CISSP® Common Body of Knowledge: Business Continuity & Disaster Recovery Planning Domain

Version: 5.9.2

Learning Objective

Business Continuity and Disaster Recover Planning ...(1/3)

The Business Continuity and Disaster Recovery Planning domain addresses the preservation of the business in the face of major disruptions to normal business operations. BCP and DRP involve the preparation, testing and updating of specific actions to protect critical business processes from the effect of major system and network failures.

Business Continuity Planning (BCP) helps to identify the organization’s exposure to internal and external threats; synthesize hard and soft assets to provide effective prevention and recovery for the organization, and maintains competitive advantage and value system integrity. BCP counteracts interruptions to business activities and should be available to protect critical business processes from the effects of major failures or disasters. It deals with the natural and man-made events and the consequences, if not dealt with promptly and effectively.

...

Reference: *CISSP CIB*, January 2012 (Rev. 5)

Learning Objective

Business Continuity and Disaster Recover Planning ...(2/3)

...

Business Impact Analysis (BIA) determines the proportion of impact an individual business unit would sustain subsequent to a significant interruption of computing or telecommunication services. These impacts may be financial, in terms of monetary loss, or operational, in terms of inability to deliver.

Disaster Recovery Plans (DRP) contains procedures for emergency response, extended backup operation and post-disaster recovery, should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objective of the disaster recovery plan is to provide the capability to process mission-essential applications, in a degraded mode, and return to normal mode of operation within a reasonable amount of time.

...

Reference: *CISSP CIB*, January 2012 (Rev. 5)

Learning Objective

Business Continuity and Disaster Recover Planning ...(3/3)

...

The candidate is expected to know the difference between business continuity planning and disaster recovery; business continuity planning in terms of project scope and planning, business impact analysis, recovery strategies, recovery plan development, and implementation. Moreover, the candidate should understand disaster recovery in terms of recovery plan development, implementation and restoration.

Reference: *CISSP CIB*, January 2012 (Rev. 5)

Topics

Business Continuity Planning (BCP) Domain

➡ Terms & Definition
- Phase I: Project Management and Initiation
- Phase II: Business Impact Analysis (BIA)
- Phase III: Recovery Strategy
- Phase IV: Plan Design & Development
- Phase V: Implementation
- Phase VI: Testing
- Phase VII: Maintenance, Awareness, and Training

Business Continuity Planning (BCP)

- Business continuity planning (BCP) addresses the preservation and recovery of business in the event of outages to normal business operations.
- Business continuity plan is an approved set of arrangements and procedures that enables an organization to:
  - Facilitate the recovery of business operations
  - Minimize loss
  - Repair or replace the damaged facilities or components as soon as possible.
- Business (/mission) impact analysis (BIA) is the process of determining impacts of an IT service disruption to business operations in terms of financial loss. BIA is a part of BCP.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP$^{®}$ Exam*

Terms & Definition

Business Continuity Planning (BCP)

- Continuity of operations plan (COOP) focuses on restoring an organization's essential business functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. It is a part of BCP.
- Business resumption planning (BRP) (or Business Recovery Planning) addresses the restoration of business processes after an emergency. It is often a part of BCP.
- Crisis communications plan is a plan for both internal and public communications in a crisis event. It is often a part of BCP.
  - Internal for coordination of organizational resources.
  - External to ensure that only approved statements are released to the public.

Reference: NIST SP 800-34, *Contingency Planning Guide for IT Systems*

IT Contingency Planning

- Cyber incident response plan is a specific BCP that establishes procedures to address cyber attacks against an organization’s IT system(s).
- Disaster recovery planning (DRP) addresses the recovery of a damaged facility or components back to normal business operations.
- Disaster recovery plan is a set of procedures that enables an organization to:
  - Respond to disaster in accordance to a pre-defined disaster level.
  - Assess damage & estimate time required to resume operations.
  - Perform salvage & repair.

Reference: NIST SP 800-34, *Contingency Planning Guide for IT Systems*

Terms & Definition

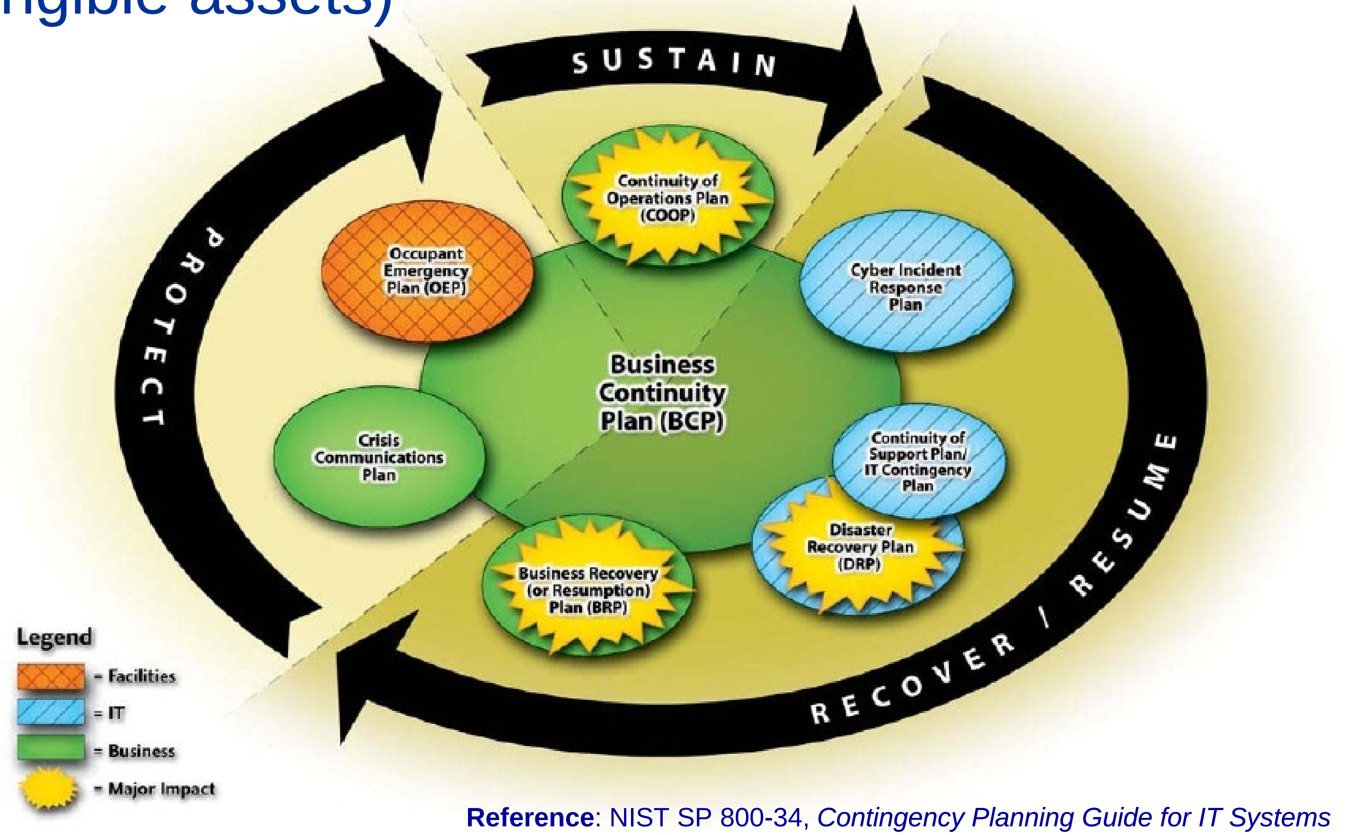
Facility Contingency Planning

- Occupant emergency plan (OEP) provides the response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property.

Reference: NIST SP 800-34, *Contingency Planning Guide for IT Systems*

Life Cycle of Business Continuity

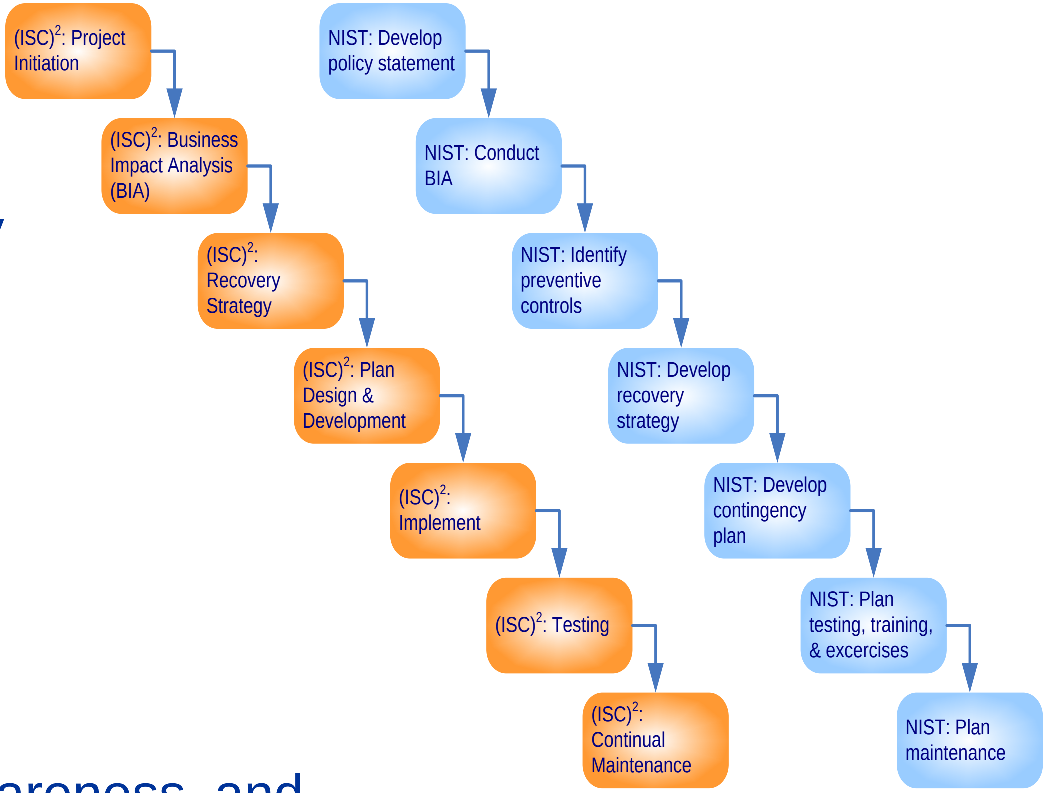
- Sustain business operations
- Recover / resume business operations
- Protect business assets (People, reputation, and tangible assets)


SUSTAIN
PROTECT
RECOVER / RESUME
Continuity of Operations Plan (COOP)
Occupant Emergency Plan (OEP)
Cyber Incident Response Plan
Business Continuity Plan (BCP)
Crisis Communications Plan
Continuity of Support Plan/ IT Contingency Plan
Disaster Recovery Plan (DRP)
Business Recovery (or Resumption) Plan (BRP)
Legend
= Facilities
= IT
= Business
= Major Impact

Reference: NIST SP 800-34, *Contingency Planning Guide for IT Systems*

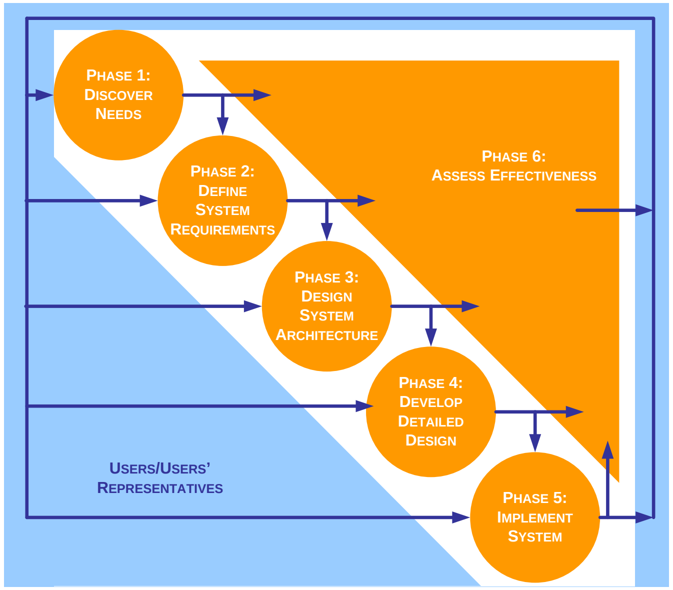
Process for Creating a BCP

- Phase I: Project Initiation
- Phase II: Business Impact Analysis (BIA)
- Phase III: Recovery Strategy
- Phase IV: Plan Design & Development
- Phase V: Implementation
- Phase VI: Testing
- Phase VII: Maintenance, Awareness, and Training


(ISC)^2: Project Initiation
(ISC)^2: Business Impact Analysis (BIA)
(ISC)^2: Recovery Strategy
(ISC)^2: Plan Design & Development
(ISC)^2: Implement
(ISC)^2: Testing
(ISC)^2: Continual Maintenance
NIST: Develop policy statement
NIST: Conduct BIA
NIST: Identify preventive controls
NIST: Develop recovery strategy
NIST: Develop contingency plan
NIST: Plan testing, training, & excercises
NIST: Plan maintenance

Systems Engineering Approach for Creating a BCP

- Understand the BCP needs
  - Phase I: Project Initiation
- Define the BCP requirements
  - Phase II: Business Impact Analysis
- Design the BCP
  - Phase III: Recovery Strategy
- Develop the BCP
  - Phase IV: Plan Design & Development
- Implement BCP
  - Phase V: Implement
- Support BCP
  - Phase VII: Maintenance
- Assess BCP effectiveness
  - Phase VI: Testing


PHASE 1: DISCOVER NEEDS
PHASE 2: DEFINE SYSTEM REQUIREMENTS
PHASE 3: DESIGN SYSTEM ARCHITECTURE
PHASE 4: DEVELOP DETAILED DESIGN
PHASE 5: IMPLEMENT SYSTEM
PHASE 6: ASSESS EFFECTIVENESS
USERS/USERS' REPRESENTATIVES

Questions:

- What is the name of a management approved plan that addresses the preservation and recovery of business in the event of outages?
  –

- What is the name of a management approved plan that addresses the restoration of an organization’s essential business functions at an alternate site for up to 30 days?
  –

- What is the name of a management approved plan that addresses both internal and public communications in a crisis event?
  –

Answers:

- What is the name of a management approved plan that addresses the preservation and recovery of business in the event of outages?
  - Business Continuity Plan (BCP)

- What is the name of a management approved plan that addresses the restoration of an organization’s essential business functions at an alternate site for up to 30 days?
  - Continuity Of Operations Plan (COOP)

- What is the name of a management approved plan that addresses both internal and public communications in a crisis event?
  - Crisis Communications Plan

Topics

Business Continuity Planning (BCP) Domain

- Terms & Definition
- ➡ Phase I: Project Management and Initiation
- Phase II: Business Impact Analysis (BIA)
- Phase III: Recovery Strategy
- Phase IV: Plan Design & Development
- Phase V: Implementation
- Phase VI: Testing
- Phase VII: Maintenance, Awareness, and Training

Phase I: Project Management and Initiation

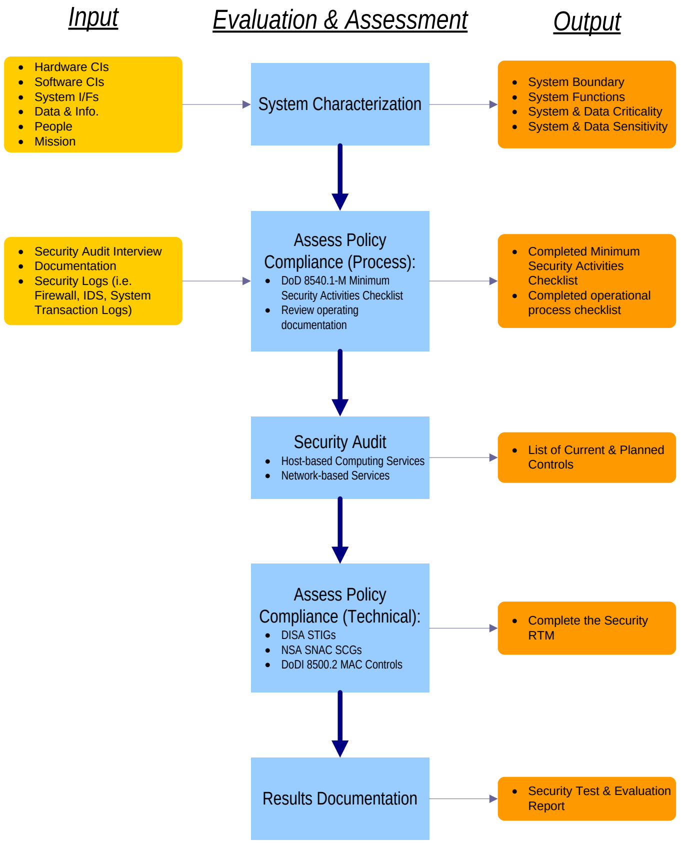
Procedure to initiate a BCP project…

- Step 1: Establish the need.
- Step 2: Obtain management support.
- Step 3: Identify stakeholders and resources.
- Step 4: Create an project management work plan.

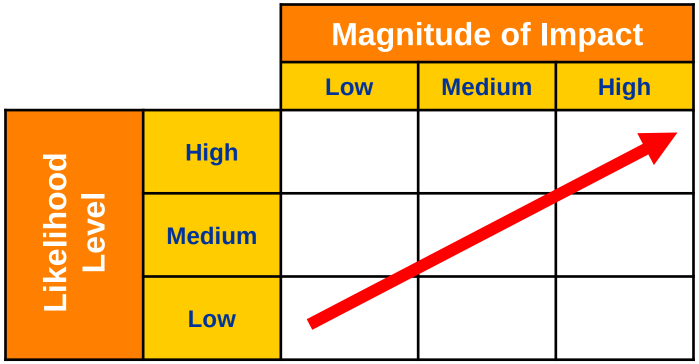
Phase I: Project Management and Initiation

Establish the Need

- Establish the need for a BCP.
  - Perform a focused risk assessment to identify and document potential contingencies to critical information and information systems.



Input	*Evaluation & Assessment*	*Output*
Hardware CIs Software CIs System I/Fs Data & Info. People Mission	System Characterization	System Boundary System Functions System & Data Criticality System & Data Sensitivity
Security Audit Interview Documentation Security Logs (i.e. Firewall, IDS, System Transaction Logs)	Assess Policy Compliance (Process): DoD 8540.1-M Minimum Security Activities Checklist Review operating documentation	Completed Minimum Security Activities Checklist Completed operational process checklist
	Security Audit Host-based Computing Services Network-based Services	List of Current & Planned Controls
	Assess Policy Compliance (Technical): DISA STIGs NSA SNAC SCGs DoDI 8500.2 MAC Controls	Complete the Security RTM
	Results Documentation	Security Test & Evaluation Report



SC $_{\text{information type}}$ = {(**confidentiality**, impact), (**integrity**, impact), (**availability**, impact)}, where the acceptable values for potential impact are low, medium, or high.

Phase I: Project Management and Initiation

Obtain Management Support & Plan Project

- Obtain management support and identify stakeholders.
- Identify strategic internal and external resources to ensure that BCP matches overall business and technology plans.
- Establish the project management work plan, including the:
  - Define scope and objectives of the project.
  - Determine methods for organizing and managing development of the BCP.
  - Establish members of the BCP team (both technical & functional).
  - Identification of related tasks and responsibilities.
  - Schedule project management reviews (PMR) and set project milestones.

Reference: NIST SP 800-34, *Contingency Planning Guide for IT Systems*

Role & Responsibility of a BCP Coordinator

- Business continuity planner/coordinator is the leader responsible for the development of BCP.
  - To serve as the liaison between the planning development team and management.
  - Have direct access and authority to interact with all employees necessary to complete the planning.
  - Possess a thorough business knowledge to understand how an outage can affect the organization.
  - Be familiar with the entire organization and in a position within the organization to balance the overall needs of the organization with the needs of individual business units that would be affected.
  - Have easy access to executive management.
  - Understand the charter, mission statement, and executive viewpoint when decisions need to be made.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Topics

Business Continuity Planning (BCP) Domain

- Terms & Definition
- Phase I: Project Management and Initiation
- ➡ Phase II: Business Impact Analysis (BIA)
- Phase III: Recovery Strategy
- Phase IV: Plan Design & Development
- Phase V: Implementation
- Phase VI: Testing
- Phase VII: Maintenance, Awareness, and Training

Business Impact Analysis (BIA)

- BIA is a management-level functional analysis that identifies the impact to business operations should an outage occur.
- BIA leverages information from risk assessment, but it is not an IT risk assessment.
- Impact is measured by:
  - Tangible attributes:
    - Allowable business interruption – Maximum Tolerable Downtime (MTD) or Maximum Tolerable Outage (MTO)
    - Financial cost considerations.
    - Regulatory requirements.
  - Intangible attributes:
    - Organizational reputation.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Purpose

The purpose of BIA is to:

- Provide written documentation to assist the organization's management in understanding the business impact associated with possible outages.
- Identify an organization's business functions and associated information systems to determine how critical those functions are to the organization.
- Identify any concerns that staff or management may have regarding the ability to function in less than optimal modes
- Prioritize critical information systems.
- Analyze impact of an outage, such as loss revenue, additional operating expenses, delay of income, and loss of competitive advantage and public confidence
- Determine recovery windows for each business function, such as determining how long the organization may be able to perform critical functions manually or through some other alternative methods.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Example – Maximum Tolerable Downtime (MTD)

- Example of Business Impact Categories & Maximum Tolerable Downtime (MTD)

Business Impact Category	MTD
Nonessential	30 Days
Normal	7 Days
Important	72 Hours
Urgent	24 Hours
Critical/Essential	Minutes to Hours

Process

Procedure to conduct BIA

- Step 1: Determine information gathering techniques.
- Step 2: Select interviewees (i.e. stakeholders.)
- Step 3: Customize questionnaire to gather economic and operational impact information.
  - Quantitative and qualitative questions.
- Step 4: Analyze collected impact information.
- Step 5: Determine time-critical business systems.
- Step 6: Determine maximum tolerable downtimes (MTD).
- Step 7: Prioritize critical business systems based on MTD.
- Step 8: Document findings and report recommendations.

Reference: *Official (ISC)²® Guide to the CISSP® Exam*

Questions:

- What is the name of a management approved plan that addresses operational processes for the recovery of a damaged facility?
  -

- What is the first step to begin a business continuity program?
  -

- Who is the person responsible for managing the business continuity program?
  -

Answers:

- What is the name of a management approved plan that addresses operational processes for the recovery of a damaged facility?
  - Disaster Recovery Plan

- What is the first step to begin a business continuity program?
  - Establish the need

- Who is the person responsible for managing the business continuity program?
  - Business continuity planner/coordinator

Topics

Business Continuity Planning (BCP) Domain

- Terms & Definition
- Phase I: Project Management and Initiation
- Phase II: Business Impact Analysis (BIA)
- ➡ Phase III: Recovery Strategy
- Phase IV: Plan Design & Development
- Phase V: Implementation
- Phase VI: Testing
- Phase VII: Maintenance, Awareness, and Training

Phase III: Disaster Recovery Strategy

- Recovery strategy is a set of predefined & management approved actions implemented in response to a business interruption from a disaster.
  - Natural / Environmental
    - Earthquakes, floods, storms, hurricanes, fires, snow/ice, etc.
  - Man made / political events
    - Explosives, disgruntled employees, unauthorized access, employee errors, espionage, sabotage, arson/fires, hazardous/toxic spills, chemical contamination, malicious code, vandalism and theft, etc.
- Recovery strategy focus on:
  - Meeting the predetermined recovery time frames (i.e. MTD).
  - Maintaining the operation of the critical business functions.
  - Compiling the resource requirements.
  - Identifying alternatives that are available for recovery.

Phase III: Disaster Recovery Strategy

Define "Disaster"

- Disaster severity should be defined for "conditioned" recovery measures. (e.g. INFOCON, DEFCON, and DHS Threat Advisory)
- Business continuity planner/coordinator should have a defined severity for declaring a "disaster".
- In general, there are two types of recovery strategy:
  - General recovery, where the critical infrastructure remain in tact and recovery is within MTD.
  - Disaster recovery, where the critical infrastructure severely disabled and contingency require alternate site(s).

Disaster Severity	Definition	Note
Level 1	Threat impact and analysis	Normal operations
Level 2	Minimal damage event	Zero impact to data systems
Level 3	Single-system failure	Failover or restore system
Level 4	Single critical failure or multiple non-critical failures	Perform general recovery procedure
Level 5 = Disaster	Imminent or actual data center failure	Enable recovery site and perform disaster recovery procedure

Procedure

Procedure for developing a recovery strategy:

- Step 1: Document all costs associated with each contingencies.
- Step 2: Obtain cost estimates for any outside services (using RFI, RFQ, or RFP).
- Step 3: Develop written agreements for outside services (i.e. Service Level Agreement (SLA)).
- Step 4: Evaluate resumption strategies based on a full loss of the facility.
- Step 5: Identify risk reduction measures and update Business Resumption Plan (BRP).
- Step 6: Document recovery strategies and present to management for comments and approval.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Phase III: Disaster Recovery Strategy

Elements of Recovery

Elements of recovery strategies:

- Business recovery strategy
  - Focus on recovery of business operations.
- Facility & supply recovery strategy
  - Focus on facility restoration and enable alternate recovery site(s).
- User recovery strategy
  - Focus on people and accommodations.
- Technical recovery strategy
  - Focus on recovery of IT services.
- Data recovery strategy
  - Focus on recovery of information assets.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Business Recovery

- Business recovery strategy focuses on recovery of business operations by identifying:
  - Critical business units and their associated business functions.
  - Critical IT system requirements for each business function.
  - Critical office equipment and supplies requirements for each business function.
  - Essential office space requirements for each business unit.
  - Key operations personnel for each business unit.
  - Supporting infrastructure (i.e. telecom., utilities, and postal service) for service redirection to recovery site(s).
  - Business unit interdependencies.
  - Off-site storage.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Phase III: Disaster Recovery Strategy

Business Recovery

Mutual Aid Agreements

- An arrangement with another company that may have similar computing needs.
- Both companies agree to support each other in the case of a disruptive event.
- In most cases, a “perfect partner” is a company’s subsidiary.

- Advantages:
  - Obtain a recovery site at little or no cost.
- Disadvantages:
  - It is highly unlikely that each organization's infrastructure will have the extra capacity to enable full operational processing during the event.
  - Need geographic diversity so that a major regional disaster doesn't disrupt both companies.

Reference: *Official (ISC)²® Guide to the CISSP® Exam*

Facility & Supply

- Facility & supply recovery strategy focuses on restoration and recovery of:
  - Facility for critical business units.
  - Facility for less critical business units.
  - Security and operational needs at recovery site(s.
    - Primarily physical security controls (i.e. personnel access control, fire/water detection & suppression, and intrusion detection systems, etc.)
  - Transportation and supply chain logistics to recovery site(s)
    - People, office supply, critical IT systems, and document, etc.
  - Redirection of supporting infrastructure to recovery site(s)
    - telecommunications, utilities, and postal service.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP$^{®}$ Exam*

User Recovery

- User recovery strategy focuses on:
  - Contingency business operations procedures (manual or automated).
  - Employee access procedure for recovery site.
  - Transport and storage of critical business documentation and forms.
  - Storage of vital records (i.e. personnel, legal business, and medical records, etc.)
  - Employee notification procedures.
  - Transportation arrangements for employee to recovery site.
  - Employee accommodations (e.g. user workspace, equipment, food, water, sleeping, and plumbing, etc.)

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Technical Recovery

- Technical recovery strategy focuses on:
  - Data Center Recovery
  - Network and Data Communication Recovery Planning
  - Telecommunications Recovery
- The key elements to the technical recovery are:
  - Subscription Services
    - Hot Site
    - Warm Site
    - Cold Site
    - Mirror Site or Multiple Processing Centers
    - Mobile site
  - Reciprocal or Mutual Aide Agreement
  - Service Bureaus

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Technical Recovery

Subscription Service: Hot Site

- A Hot Site is a fully configured computer facility with complete customer required systems
  - Computing infrastructure (i.e. servers, workstations, and networks)
  - Critical infrastructure (i.e. electricity, water, HVAC, physical security, etc.)
- Advantage
  - 24/7 availability.
- Disadvantage
  - Expensive to maintain.
  - Need data restoration from backup. (Data is not mirrored)
  - The service provider might oversell capacity, thus create possible contentions for resources between multiple companies during a regional disaster.
  - Security control of information asset must be maintained in multiple places.

Reference: *Official (ISC)2® Guide to the CISSP® Exam*

Technical Recovery

Subscription Service: Warm Site

- A Warm Site is a facility readily available with electrical power and HVAC and computers, but the applications may not be installed.
- Advantages
  - Availability is assured for longer timeframes.
  - Cost is less than a hot site subscription service.
  - Flexible in the choice of sites (i.e. locations).
  - Uses less administrative resources than a hot site.
- Disadvantage
  - Operational testing is not possible.
  - Required resources may not be immediately available. (i.e. data restoration).
  - More expensive than a cold site or in-house recovery sites.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP$^{®}$ Exam*

Technical Recovery

Subscription Service: Cold Site

- A Cold Site is a facility with critical infrastructure services only. It does not include any IT equipment, or resources.
- Advantages
  - Lower cost than hot or warm site subscription service.
  - Available for longer periods of time.
  - Site can be in various locations.
- Disadvantage
  - Required resources may not be immediately available. (i.e. equipment transport, setup, and data restoration)
  - Operating testing is not possible.
  - Costs are more expensive than in-house facilities.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP$^{®}$ Exam*

Technical Recovery

Mirror Site or Multiple Processing Centers

- The information processing is distributed over multiple data centers. The available resources are shared & fully redundant.
- Advantage
  - No MTD issue, minimal business impact when there is a disaster at one site.
  - The organization have full control over all data centers.
  - Resources are fully available.
- Disadvantage
  - For distributed Multiple Processing Centers: Shared computing resources may not maintain excess capacity, then a major disaster could easily overtake the processing capability of processing sites.
  - If maintain excess capacity for major disaster, it can be cost prohibitive.
  - Logistics of maintaining multiple sites may lead to CM problems.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Phase III: Disaster Recovery Strategy

Technical Recovery

Mobile Site

- A Mobile Site is self-contained, transportable shelter custom-fitted with specific telecommunications and IT equipment.
- Advantage
  - The organization have full control over all equipment.
- Disadvantage
  - May offer limited information processing capacity (, as compared to the primary data center.)
  - Require advance coordination, resources may not be immediately available (i.e. equipment transport, setup, and data restoration.)

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Technical Recovery

Service Bureaus (i.e. Business Process Outsourcing)

- Service bureaus offer data processing services to many organizations.
- Advantage
  - Quick response and availability.
  - Testing is possible.
- Disadvantage
  - Organization do not have full control of protection to its information asset.
  - Most of service bureaus are optimized for current client base, adding additional processing loads during a major disaster may create resource contention.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Data Recovery

- Data recovery strategy focuses on recovery of information:
  - Backup and off-site storage
    - Full backup
    - Incremental backup
    - Differential backup
  - Electronic vaulting
    - Online tape vaulting
    - Remote journaling
    - Database shadowing
  - Standby service
  - Software escrow
  - Recovery Management

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Contingency Planning – Data Backups …(1/4)

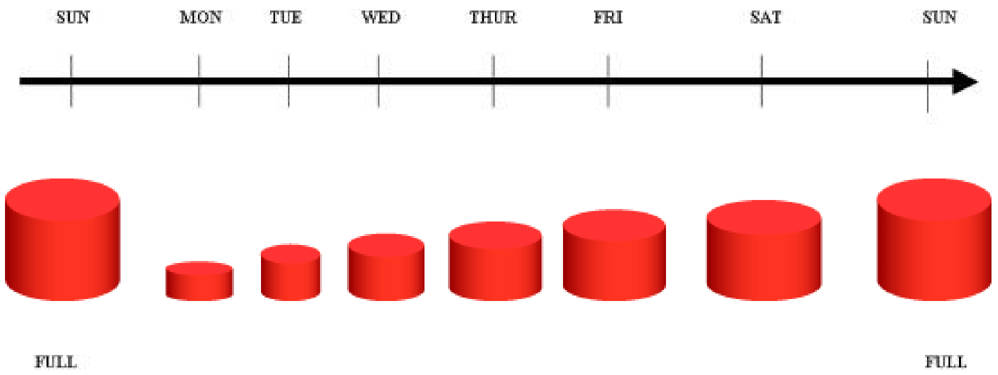
Three types of data backups:

- Full volume backup is backup performed on an entire disk volumes of a system(s).
- Differential backup is a backup of changes since last full backup, but does not change the archive bit value.
- Incremental backup is a backup of changes since last full or incremental backup and sets the archive bit to 0.

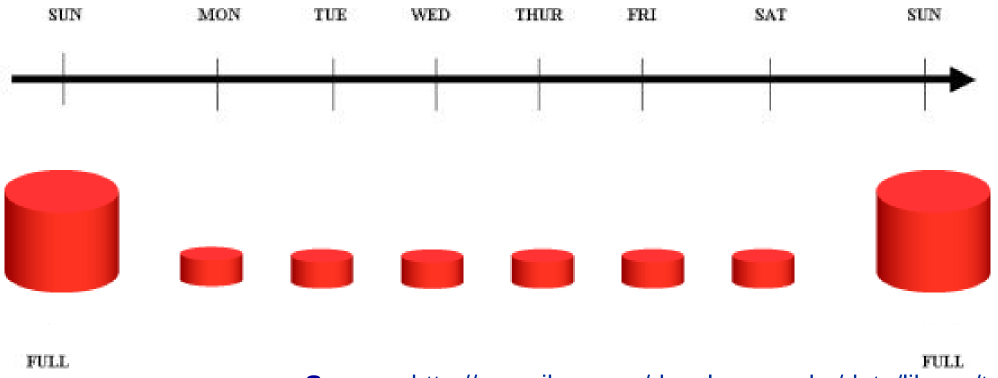
Source: *All-in-One CISSP Exam Guide, 5th Ed,* 2010.

Contingency Planning – Data Backups …(2/4)

- Recovery steps: Full + differential backup.



- Recovery steps: Full + sequence incremental backups



Source: http://www.ibm.com/developerworks/data/library/techarticle/dm-0407tham/index.html

Data Recovery

Off-site storage requirements:

- Facility
  - Security controls. (i.e. access controls, inventory control, physical security, etc.)
  - Environmental controls. (i.e. humidity & temperature controls, fire & water protection measures)
  - Location. (i.e. distance to service clients)
- Transportation
  - Delivery vehicles are secure. (i.e. physical access controls & insured for liability)
  - Defined handling procedure. (i.e. access controls & inventory controls for integrity & accountability)
  - Transport availability. (i.e. 24/7 in case of an emergency)
- Personnel
  - Knowledgeable personnel with appropriate security clearances, and background checks, etc.
  - Follow handling security procedure.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Data Recovery

- Standby services represent the operation of critical operating systems and applications at an alternate site when called upon.
- Software escrow is when a vendor places a copy of critical source code with a trusted 3rd party so that it can be obtained in the event that the vendor goes out of business.
- Recovery management is a part of coordinated execution of data recoveries in a controlled manner.

Reference: *Official (ISC)²® Guide to the CISSP® Exam*

Leaving the Primary Site…

Business Recovery Operations

- Understand the severity of “disaster”
- Coordinate the BCP (/ crisis) team
- Execute the BCP according to the “disaster” :
  - Business recovery,
  - Facility & supply recovery,
  - User recovery,
  - Technical recovery,
  - Data recovery
- and the approved plan of actions:
  - Business Resumption Plan
  - IT Contingency Plan
  - Crisis Communications Plan
  - Cyber Incident Response Plan
  - Disaster Recovery Plan
- Communicate the crisis
  - Crisis Communications Plan
- Secure the primary site

Reference: *CISSP Certification All-in-One Exam Guide*, 4th Ed.

Returning to the Primary Site…

Restoration Operations

- Complete a detailed assessment of all damage.
- Review insurance policies and document information, as needed and coordinate with insurance company.
- Contact restoration service contractors to salvage or disposal of damaged equipment, and procure new equipment.
- Coordinate activities to have repairs made to the damaged area within the primary site.
- Restore the primary site to minimum operating conditions.
  - … reconstruction and restoration of facility (including government inspections)
  - … restore critical infrastructure services (i.e. utilities, water, etc.)
- Reactivate physical perimeter security systems (fire, IDS, water, etc.)
- Implement and test the IT infrastructure. (i.e. networks, DNS, e-mail, etc.)
- Certify the system is ready for operations.

Reference: *CISSP Certification All-in-One Exam Guide*, 4th Ed.

Questions:

- What is the name of a written analysis that states the possible business impact associated with an outage?

  –

- In order to define the level of recovery effort, one has to define the severity of ____?

  –

- What are the five key elements in recovery strategy?

  –

  –

  –

  –

  –

Answers:

- What is the name of a written analysis that states the possible business impact associated with an outage?
  - Business Impact Analysis (BIA)

- In order to define the level of recovery effort, one has to define the severity of _____?
  - Disaster

- What are the five key elements in recovery strategy?
  - Business recovery
  - Facility & supply recovery
  - User recovery
  - Technical recovery
  - Data recovery

Questions:

- In most cases, who may be the best business recovery partner to enter into a mutual-aid agreement with?
    - –

- What is a fully configured computing facility with complete customer required information systems but requires data restoration from backups?
    - –

- What is an empty facility that equipped with critical infrastructure services only (e.g., water, electricity, HVAC)
    - –

Answers:

- In most cases, who may be the best business recovery partner to enter into a mutual-aid agreement with?
  - A company's subsidiary

- What is a fully configured computing facility with complete customer required information systems but requires data restoration from backups?
  - A "Hot Site"

- What is an empty facility that equipped with critical infrastructure services only (e.g., water, electricity, HVAC)
  - A "Cold Site"

Questions:

- What are the three types of data backups?
  - –
  - –
  - –

- What is the name of a software recovery service that involves storage of specialized software in an entrusted 3rd party?
  - –

Answers:

- What are the three types of data backups?
  - Full complete backup
  - Incremental backup
  - Differential backup

- What is the name of a software recovery service that involves storage of specialized software in an entrusted 3rd party?
  - Software escrow service

Business Continuity Planning (BCP) Domain

- Terms & Definition
- Phase I: Project Management and Initiation
- Phase II: Business Impact Analysis (BIA)
- Phase III: Recovery Strategy
- Phase IV: Plan Design & Development
- Phase V: Implementation
- Phase VI: Testing
- Phase VII: Maintenance, Awareness, and Training

Procedure … (1/3)

Procedure for developing BCP:

- Step 1: Determine management concerns & priorities.
- Step 2: Determine planning scope such as geographical concerns, organizational issues, and the various recovery functions to be covered in the plan.
- Step 3: Establish outage assumptions.
- Step 4: Define prevention strategies for risk management, physical security, information security, insurance coverage, and how to mitigate the emergency.
- Step 5: Identify resumption strategies for mission critical- and non-mission critical-systems at alternate sites.
- Step 6: Identify the location for the emergency operations center/ command center.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Procedure … (2/3)

Procedure for developing BCP: …(continued)

- Step 7: Develop service function recovery plans, including information processing, telecommunications, etc.
- Step 8: Develop business function recovery plans and procedures.
- Step 9: Develop facility recovery plans.
- Step 10: Identify the response procedures, including:
  - Evacuation and safety of personnel
  - Notification of disaster
  - Notifying alternate site(s)
  - Initial damage assessment
  - Securing home site
  - Activating recovery teams, and emergency operations center/command center
  - Relocating to alternate site(s)

Reference: *Official (ISC)²® Guide to the CISSP® Exam*

Phase IV: Plan Design & Development

Procedure … (3/3)

Procedure for developing BCP: …(continued)

- Step 11: Gather data required for plan completion. Develop support service plans, including human resources, public relations, transportation, facilities, information processing, telecommunications, etc.
- Step 12: Review and outline how the organization will interface with external groups.
- Step 13: Review and outline how the organization will cope with other complications beyond the actual disaster.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP$^{®}$ Exam*

Topics

Business Continuity Planning (BCP) Domain

- Terms & Definition
- Phase I: Project Management and Initiation
- Phase II: Business Impact Analysis (BIA)
- Phase III: Recovery Strategy
- Phase IV: Plan Design & Development
- Phase V: Implementation
- Phase VI: Testing
- Phase VII: Maintenance, Awareness, and Training

Phase V: Implementation

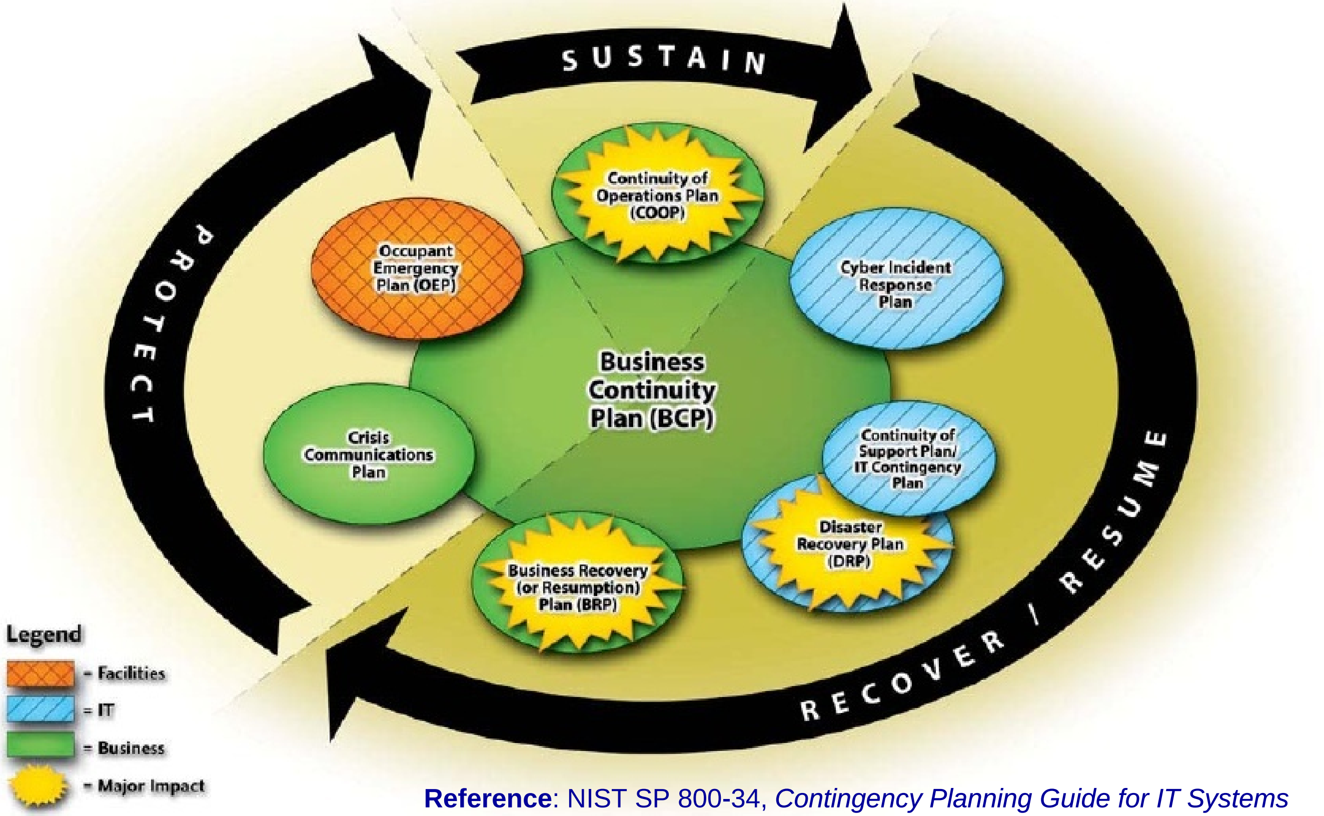
- Execute BCP as an integrated program that consists of…
  - Business Resumption Plan
  - Continuity of Operations (COOP) Plan
  - IT Contingency Plan
  - Crisis Communications Plan
  - Cyber Incident Response Plan
  - Disaster Recovery Plan
  - Occupant Emergency Plan

Reference: *CISSP Certification All-in-One Exam Guide*, 4th Ed.

Phase V: Implementation

Business Continuity Life Cycle

- Sustain business operations (COOP)
- Recover / resume business operations (Business Recovery Plan, Incident Response Plan, IT Contingency Plan, and Disaster Recovery Plan)
- Protect business assets (People, reputation, and tangible assets) (Crisis Communications Plan, Occupant Emergency Plan)


SUSTAIN
RECOVER / RESUME
PROTECT
Continuity of Operations Plan (COOP)
Cyber Incident Response Plan
Continuity of Support Plan/ IT Contingency Plan
Disaster Recovery Plan (DRP)
Business Recovery (or Resumption) Plan (BRP)
Crisis Communications Plan
Occupant Emergency Plan (OEP)
Business Continuity Plan (BCP)
Legend
= Facilities
= IT
= Business
= Major Impact

Reference: NIST SP 800-34, *Contingency Planning Guide for IT Systems*

Topics

Business Continuity Planning (BCP) Domain

- Terms & Definition
- BCP Phase I: Project Management and Initiation
- BCP Phase II: Business Impact Analysis (BIA)
- BCP Phase III: Recovery Strategy
- BCP Phase IV: Plan Design & Development
- BCP Phase V: Implementation
- ➡ BCP Phase VI: Testing
- BCP Phase VII: Maintenance, Awareness, and Training

Phase VI: Testing, Maintenance, Awareness, & Training

Types of Tests

- Structured walk-through: Step-by-step review of BCP plans with organization's functional representatives
- Checklist test: Each functional representatives review BCP plans and check off the points that are listed to ensure all concerns and activities are addressed.
- Simulation: A scenario-based practice execution of the BCP plans.
- Parallel test: Operational test conducted at the alternate site(s).
- Full interruption test: Full scale operational test including shutdown of primary site and recovery of business operations at alternate site(s).

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

Topics

Business Continuity Planning (BCP) Domain

- Terms & Definition
- BCP Phase I: Project Management and Initiation
- BCP Phase II: Business Impact Analysis (BIA)
- BCP Phase III: Recovery Strategy
- BCP Phase IV: Plan Design & Development
- BCP Phase V: Implementation
- BCP Phase VI: Testing
- ➡ BCP Phase VII: Maintenance, Awareness, and Training

Phase VII: Testing, Maintenance, Awareness, & Training

Plan Maintenance

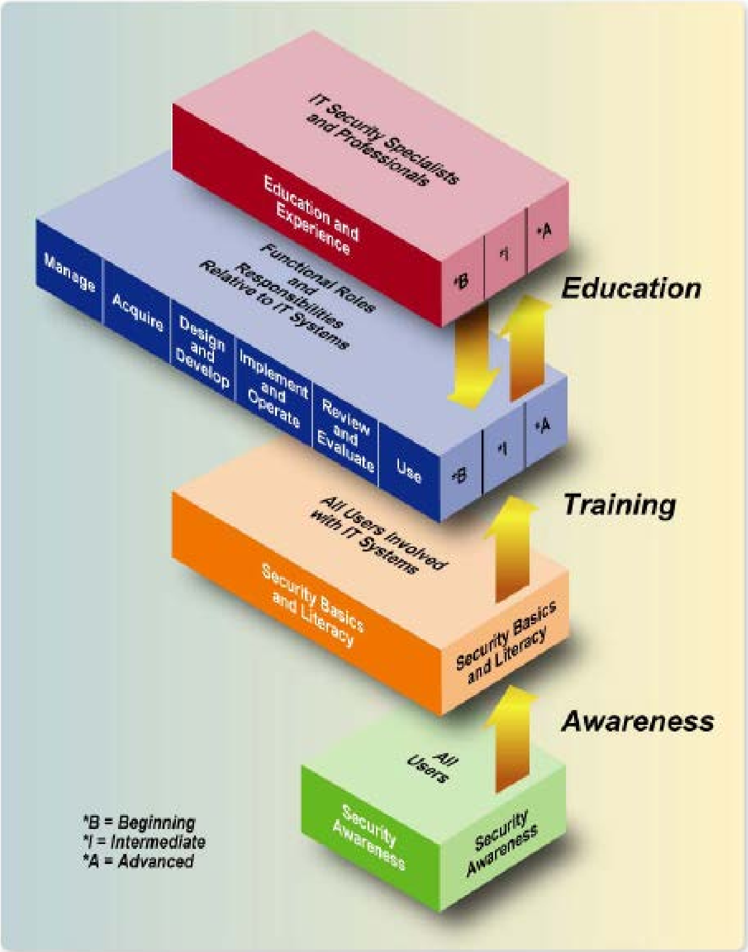
- Monitor configuration management (CM) and update BCP plans accordingly.
- Plan & schedule BCP maintenance reviews (Minimum: Annually review).
- Distribute updates to BCP plans.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP$^{®}$ Exam*

Phase VII: Testing, Maintenance, Awareness, & Training

BCP Awareness and Training

- Like Security Awareness & Training…
- BCP awareness on policy and procedures should be conducted annually to all employees & contractors.
- BCP training should role-based that focuses on a specific functional area(s).



Reference: NIST SP800-50, *Building an IT Security Awareness and Training Program*