Unit #12

Incident and Disaster Response

MIS 5214

Agenda

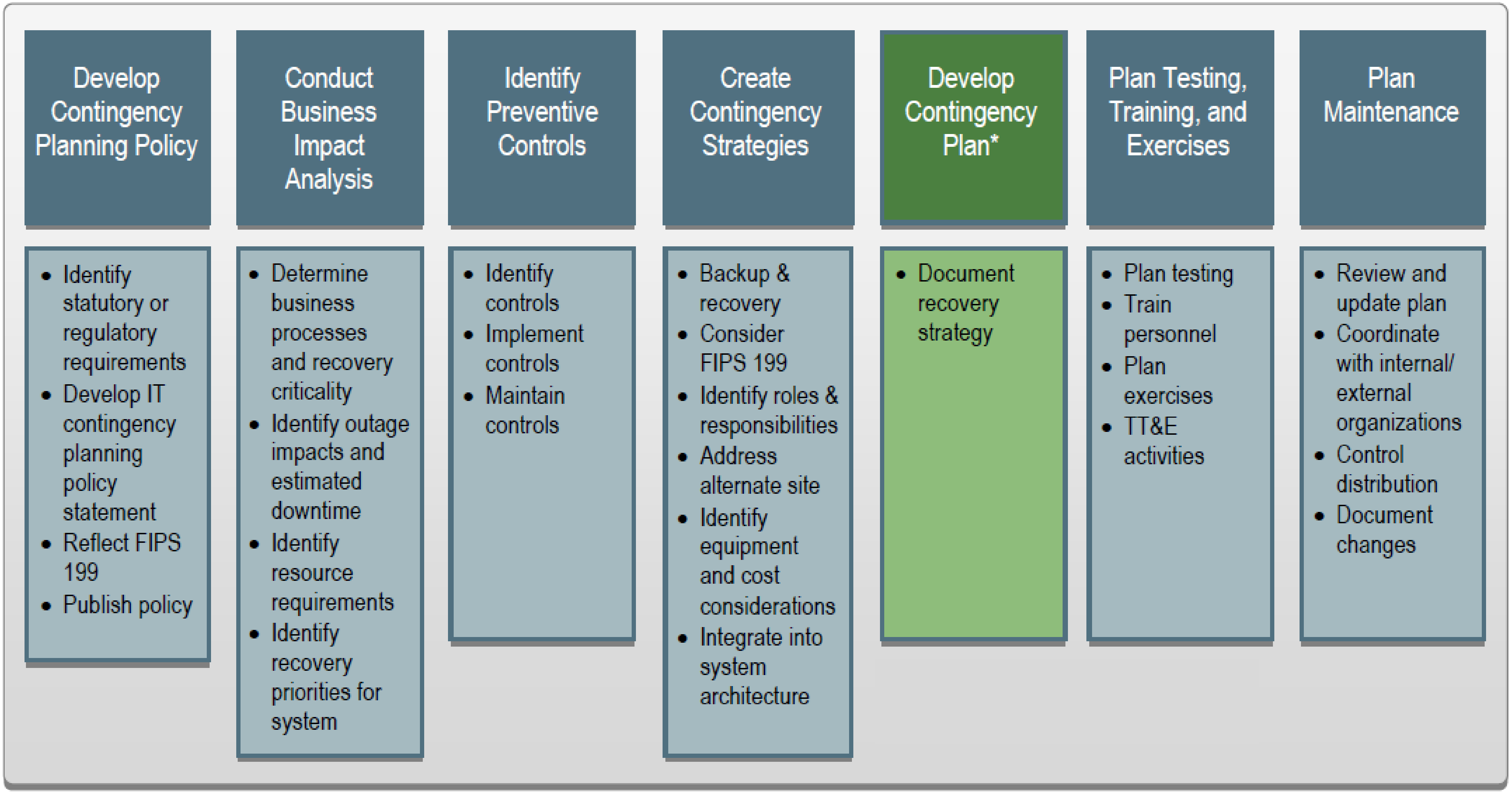
- In The News exercise
- Incident & Disaster Response Planning
- Team Project Schedule
- Final Exam
- Student Feedback Form (eSFF)
- SSP discussion

Business Impact Analysis Exercise

1. Read the following article:
   - https://www.nytimes.com/2019/04/10/nyregion/nyc-gps-wireless.html

2. Answer the following information security questions:
   a) What is the threat?
   b) What New York City Organizations are affected?
   c) What are the vulnerabilities?
   d) What more do you want to know?

Incident & Disaster Response Planning



Develop Contingency Planning Policy

- Identify statutory or regulatory requirements
- Develop IT contingency planning policy statement
- Reflect FIPS 199
- Publish policy

Conduct Business Impact Analysis

- Determine business processes and recovery criticality
- Identify outage impacts and estimated downtime
- Identify resource requirements
- Identify recovery priorities for system

Identify Preventive Controls

- Identify controls
- Implement controls
- Maintain controls

Create Contingency Strategies

- Backup & recovery
- Consider FIPS 199
- Identify roles & responsibilities
- Address alternate site
- Identify equipment and cost considerations
- Integrate into system architecture

Develop Contingency Plan*

- Document recovery strategy

Plan Testing, Training, and Exercises

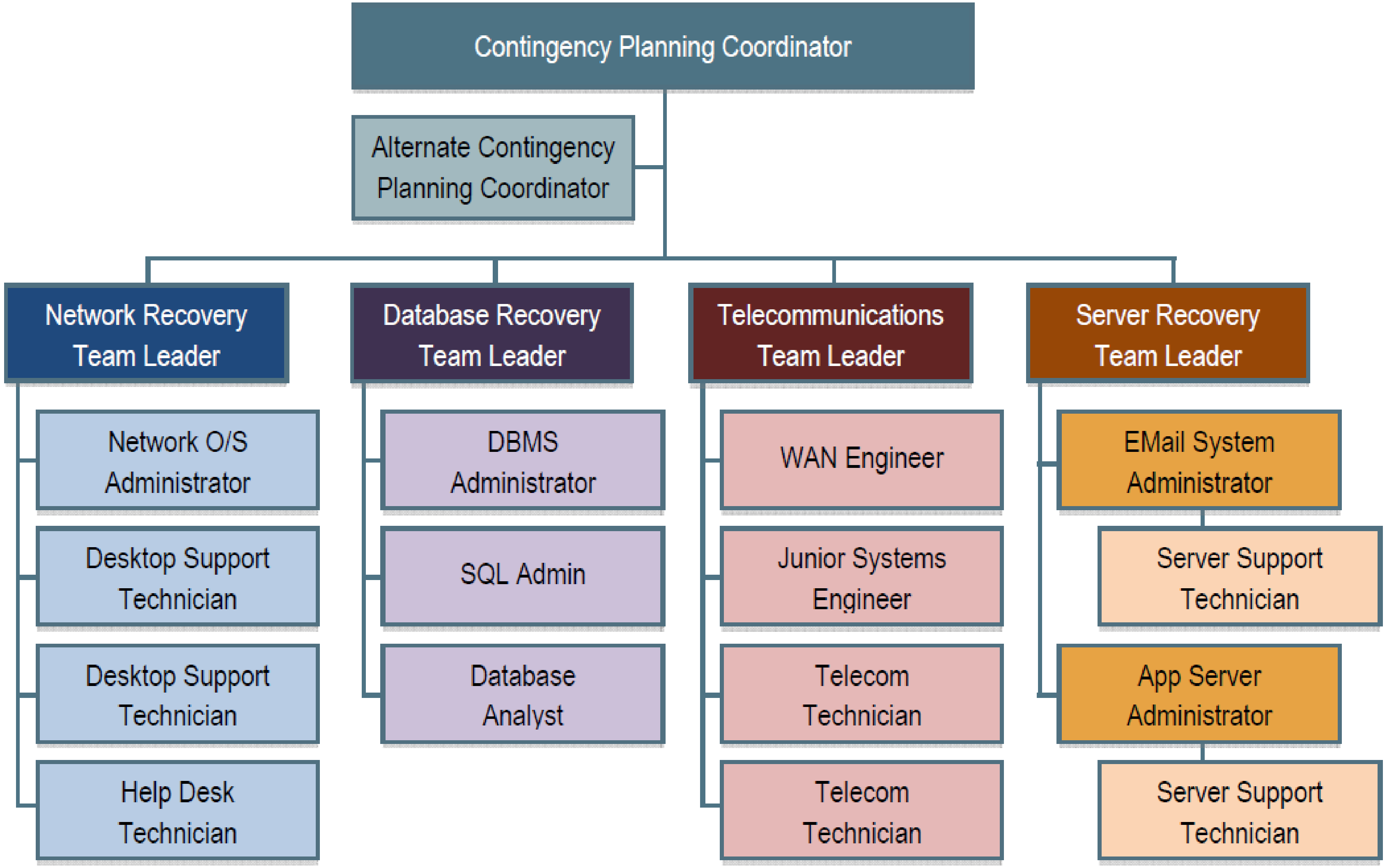
- Plan testing
- Train personnel
- Plan exercises
- TT&E activities

Plan Maintenance

- Review and update plan
- Coordinate with internal/ external organizations
- Control distribution
- Document changes

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

Response Roles and Responsibilities example



Contingency Planning Coordinator

Alternate Contingency Planning Coordinator

Network Recovery Team Leader
- Network O/S Administrator
- Desktop Support Technician
- Desktop Support Technician
- Help Desk Technician

Database Recovery Team Leader
- DBMS Administrator
- SQL Admin
- Database Analyst

Telecommunications Team Leader
- WAN Engineer
- Junior Systems Engineer
- Telecom Technician
- Telecom Technician

Server Recovery Team Leader
- EMail System Administrator
  - Server Support Technician
- App Server Administrator
  - Server Support Technician

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

3 Phase Approach to Incident & Disaster Response

1. **Activation/Notification Phase**

   The process of activating the plan based on impacts and notifying recovery personnel

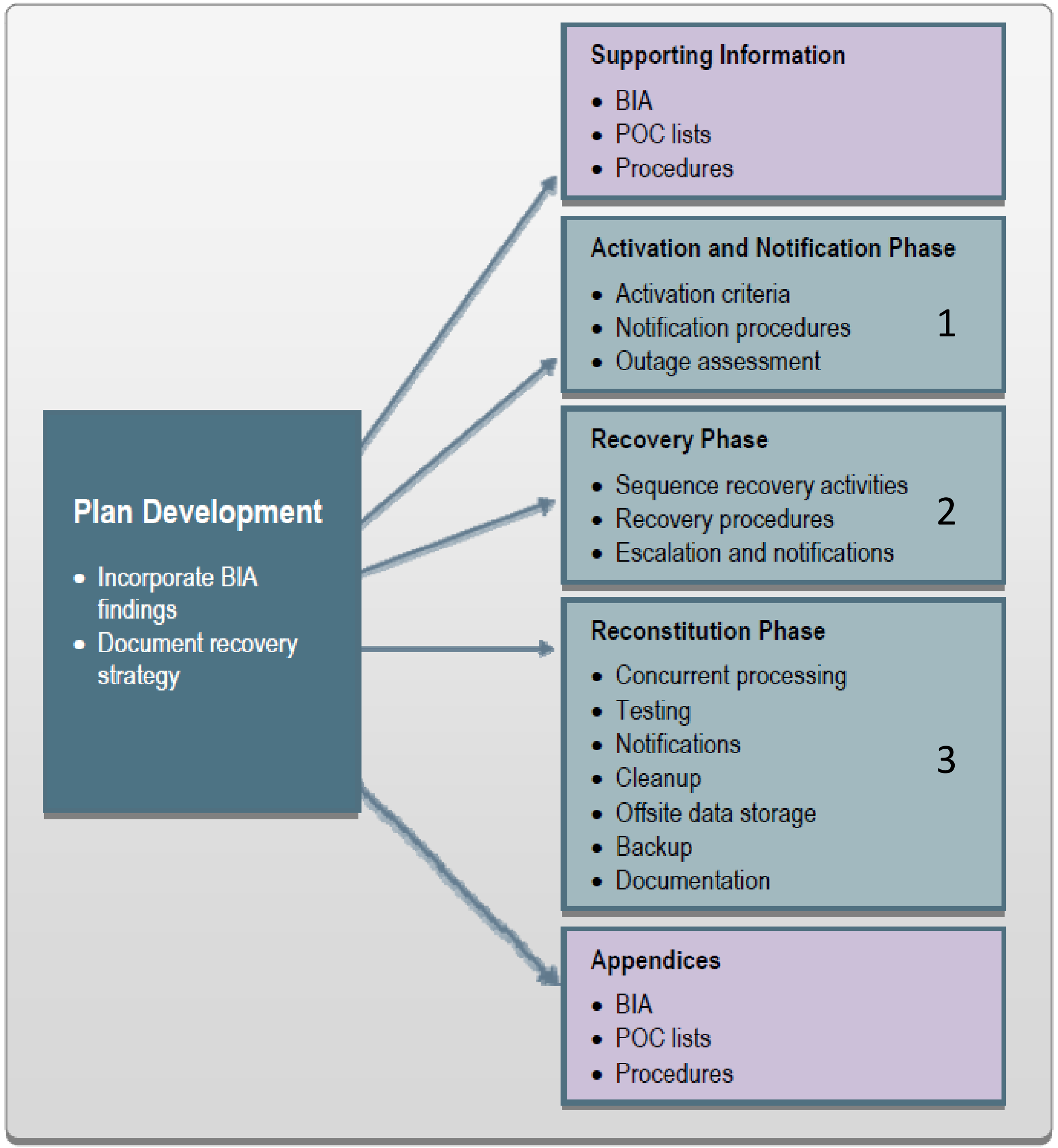
2. **Recovery Phase**

   Implements a course of action for recovery teams to mitigate impacts and restore system operations at an alternate site or using contingency capabilities

3. **Reconstitution Phase**

   Includes activities to test and validate system capability and functionality and actions taken to return the system to normal operating condition and prepare the system against future impacts or outages

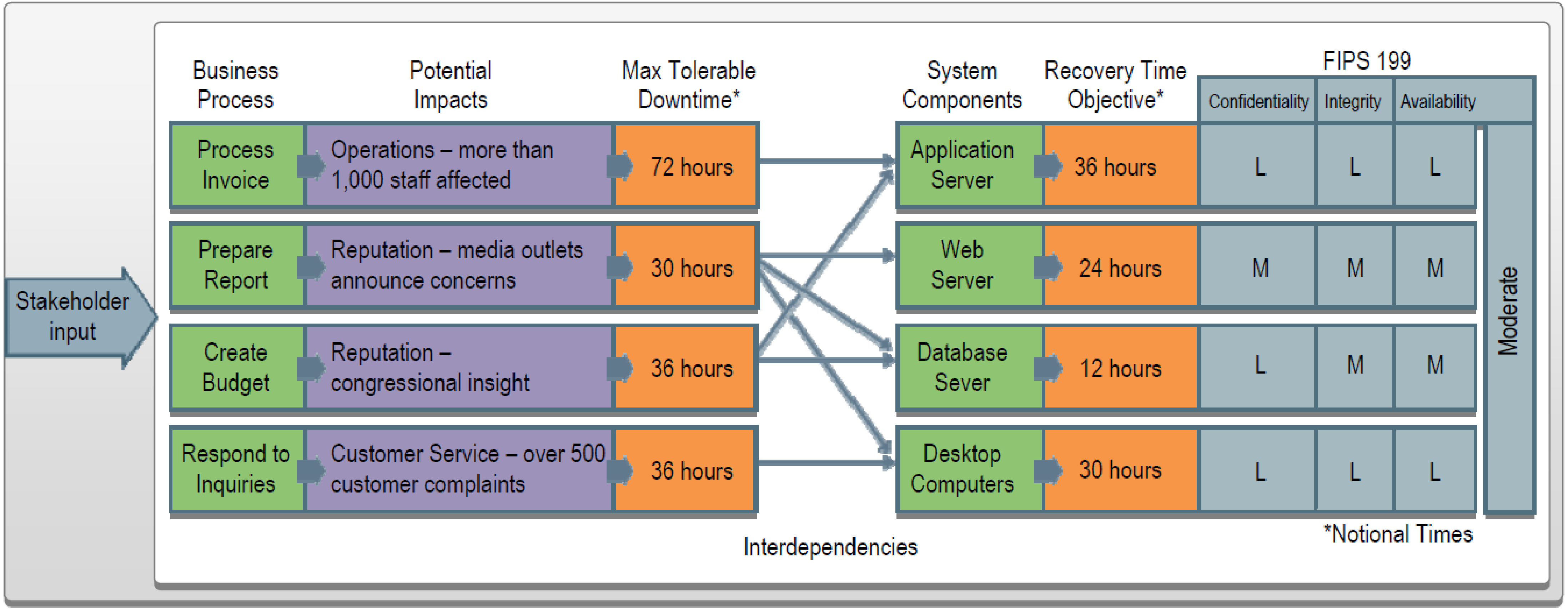
3-Phase Response Plan



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

Business Impact Analysis (BIA)

- Determine Business Processes and Recovery Criticality
- Identify Information and IT Resource Requirements
- Identify Information System Resource Recovery Priorities

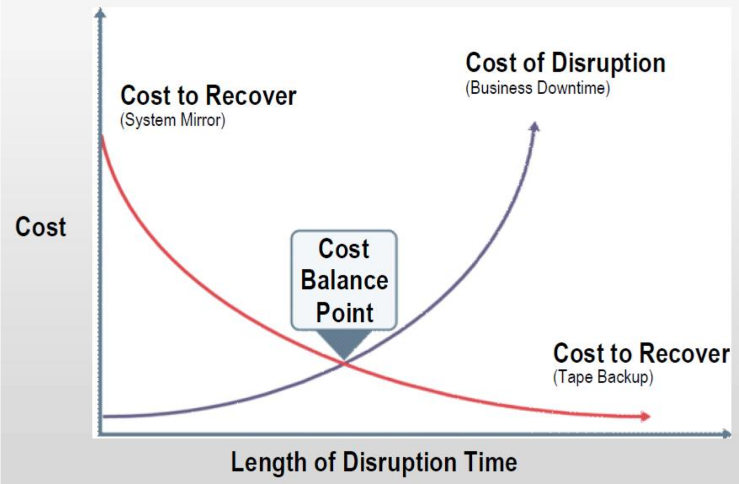


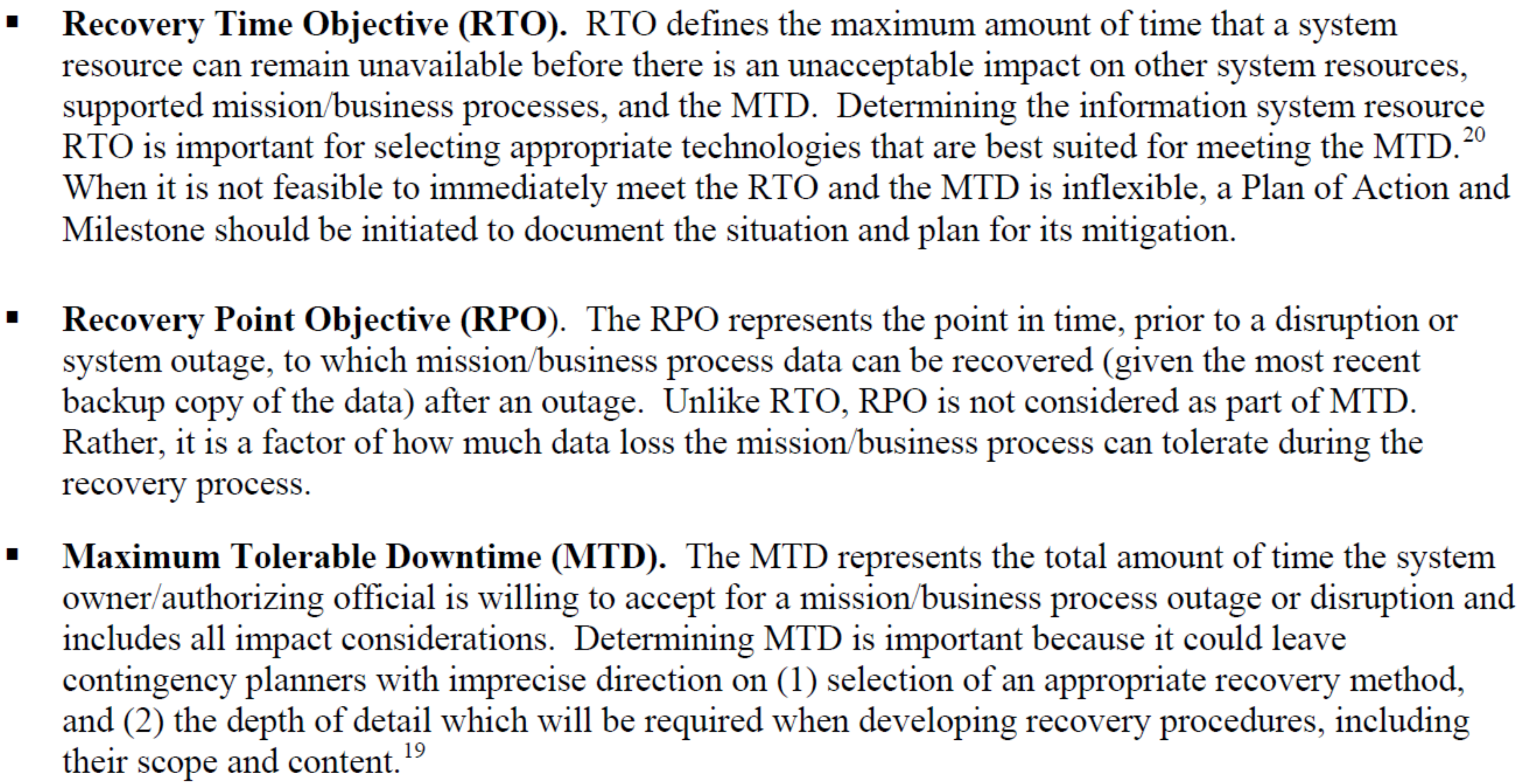
Business Process	Potential Impacts	Max Tolerable Downtime*	System Components	Recovery Time Objective*	FIPS 199		
					Confidentiality	Integrity	Availability
Process Invoice	Operations – more than 1,000 staff affected	72 hours	Application Server	36 hours	L	L	L
Prepare Report	Reputation – media outlets announce concerns	30 hours	Web Server	24 hours	M	M	M
Create Budget	Reputation – congressional insight	36 hours	Database Sever	12 hours	L	M	M
Respond to Inquiries	Customer Service – over 500 customer complaints	36 hours	Desktop Computers	30 hours	L	L	L

*Notional Times

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

Time Dimensions





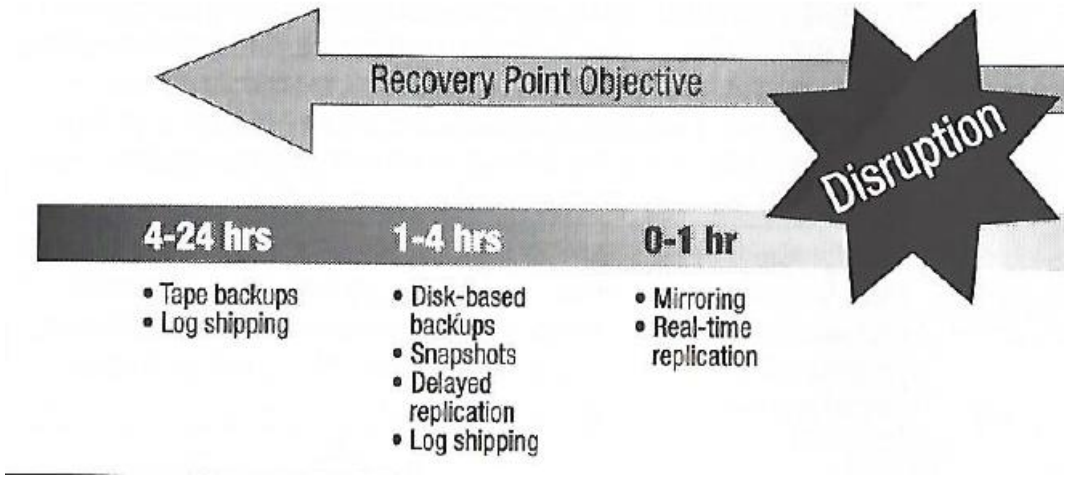
- **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.[20] When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.

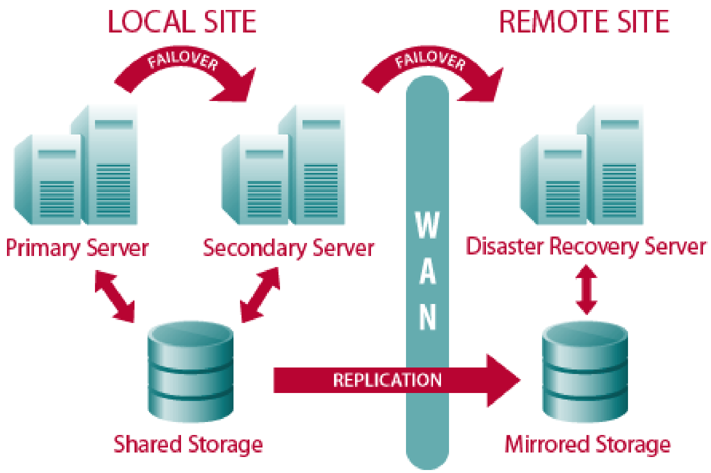
- **Recovery Point Objective (RPO**). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.

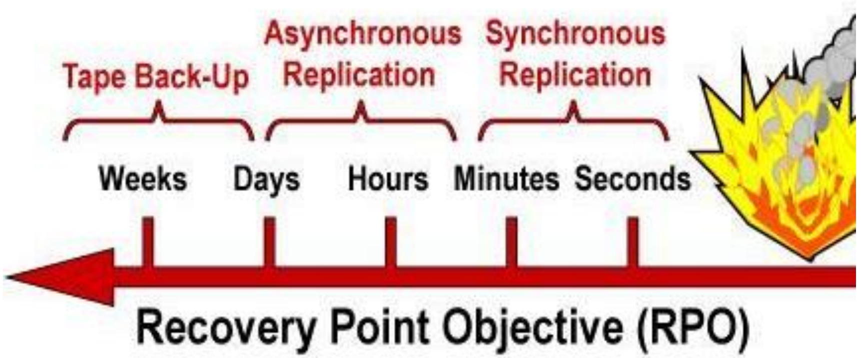
- **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.[19]

Data backup systems and redundancies

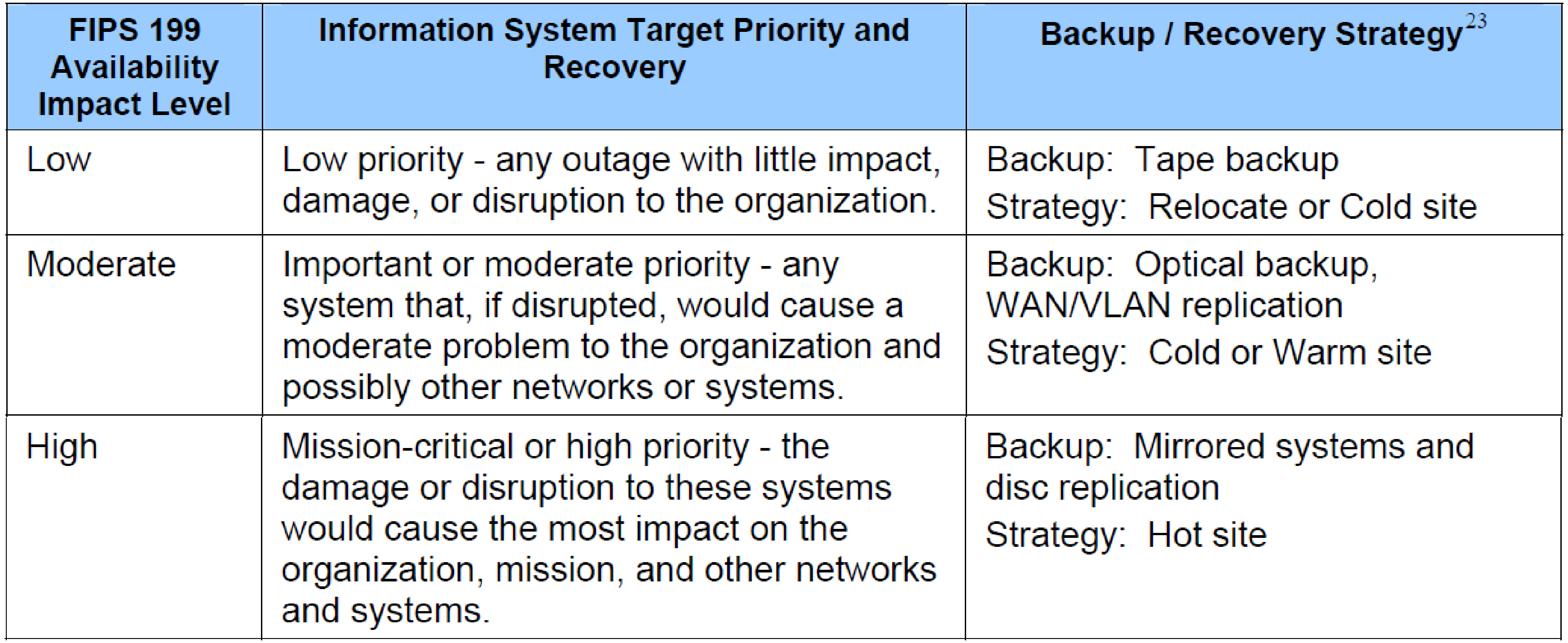
- **Database shadowing**
- **Electronic vaulting**
- **Remote journaling**
- **Storage area network and hierarchical storage management**
- **Shared storage**
- **RAID**
- **Failover clustering**



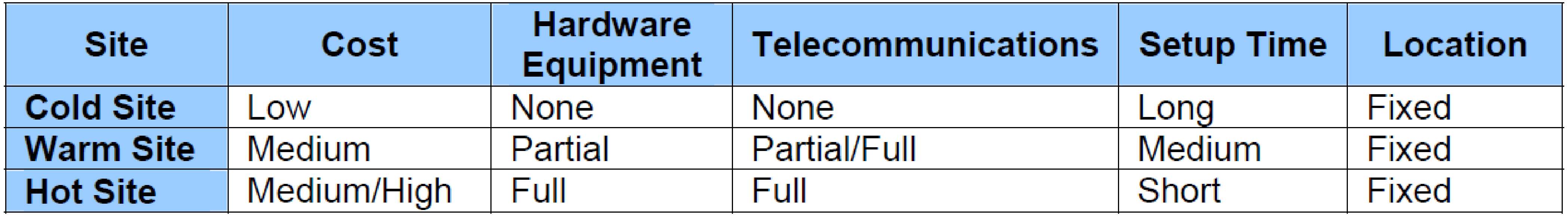




Backup and Recovery Strategies



FIPS 199 Availability Impact Level	Information System Target Priority and Recovery	Backup / Recovery Strategy[23]
Low	Low priority - any outage with little impact, damage, or disruption to the organization.	Backup: Tape backup Strategy: Relocate or Cold site
Moderate	Important or moderate priority - any system that, if disrupted, would cause a moderate problem to the organization and possibly other networks or systems.	Backup: Optical backup, WAN/VLAN replication Strategy: Cold or Warm site
High	Mission-critical or high priority - the damage or disruption to these systems would cause the most impact on the organization, mission, and other networks and systems.	Backup: Mirrored systems and disc replication Strategy: Hot site



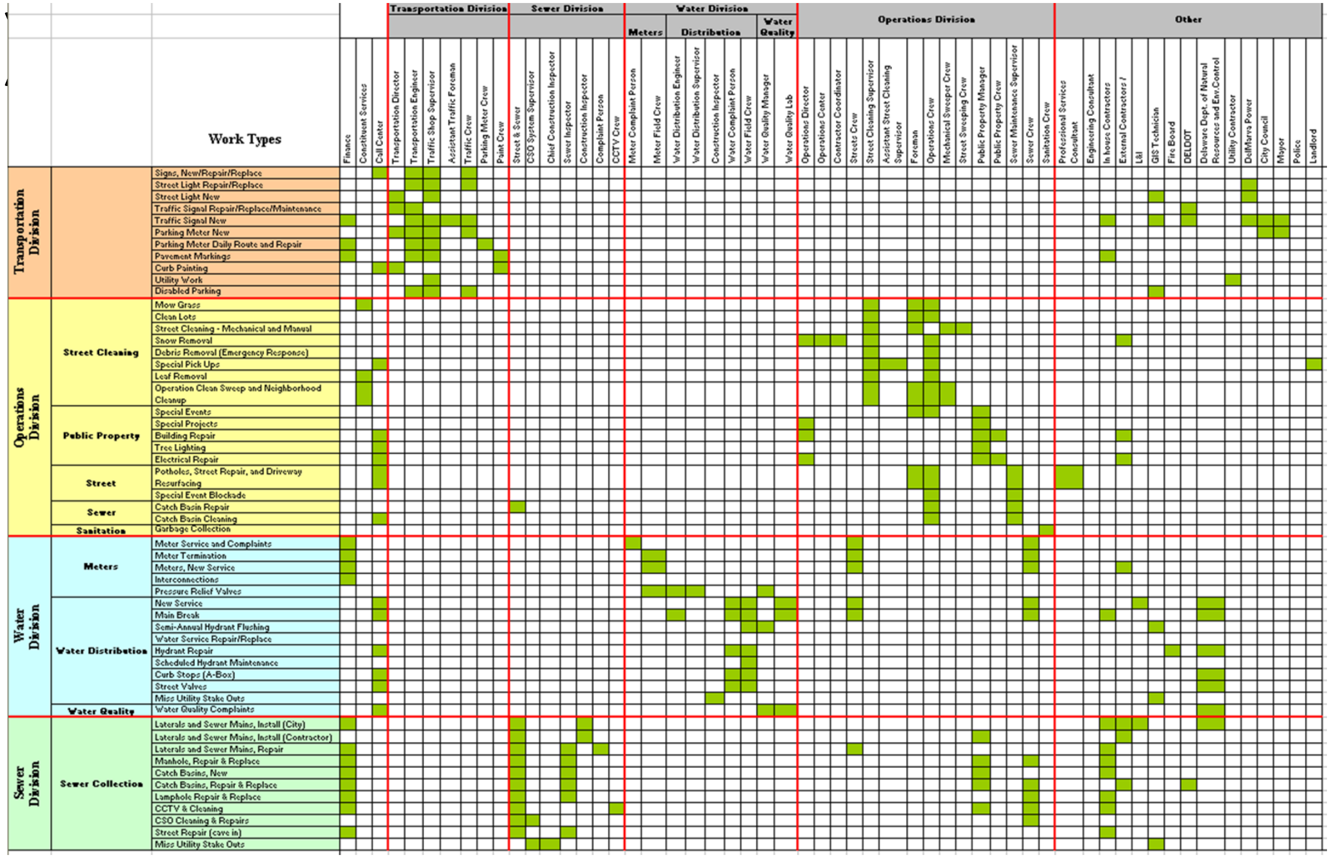
Site	Cost	Hardware Equipment	Telecommunications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/High	Full	Full	Short	Fixed

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

Business process inventory for an information system

Service request and utility maintenance management work order information system for a City's Public Works Department

- 4 Divisions (230 employees)
  - Sewer
  - Water
  - Transportation
  - Operations



Transportation Division | Sewer Division | Water Division: Meters, Distribution, Water Quality | Operations Division | Other

Finance, Constituent Services, Call Center

Transportation Division: Transportation Director, Transportation Engineer, Traffic Shop Supervisor, Assistant Traffic Foreman, Traffic Crew, Parking Meter Crew, Paint Crew

Sewer Division: Street & Sewer, CSO System Supervisor, Chief Construction Inspector, Sewer Inspector, Construction Inspector, Complaint Person, CCTV Crew

Water Division – Meters: Meter Complaint Person, Meter Field Crew

Water Division – Distribution: Water Distribution Engineer, Water Distribution Supervisor, Construction Inspector, Water Complaint Person, Water Field Crew

Water Division – Water Quality: Water Quality Manager, Water Quality Lab

Operations Division: 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

Other: Professional Services Consultant, Engineering Consultant, In house Contractors, External Contractors /, I&I, GIS Technician, Fire Board, DELDOT, Delaware Dept. of Natural Resources and Env.Control, Utility Contractor, DelMarva Power, City Council, Mayor, Police, Landlord

Work Types

Transportation Division: Signs, New/Repair/Replace; Street Light Repair/Replace; Street Light New; Traffic Signal Repair/Replace/Maintenance; Traffic Signal New; Parking Meter New; Parking Meter Daily Route and Repair; Pavement Markings; Curb Painting; Utility Work; Disabled Parking

Operations Division – Street Cleaning: Mow Grass; Clean Lots; Street Cleaning - Mechanical and Manual; Snow Removal; Debris Removal (Emergency Response); Special Pick Ups; Leaf Removal; Operation Clean Sweep and Neighborhood Cleanup

Operations Division – Public Property: Special Events; Special Projects; Building Repair; Tree Lighting; Electrical Repair

Operations Division – Street: Potholes, Street Repair, and Driveway Resurfacing; Special Event Blockade

Operations Division – Sewer: Catch Basin Repair; Catch Basin Cleaning

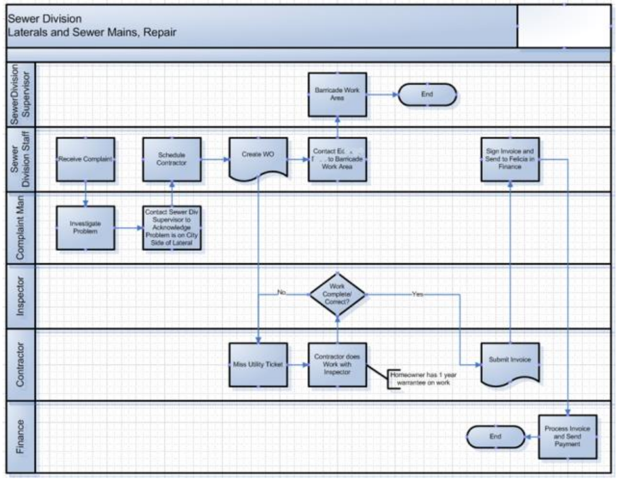
Operations Division – Sanitation: Garbage Collection

Water Division – Meters: Meter Service and Complaints; Meter Termination; Meters, New Service; Interconnections; Pressure Relief Valves

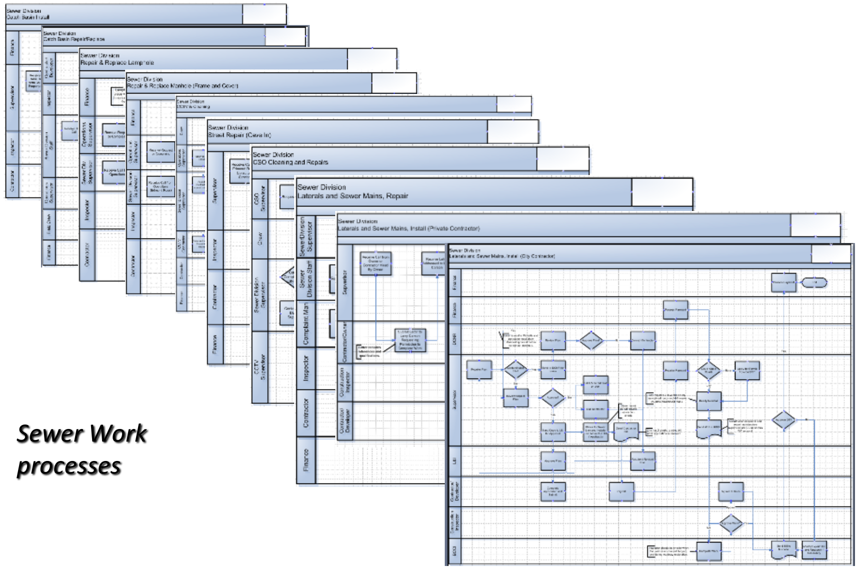
Water Division – Water Distribution: New Service; Main Break; Semi-Annual Hydrant Flushing; Water Service Repair/Replace; Hydrant Repair; Scheduled Hydrant Maintenance; Curb Stops (A-Box); Street Valves; Miss Utility Stake Outs

Water Division – Water Quality: Water Quality Complaints

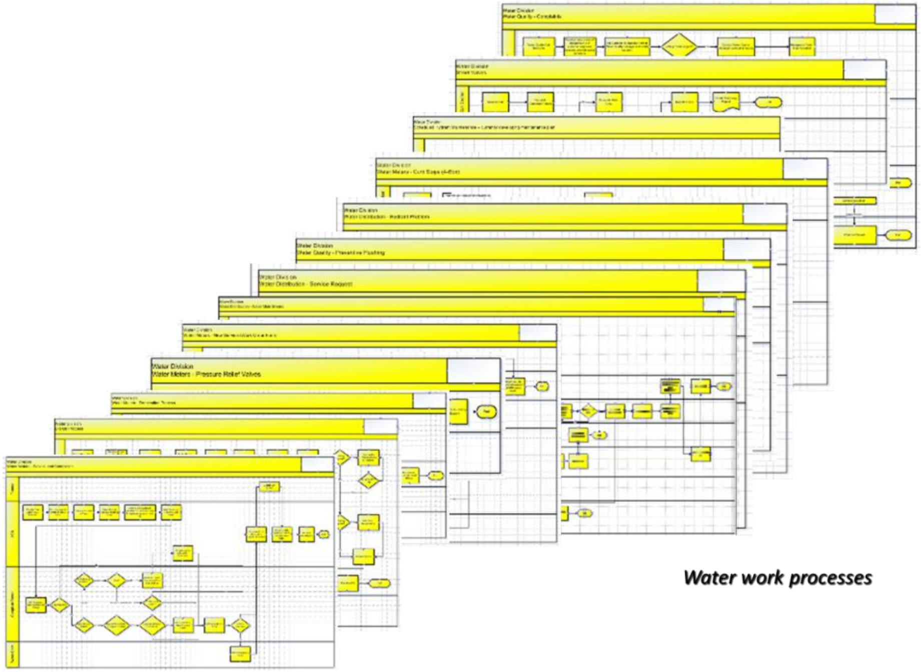
Sewer Division – Sewer Collection: Laterals and Sewer Mains, Install (City); Laterals and Sewer Mains, Install (Contractor); Laterals and Sewer Mains, Repair; Manhole, Repair & Replace; Catch Basins, New; Catch Basins, Repair & Replace; Lamphole Repair & Replace; CCTV & Cleaning; CSO Cleaning & Repairs; Street Repair (cave in); Miss Utility Stake Outs


Sewer Division
Laterals and Sewer Mains, Repair
SewerDivision Supervisor
Sewer Division Staff
Complaint Man
Inspector
Contractor
Finance
Receive Complaint
Schedule Contractor
Create WO
Contact Ed to Barricade Work Area
Barricade Work Area
End
Sign Invoice and Send to Felicia in Finance
Investigate Problem
Contact Sewer Div Supervisor to Acknowledge Problem is on City Side of Lateral
No
Work Complete/ Correct?
Yes
Miss Utility Ticket
Contractor does Work with Inspector
Homeowner has 1 year warrantee on work
Submit Invoice
End
Process Invoice and Send Payment

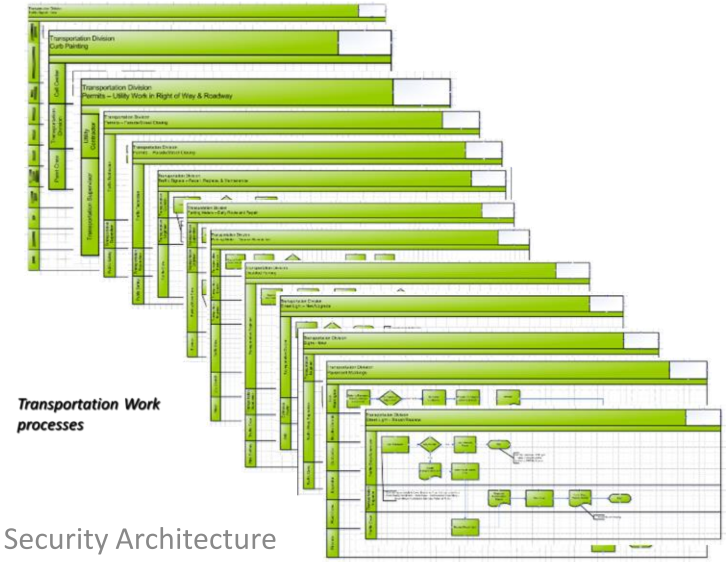
Business processes – modeled as swim lanes


Sewer Division
CSO Cleaning and Repairs
Sewer Division
Laterals and Sewer Mains, Repair
Sewer Division
Laterals and Sewer Mains, Install (Private Contractor)

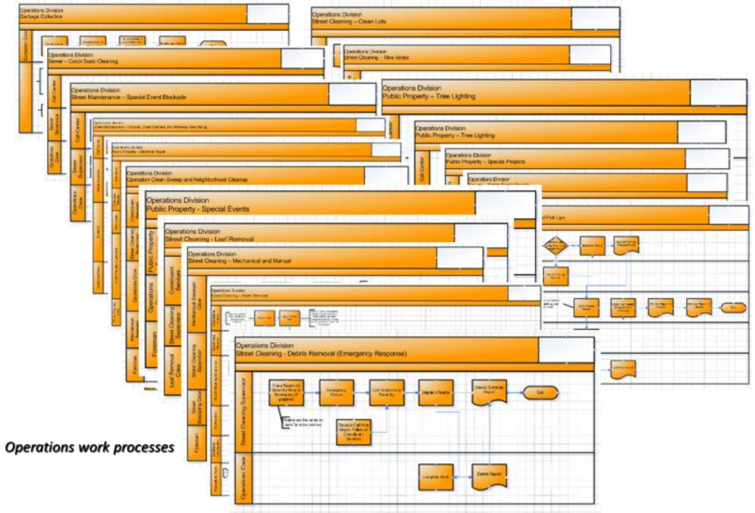
Sewer Work processes



Water work processes

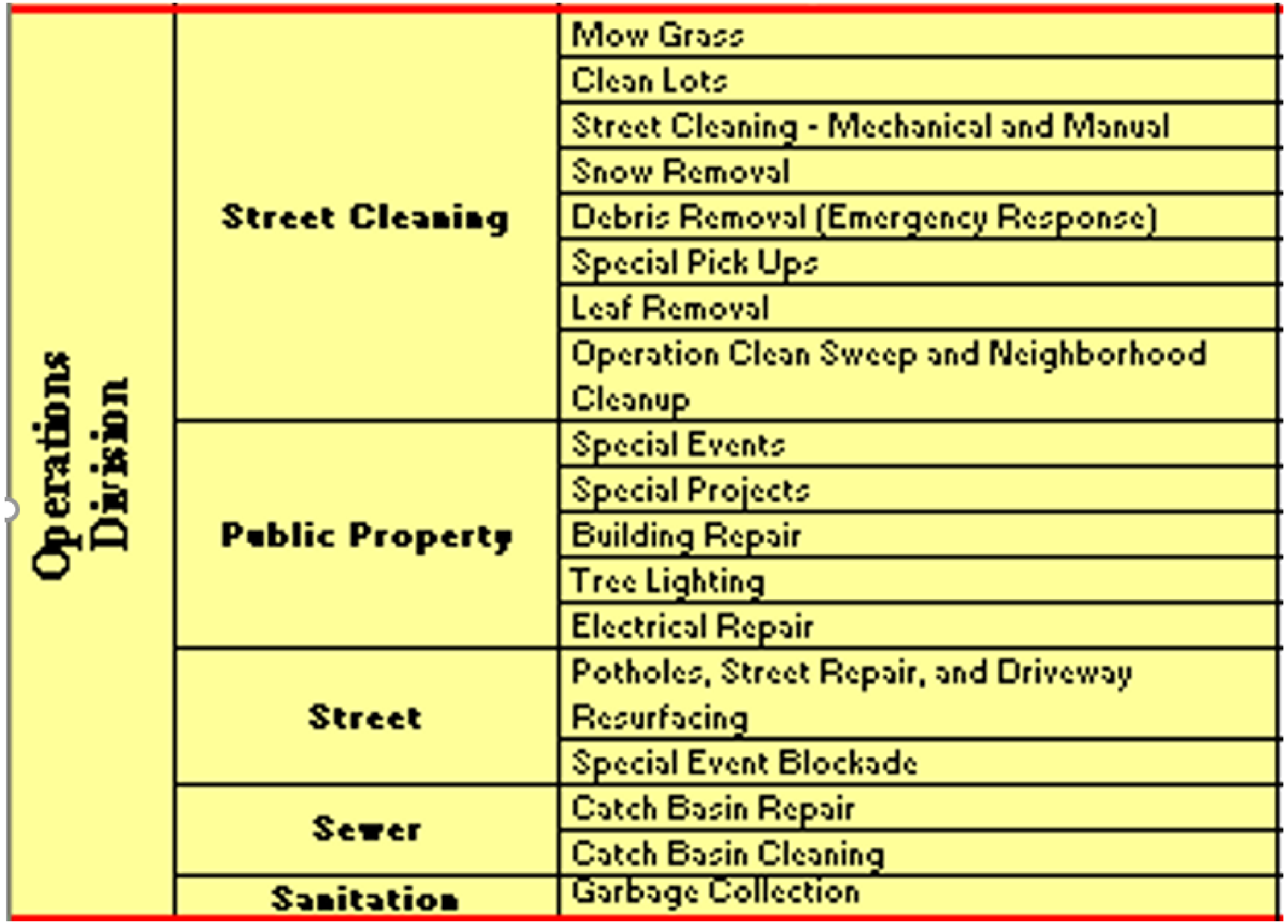


Transportation Work processes


Operations Division
Public Property – Tree Lighting
Operations Division
Public Property - Special Events
Operations Division
Street Cleaning - Leaf Removal
Operations Division
Street Cleaning - Debris Removal (Emergency Response)

Operations work processes

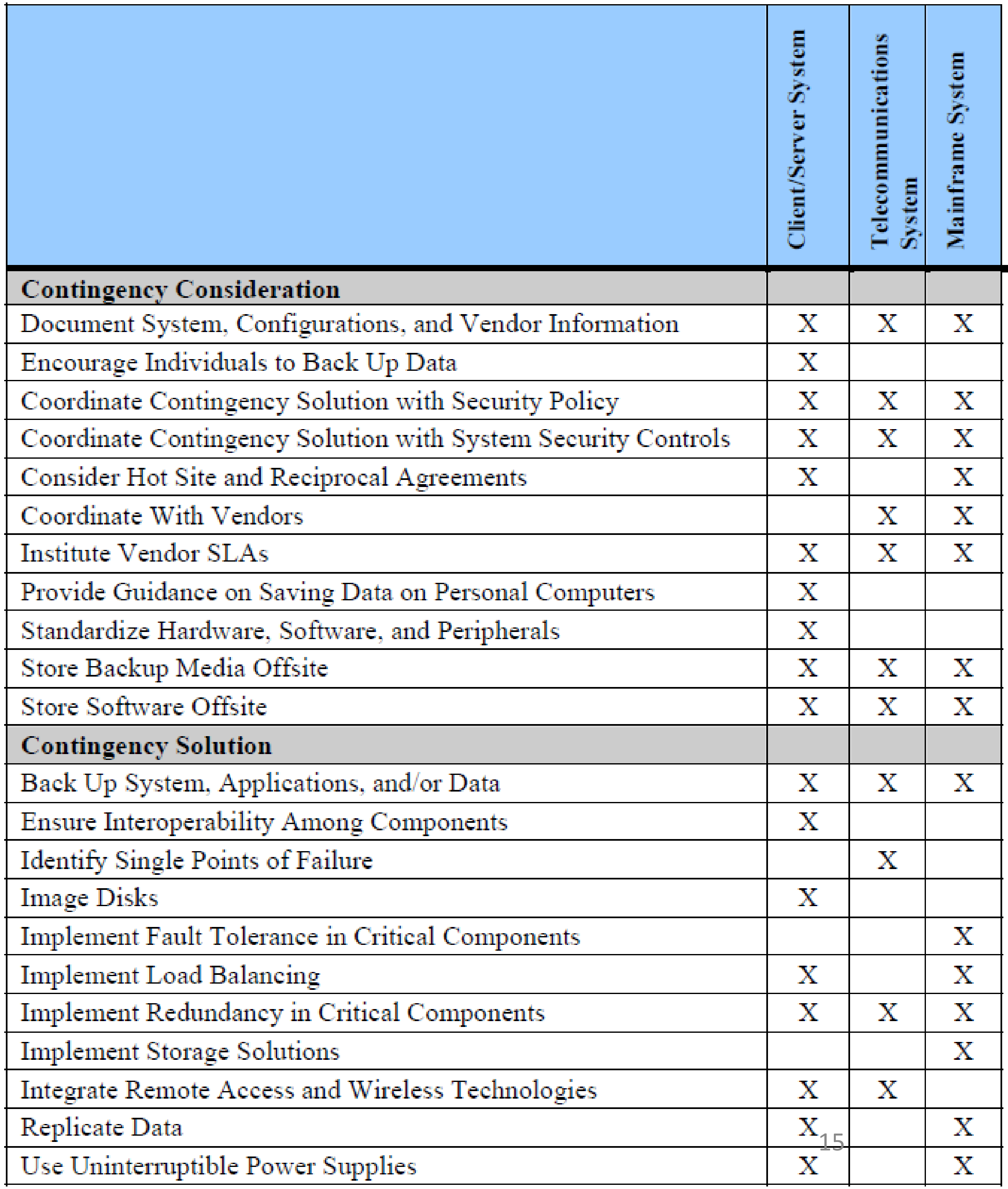
How would you recommend the City prioritize the following business processes for recovery?



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

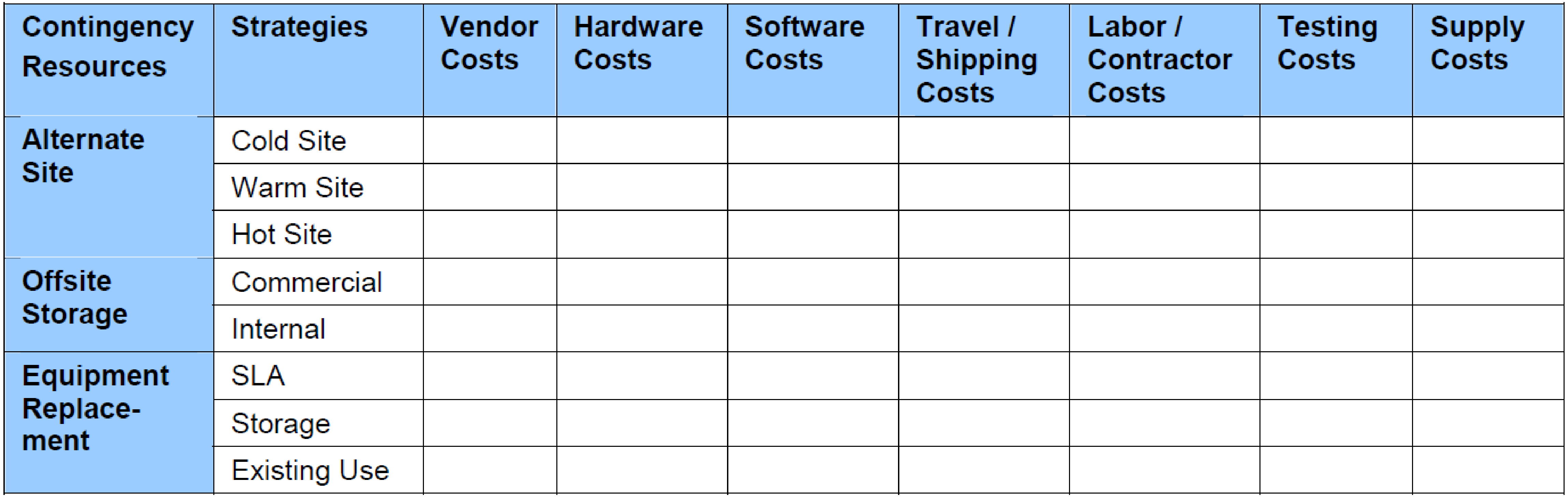
NIST SP 800-34 R1 – Contingency Planning Guide for Federal Information Systems

Contingency Planning Considerations & Solutions



	Client/Server System	Telecommunications System	Mainframe System
Contingency Consideration			
Document System, Configurations, and Vendor Information	X	X	X
Encourage Individuals to Back Up Data	X		
Coordinate Contingency Solution with Security Policy	X	X	X
Coordinate Contingency Solution with System Security Controls	X	X	X
Consider Hot Site and Reciprocal Agreements	X		X
Coordinate With Vendors		X	X
Institute Vendor SLAs	X	X	X
Provide Guidance on Saving Data on Personal Computers	X		
Standardize Hardware, Software, and Peripherals	X		
Store Backup Media Offsite	X	X	X
Store Software Offsite	X	X	X
Contingency Solution			
Back Up System, Applications, and/or Data	X	X	X
Ensure Interoperability Among Components	X		
Identify Single Points of Failure		X	
Image Disks	X		
Implement Fault Tolerance in Critical Components			X
Implement Load Balancing	X		X
Implement Redundancy in Critical Components	X	X	X
Implement Storage Solutions			X
Integrate Remote Access and Wireless Technologies	X	X	
Replicate Data	X		X
Use Uninterruptible Power Supplies	X		X

Considerations - Budget



Contingency Resources	Strategies	Vendor Costs	Hardware Costs	Software Costs	Travel / Shipping Costs	Labor / Contractor Costs	Testing Costs	Supply Costs
Alternate Site	Cold Site							
	Warm Site							
	Hot Site							
Offsite Storage	Commercial							
	Internal							
Equipment Replace-ment	SLA							
	Storage							
	Existing Use							

Contingency Plan

For High, Moderate and Low templates see:
NIST SP 800-34 R1
Contingency Planning Guide
for Federal Information Systems

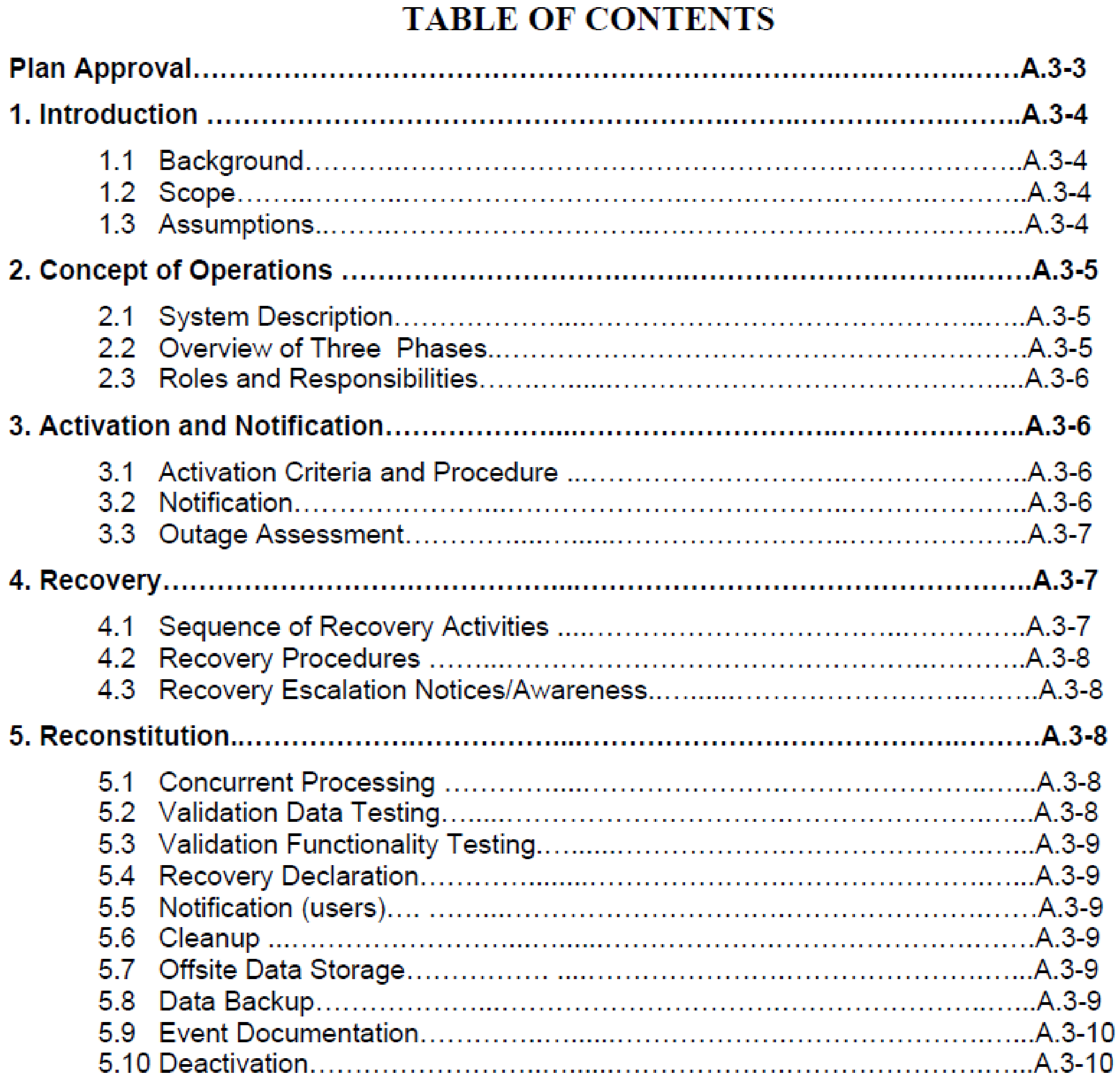
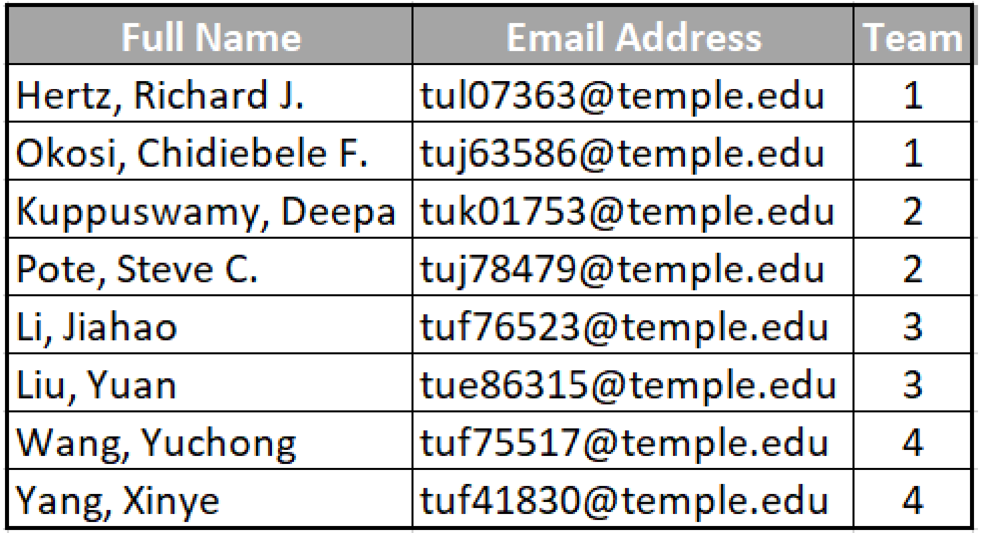


TABLE OF CONTENTS

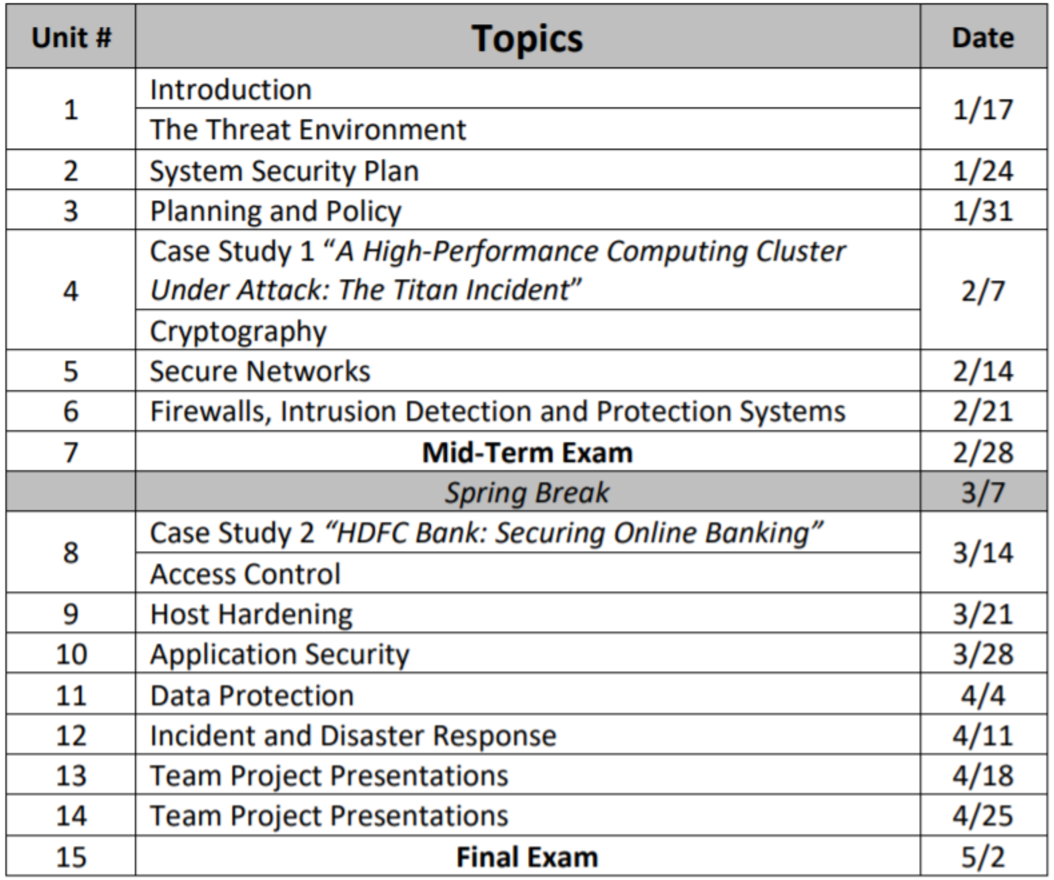
Agenda

- ✓In The News exercise
- ✓Incident & Disaster Response Planning
- Team Project Schedule
- Final Exam
- Student Feedback Form (eSFF)
- SSP discussion

Team Project Schedule



Full Name	Email Address	Team
Hertz, Richard J.	tul07363@temple.edu	1
Okosi, Chidiebele F.	tuj63586@temple.edu	1
Kuppuswamy, Deepa	tuk01753@temple.edu	2
Pote, Steve C.	tuj78479@temple.edu	2
Li, Jiahao	tuf76523@temple.edu	3
Liu, Yuan	tue86315@temple.edu	3
Wang, Yuchong	tuf75517@temple.edu	4
Yang, Xinye	tuf41830@temple.edu	4



Unit #	Topics	Date
1	Introduction	1/17
	The Threat Environment	
2	System Security Plan	1/24
3	Planning and Policy	1/31
4	Case Study 1 *"A High-Performance Computing Cluster Under Attack: The Titan Incident"*	2/7
	Cryptography	
5	Secure Networks	2/14
6	Firewalls, Intrusion Detection and Protection Systems	2/21
7	**Mid-Term Exam**	2/28
	Spring Break	3/7
8	Case Study 2 *"HDFC Bank: Securing Online Banking"*	3/14
	Access Control	
9	Host Hardening	3/21
10	Application Security	3/28
11	Data Protection	4/4
12	Incident and Disaster Response	4/11
13	Team Project Presentations	4/18
14	Team Project Presentations	4/25
15	**Final Exam**	5/2

Final Exam

Monday May 2, 9:00 AM – 11:30 AM

- Taken in class
- Using Canvas
- Closed book
- 50 multiple-choice CISA/CISSP style questions

Agenda

- ✓In The News exercise
- ✓Incident & Disaster Response Planning
- ✓Team Project Schedule
- ✓Final Exam
- ✓Student Feedback Form (eSFF)
- ✓SSP discussion