CS4050 – WEEK 12: INFORMATION SYSTEMS AUDIT AND CONTROL

FAST NUCES – SPRING 2024

BS COMPUTER SCIENCE

CHAPTER 4: INFORMATION SYSTEMS OPERATIONS & BUSINESS RESILIENCE

- Part A: Information Systems Operations
  - Common Technology Components
  - IT Asset Management
  - Job Scheduling & Production Process Automation
  - System Interfaces
  - End-User Computing
  - Data Governance
  - Systems Performance Management
  - Problem & Incident Management
  - Change, Configuration, Release and Patch Management
  - IT Service Level Management.
  - Database Management

- Part B: Business Resilience
  - Business Impact Analysis
  - System Resiliency
  - Data Backup, Storage and Restoration
  - Business Continuity Plan
  - Disaster Recovery Plans

CHANGE, CONFIGURATION, RELEASE & PATCH MANAGEMENT

Change Management: It is used when changing hardware, installing or upgrading to new releases of off-the-shelf applications, installing a software patch and configuring various network devices (e.g., firewalls, routers and switches).

- All relevant personnel are informed of the change and when it is happening.
- System, operations & program documentation are complete, up to date and in compliance with the established standards.
- Job preparation, scheduling and operating instructions have been established.
- System and program test results have been reviewed and approved by user and project management.
- Data file conversion, if necessary, has occurred accurately & completely as evidenced by review, approval by user management.
- System conversion has occurred accurately and completely as evidenced by review and approval by user management.
- All aspects of jobs turned over have been tested, reviewed and approved by control/operations personnel.
- Legal or compliance aspects have been considered.
- The risk of adversely affecting the business operation are reviewed and a rollback plan is developed.

CHANGE, CONFIGURATION, RELEASE & PATCH MANAGEMENT

Patch Management: It is an area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system to maintain up-to-date software and often to address security risk.

- Maintain current knowledge of available patches.
- Decide what patches are appropriate for particular systems.
- Ensure that patches are installed properly; testing systems after installation.
- Document all associated procedures, such as specific configurations required.

CHANGE, CONFIGURATION, RELEASE & PATCH MANAGEMENT

Release Management: The term release is used to describe a collection of authorized changes. The release will typically consist of several problem fixes and enhancements to the service.

Major Releases

- Normally contain a significant change or addition of new functionality
- Grouping together several changes facilitates more comprehensive testing and planned user training. Minor Software Releases

Minor Releases

- Upgrades, normally containing small enhancements and fixes.
- Minor releases are generally used to fix small reliability or functionality problems that cannot wait until the next major release.

Emergency Software Releases

- Emergency releases are fixes that require implementation as quickly as possible to prevent significant user downtime to business-critical functions.
- Such changes should be avoided whenever possible because they increase the risk of errors being introduced.

IT SERVICE LEVEL MANAGEMENT

- Concept of ITSM is that IT can be managed through a series of discrete processes that provide service to the business.
- The processes, after defined, can be better managed through SLAs that serve to maintain and improve customer satisfaction (i.e., with the end business).
- Key elements to define effective ITSM are:
   i. Service Level Agreements: Exception Reports, System and Application Logs, Operator Problem Reports, Operator Work Schedules)
   ii. Monitoring of Service Levels
   iii. Service Levels and Enterprise Architecture

DATABASE MANAGEMENT

- DBMS software aids in organizing, controlling and using the data needed by application programs.
- A DBMS provides the facility to create and maintain a well-organized database.
- Primary functions include reduced data redundancy, decreased access time and basic security over sensitive data.
- Four key concepts to understand for effective DB management are:
  - DBMS Architecture
  - Database Structure
  - Database Controls
  - Database Reviews

APPLICATION SYSTEM TESTING – ASSIGNMENT # 2

- Review the table 3.20 in the CISA Review Manual, highlighting different ways to test application systems. Answer the following:

Q1: Which testing model is the best to ensure the data processing is performed correctly.

Q2: Which testing model you will use to test the flow of data in procurement application, processing the Purchase Orders, Invoices and Payments?

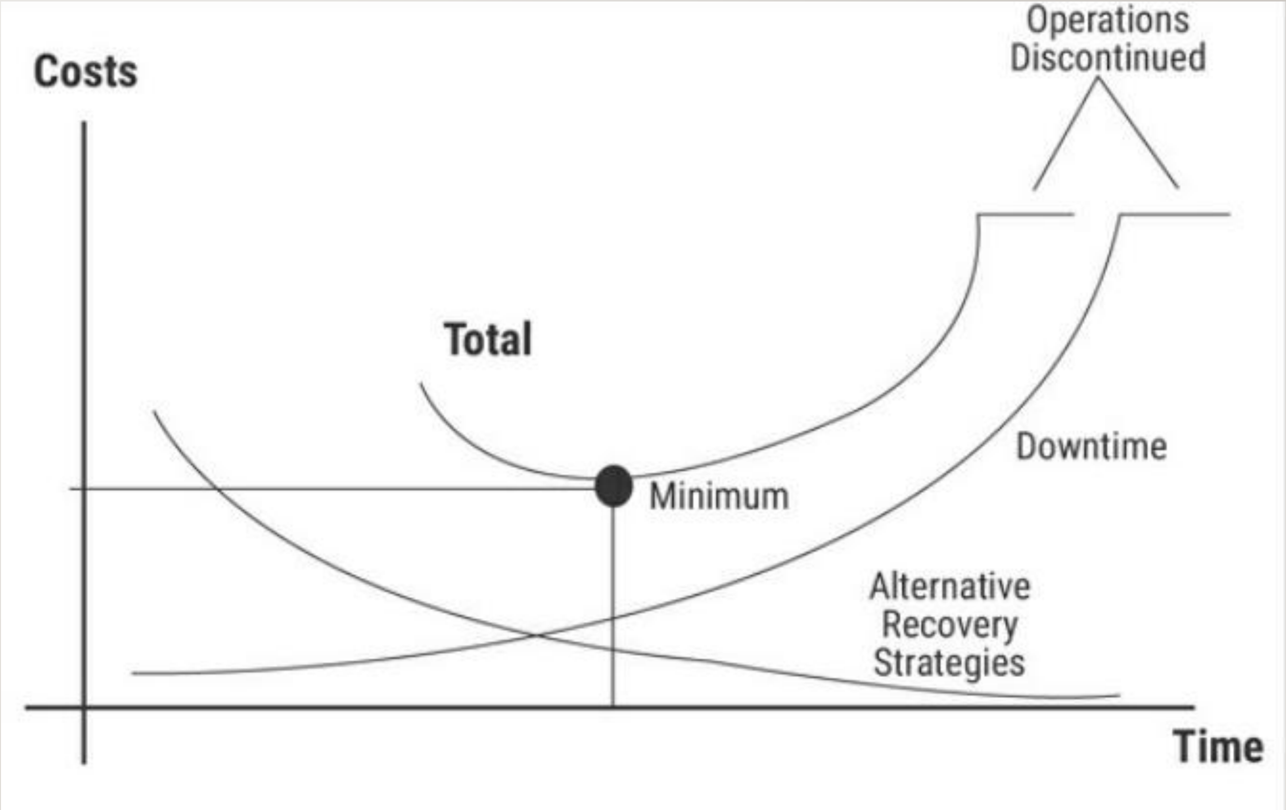
Q3: You are auditing the application to verify that fuel pump is recording the volume of oil correctly. Which testing model you will use for this purpose and why?

PART B: BUSINESS RESILIENCE

- Business Impact Analysis
- System Resiliency
- Data Backup, Storage and Restoration
- Business Continuity Plan
- Disaster Recovery Plans

BUSINESS IMPACT ANALYSIS

- BIA is used to evaluate the critical processes (and IT components supporting them) and to determine time frames, priorities, resources and interdependencies.
- To perform BIA successfully, one should obtain an understanding of the organization, key business processes and IT resources to support the key business processes.
- Post BIA - identify the various recovery strategies and available alternatives for recovering from an interruption and/or disaster.



Analysis - Disruption Cost Vs. Recovery Cost

SYSTEM RESILIENCY

- It is the ability of a system to withstand a major disruption within set metrics and recovery times. This can include the ability to maintain capability during the disruption
- Application Resiliency And Disaster Recovery Methods – Clustering, higher availability
- Telecommunication Networks Resiliency and Disaster Recovery Methods – Redundancy, alternative routing, diverse routing, long-haul network diversity, last-mile circuit protection, voice recovery

DATA BACKUP, STORAGE AND RESTORATION

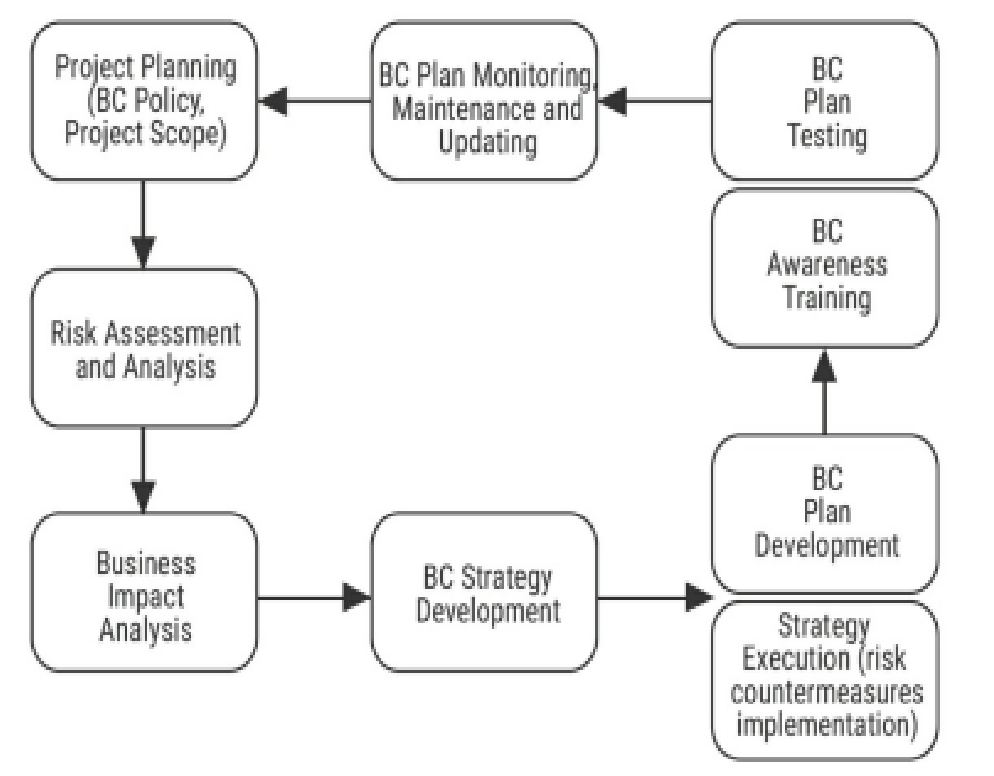
- Data Storage Resiliency and Disaster Recovery Methods
- Backup And Restoration
  - Recovery Point Objective (RPO): It is the maximum amount of data that the organization can tolerate losing
  - Recovery Time Objective (RTO): It is the maximum amount of time that should pass after an outage or data loss for operations to return to normal
- Backup Schemes: Full, incremental and differential

BUSINESS CONTINUITY PLAN (BCP)

- The purpose of business continuity/disaster recovery (DR) is to enable a business to continue offering critical services in the event of a disruption and to survive a disastrous interruption to activities. Rigorous planning and commitment of resources is necessary to adequately plan for such an event.
- BCP takes into consideration:
    - Those critical operations that are necessary to the survival of the organization
    - The human/material resources supporting them
- The BCP includes:
    - The DRP that is used to recover a facility rendered inoperable, including relocating operations into a new location
    - The restoration plan that is used to return operations to normality whether in a restored or new facility

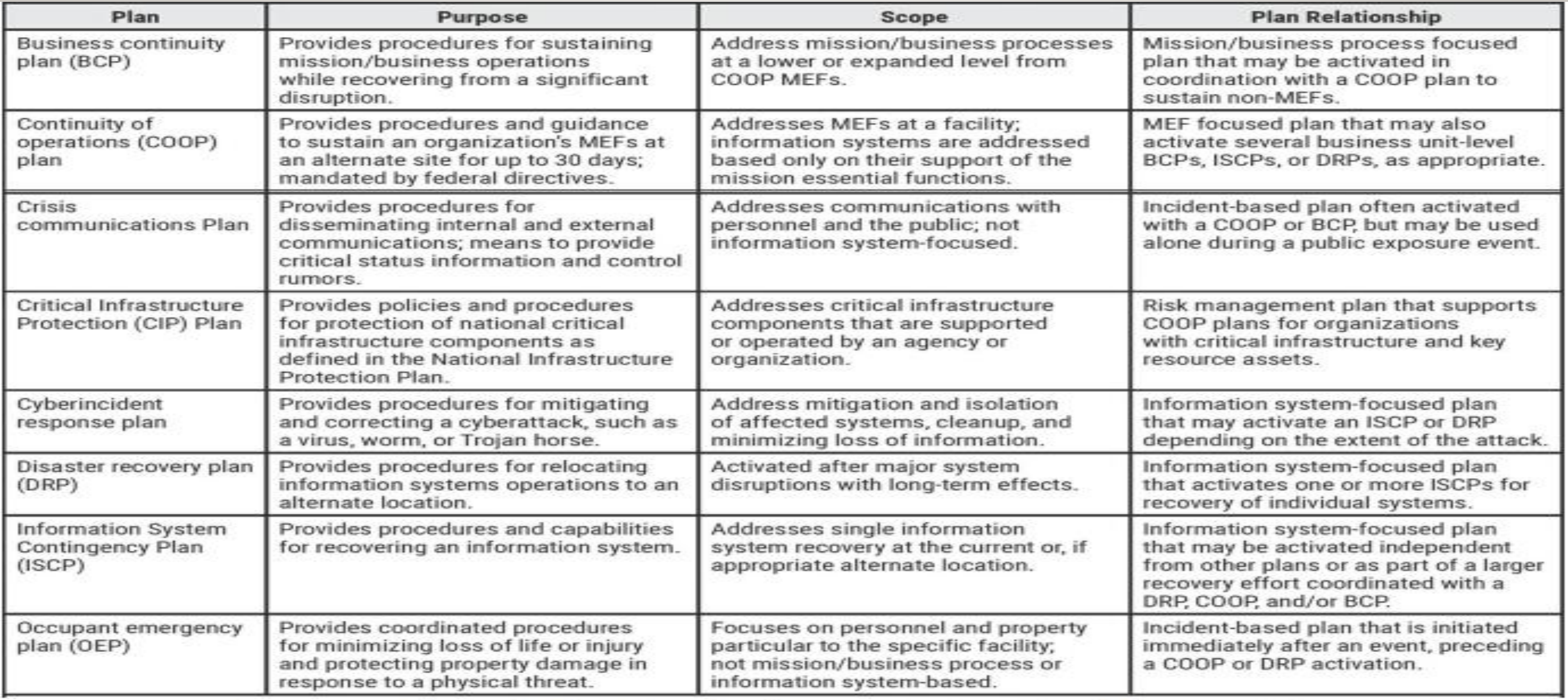
BUSINESS CONTINUITY PLAN (BCP)

- IT Business Continuity Planning
- A BCP identifies what the business will do in the event of a disaster. For example;
  - *where will employees report to work,*
  - *how will orders be taken while the computer system is being restored,*
  - *which vendors should be called to provide needed supplies*
- A subcomponent of the BCP is the IT DRP
- Disasters and Other Disruptive Events


Project Planning (BC Policy, Project Scope)
BC Plan Monitoring, Maintenance and Updating
BC Plan Testing
BC Awareness Training
Risk Assessment and Analysis
BC Plan Development
Business Impact Analysis
BC Strategy Development
Strategy Execution (risk countermeasures implementation)

Business Continuity Planning Life Cycle

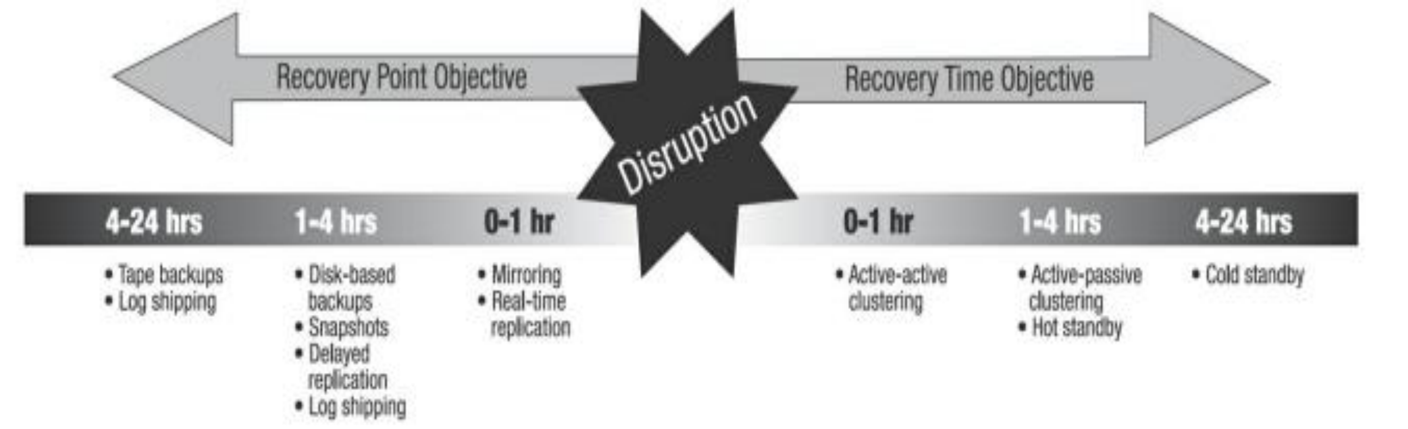
COMPONENTS OF BUSINESS CONTINUITY PLAN (BCP)



Plan	Purpose	Scope	Plan Relationship
Business continuity plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Address mission/business processes at a lower or expanded level from COOP MEFs.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs.
Continuity of operations (COOP) plan	Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives.	Addresses MEFs at a facility; information systems are addressed based only on their support of the mission essential functions.	MEF focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate.
Crisis communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system-focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components as defined in the National Infrastructure Protection Plan.	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
Cyberincident response plan	Provides procedures for mitigating and correcting a cyberattack, such as a virus, worm, or Trojan horse.	Address mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP depending on the extent of the attack.
Disaster recovery plan (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	Information system-focused plan that activates one or more ISCPs for recovery of individual systems.
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
Occupant emergency plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

DISASTER RECOVERY PLAN (DRP)

- Defining RPO and RTO
- Recovery Alternatives: cold, hot, warm sites, mobile site, mirrored site, reciprocal agreement
- Developing Disaster Recovery Plans
- DRP and BCP Testing Methods
- Invoking Disaster Recovery Test Plans


Recovery Point Objective
Disruption
Recovery Time Objective
4-24 hrs
• Tape backups
• Log shipping
1-4 hrs
• Disk-based backups
• Snapshots
• Delayed replication
• Log shipping
0-1 hr
• Mirroring
• Real-time replication
0-1 hr
• Active-active clustering
1-4 hrs
• Active-passive clustering
• Hot standby
4-24 hrs
• Cold standby