Institute of Forensic Science
M.Tech. Cyber Security & Incident Response
(*Semester* – MCSIR SI P1: Introduction to Cyber Security)

Business Continuity Planning and Disaster Recovery

Source:
1. *Official (ISC)^{2}® Guide to the CISSP® Exam*
2. *CISSP CIB, January 2012 (Rev. 5)*
3. NIST SP 800-34, *Contingency Planning Guide for IT Systems*

Syllabus

MCSIR SI P1: Introduction to Cyber Security- Unit 5

- Introduction to Risk Analysis,
- Risk Assessment,
- Risk Mitigation
- Need for BCP,
- Overview of BCP Life Cycle,
- Identifying and Selecting Business Continuity Strategies,
- DR Strategies,
- Plans for Business Resumption,
- BCM Program Management and
- System Audit.

Organization of Sessions

Session 1

- **Introduction to Risk Analysis,**
- **Risk Assessment,**
- **Risk Mitigation**

Session 2

- **Need for BCP,**
- **Overview of BCP Life Cycle,**
- **Identifying and Selecting Business Continuity Strategies,**
- **DR Strategies,**
- **Plans for Business Resumption,**

Session 3

- **BCM Program Management and**
- **System Audit.**

Scope Session 2

- Need for Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP)
- Generally used Terms & Definitions
- Business Continuity Life Cycle
- 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

Need for BCP & DRP

Business Continuity & Disaster Recovery Planning

- **The Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) 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.**

- **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.**

Business Continuity & Disaster Recovery Planning..

- **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 operations 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.

Business Continuity & Disaster Recovery Planning..

- This is a subset of BCP. The goal of a DRP is to minimize the effects of a disaster and take necessary steps to ensure that the resources, personnel and business processes are able to resume operation in a timely manner.

- There is a difference between business continuity planning and disaster recovery.

- The business continuity planning addresses issues in terms of project scope and planning, business impact analysis, recovery strategies, recovery plan development, and implementation.

- Disaster recovery addresses issues in terms of recovery plan development, implementation and restoration.

Business Disruption

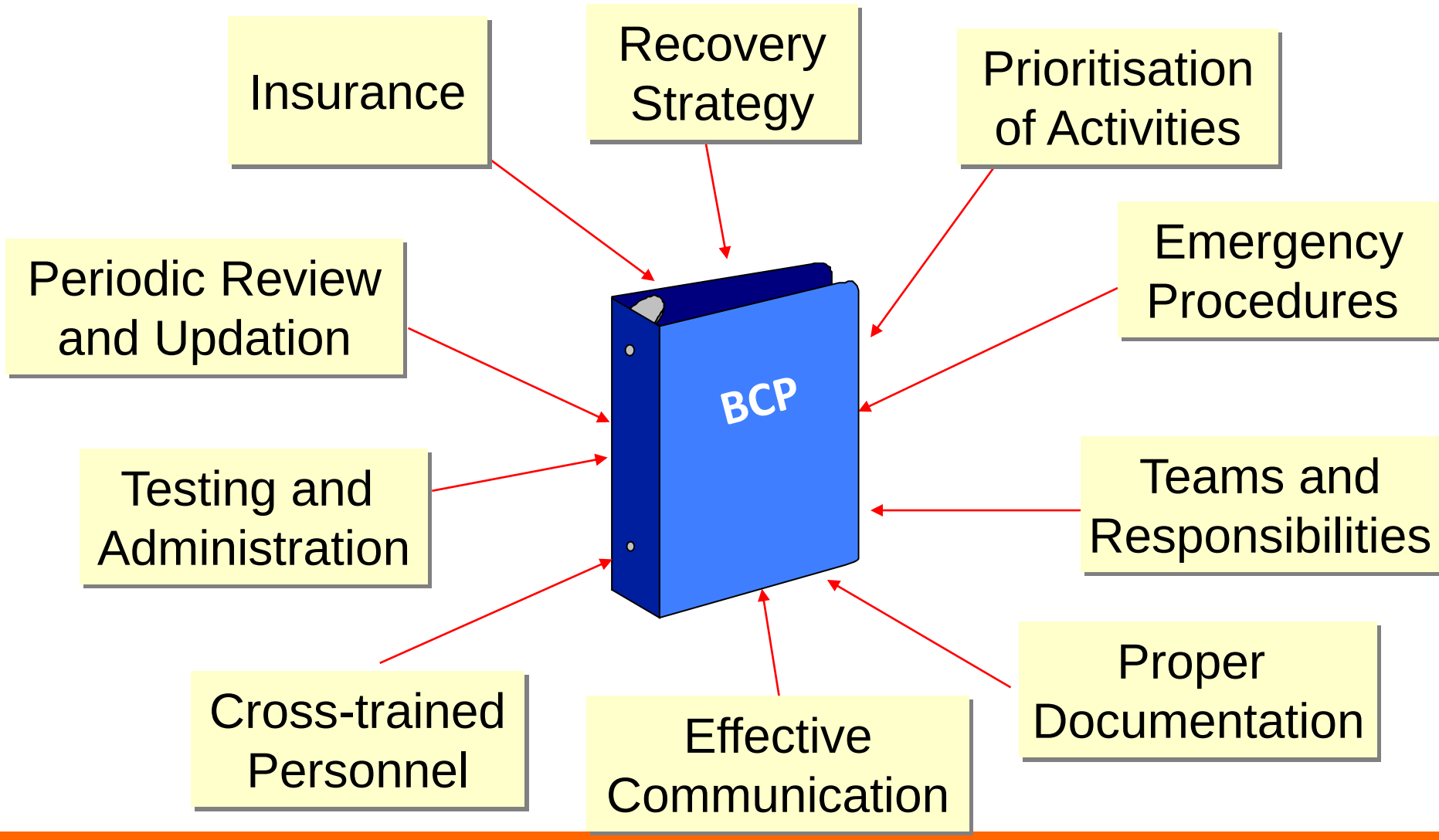
Business Disruption:

- An organization is dependant on resources, personnel and tasks performed on a daily bases to be healthy and profitable. Loss or disruption of these resources can be detrimental. Causing great damage or even complete destruction of the business.

- Business MUST have a plan to deal with unforeseen events.

Framework for e-Business Continuity

Building Blocks



Why a Business Requires BCP? To…

- Provide an immediate response to emergency situations
- Protect lives and ensure safety
- Reduce business impact
- Resume critical business functions
- Reduce confusion during a crisis
- Ensure survivability of the business
- Get up and running ASAP after a disaster

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.

Terms & Definitions

Commonly Used Terms

- **Business Continuity Plan** – a document describing how an organization responds to an event to ensure critical Business functions continue without unacceptable delay or change.

- **Business Continuity Planning** – Planning to help organizations identify the impacts of potential data processing and operation disruptions and data loss, formulate recovery plans to ensure the availability of data processing and operational resources.

- **Business Impact Analysis** – Process of analyzing all business functions within the organization to determine the impact of a data processing outage.

- **Business Resumption Planning**– BRP develops procedures to initiate the recovery of business operations immediately following and outage or disaster.

Commonly Used Terms…

- **Contingency Plan** – a document providing the procedures for recovering a major application or information system network in the event of an outage or disaster.

- **Continuity of Operations Plan** – A document describing the procedures and capabilities to sustain an organization's essential strategic functions at an alternate site for up to 30 days.

- **Critical Business Functions** – The business functions and processes that **MUST** be restored immediately to ensure the organization's assets are protected, goals met and that the organization is in compliance with any regulations and legal responsibilities.

Commonly Used Terms…

- **Cyber Incident Response Plan** – strategies to detect, respond and limit the consequences of cyber incidents.

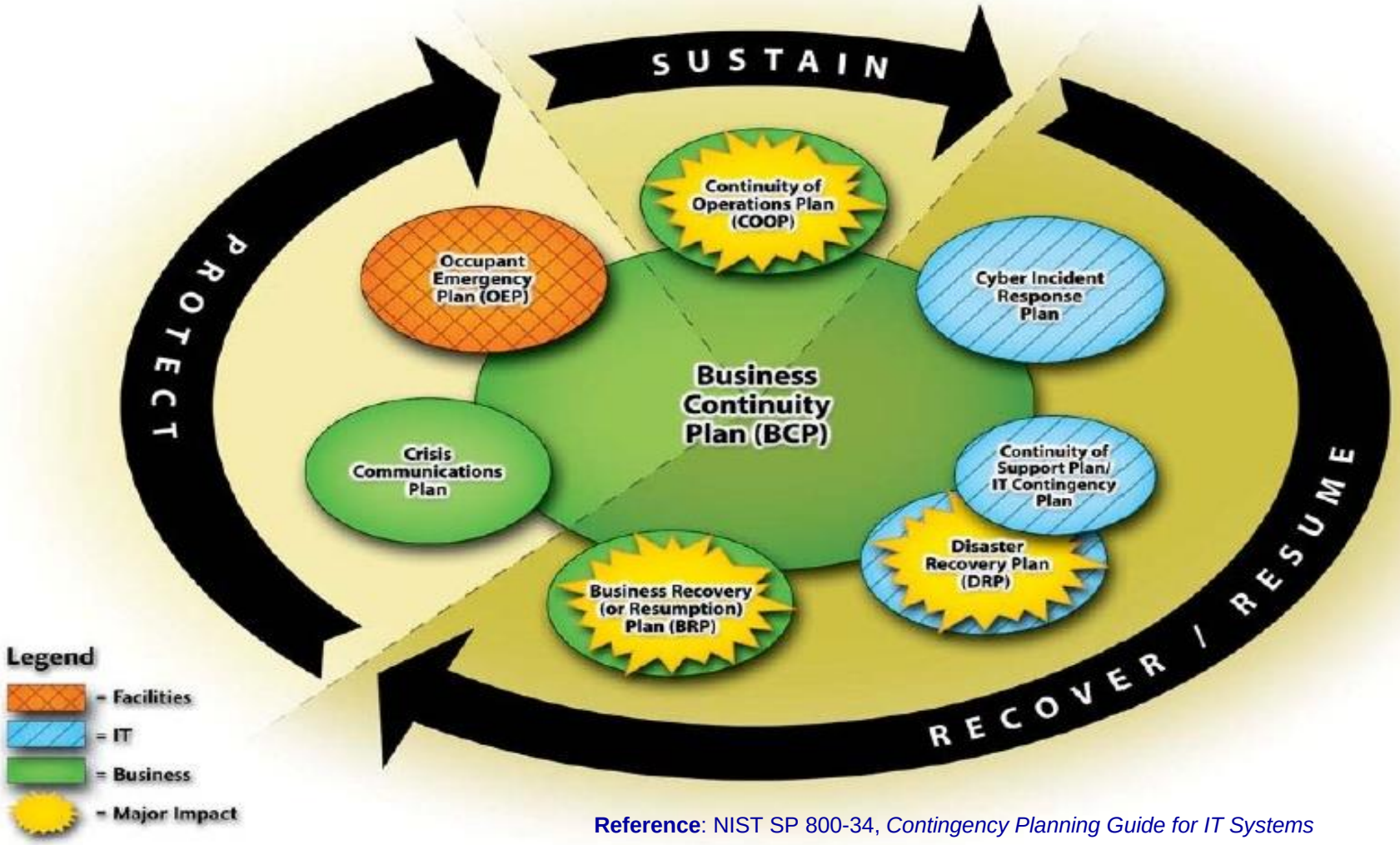
- **Disaster Recovery Plan** – A plan that provides detailed procedures to facilitate recovery of capabilities at an alternate site.

- **Disaster Recovery Planning** – The process to develop and maintain a disaster Recovery Plan

Business Continuity Life Cycle

Life Cycle of Business Continuity

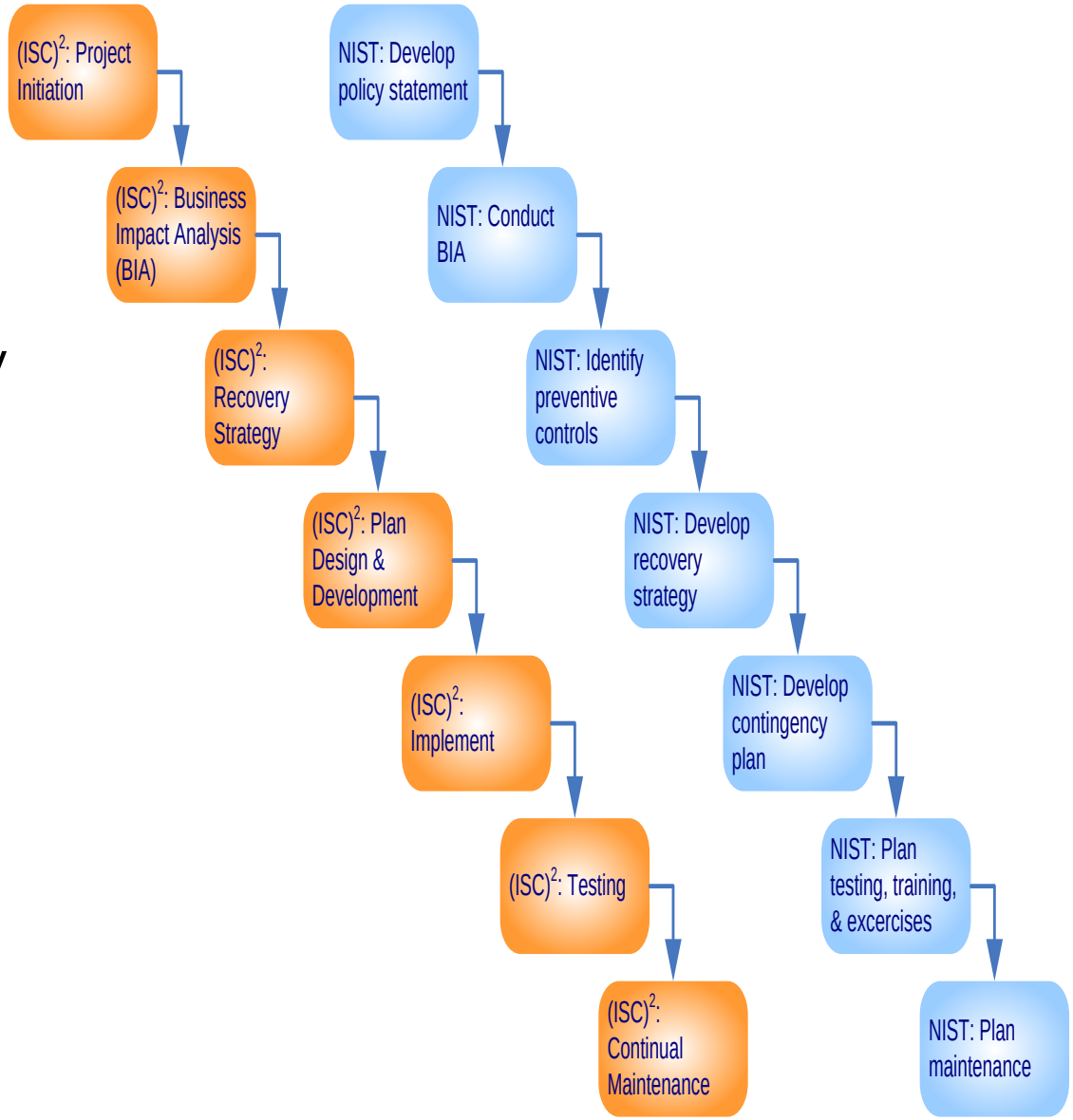
- **Sustain business operations**
- **Recover / resume business operations**
- **Protect business assets (People, reputation, and tangible assets)**



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

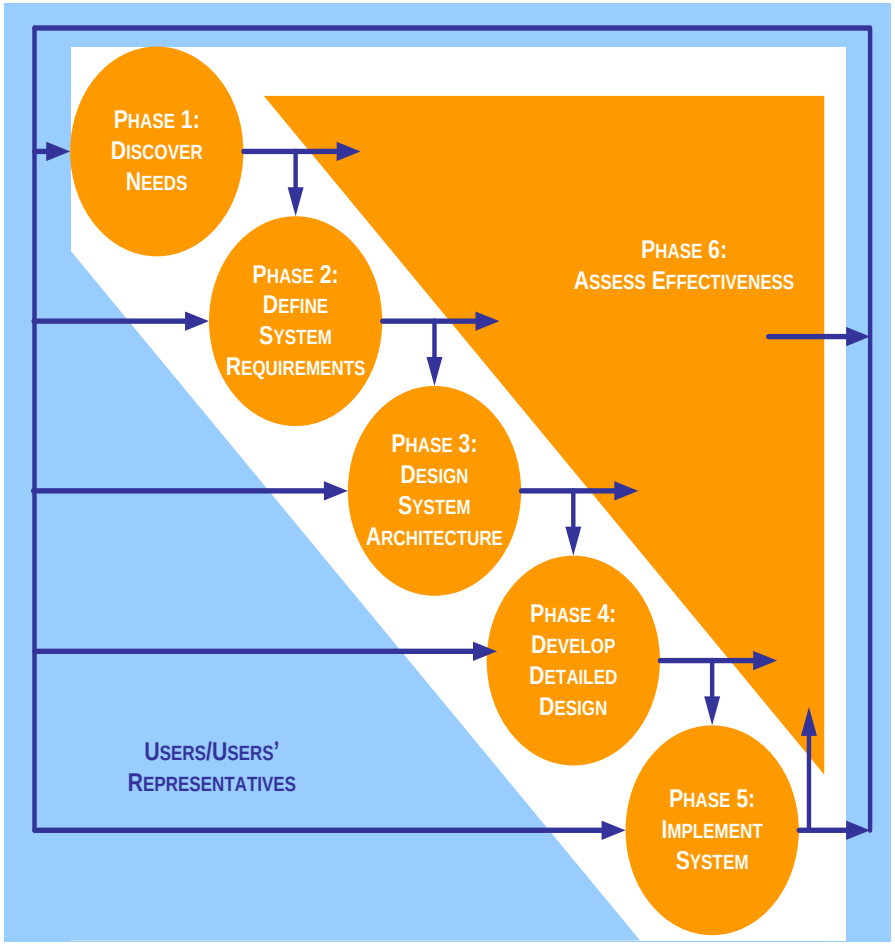
Process for Creating a BCP

- 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



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



BCP Overview

The is to help a company resume operating of business functions as soon as possible after a damaging event. A BCP should be part of the security policy* ISC states 5 Phases in BCP:

- **Project Initialization** – establish a project team and obtain management support
- **Conduct BIA** – identify time-critical business processed and determine maximum “outages”
- **Identify Preventative controls**
- **Recovery Strategy** – identify and select the recovery alternatives to meet the recovery time requirements

BCP Overview

5. **Develop the contingency plan** – document the results of the BIA findings and recovery strategies in a written plan

6. **Testing, Awareness, and Training** – establish the processes for testing the recovery strategies, maintaining the BCP, and ensuring that those involved are aware and trained in the recovery strategies.

6. **Maintenance** – Maintain the plan

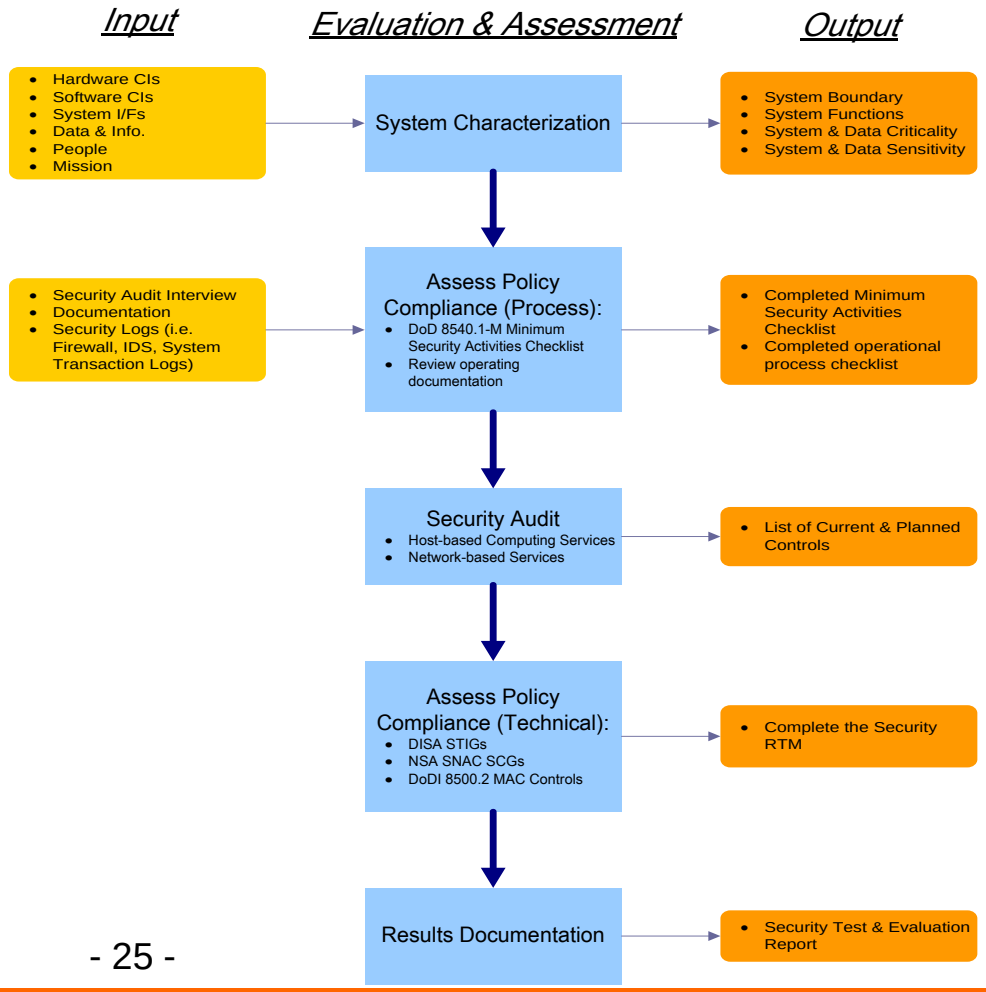
Phase I: Project Management and Initiation

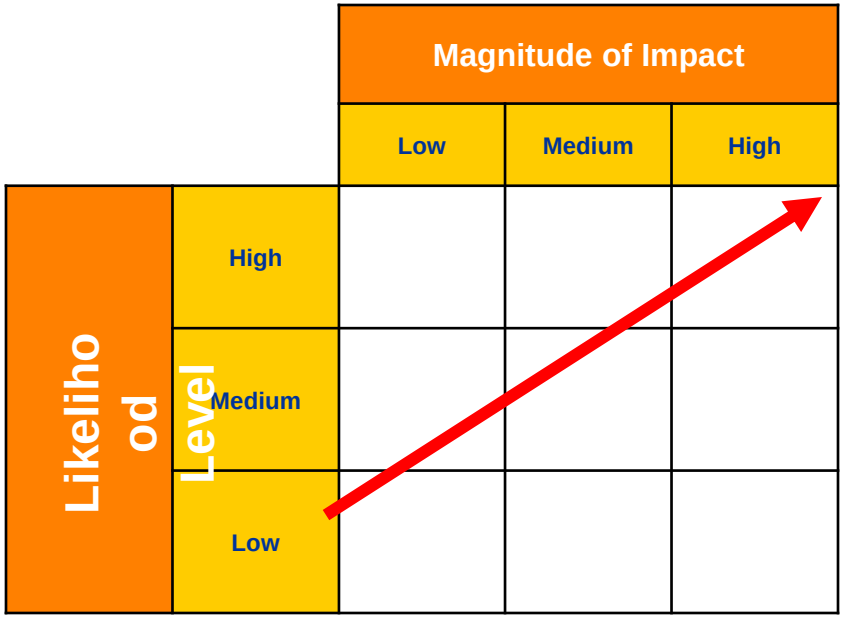
Procedure to initiate a BCP project…

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

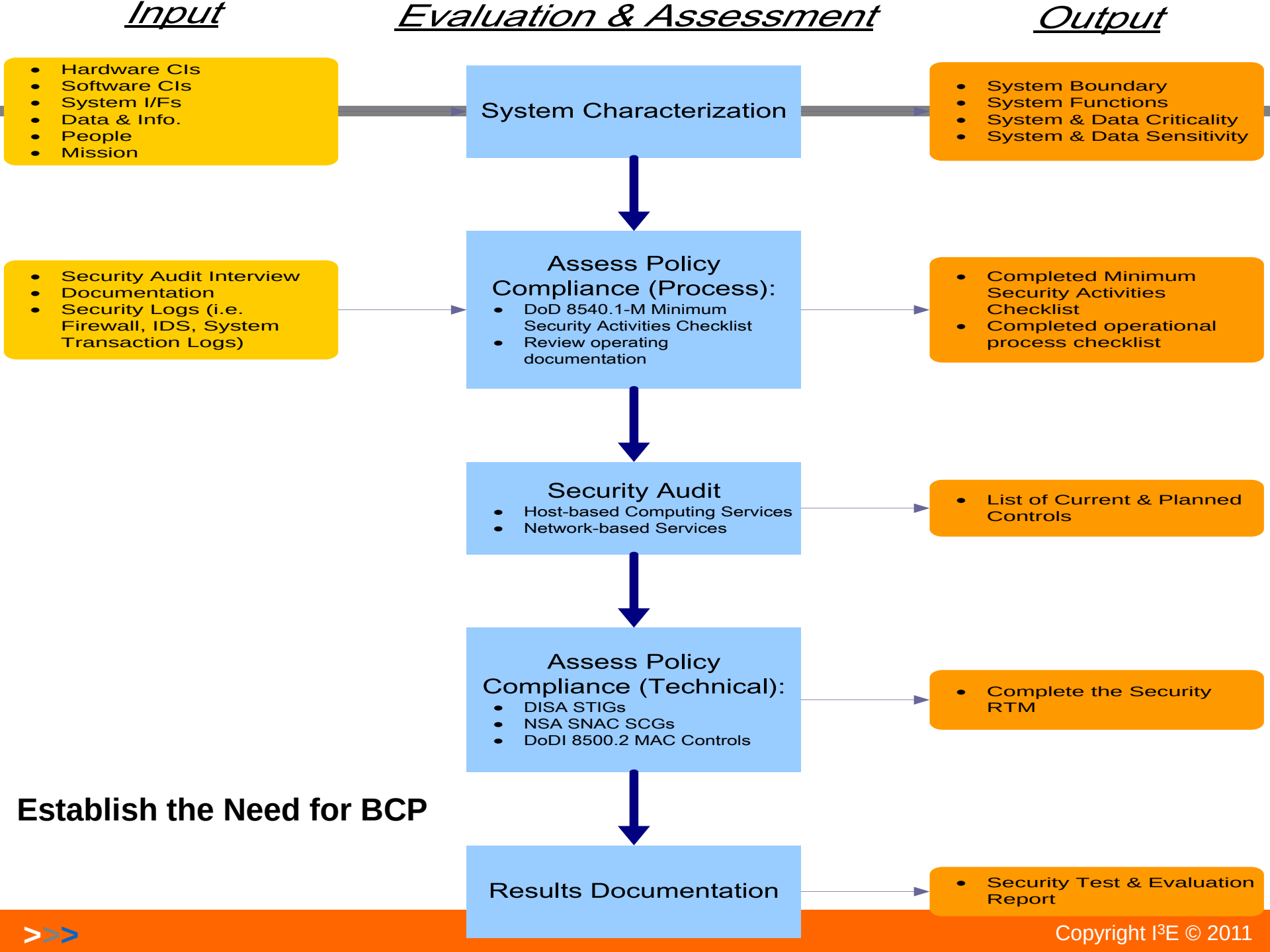
Establish the Need for BCP

Perform a focused risk assessment to identify and document potential contingencies to critical information and information systems.





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



BCP: Phase 1

Project Management and Initialization:

In this step

- we must solidify managements support, because without management support, NOTHING will be successful.
- Develop a “Continuity Planning Policy Statement” – lays out the scope of the BCP project, roles and members, and goals.
- We then must identify a “Business Continuity Coordinator”* (the BCP team leader)
- Establish a BCP team
  - What types of people/roles should be on the team…
  - Which people will be chosen for the team

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.

Phase II: Business Impact Analysis (BIA)

Purpose of Business Impact Analysis (BIA)

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 of 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.

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 only 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*

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

Phase 2 of the BCP steps is to conduct a Business Impact Analysis. In short this step is to outline what procedures and resources the company depends on, how important each processes is and how long the business can do without each resource. The formalized step are conversed next.

- 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.

BCP Phase 2: BIA…

Step 1 – Determine Information Gathering Techniques

- In this step the BCP committee needs to identify the types of people that will be part of the BIA gathering sessions.
- These people should represent the different departments that make up the business.
- After determining the general roles, we need to actually find the actual employees that fill these roles, so we can interview them.

Step 2 – Select Interviewees

- In this phase the BCP team must create data gathering techniques to use when interviewing and gathering other information to support the BCP objectives. (surveys, questionnaires etc)

BCP Phase 2: BIA…

Step 3 – Identify Critical Business Functions: Based on the information gathered by the interviews and the data gathering techniques, we identify which business processes and functions are critical for the successful operation of the business.

Step 4 Analyze information: What are the important processes that we need to determine, what are the resources that these processes depend upon. These resources can be all kinds of things such as servers, data, people, buildings etc! (not just IT related things)

Determine “cost” whether qualitative or quantitative

BCP Phase 2: BIA…

Step 5 – Determine MTD and prioritization: Now we need to prioritize and calculate the maximum time we can survive without the business processes identified in Step 3. This maximum time is called the "Maximum Tolerable Downtime (MTD)*" here are some common MTD classifications.

- Crititical: 1 – 4 hours
- Urgent: 24 hours
- Important: 72 hours
- Normal: 7 days
- Nonessential: 30 days

Keep in mind when prioritizing things, we have to use quantitative and qualitative analysis to determine just what is critical.

BCP Phase 2: BIA…

For example loss of some process might not cause immediate financial loss, but could damage reputation or competitive advantage, and that damage could be devastating. Here are some common MTD classifications

Step 6 – Threats: We need to identify vulnerabilities and threats to these processes and the resources that are required for reviving them. (remember Risk Management/Risk Analysis!

Example of threats:

- Equipment malfunction
- Hacking
- Failure in utilities (power, WAN connections)
- Critical personal becoming unavailable
- Vendors going out of business
- Data Corruption
- Physical Damage (hurricane, earthquake)

BCP Phase 2: BIA…

Step 7: Determine the probability/risk for each business function.

Step 8: Once we have done this research, we must document and provide our findings to management.

Note at this point we really have not started creating a Business Continuity Plan yet, We've just done the research. Once Management reviews findings and gives the OK to proceed, we will actually develop the plan

Phase III: Recovery Strategy

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 focuses 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.

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.**

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.

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.

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.

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.

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.)

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

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.

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.

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.

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.

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.)

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.

Technical 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**

Contingency Planning – Data Backups

Three types of data backups:

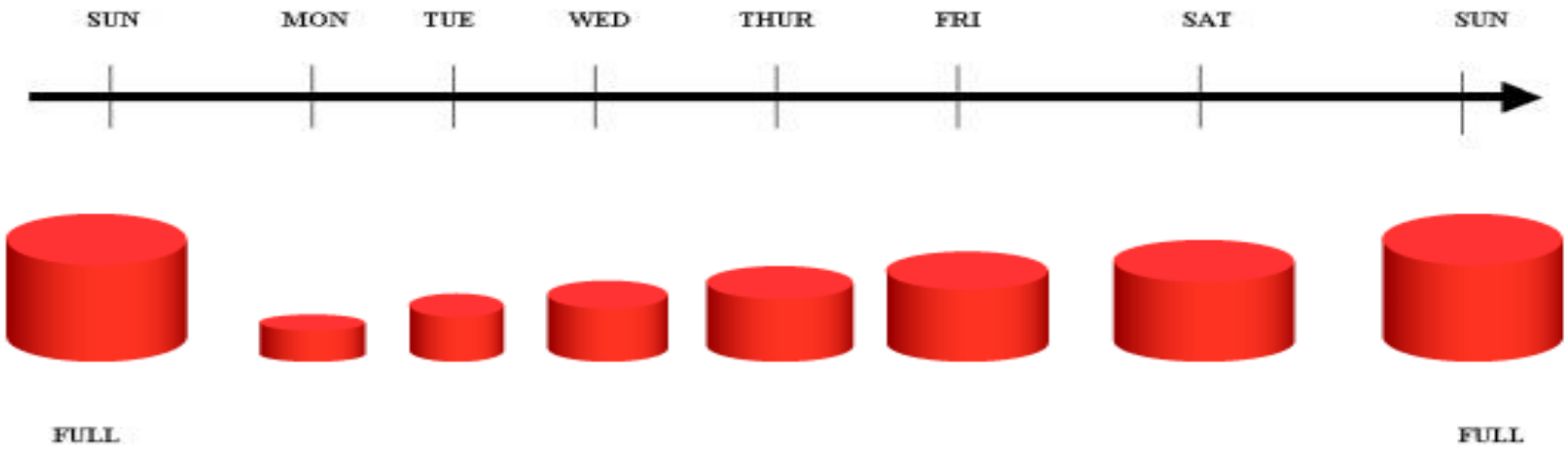
- **Full volume backup** is backup performed on an entire disk volumes of a system(s).

- **Differential backup** is a backup of changes since last full backup, but does not change the archive bit value.

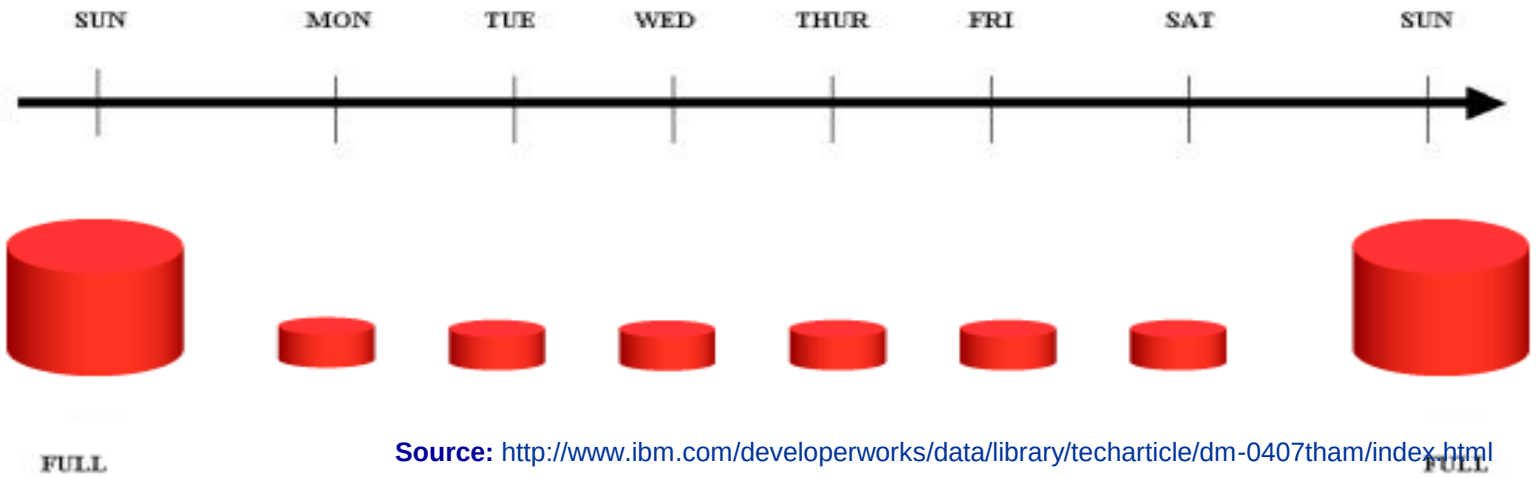
- **Incremental backup** is a backup of changes since last full or incremental backup.

Contingency Planning – Data Backups…

- **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.

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.

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**

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.

Phase IV: Plan Design & Development

Procedure

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.

Procedure…

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)

Procedure…

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.

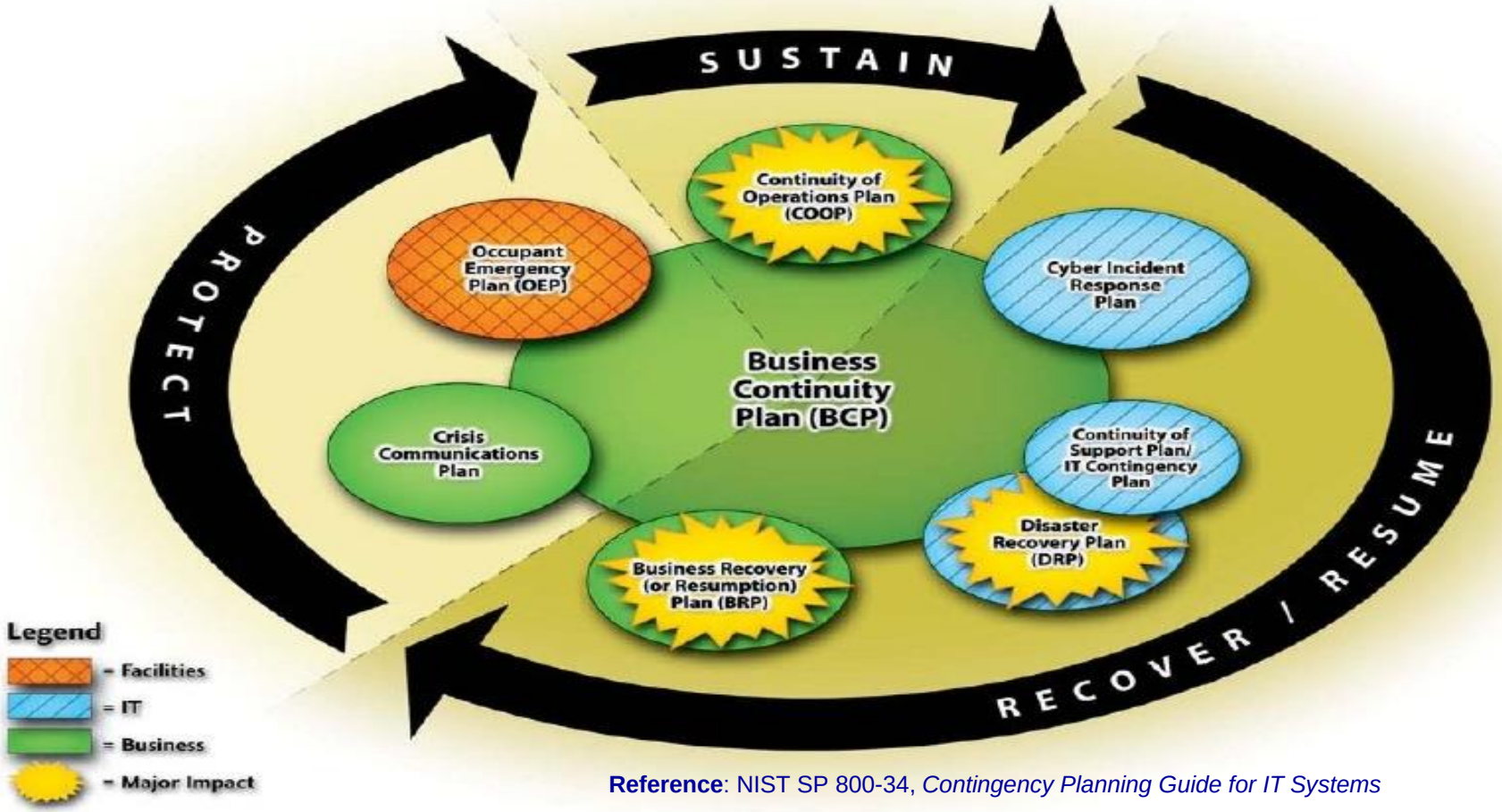
Phase V: Implementation

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**

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)**



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

BCP Phase VI: Testing

Testing

Types of Tests

- **Structured walk-through**: Representatives from each department come together AS A GROUP, they walk through the plan and different scenarios from beginning to end to make sure nothing is left out.
- **Checklist test:** BCP is distributed to departments and functional areas for review. The Managers read over and indicate if anything is missing or should be modified. (Manager “checks” off that the plan is OK for their department). Each functional representatives review BCP plans and check off the points that are listed to ensure all concerns and activities are addressed.

Testing

Types of Tests

- **Simulation:** A specific scenario is proposed, all required employees come together and start to simulate that the event has happened and start taking action to recover. The idea is to see if any problems come up or if any concerns were left out.

- **Parallel test:** Some systems are moved to the alternate site and processing takes place. The results are compared to the real processing to see if anything needs to change.

- **Full interruption test:** Full scale operational test including shutdown of primary site and recovery of business operations at alternate site(s).

Testing

Full Interruption test: Most intrusive test.. The original site is actually shutdown and processing is moved to the alternate site (really needs to be a hot site). The recovery team fulfils it's obligation in preparing the systems and environment for the alternate site.

- This is a full blown drill
- Requires tons of planning and co-ordination
- These are risky and can cause damage if not managed properly.
- Senior management approval is required due to the risk involved.

BCP Phase VII: Maintenance, Awareness, and Training

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.**

Maintaining the Plan

Now that we have the plan we need to maintain it! Systems and processes become out of date and need constant “refresh” why?

- BCP plan may not be integrated into change management process (it should be though!)
- Infrastructure or environment changes (that never changes…)
- Company re-organization, layoffs etc
- Changes in hardware or software
- Employee turn over

Maintaining the Plan…

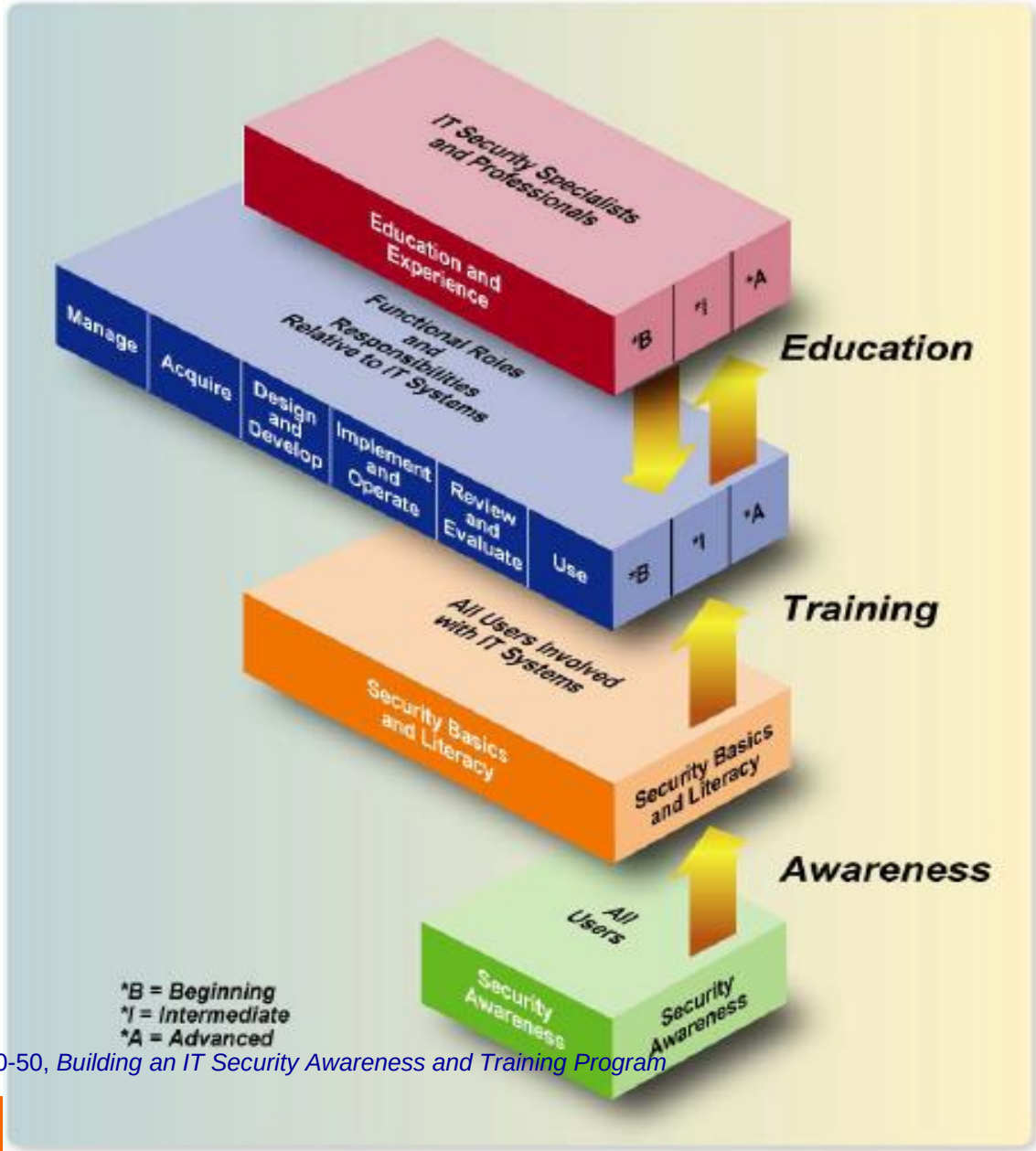
We can help keep the plan updated by taking the following actions

- Make BCP planning part of every business decision!
- Insert BCP maintenance responsibilities into job descriptions
- Include maintenance in personnel evaluations
- Perform internal audits that include DR and BCP procedures
- Test the plan yearly

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*

Thank You

Dr Prem Chand

premchand64@gmail.com

Ph: +91-981129807