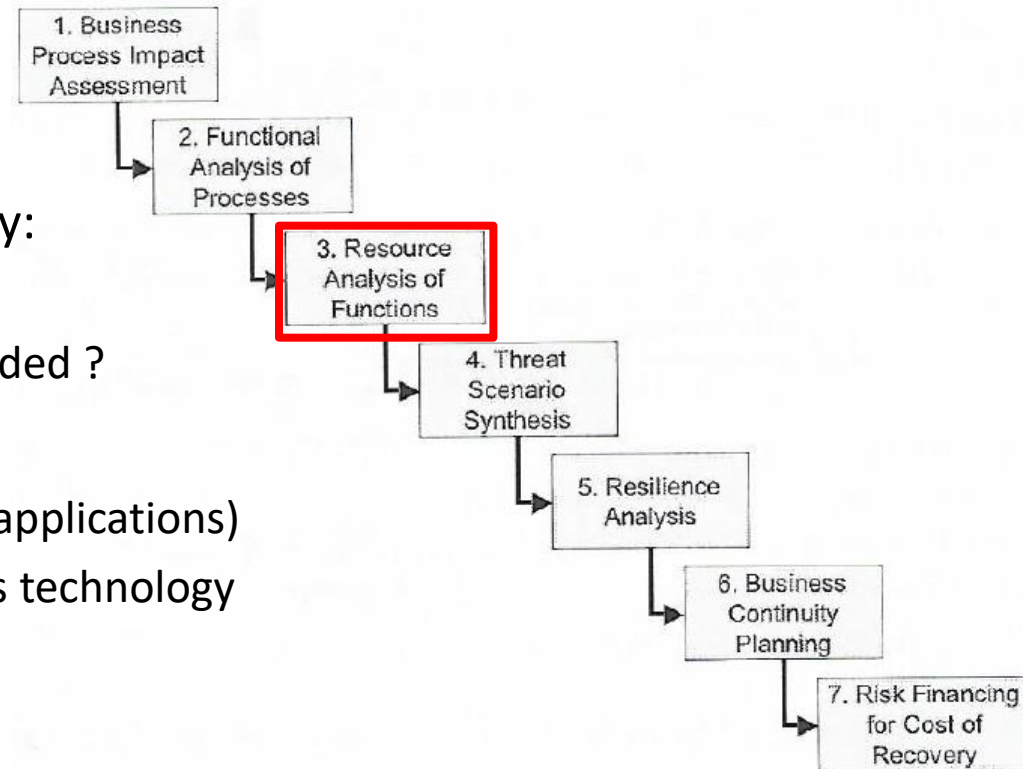


Operations work processes

Auditing the Business Continuity Plan

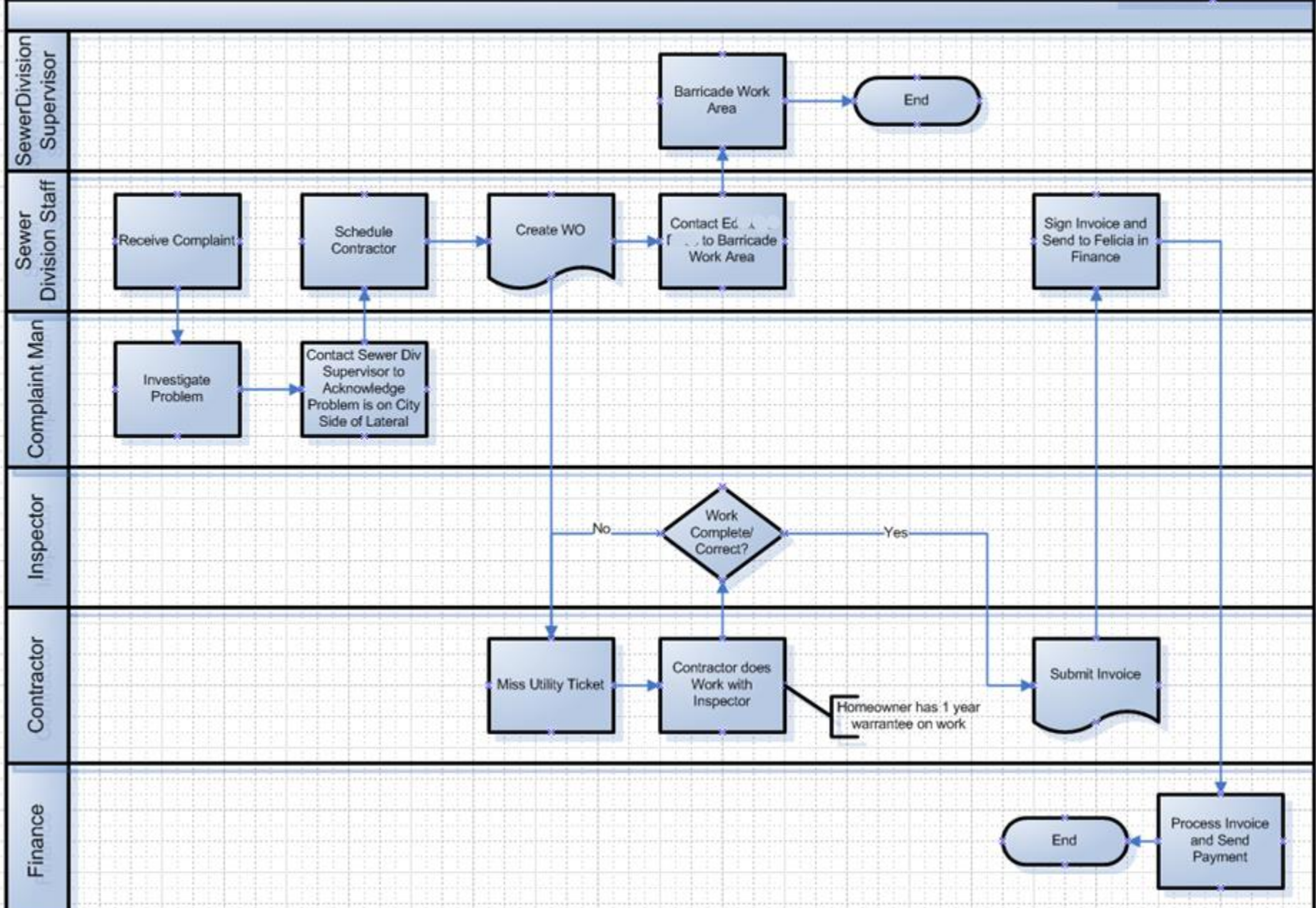
Step 3

- 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
 - ...



Sewer Division
 Laterals and Sewer Mains, Repair

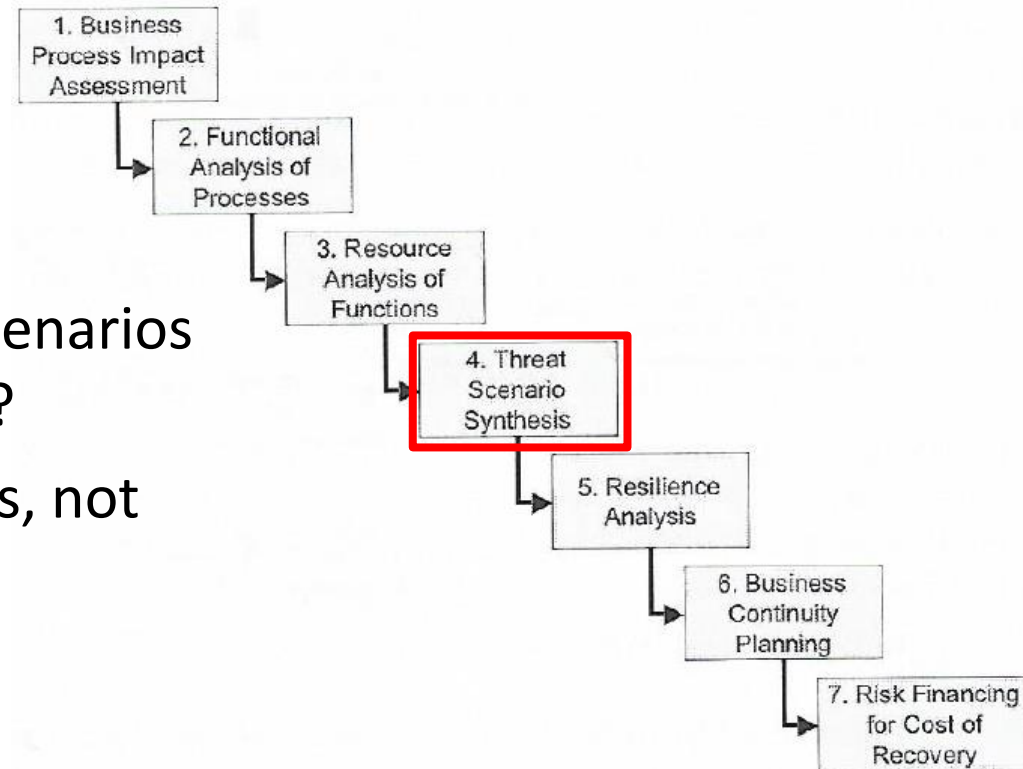
Have they documented the communications needed to coordinate resources?



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?

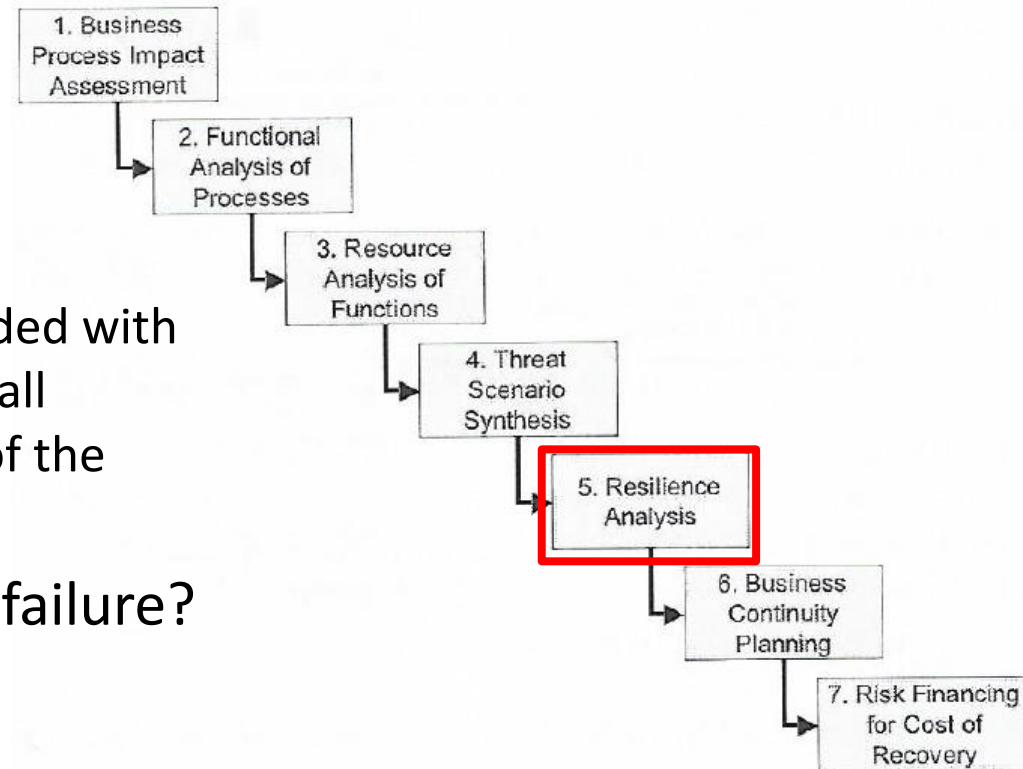


Sherwood, J., Clark, A. and Lynas D. (2005), Enterprise Security Architecture, CRC Press

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?

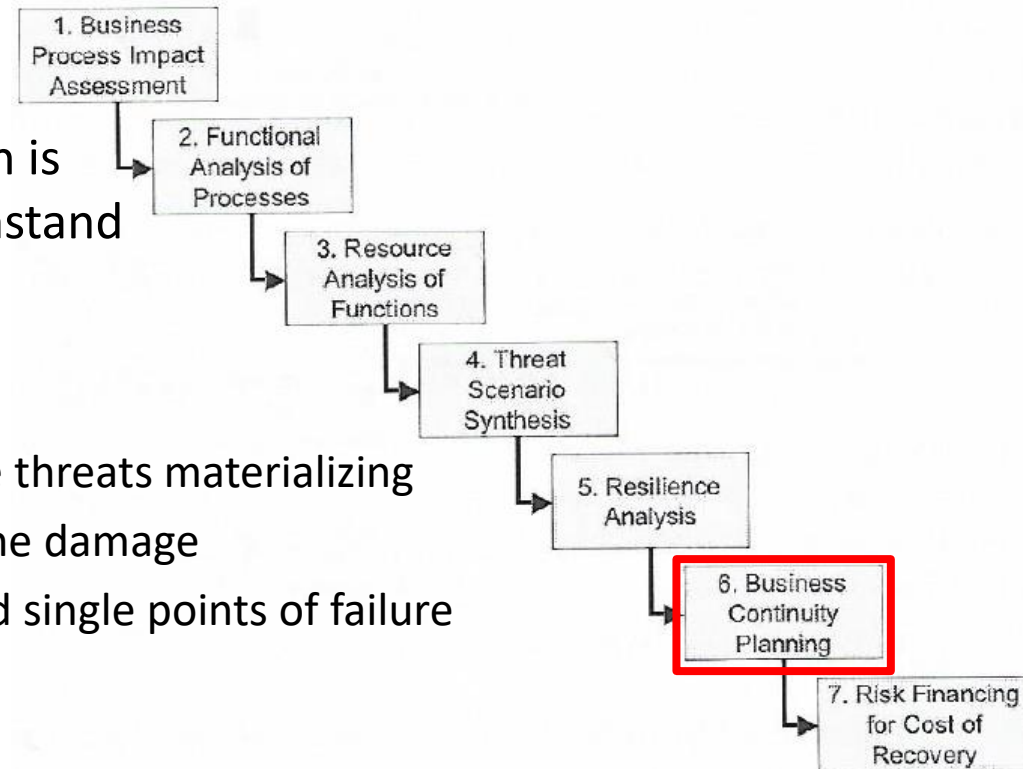


Sherwood, J., Clark, A. and Lynas D. (2005), Enterprise Security Architecture, CRC Press

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

CP-2	CONTINGENCY PLAN
	ASSESSMENT OBJECTIVE: <i>Determine if the organization:</i>

ASSESSMENT OBJECTIVE: <i>Determine if the organization:</i>			<i>in for the information system that:</i>
<i>develops and documents a contingency plan for the information system that:</i>			<i>and business functions and associated</i>
CP-2(a)	CP-2(a)(1)	<i>identifies essential missions and business functions and associated contingency requirements;</i>	<i>covery objectives;</i>
CP-2(a)(2)	CP-2(a)(2)[1]	<i>provides recovery objectives;</i>	<i>oration priorities;</i>
	CP-2(a)(2)[2]	<i>provides restoration priorities;</i>	<i>rics;</i>
	CP-2(a)(2)[3]	<i>provides metrics;</i>	<i>ntingency roles;</i>
CP-2(a)(3)	CP-2(a)(3)[1]	<i>addresses contingency roles;</i>	<i>ntingency responsibilities;</i>
	CP-2(a)(3)[2]	<i>addresses contingency responsibilities;</i>	<i>signed individuals with contact</i>
	CP-2(a)(3)[3]	<i>addresses assigned individuals with contact information;</i>	<i>tial missions and business functions n disruption, compromise, or failure;</i>
CP-2(a)(4)	<i>addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;</i>		<i>mation system restoration without safeguards originally planned and</i>
CP-2(a)(5)	<i>addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented;</i>		<i>nnel or roles to review and approve cy plan for the information system;</i>
CP-2(a)(6)	CP-2(a)(6)[1]	<i>defines personnel or roles to review and approve the contingency plan for the information system;</i>	<i>nd approved by organization-defined roles;</i>
	CP-2(a)(6)[2]	<i>is reviewed and approved by organization-defined personnel or roles;</i>	<i>onnel (identified by name and/or by nents to whom copies of the istributed;</i>
			<i>tingency plan to organization-defined nd organizational elements;</i>
			<i>es with incident handling activities;</i>
			<i>v the contingency plan for the</i>
			<i>1 with the organization-defined</i>
			<i>information system, or environment of</i>

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

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)

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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
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

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

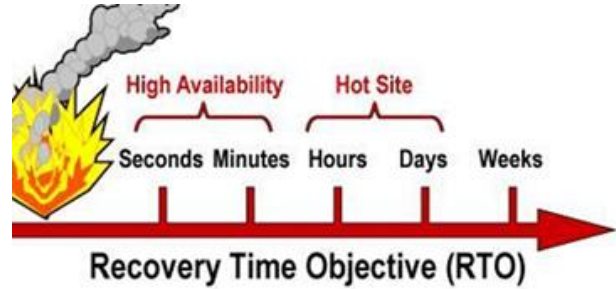
What kind of offsite alternative recovery facility do they have ?

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



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

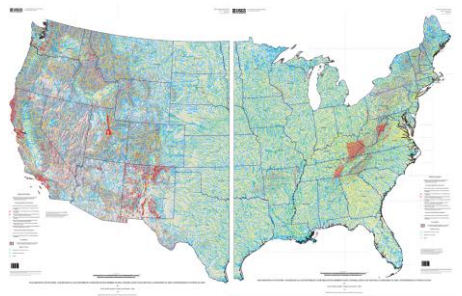
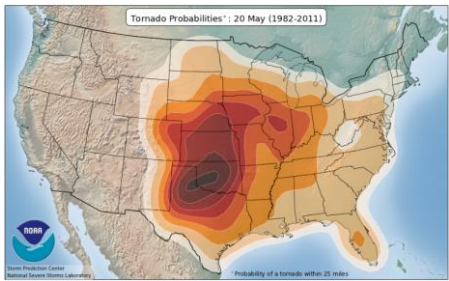
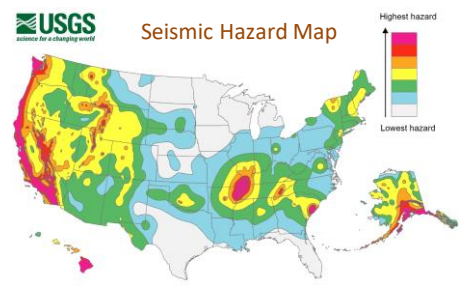
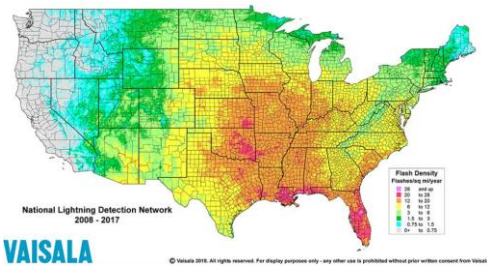
Shared site: Least expensive arrangement (“reciprocal agreements”) with compatible companies who agree to host each other's employees and business functions in the event of a disaster

- *Most risky alternative - 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

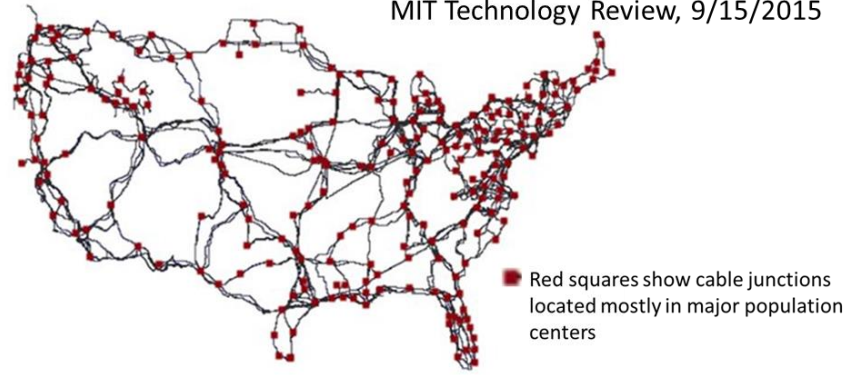
Disaster recovery site should be in a different geophysical area not susceptible to same disaster as the primary operations facility

Note: even the cloud is located somewhere...



With multiple providers of:

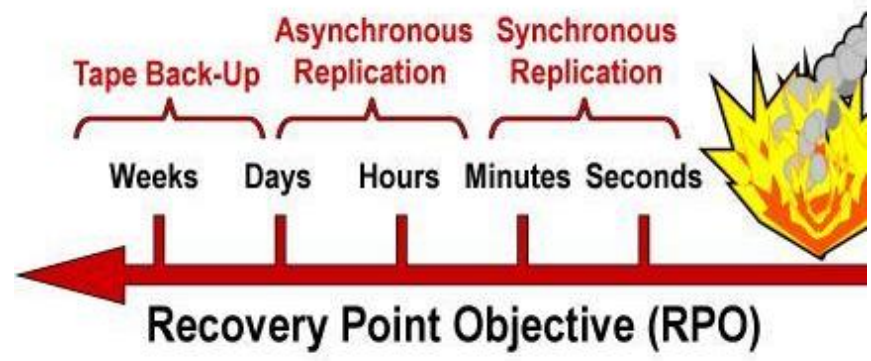
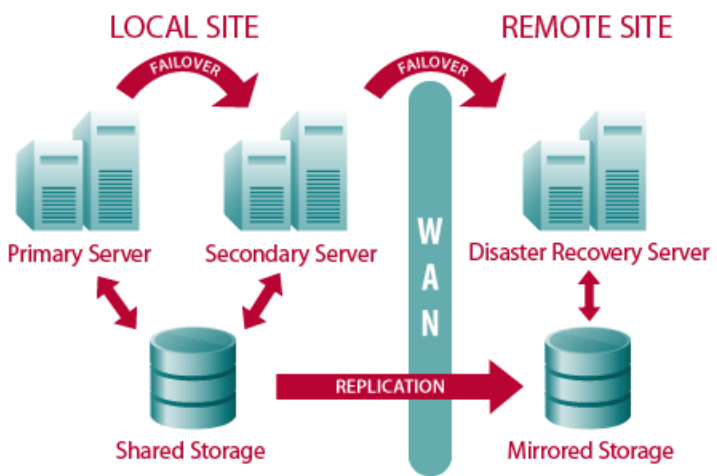
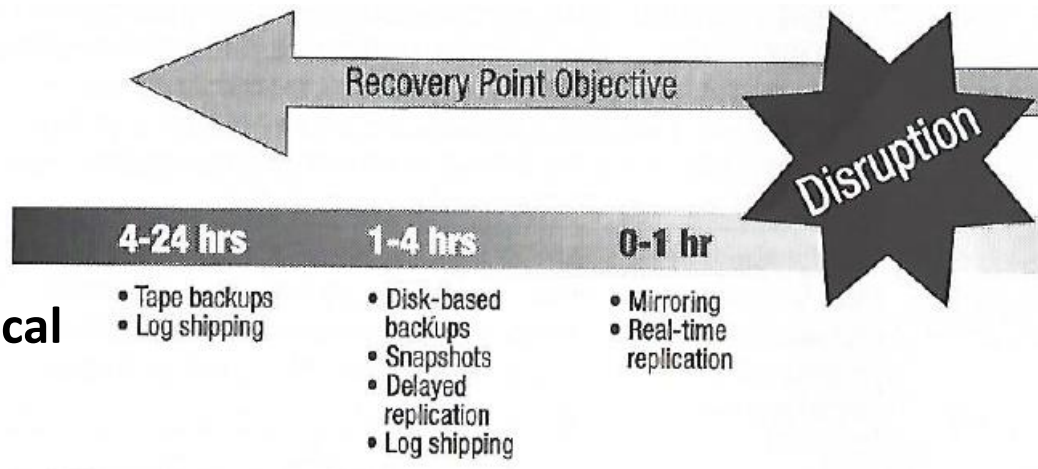
US Long-haul High-Speed Internet Fiber Network
MIT Technology Review, 9/15/2015



- 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

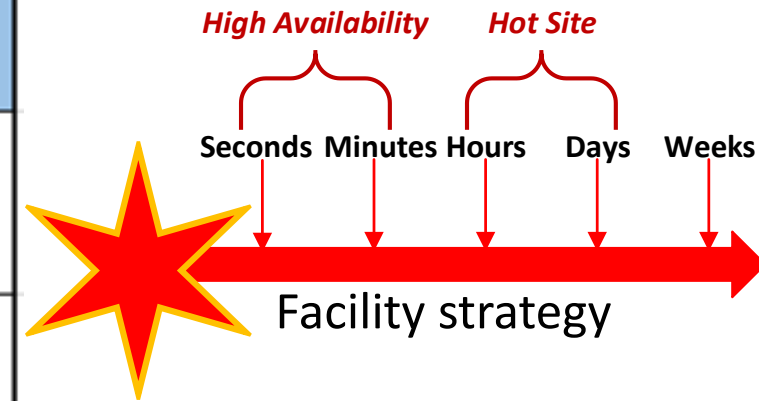


Recovery Site Options: Location strategy & Backup technology

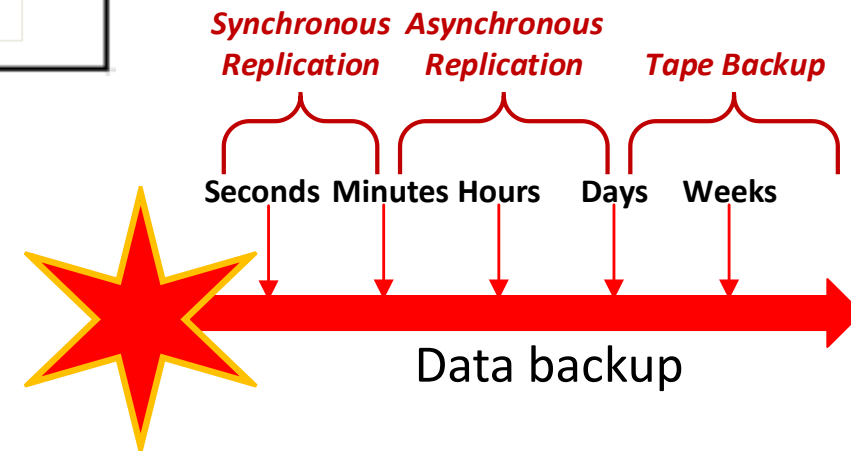
Information System Recovery Priority	Backup / Recovery Strategy
High priority	Backup: Mirrored systems and disc replication Strategy: Hot site \$\$\$
Moderate priority	Backup: Optical backup and WAN/VLAN replication Strategy: Warm or Cold site \$\$
Low priority	Backup: Tape backup Strategy: Cold site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

[NIST SP 800-34 R1](#)
[Contingency Planning Guide for Federal Information Systems](#)

Recovery Time Objective



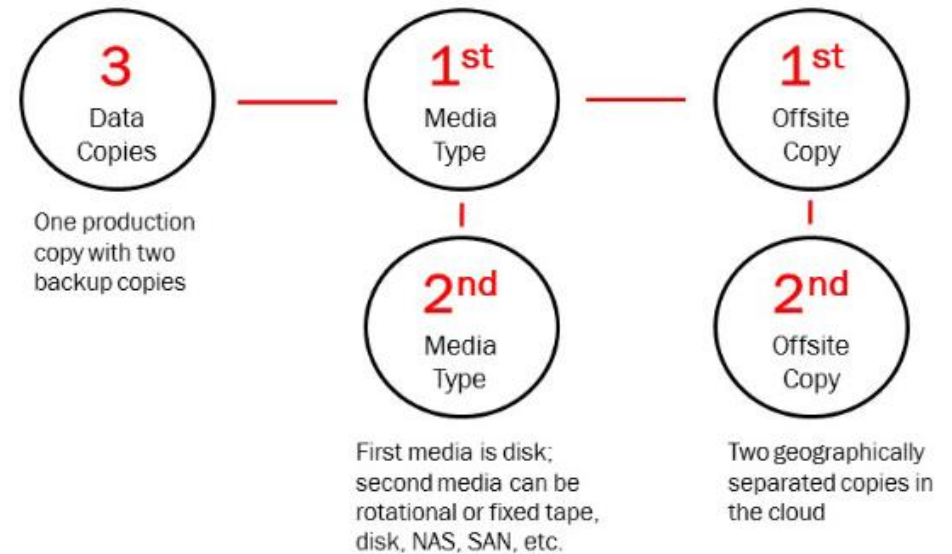
Recovery Point Objective



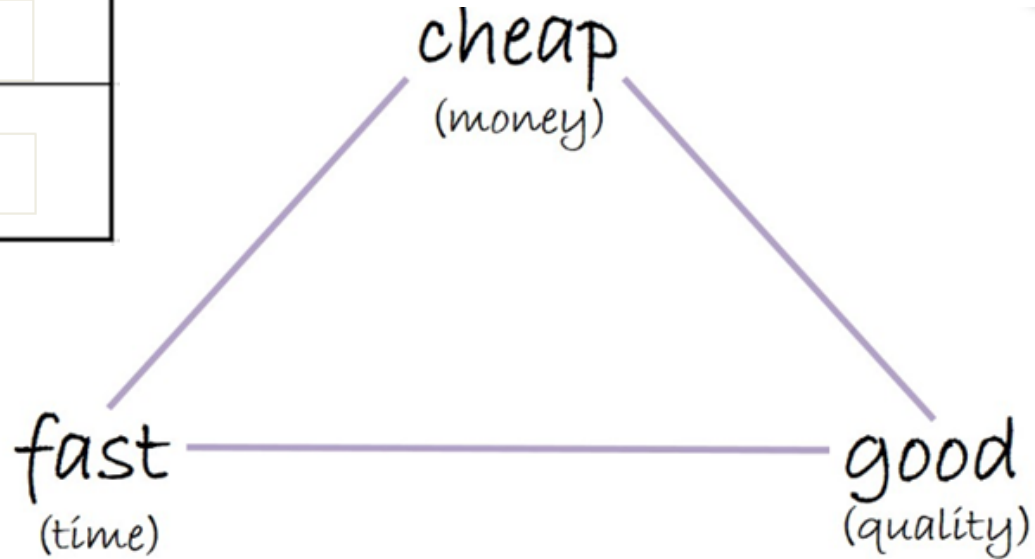
Backup Mitigation – Best Practice

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 <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-left: 20px;">\$\$\$</div>
Moderate priority	Backup: Optical backup and WAN/VLAN replication Strategy: Warm or Cold site <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-left: 20px;">\$\$</div>
Low priority	Backup: Tape backup Strategy: Cold site <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-left: 20px;">\$</div>



The Quality Triangle:

Pick Two

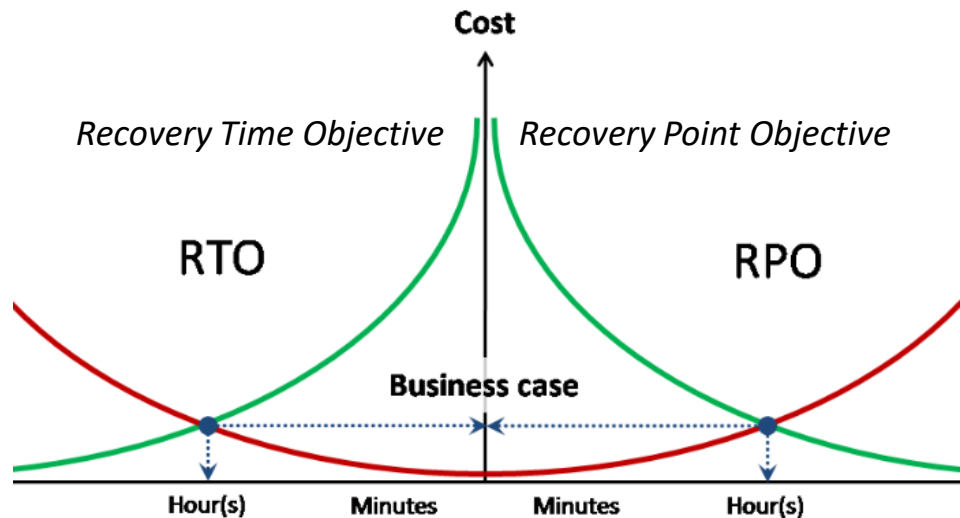
Disaster recovery time targets

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: <i>Determine if the organization:</i>

ASSESSMENT OBJECTIVE: <i>Determine if the organization:</i>			<i>in for the information system that:</i>
<i>develops and documents a contingency plan for the information system that:</i>			<i>and business functions and associated</i>
CP-2(a)	CP-2(a)(1)	<i>identifies essential missions and business functions and associated contingency requirements;</i>	<i>covery objectives;</i>
CP-2(a)(2)	CP-2(a)(2)[1]	<i>provides recovery objectives;</i>	<i>oration priorities;</i>
	CP-2(a)(2)[2]	<i>provides restoration priorities;</i>	<i>rics;</i>
	CP-2(a)(2)[3]	<i>provides metrics;</i>	<i>ntingency roles;</i>
CP-2(a)(3)	CP-2(a)(3)[1]	<i>addresses contingency roles;</i>	<i>ntingency responsibilities;</i>
	CP-2(a)(3)[2]	<i>addresses contingency responsibilities;</i>	<i>signed individuals with contact</i>
	CP-2(a)(3)[3]	<i>addresses assigned individuals with contact information;</i>	<i>tial missions and business functions n disruption, compromise, or failure;</i>
CP-2(a)(4)	<i>addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;</i>		<i>mation system restoration without safeguards originally planned and</i>
CP-2(a)(5)	<i>addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented;</i>		<i>nnel or roles to review and approve cy plan for the information system;</i>
CP-2(a)(6)	CP-2(a)(6)[1]	<i>defines personnel or roles to review and approve the contingency plan for the information system;</i>	<i>nd approved by organization-defined roles;</i>
	CP-2(a)(6)[2]	<i>is reviewed and approved by organization-defined personnel or roles;</i>	<i>onnel (identified by name and/or by nents to whom copies of the istributed;</i>
			<i>tingency plan to organization-defined nd organizational elements;</i>
			<i>es with incident handling activities;</i>
			<i>v the contingency plan for the</i>
			<i>1 with the organization-defined</i>
			<i>information system, or environment of</i>

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

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

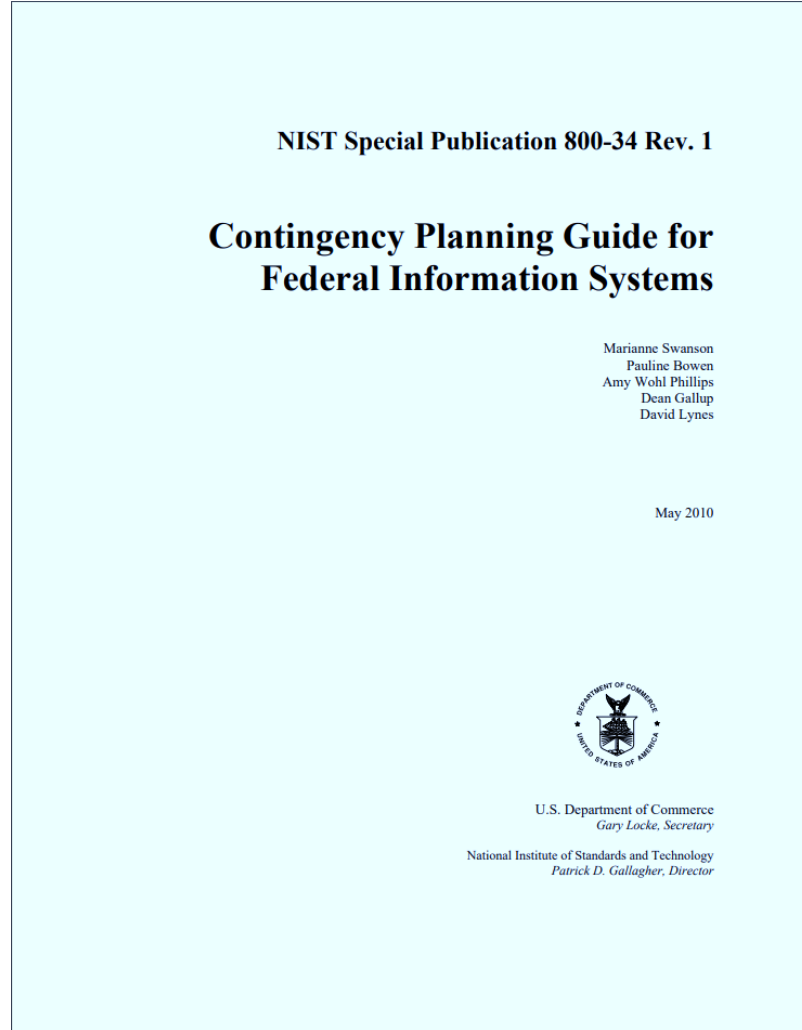


TABLE OF CONTENTS

Plan Approval.....	A.3-3
1. Introduction	A.3-4
1.1 Background.....	A.3-4
1.2 Scope.....	A.3-4
1.3 Assumptions.....	A.3-4
2. Concept of Operations	A.3-5
2.1 System Description.....	A.3-5
2.2 Overview of Three Phases.....	A.3-5
2.3 Roles and Responsibilities.....	A.3-6
3. Activation and Notification.....	A.3-6
3.1 Activation Criteria and Procedure	A.3-6
3.2 Notification.....	A.3-6
3.3 Outage Assessment.....	A.3-7
4. Recovery.....	A.3-7
4.1 Sequence of Recovery Activities	A.3-7
4.2 Recovery Procedures	A.3-8
4.3 Recovery Escalation Notices/Awareness.....	A.3-8
5. Reconstitution.....	A.3-8
5.1 Concurrent Processing	A.3-8
5.2 Validation Data Testing.....	A.3-8
5.3 Validation Functionality Testing.....	A.3-9
5.4 Recovery Declaration.....	A.3-9
5.5 Notification (users).....	A.3-9
5.6 Cleanup	A.3-9
5.7 Offsite Data Storage.....	A.3-9
5.8 Data Backup.....	A.3-9
5.9 Event Documentation.....	A.3-10
5.10 Deactivation.....	A.3-10

Question

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

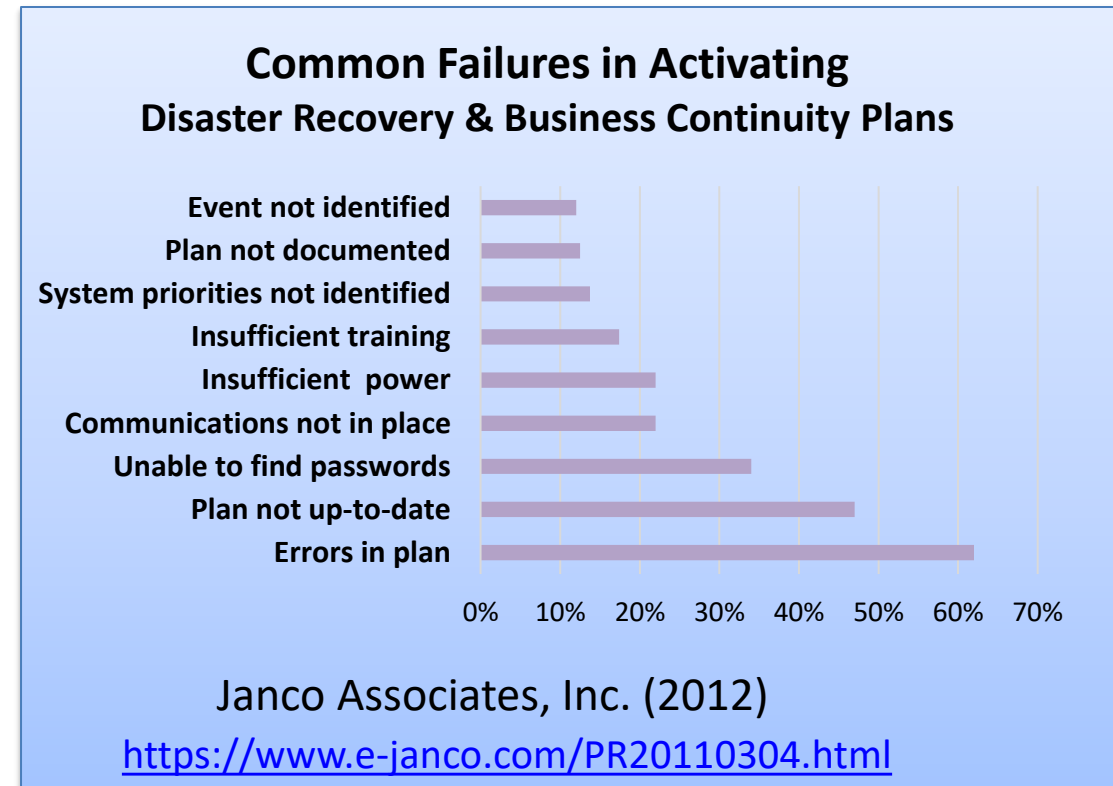
- *Why might it not be practical?*
- *If it is not practical, what alternative ways can you recommend for testing a BCP?*

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*



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 describes 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



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



Audit Focus

Areas for
IT Audit
evaluation:

**Figure 3—Possible Tests/Procedures
for Backup and Recovery**

Data	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Review the plan's provisions.• Observe or inquire about the provisions and location.
Recovery team	<ul style="list-style-type: none">• 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

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
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

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
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

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