

# Protecting Information Assets

## - Unit#3c -

# Business Continuity and Disaster Recovery Planning

# Agenda

- IT Security Control Classes and Families
- Business Continuity and Disaster Recovery Planning
- Business Impact Analysis
- Disaster Recovery
- Disaster Recovery Testing
- Test Taking Tip
- Quiz

# IT Security Control Classes and Families

	CLASS	FAMILY	IDENTIFIER
→	Management	Risk Assessment	RA
	Management	Planning	PL
	Management	System and Services Acquisition	SA
	Management	Certification, Accreditation, and Security Assessments	CA
	Operational	Personnel Security	PS
→	Operational	Physical and Environmental Protection	PE
	Operational	Contingency Planning	CP
	Operational	Configuration Management	CM
	Operational	Maintenance	MA
	Operational	System and Information Integrity	SI
	Operational	Media Protection	MP
	Operational	Incident Response	IR
→	Operational	Awareness and Training	AT
	Technical	Identification and Authentication	IA
	Technical	Access Control	AC
	Technical	Audit and Accountability	AU
	Technical	System and Communications Protection	SC

# Contingency Planning (CP)

Control	Control Name
CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-3	Contingency Training
CP-4	Contingency Plan Testing
CP-6	Alternate Storage Site
CP-7	Alternate Processing Site
CP-8	Telecommunications Services
CP-9	Information System Backup
CP-10	Information System Recovery and Reconstitution

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	WITHDRAWN	ASSURANCE	CONTROL BASELINES		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
CP-2(5)	CONTINGENCY PLAN   CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS					X
CP-2(6)	CONTINGENCY PLAN   ALTERNATE PROCESSING / STORAGE SITE					
CP-2(7)	CONTINGENCY PLAN   COORDINATE WITH EXTERNAL SERVICE PROVIDERS					
CP-2(8)	CONTINGENCY PLAN   IDENTIFY CRITICAL ASSETS				X	X
CP-3	Contingency Training		X	X	X	X
CP-3(1)	CONTINGENCY TRAINING   SIMULATED EVENTS		X			X
CP-3(2)	CONTINGENCY TRAINING   AUTOMATED TRAINING ENVIRONMENTS		X			
CP-4	Contingency Plan Testing		X	X	X	X
CP-4(1)	CONTINGENCY PLAN TESTING   COORDINATE WITH RELATED PLANS		X		X	X
CP-4(2)	CONTINGENCY PLAN TESTING   ALTERNATE PROCESSING SITE		X			X
CP-4(3)	CONTINGENCY PLAN TESTING   AUTOMATED TESTING		X			
CP-4(4)	CONTINGENCY PLAN TESTING   FULL RECOVERY / RECONSTITUTION		X			
CP-5	Contingency Plan Update	X	Incorporated into CP-2.			
CP-6	Alternate Storage Site				X	X
CP-6(1)	ALTERNATE STORAGE SITE   SEPARATION FROM PRIMARY SITE				X	X
CP-6(2)	ALTERNATE STORAGE SITE   RECOVERY TIME / POINT OBJECTIVES					X
CP-6(3)	ALTERNATE STORAGE SITE   ACCESSIBILITY				X	X
CP-7	Alternate Processing Site				X	X
CP-7(1)	ALTERNATE PROCESSING SITE   SEPARATION FROM PRIMARY SITE				X	X
CP-7(2)	ALTERNATE PROCESSING SITE   ACCESSIBILITY				X	X
CP-7(3)	ALTERNATE PROCESSING SITE   PRIORITY OF SERVICE				X	X
CP-7(4)	ALTERNATE PROCESSING SITE   PREPARATION FOR USE					X
CP-7(5)	ALTERNATE PROCESSING SITE   EQUIVALENT INFORMATION SECURITY SAFEGUARDS	X	Incorporated into CP-7.			
CP-7(6)	ALTERNATE PROCESSING SITE   INABILITY TO RETURN TO PRIMARY SITE					
CP-8	Telecommunications Services				X	X
CP-8(1)	TELECOMMUNICATIONS SERVICES   PRIORITY OF SERVICE PROVISIONS				X	X
CP-8(2)	TELECOMMUNICATIONS SERVICES   SINGLE POINTS OF FAILURE				X	X
CP-8(3)	TELECOMMUNICATIONS SERVICES   SEPARATION OF PRIMARY / ALTERNATE PROVIDERS					X
CP-8(4)	TELECOMMUNICATIONS SERVICES   PROVIDER CONTINGENCY PLAN					X
CP-8(5)	TELECOMMUNICATIONS SERVICES   ALTERNATE TELECOMMUNICATION SERVICE TESTING					
CP-9	Information System Backup			X	X	X
CP-9(1)	INFORMATION SYSTEM BACKUP   TESTING FOR RELIABILITY / INTEGRITY				X	X

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-9(2)	INFORMATION SYSTEM BACKUP   TEST RESTORATION USING SAMPLING					X
CP-9(3)	INFORMATION SYSTEM BACKUP   SEPARATE STORAGE FOR CRITICAL INFORMATION					X
CP-9(4)	INFORMATION SYSTEM BACKUP   PROTECTION FROM UNAUTHORIZED MODIFICATION	X	Incorporated into CP-9.			
CP-9(5)	INFORMATION SYSTEM BACKUP   TRANSFER TO ALTERNATE STORAGE SITE					X
CP-9(6)	INFORMATION SYSTEM BACKUP   REDUNDANT SECONDARY SYSTEM					
CP-9(7)	INFORMATION SYSTEM BACKUP   DUAL AUTHORIZATION					
CP-10	Information System Recovery and Reconstitution			X	X	X
CP-10(1)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION   CONTINGENCY PLAN TESTING	X	Incorporated into CP-4.			
CP-10(2)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION   TRANSACTION RECOVERY				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

## Contingency Planning Control Inventory and Baselines

# Contingency Planning

From a business perspective, contingency planning is:

- Business Continuity Planning (BCP) and
- Disaster Recovery Planning (DRP)

# Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)

- *Operating disruptions can occur with or without warning*
- *Results may be predictable or unanticipated*
- *It is important that the mission of the enterprise is sustained during any emergency*
  
- ***The first priority is always the safety of the people:***  
*Employees, Service and Support Staff and Visitors*

# 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



# Question?

Are the terms: Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) synonyms or are they different?

If they are different, what are the differences?

# Business Continuity - versus - Disaster Recovery



Business  
Continuity  
Plan (BCP)

Provides procedures for sustaining mission/business operations while recovering from a significant disruption caused by a natural or human-induced disaster

*Disaster  
Recovery  
Planning (DRP)*

Provides procedures for relocating critical information systems operations to an alternative location after a significant disruption caused by a natural or human-induced disaster

# Business Continuity Management

## An important and big topic:

- How to maintain the continued operation of the business' processes?
- Based on conducting a **Business Impact Analysis (BIA)**

# Business Continuity Plan (BCP)

**Prerequisite:** Good documented models of the business' processes, broken down into a series of hierarchical layers of sub-processes, sub-sub processes...

*What are the:*

- 1. Business processes ?*
  - 2. Information systems and resources needed to run the processes ?*
  - 3. Threats, vulnerabilities and risks ?*
  - 4. **Business Impact Analysis (BIA) results ?***
  - 5. Recovery strategies ?*
  - 6. Recovery plans ?*
  - 7. Testing done to validate and improve the recovery plans?*
    - Maintenance (update), Awareness, Training (practice)*
- ... answer, improve and repeat... back to 1...*

# Exercise

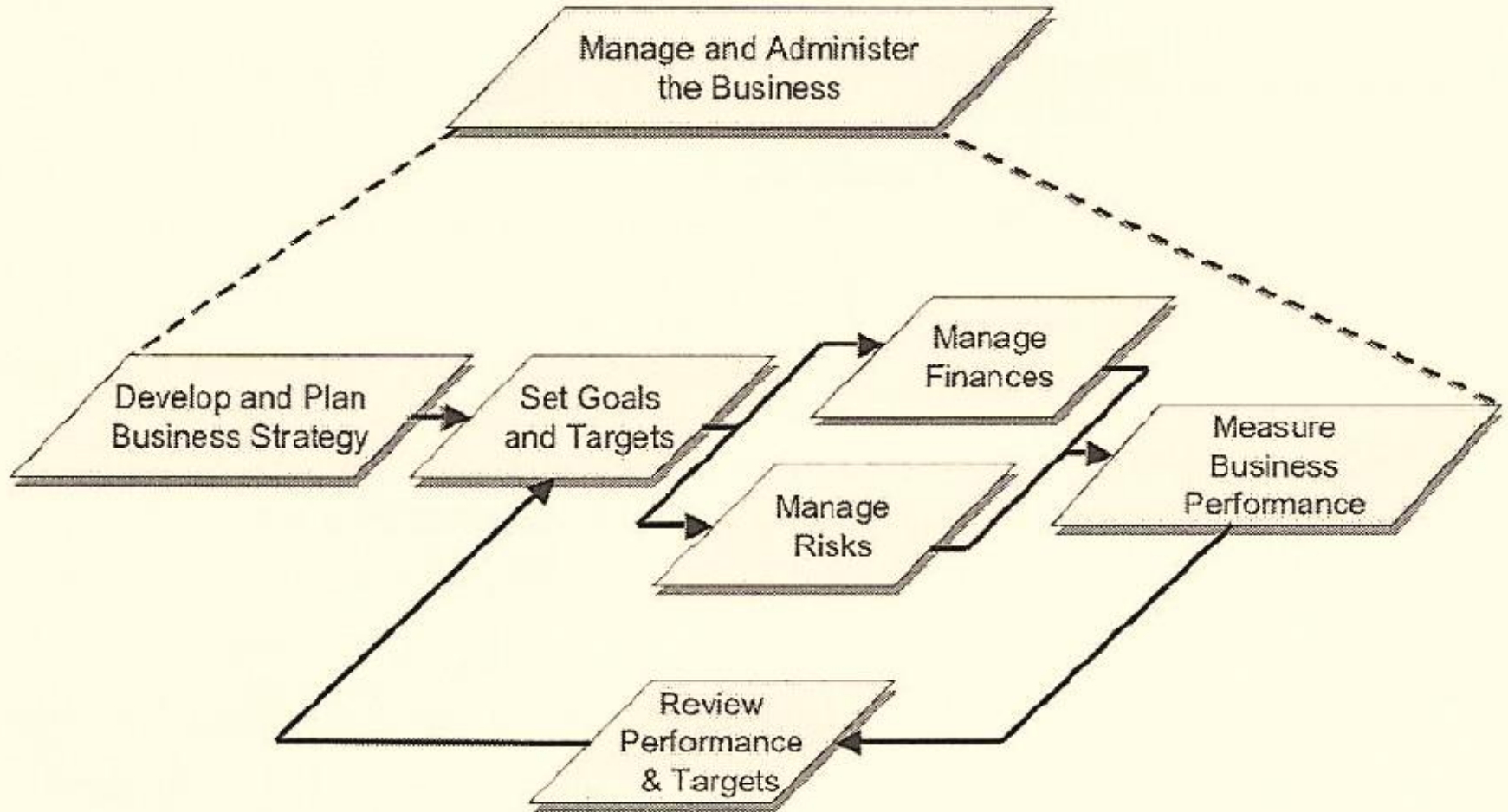
- Identify a business
- What are the high-level business processes or organizational functions of the business?

# Meta processes of 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 and administer the business***
  - *For example has 6 sub-processes...*

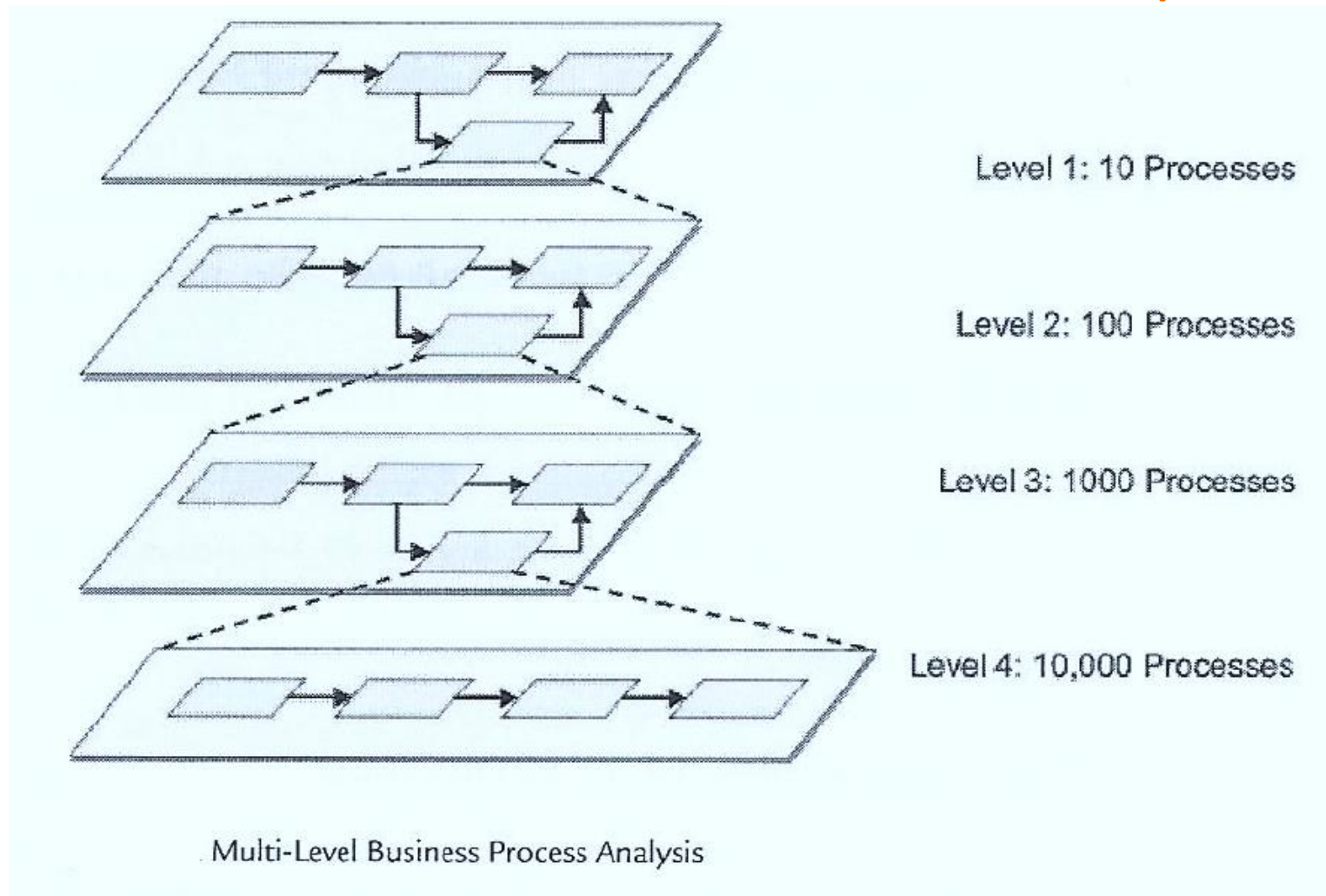
# “Manage the business”



Example of Top-Down Business Process Analysis

# Top-down business process analysis

Also known as: *Structured decomposition*



*Organizations that achieve this level of detail have an excellent model for understanding their business and business continuity management*

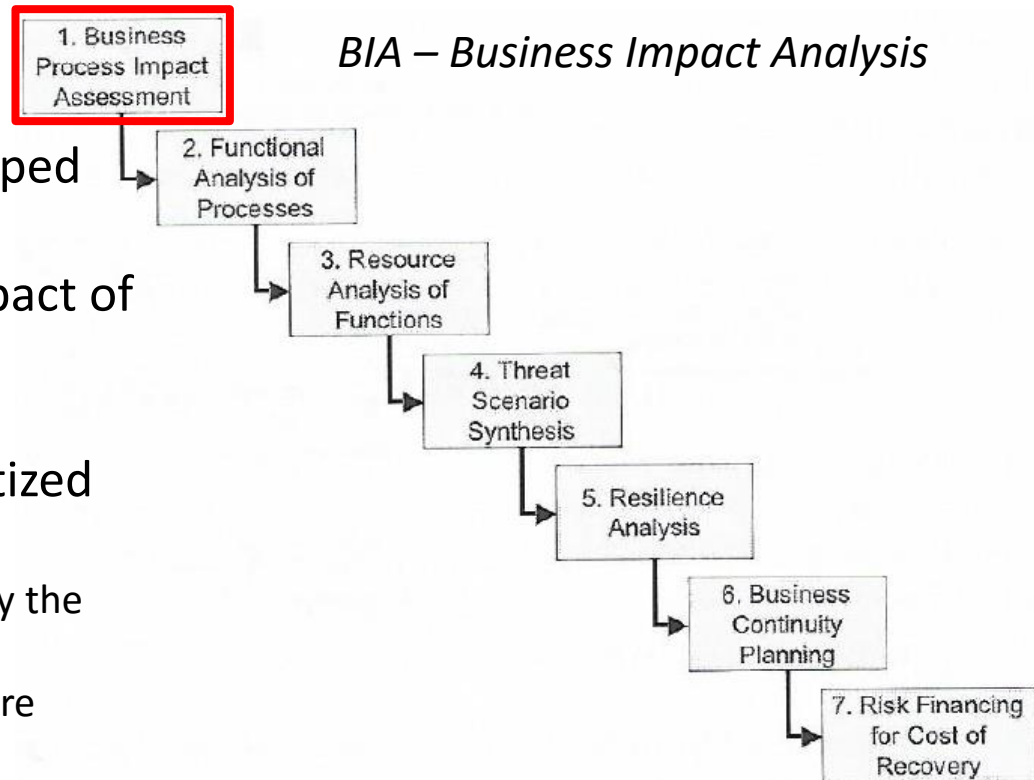


# Auditing the Business Continuity Plan

## Step 1

- Has the business identified and mapped their business processes?
- Have they assessed the business impact of loss of each business process?
- Have they classified and ranked the business processes into 3 or 4 prioritized groups:

1. **Critical** – Loss of this process will destroy the business
2. **Severe** – Loss will cause persistent, severe damage to the business
3. **Significant** (optional) – Loss will cause significant damage
4. **Other** – Damage caused by loss of this process can be absorbed



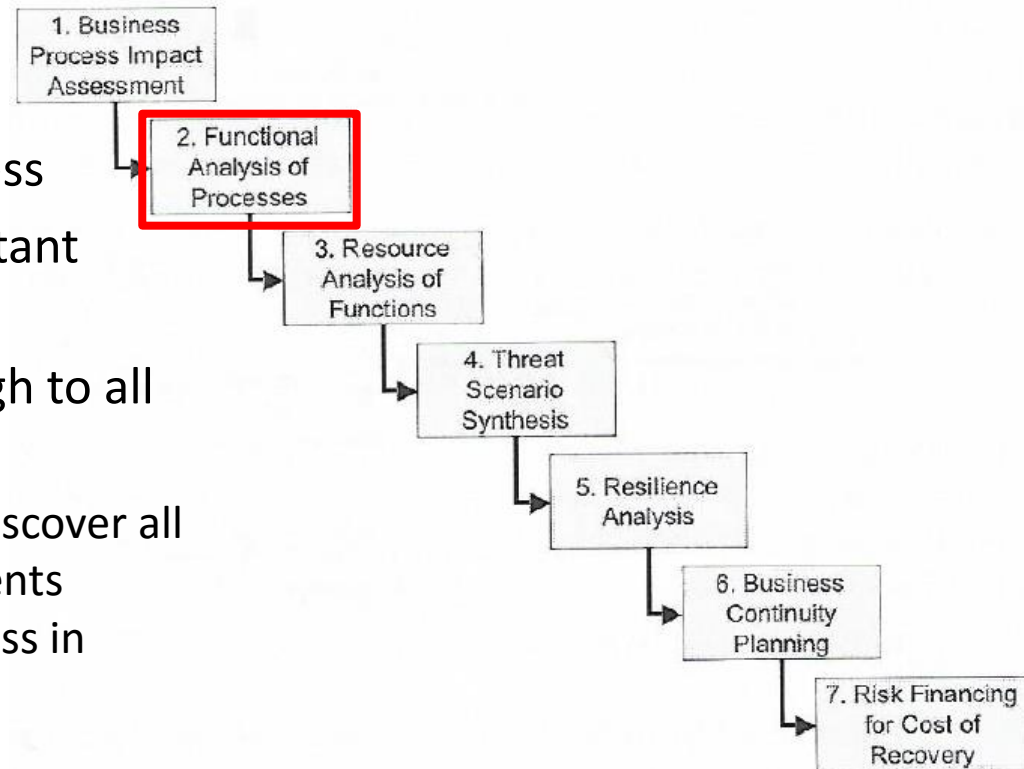
# Business Impact Analysis (BIA) goals:

1. Have they identified the most critical business functions necessary for business to survive?
2. Have they identified necessary resources for those critical functions?
3. Have they calculated the following for each critical IT resource:
  - **Recover time objective (RTO):**
    - Maximum acceptable amount of downtime the company can endure for each IT resource
  - **Recovery point objective (RPO):**
    - Maximum acceptable amount of 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 the Business Impact Analysis

## Step 2

- Select each Critical and Severe process
- Does documentation of these important business processes exist?
- Can your analysis follow trace through to all sub-processes
  - Down to single functional steps to discover all the process and functional components needed to keep this high-level process in continuous operation?



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

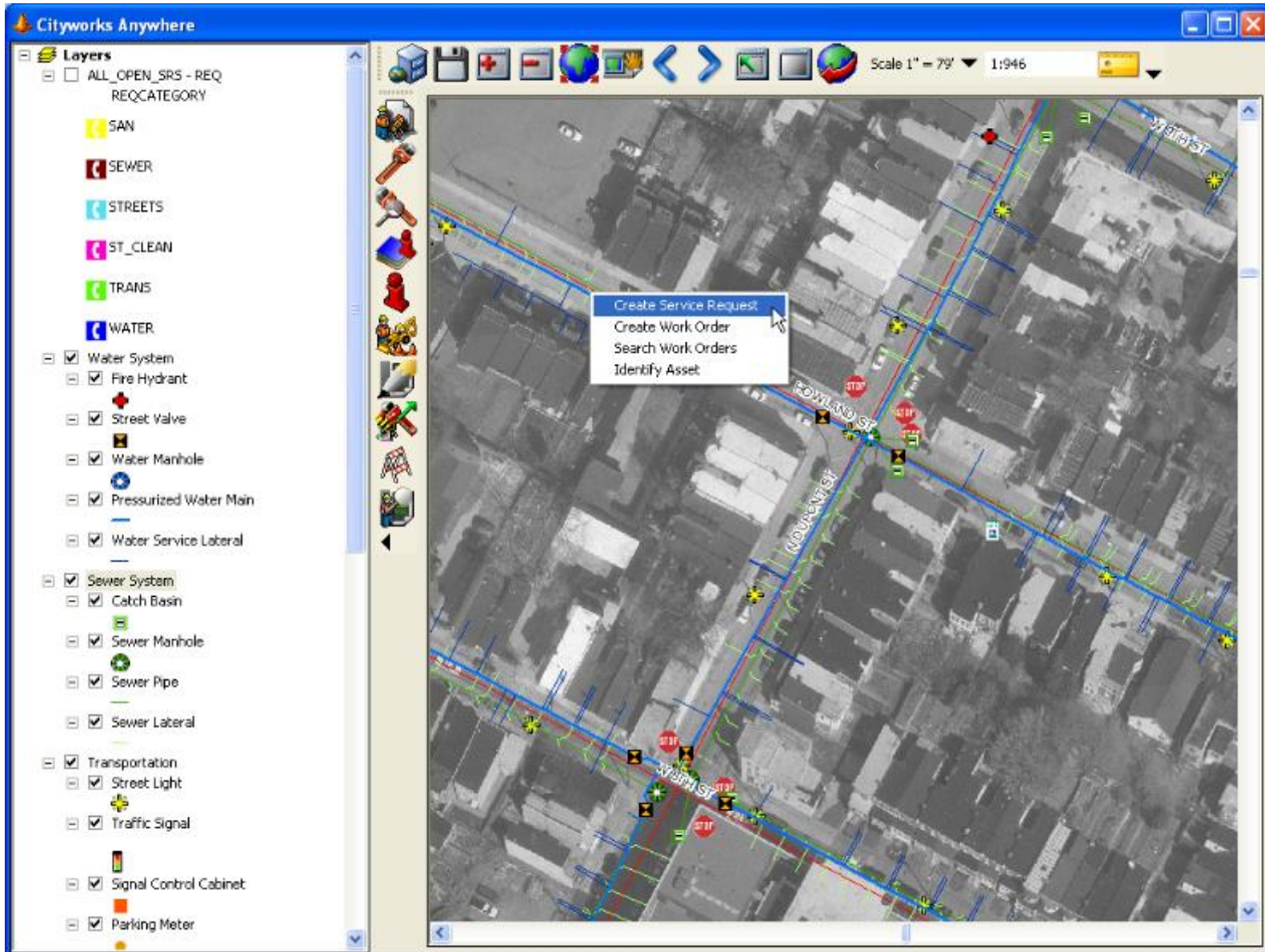
Example:

**Service request and utility maintenance management work order information system**

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

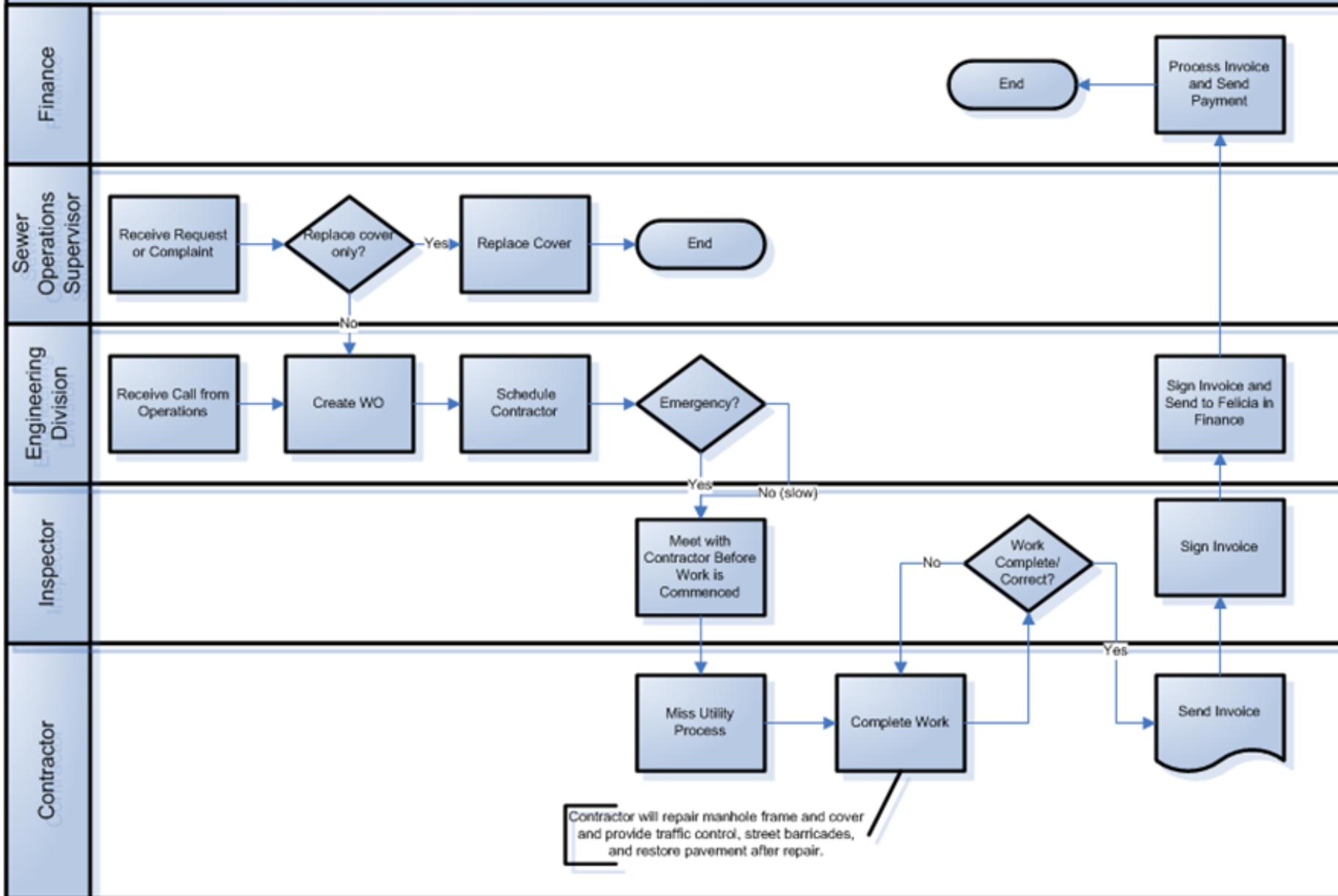
# Service Request / Work Order System

“Computerized Maintenance Management System (CMMS)”



Sewer Division  
 Repair & Replace Manhole (Frame and Cover)

Contributor(s) to this Process:  
 Michelle  
 Edmond



### Service Request

Request Recent Search Save Close New Print Tools

Search for Request ID 
Recently Opened

Apply To All

Domain:

Select a Problem from the Tree

- [-] OPERATIONS
  - [-] SEWER/STORM
    - [-] CATCH BASINS
    - [-] GENERAL
    - [-] MANHOLES/LAMPHOLES
      - LAMPHOLE\_REPAIR/REPL
      - MANHOLE\_REPAIR
      - MISSING\_LAMPHOLE\_COV
      - MISSING\_MANHOLE\_COV
  - [-] TRANSPORTATION
    - [-] GENERAL
    - [-] PARKING METERS
    - [-] SIGNS
    - [-] STREET LIGHTS
    - [-] TRAFFIC SIGNALS
  - [-] WATER
    - [-] GENERAL
    - [-] HYDRANTS
    - [-] METERS/BILLING
    - [-] QUALITY
    - [-] SERVICE LINES
    - [-] VALVES

Date/Time:  Account:

Mr  Ms

**First Name**  **Last**

**Address**

**City**  **Zip**

**Phone**

Email:

Follow-up Call Required?  
 Follow-up Call Completed?

**Problem Addr.**  Locate Using

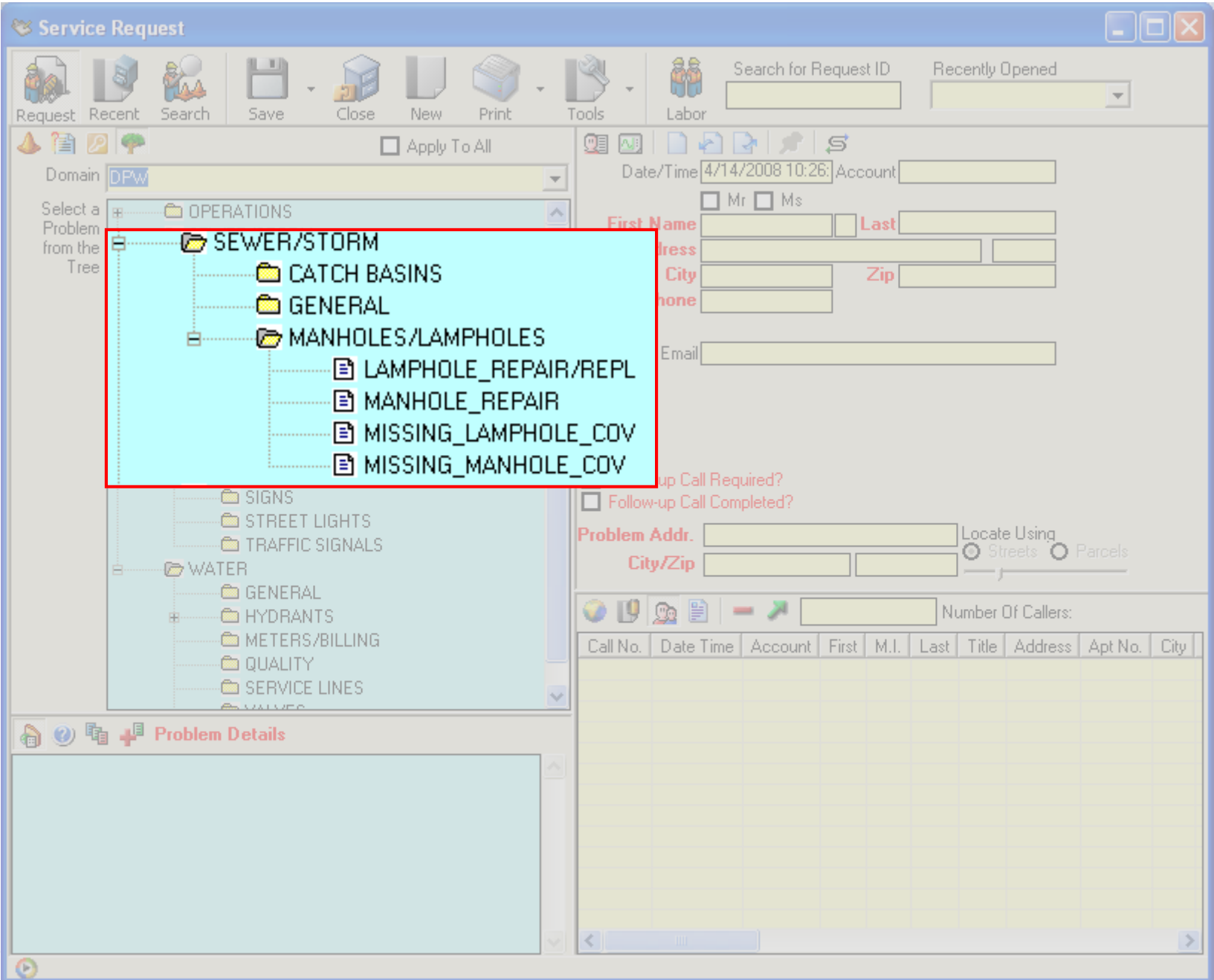
**City/Zip**    Streets  Parcels

Number Of Callers:

Call No.	Date Time	Account	First	M.I.	Last	Title	Address	Apt No.	City

**Problem Details**

M







- 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

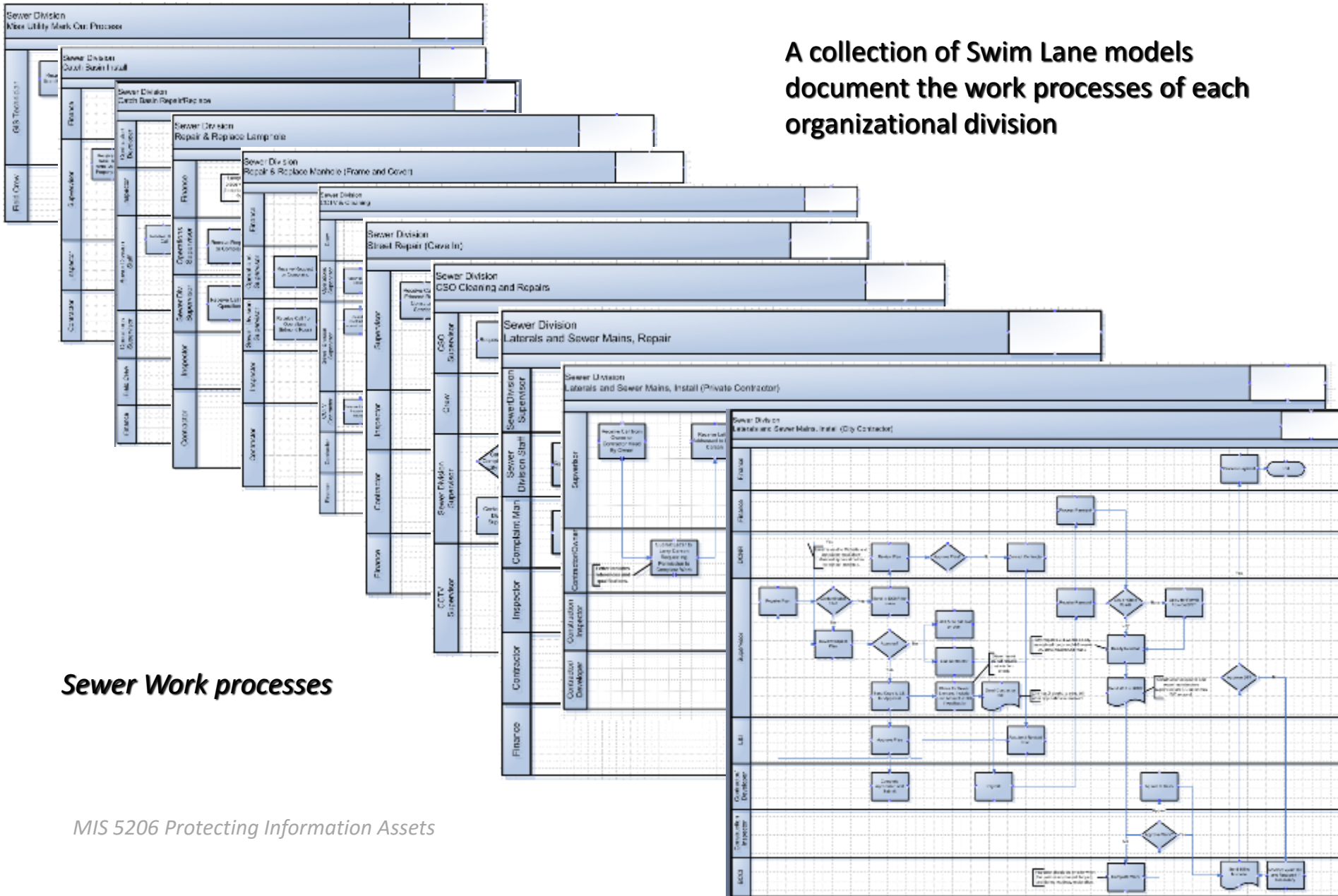
Scale 1" = 79' 1:946



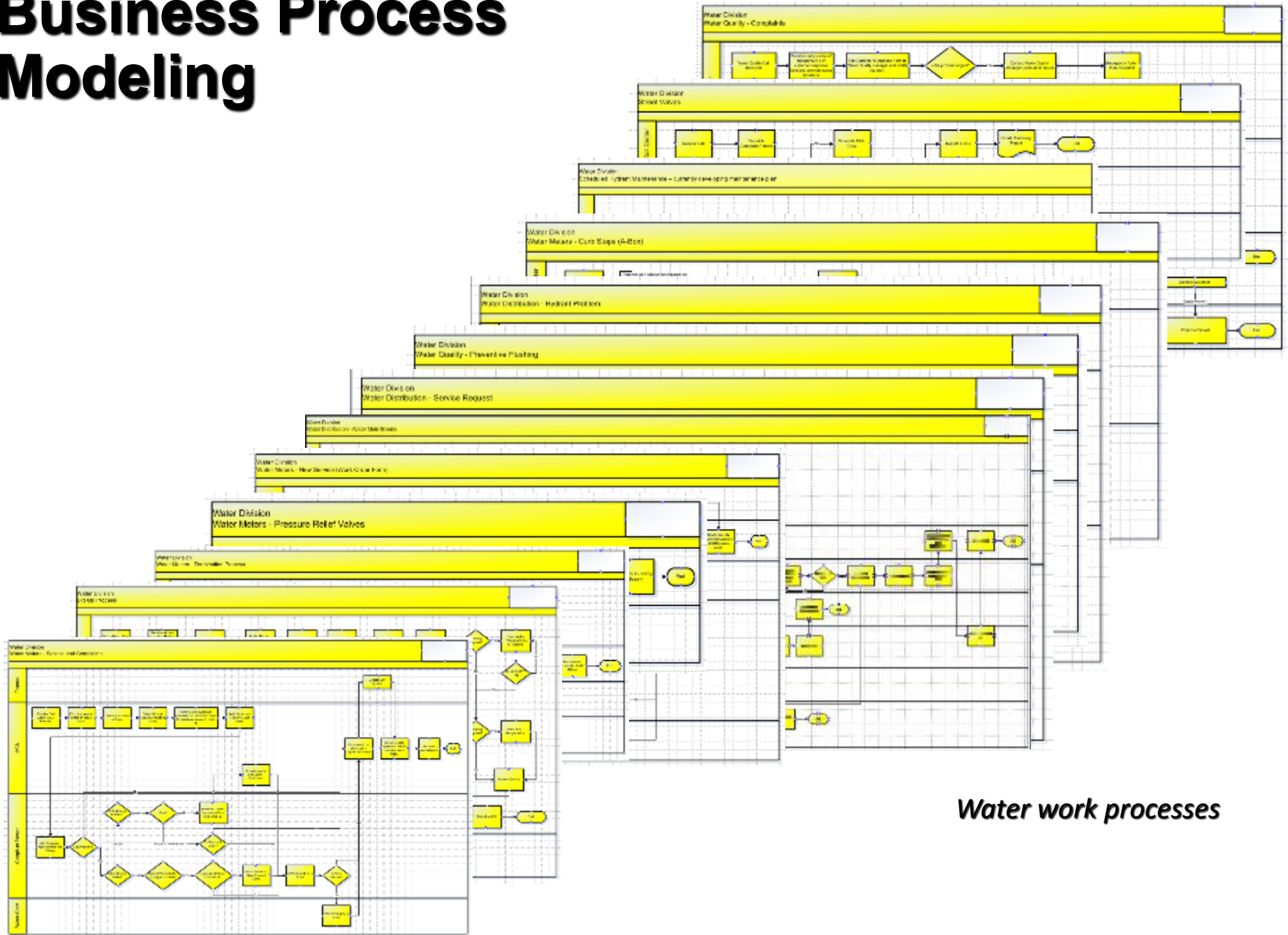
# Business Process Modeling

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

*Sewer Work processes*

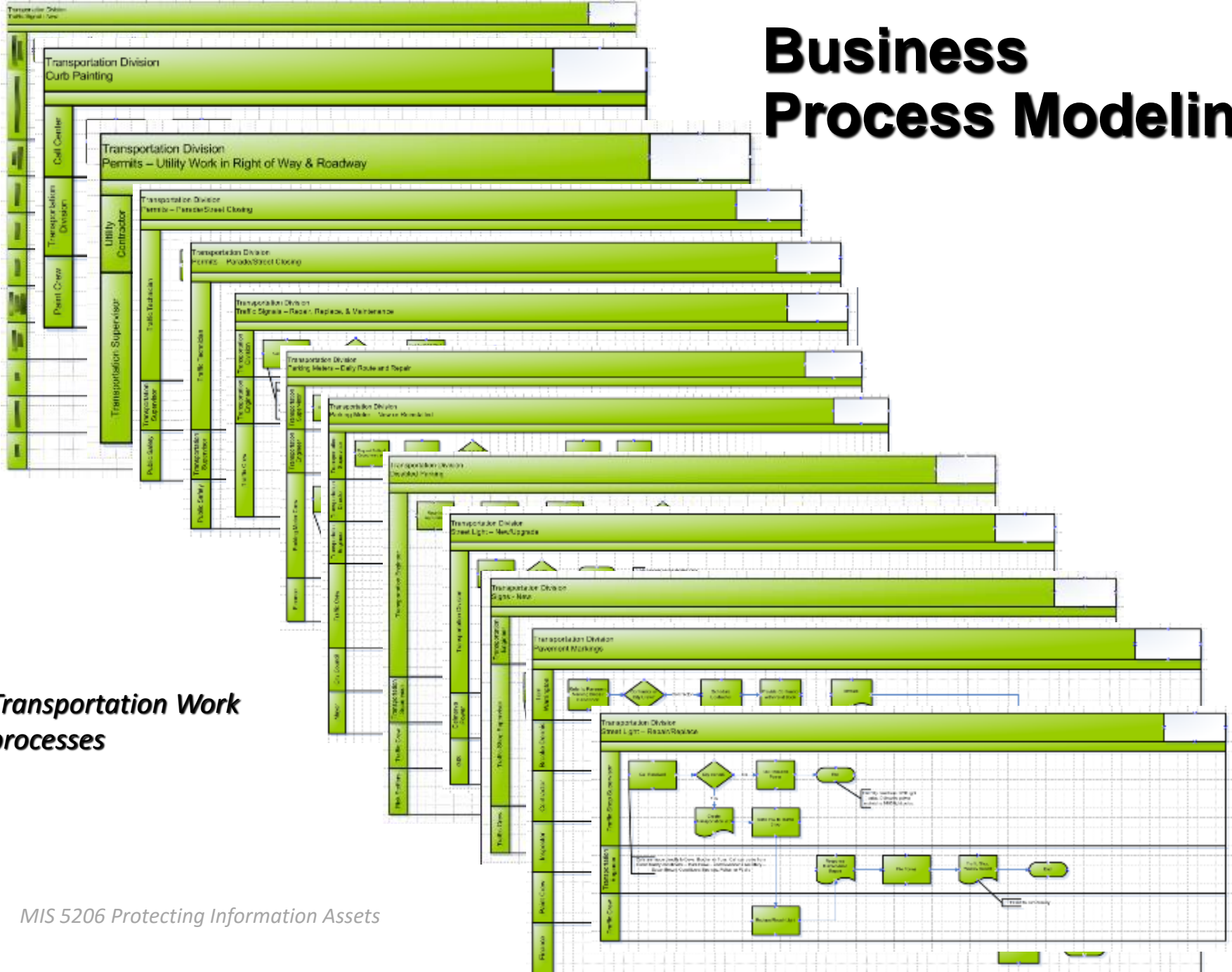


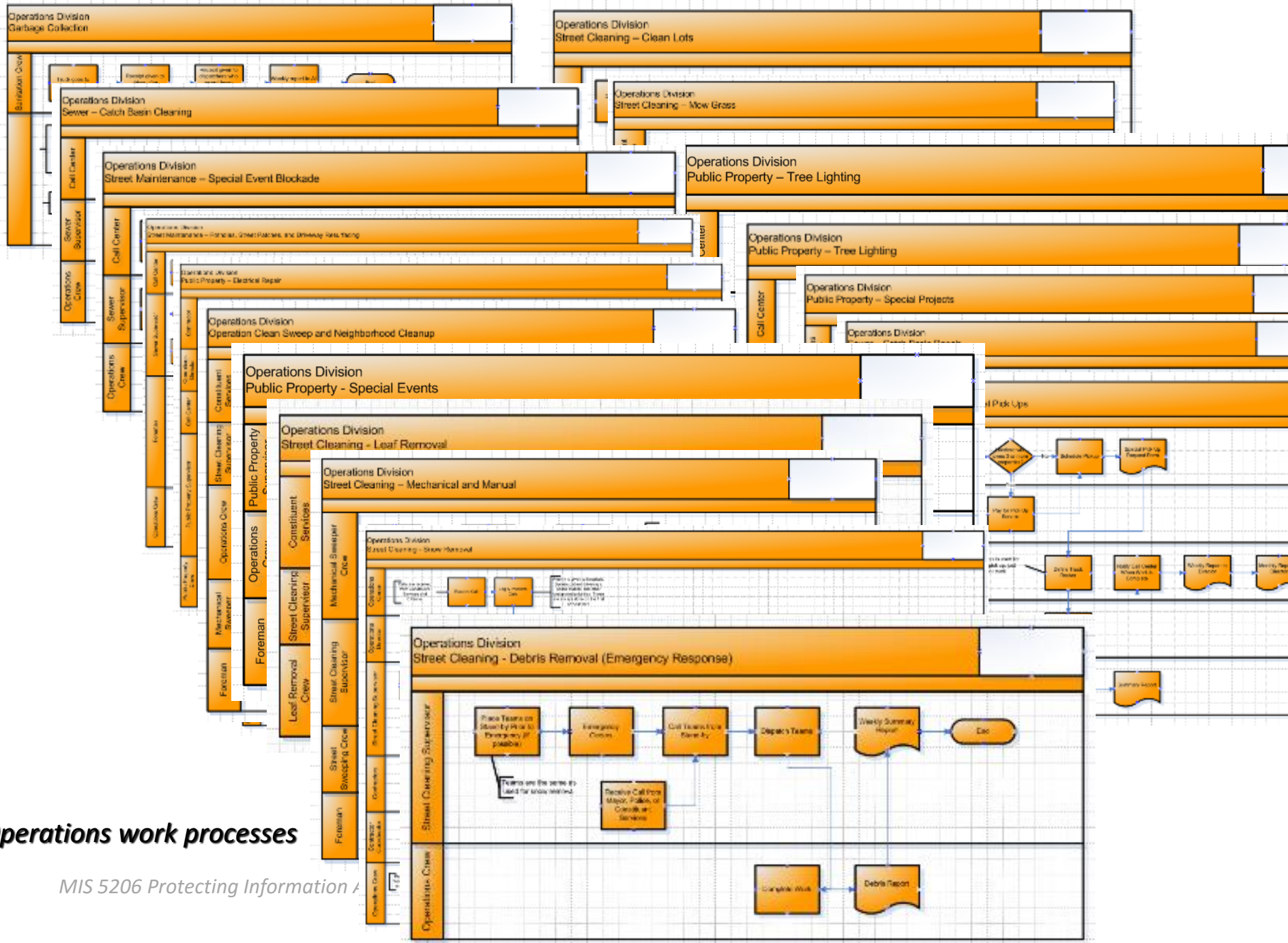
# Business Process Modeling



*Water work processes*

# Business Process Modeling



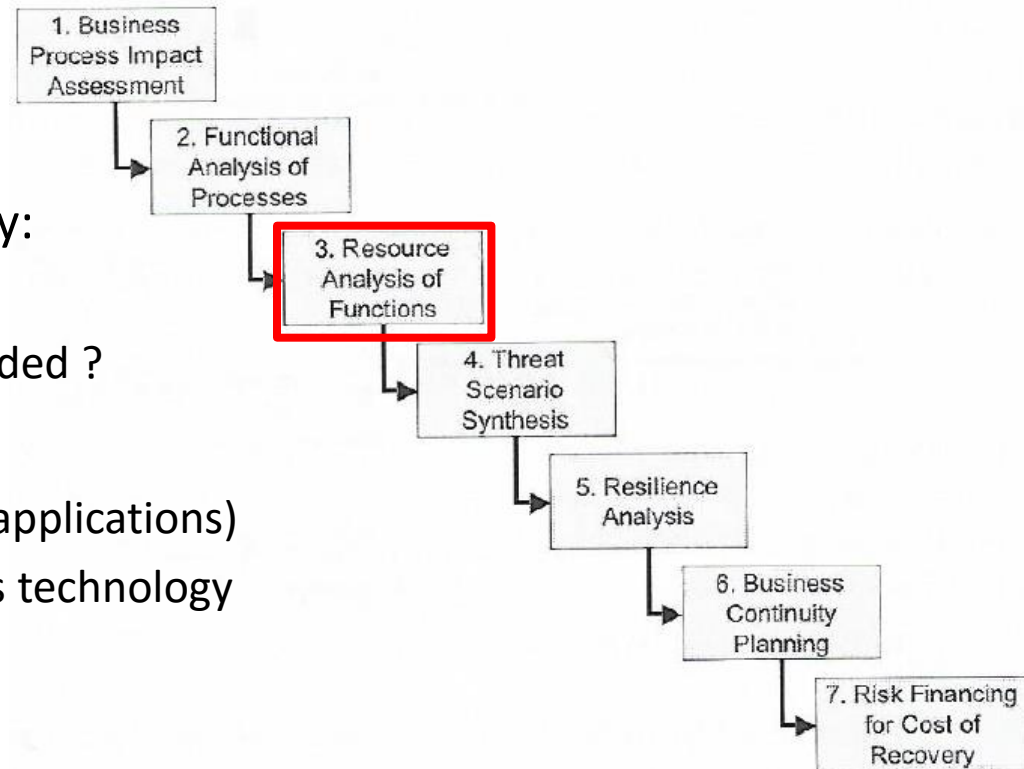


**Operations work processes**


# Business Continuity Management Process

## 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
    - ...



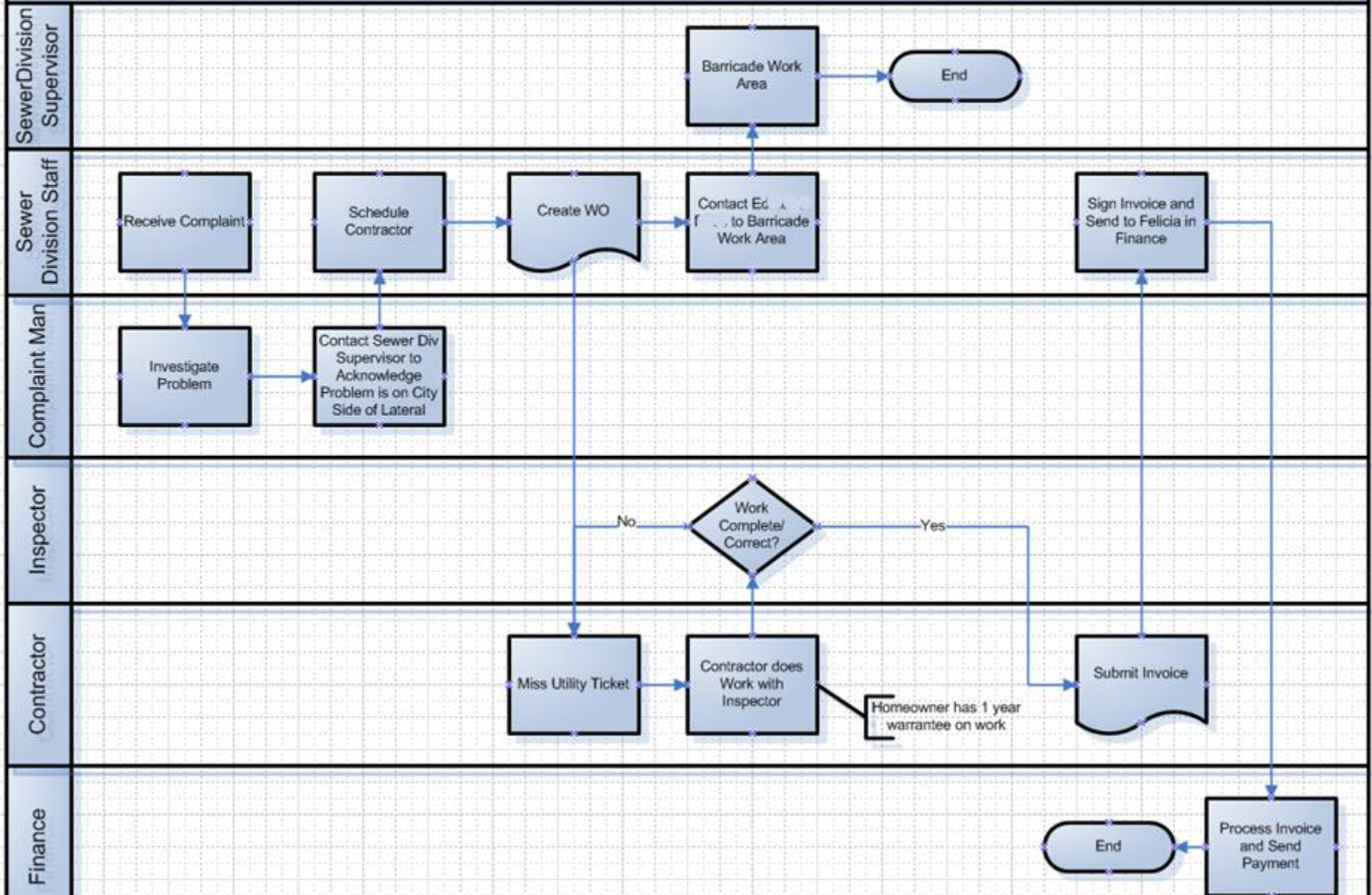
Have they mapped out the work processes and staff resources needed from each department?

			Sewer Division						
Work Types			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

*Have they documented the communications  
needed to coordinate resources?*



# Can you understand the cross organizational workflows...

		Operations Division														Other																					
		Work Types																																			
		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	La&I	GIS Technician	Fire Board	DELDOT	Delaware Dept. of Natural Resources and Env. Control	Utility Contractor	DelMarva Power	City Council	Mayor	Police	Landlord					
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																																			

*Identifying dependencies on critical paths for completing prioritized work processes*

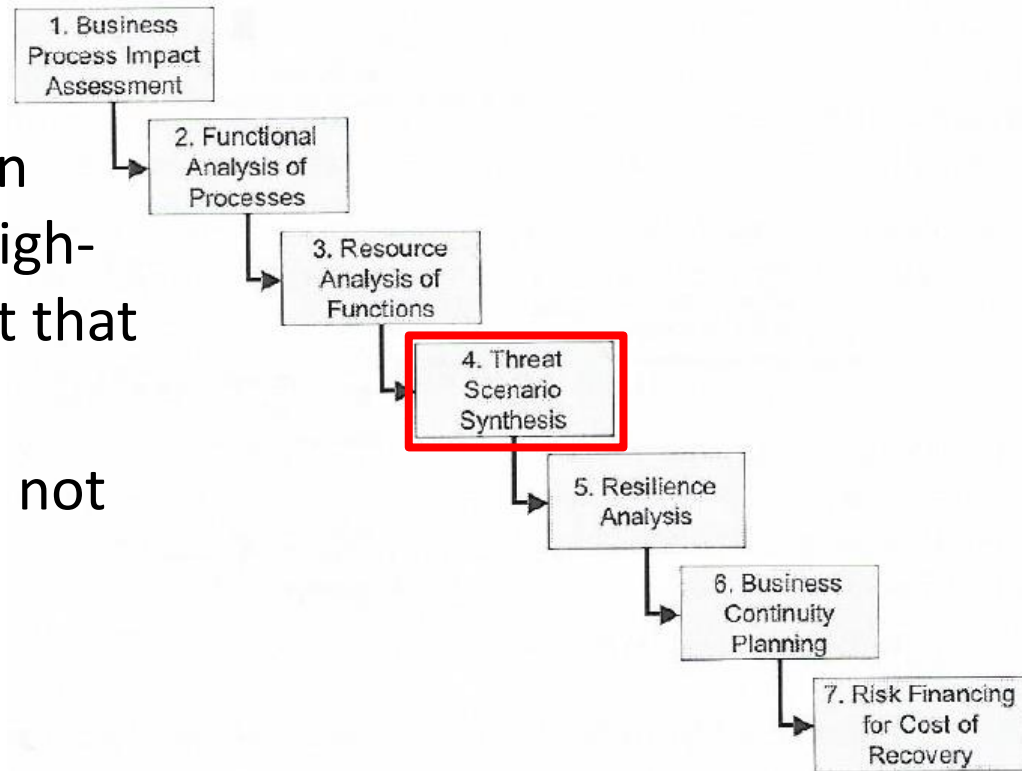




# Business Impact Analysis

## Step 4

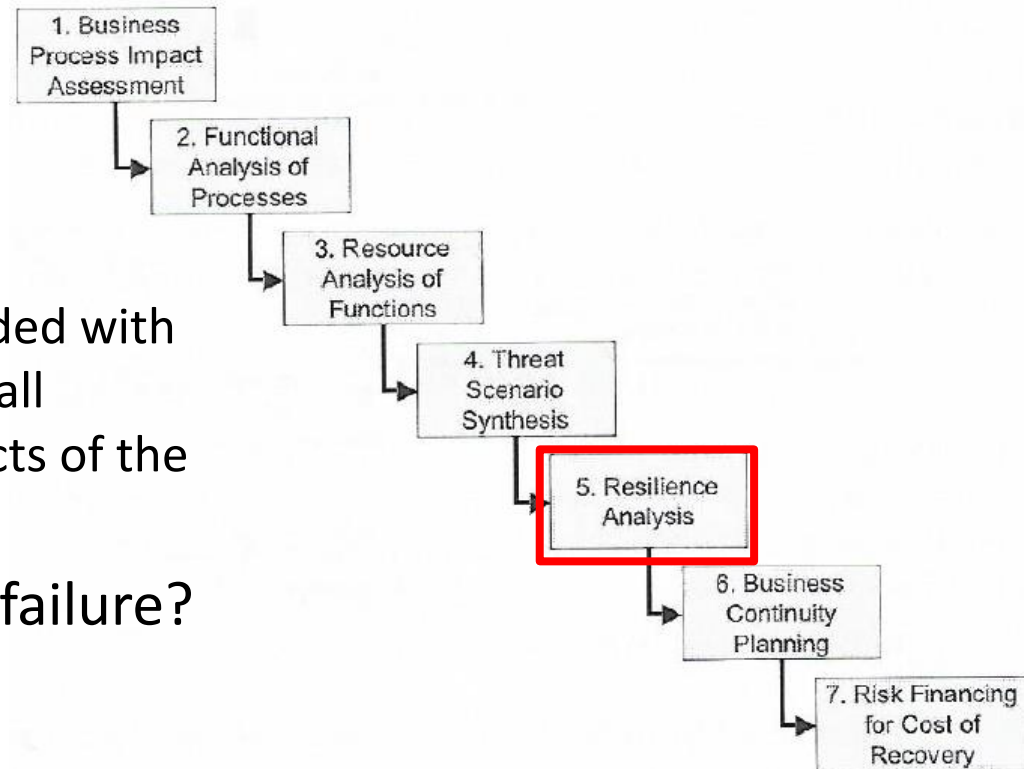
- For each resource identified in Step 3, have they identified high-level threat scenarios that put that resource at risk?
- Have they focused on effects, not causes?



# Business Impact Analysis

## Step 5

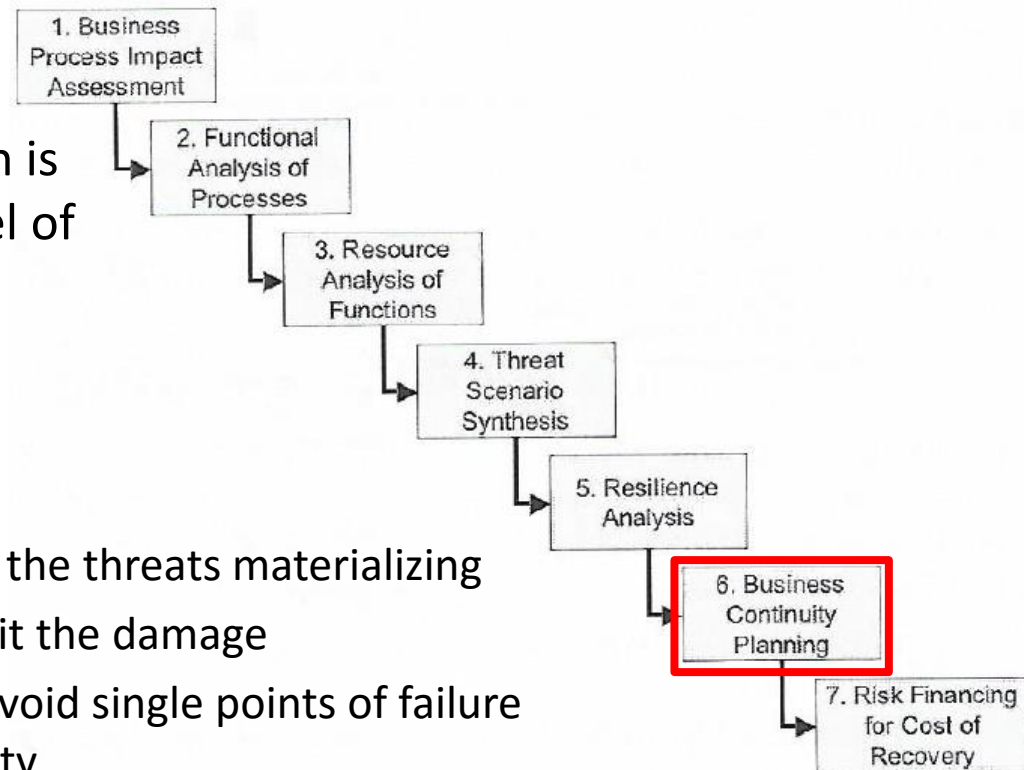
- For each resource/scenario combination
  - Are the current resources provided with sufficient resilience for the overall business to withstand the impacts of the scenario?
- Are there any single points of failure?



# Business Impact Analysis

## Step 6

- What additional resource protection is needed to provide the required level of resource resilience so the 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 including (**DRP!**)
  - Recovery plans to resume business following an incident
  - Training and awareness



# Disaster Recovery Planning

- Does a planning group exist?
- Do they know their priorities for applications, data and networks?
- Do they have recovery strategies
- Is the plan documented?
- Have they tested and verified that the plan will work?
- Is the plan implemented?





# Exercise

- What elements are needed for a disaster recovery plan?

# Disaster Recovery Plan Elements

- **Primary facility recovery and backup sites:**
  - If primary site is destroyed, where should processing take place
- **People:**
  - Human resources is the resource most forgotten
  - Employees' responsibilities to families during disaster may block DRP implementation:
    - May need to tend to their families instead of helping the company get back on its feet
- **Hardware setup and access:**
  - Replacement time requirements, Service Level Agreements with suppliers, dangers of legacy or proprietary devices
- **Software implementation:**
  - Critical applications, and supporting utilities and operating systems for production
- **Data restoration:**
  - If not fault-tolerant (e.g. mirroring), will need to load backed up data to restore processing
- **Communication to different groups after a disaster:**
  - Employees, customers, suppliers, stock holders, media
- **Security needed throughout:**
  - Protecting against looting and fraudulent activities after a disaster
- **Legal responsibilities**

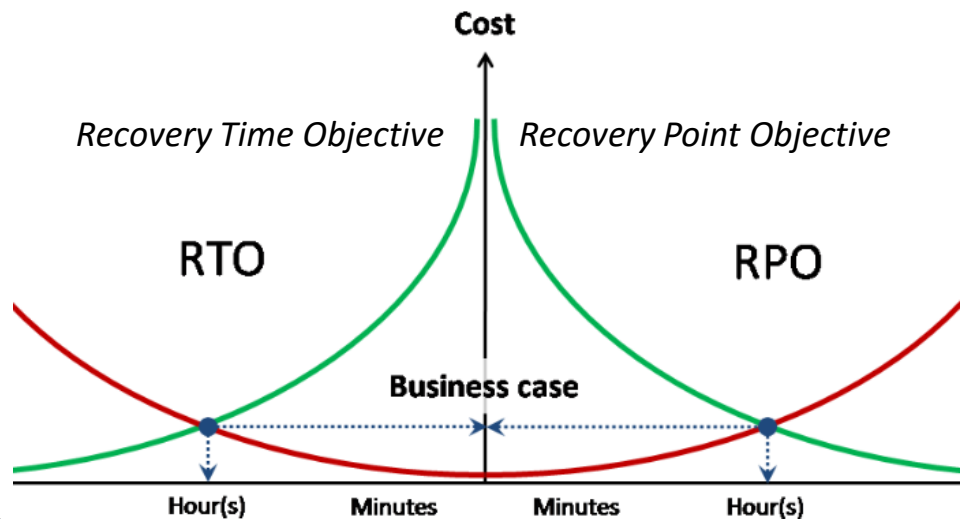
# Disaster recovery time targets

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

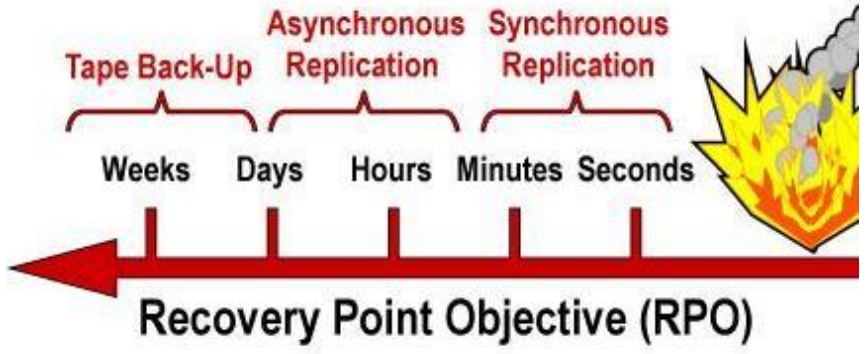
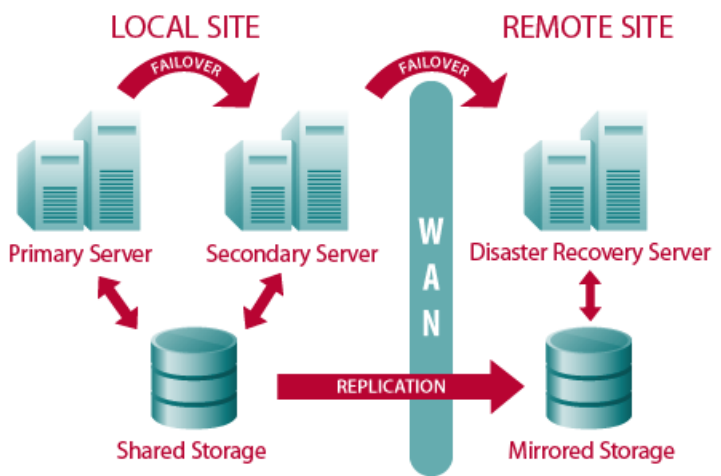
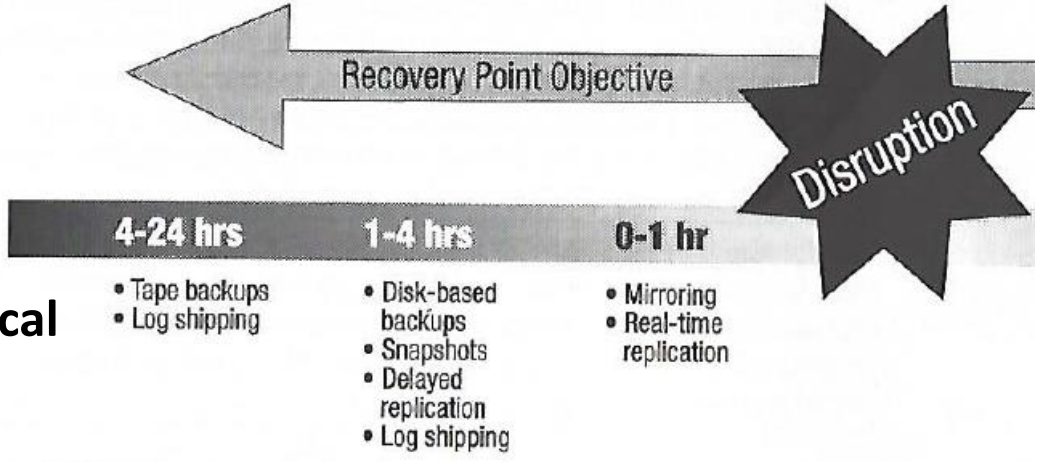
Speed of recovery must be traded off against cost

- 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 worked out in detail to plan disaster recovery
  - Remember: *The only goal is to create effective business continuity, whatever that turns out to be*



# Data backup systems and redundancies

- Database shadowing
- Electronic vaulting
- Remote journaling
- Storage area network and hierarchical storage management
- Shared storage
- RAID
- Failover clustering



# Auditing Recovery Plans

Have they documented:

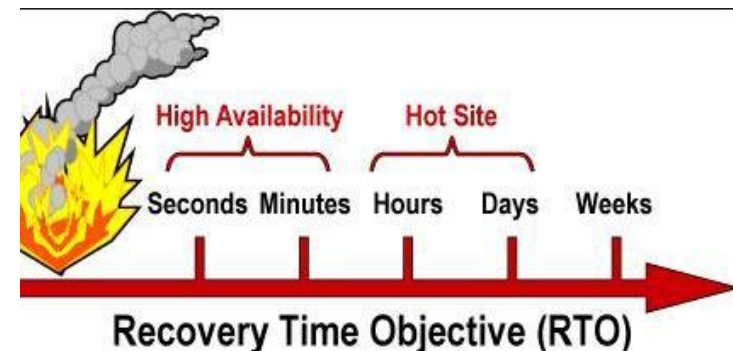
1. Strategies, resources, timelines and dependencies?
  2. Approaches to “re-initiate” crucial business functions and resume on-going operations?
- Have the plans been reviewed and confirmed by function owners in the business as well as executives

# What kind of offsite alternative recovery facility do they have for the information systems?

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

**Warm site:** Less expensive alternative to hot site, includes communications components but computers are not installed – will need to be delivered and setup

**Cold site:** Less expensive than warm site, provides only the basic environment that can be outfitted with communication components and computers, though this may take from one to several weeks



# 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*

# Have they classified their application systems and scheduled their restoration?

## 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

***SANS Institute (officially the Escal Institute of Advanced Technologies)***



# 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
- A program built for a particular version of an operating system, will not run if the 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

# Have they planned the availability of people after disaster?

- Attention focused on backing up data and technology, often overlooks people and necessary skillsets for continuing the operation of the enterprise
- Employees may not be available after a disaster:
  - Death, injury, or family responsibilities
  - Business continuity committee
    - Must identify the necessary skill set for each critical task
    - Come up with 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:

- ***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 the documents detailing the sequence of events, to actually rehearsing the plan up to the point of actual data or resource recovery at the main site.

- ***Salvage team***

- Assesses damage and works to bring the businesses' primary facility back on-line

# What mechanisms exist to support disaster recovery services:

- **Contingency sites**
  - Redundancy of hardware and communications lines for resilient operations
- **Data management tasks**
  - Taking appropriate backups of data and software
  - Providing backup management: labeling, indexing, storage
  - Off-site storage
  - Data recovery and restoration procedures
- **Recovery plans and procedures**
- **Incident management responsibilities**
- **Activation plans**

# Questions

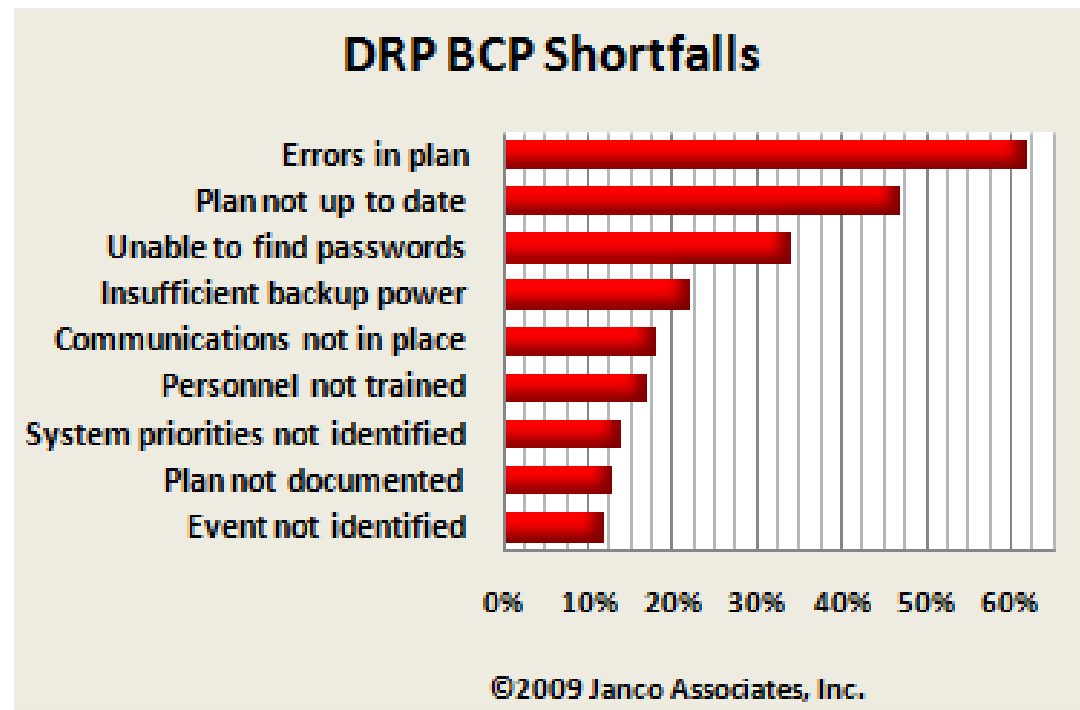
- Is it practical to conduct a thorough test of a Business Continuity Plan (BCP)?
- Why might it not be practical?
- If it is not practical, what alternative ways can you recommend for testing a BCP?

# Have they tested their Disaster Recovery Plan (DRP)?

Tests are conducted to be sure plan is good, everyone is prepared and knows what to do

These 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 individual has a checklist of responsibilities under the DRP
  - During testing, each individual reviews his/her checklist
  - Can be done as a group or individually
- Tabletop exercise
  - Test facilitator describe 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?

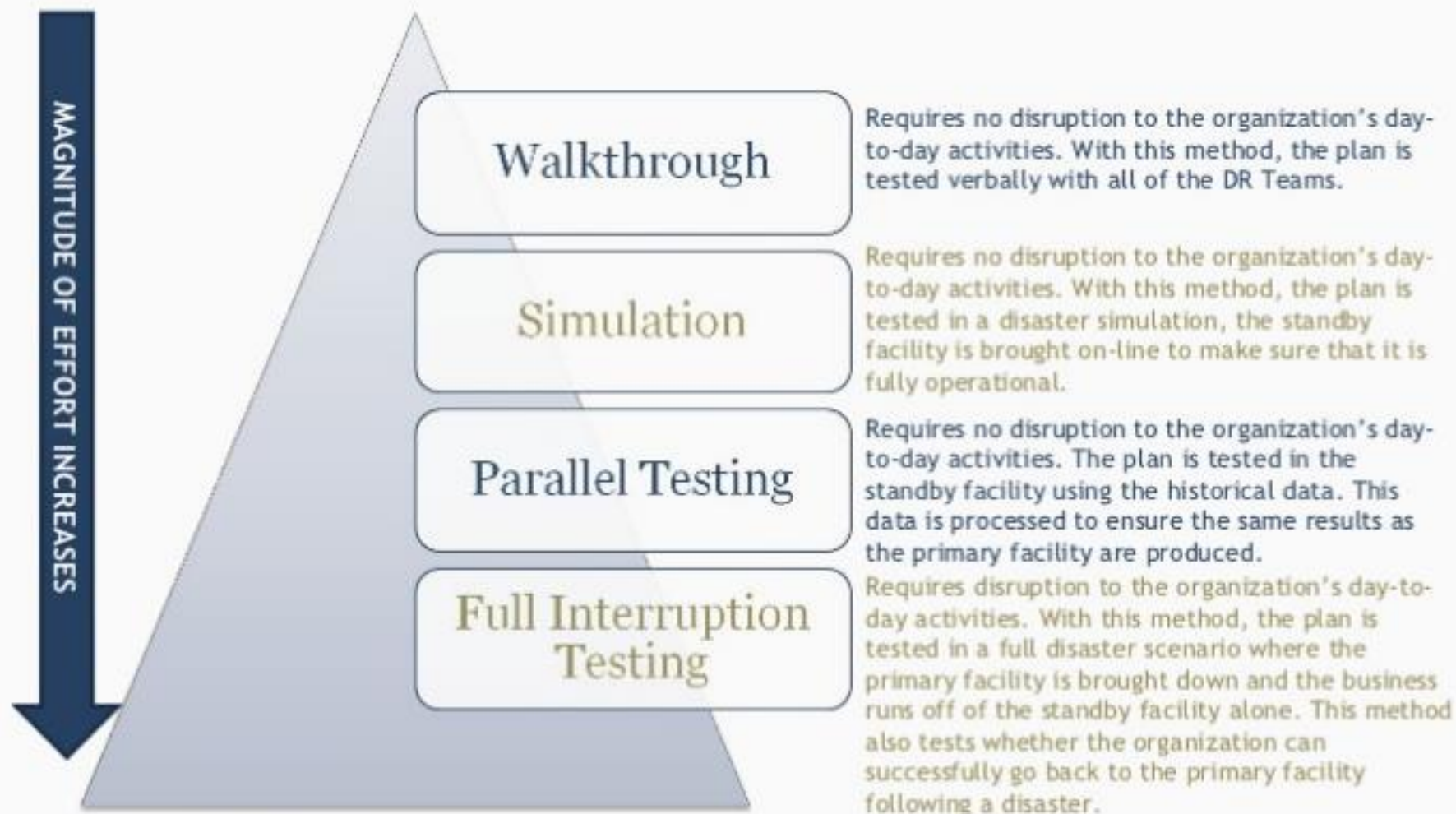
- **Structured walk-through**
  - More formal troubleshooting of the plan by simply walking through the documents detailing the sequence of events
- **Dry-Run tests**
  - Can be conducted on a function by function basis
  - Do not have test all functions for each cycle
  - Tests should involve actual interruptions and recoveries
  - Actually rehearsing the plan up to the point of actual data or resource recovery at the main site





# Testing is necessary for all DRPs

Perform testing on the DRP periodically to ensure that the plan works and that the entire organization knows what to do in the event of a disaster.



# Audit Focus

Areas for  
audit  
evaluation:

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

Data	<ul style="list-style-type: none"><li>• Review or observe backup procedures.</li><li>• Review documentation of a successful restore (within the last year).</li><li>• Verify restoration personally (when risk is high or restoration is an audit objective).</li></ul>
Site/computers/ OS	<ul style="list-style-type: none"><li>• Review the provisions of the BCP/DRP.</li><li>• Review a contract (hot site, cold site, mutual aid, etc.).</li><li>• Verify the ability to restore these aspects.</li></ul>
Applications	<ul style="list-style-type: none"><li>• Review the plan's provisions.</li><li>• Review the critical applications list, including ranking.</li><li>• Verify the ability to restore (personally, when risk is high or restoration is an audit objective).</li><li>• Observe or inquire about the backups of application software and location.</li></ul>
Supplies/ documentation	<ul style="list-style-type: none"><li>• Review the plan's provisions.</li><li>• Observe or inquire about the provisions and location.</li></ul>
Recovery team	<ul style="list-style-type: none"><li>• Review the plan's provisions.</li><li>• Interview one or more members of the team, and ask about roles and responsibilities.</li><li>• Gain assurance that there is provision for adequate personnel for a successful restoration.</li></ul>

# 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

# Quiz

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
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
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

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
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
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